UnB
FACE | Faculdade de Economia, Administração Contabilidade e Gestão de Políticas Públicas

RODRIGO ILDSON LIMA FERNANDES

DA SENSIBILIZAÇÃO À PROTEÇÃO: APLICAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, UM ESTUDO DE CASO NA UNB.

BRASÍLIA, DF
2025

RODRIGO ILDSON LIMA FERNANDES

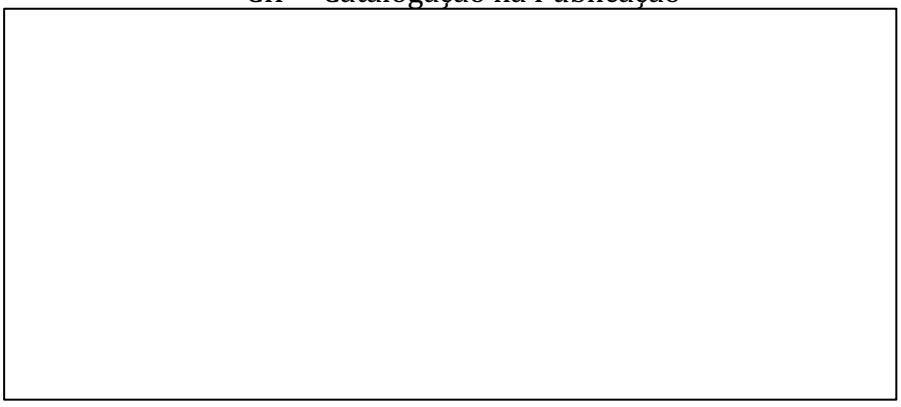
DA SENSIBILIZAÇÃO À PROTEÇÃO: APLICAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, UM ESTUDO DE CASO NA UNB.

Trabalho de Conclusão de Curso apresentado ao Programa de Pós-Graduação em Governança e Inovação em Políticas Públicas (PPG-GIPP), da Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas, como requisito parcial para obtenção do título de Mestre em Governança e Inovação em Políticas Públicas.

Orientador: Prof. Dr. Alexandre Kehrig Veronese Aguiar.
Coorientadora: Profa. Dra. Ludmila de Melo Souza.

BRASÍLIA, DF
2025

CIP – Catalogação na Publicação



RODRIGO ILDSON LIMA FERNANDES

DA SENSIBILIZAÇÃO À PROTEÇÃO: APLICAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, UM ESTUDO DE CASO NA UNB.

Trabalho de Conclusão de Curso apresentado ao Programa de Pós-Graduação em Governança e Inovação em Políticas Públicas (PPG-GIPP), da Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas, como requisito parcial para obtenção do título de Mestre em Governança e Inovação em Políticas Públicas.

Data da defesa: ___/___ /___

Comissão Examinadora:

_____

Professor Doutor Alexandre Kehrig Veronese Aguiar
Orientador
PPG-GIPP/UnB

_____

Professora Doutora Liliane Campos Machado
Examinador
Interno / UnB

_____

Professor Doutor José Brant de Campos
Examinador
Externo / UERJ

_____

Professora Doutora Fernanda de Carvalho Lage
Examinador
Suplente / UnB

AGRADECIMENTOS

À minha amada família, cuja fonte inesgotável de amor incondicional, apoio e compreensão iluminou cada momento dedicado a este trabalho. Sem o incentivo e a confiança de vocês, este estudo jamais teria se concretizado – com menção especial à minha ilustríssima esposa.

Aos meus orientadores, Alexandre Kehrig Veronese Aguiar e Ludmila de Melo Souza, por sua orientação e apoio, que foram essenciais para a conclusão deste estudo.

Aos ilustres professores do programa de pós-graduação, pelas aulas inspiradoras e ensinamentos que ampliaram meus horizontes e enriqueceram meu conhecimento.

Aos queridos colegas de curso, pela amizade sincera, colaboração e pelas enriquecedoras trocas de experiências ao longo do mestrado. Em especial, a Jéssica, por toda a parceria e pelos sorrisos generosamente oferecidos, tornando a jornada mais leve e repleta de alegria.

Aos dedicados servidores técnico-administrativos e docentes da Faculdade de Educação da Universidade de Brasília, que gentilmente participaram desta pesquisa, doando seu tempo e compartilhando percepções valiosas que enriqueceram este estudo.

A todos os amigos e familiares que, de forma direta ou indireta, contribuíram para a concretização deste trabalho, expresso meu sincero e profundo agradecimento.

“**Quando eu estiver contigo no fim do dia, poderás ver as minhas cicatrizes...
então saberás que eu me feri e me curei.**"

- I stand before thee at the day's end thou shalt see my scars
and know that I had my wounds and also my healing.

- A Tagore reader, Rabindranath Tagore, Amiya
Chandra Chakravarty - Macmillan, 1961.

RESUMO

Este estudo propõe um Programa de Sensibilização em Segurança da Informação com o objetivo de fortalecer a compreensão e adesão dos servidores técnico-administrativos e docentes da Faculdade de Educação da Universidade de Brasília (UnB) à Política de Segurança da Informação e Comunicação (PoSIC). A pesquisa aborda duas questões centrais: qual o nível de maturidade e conhecimento dos servidores em relação às políticas de segurança da UnB e como a integração de estratégias de sensibilização em segurança da informação com soluções tecnológicas pode melhorar a adesão e a eficácia dessas políticas em instituições de ensino superior. A metodologia envolveu questionários e entrevistas que revelaram lacunas significativas no conhecimento e na aplicação das políticas de segurança, demonstrando a necessidade de uma abordagem mais estruturada e educativa. A proposta do programa visa mitigar essas deficiências e promover uma cultura de segurança mais alinhada aos normativos institucionais. Os resultados indicam que a implementação eficaz do Programa de Sensibilização em Segurança da Informação pode melhorar a resiliência institucional, além de criar um ambiente mais seguro para enfrentar as ameaças cibernéticas. As estratégias propostas, baseadas em análises temáticas e estatísticas, oferecem soluções práticas e contínuas para aprimorar a gestão da segurança da informação. Este estudo oferece diretrizes claras para a transformação da cultura de segurança, sendo especialmente relevante para gestores de instituições educacionais que buscam integrar soluções tecnológicas e comportamentais na proteção de seus dados sensíveis.

PALAVRAS-CHAVE: Segurança da Informação; Política de Segurança da Informação; Cultura de Segurança; Sensibilização; Instituições de Ensino Superior.

ABSTRACT

This study proposes an Information Security Awareness Program aimed at enhancing the understanding and adherence of the administrative and academic staff at the Faculdade de Educação at the Universidade de Brasília (UnB) to the university's Information and Communication Security Policy (PoSIC). The research addresses two central questions: what is the level of maturity and knowledge of staff regarding the security policies at UnB and, how can the integration of awareness strategies with technological solutions improve both the adherence to and effectiveness of these security policies in higher education institutions. The methodology involved the use of questionnaires and interviews, which revealed significant gaps in the knowledge and application of security policies, highlighting the need for a more structured and educational approach. The proposed program aims to address these deficiencies, fostering a security culture more aligned with institutional regulations. The findings suggest that the effective implementation of the Information Security Awareness Program can enhance institutional resilience while creating a safer environment to face current cyber threats. The proposed strategies, based on thematic and statistical analyses, offer practical and continuous solutions for improving information security management. This study provides clear guidelines for transforming the security culture, making it particularly relevant for educational institution managers seeking to integrate technological and behavioral solutions to protect sensitive data and ensure the integrity of academic and administrative processes.

KEYWORDS: Information Security; Information Security Policy; Security Culture; Awareness; Higher Education Institutions.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

SUMÁRIO

1. APRESENTAÇÃO

No contexto atual de crescente digitalização dos processos acadêmicos e administrativos, a segurança da informação emergiu como um tema de vital importância em instituições de ensino superior. O aumento das ameaças cibernéticas exige medidas eficazes para proteger os ativos informacionais e garantir a integridade, confidencialidade e disponibilidade dos dados. Neste cenário, este trabalho aborda a implementação da Política de Segurança da Informação e Comunicação (PoSIC) na Universidade de Brasília (UnB), com foco específico na Faculdade de Educação (FE).

O estudo divide-se em duas partes principais: um artigo acadêmico (Capítulo 2) e um relatório técnico-tecnológico (Capítulo 3). O artigo acadêmico, intitulado "**Avaliação Da Maturidade e Adesão à Política de Segurança da Informação: Um Estudo na Faculdade de Educação da UnB**", investiga como os servidores técnico-administrativos e docentes da FE compreendem e aderem às diretrizes estabelecidas pela PoSIC. Através de análise documental, questionários e entrevistas, busca-se avaliar o nível de conhecimento e as práticas desses servidores em relação à segurança da informação, identificando lacunas e áreas que demandam melhorias.

O relatório técnico-tecnológico (Capítulo 3) dedica-se ao desenvolvimento do **Programa de Sensibilização em Segurança da Informação** (PSSI), uma proposta de intervenção projetada para fortalecer a cultura de segurança entre os servidores da FE mas que pode ser estendido para outros institutos, núcleos e faculdades. Fundamentado nos dados coletados, o programa visa não apenas sensibilizar os servidores sobre a importância da segurança da informação, mas também propor estratégias concretas para aumentar a adesão às normas da PoSIC.

Este estudo apresenta uma abordagem teórico-prática para enfrentar os desafios da segurança da informação na FE, contribuindo para uma gestão mais eficiente dos riscos cibernéticos na universidade. Ao integrar as estratégias propostas no cotidiano dos servidores, espera-se promover um ambiente acadêmico mais seguro e resiliente.

Espera-se que as descobertas e propostas deste trabalho não só fortaleçam a segurança da informação na FE, mas também sirvam como modelo para outras unidades da UnB, promovendo uma cultura de segurança madura e sustentável. Desta forma, o estudo avança na direção de uma compreensão mais integrada e holística dos desafios e oportunidades relacionados à gestão da segurança da informação em instituições de ensino superior.

2. AVALIAÇÃO DA MATURIDADE E ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO NA FACULDADE DE EDUCAÇÃO DA UNB

2.1. INTRODUÇÃO

A segurança da informação evoluiu paralelamente ao avanço tecnológico, especialmente com o surgimento da internet e a digitalização dos dados. Inicialmente, as medidas de proteção concentravam-se nos equipamentos e na prevenção de acessos não autorizados. No entanto, à medida que o ciberespaço se expandiu, novas ameaças digitais emergiram, tornando a proteção de dados o foco central das políticas de segurança (Ghonaimy; El-Hadidi; Aslan, 2002; Perwej *et al*., 2021). Ataques como o *ransomware* 'WannaCry' em 2017 expuseram vulnerabilidades em larga escala e consolidaram o cibercrime como uma ameaça global (Aslan *et al*., 2023).

No estudo, intitulado *The New Frontier of Cybersecurity: Emerging Threats and Innovations*, os autores Dave et al. (2023) examinam detalhadamente as ameaças cibernéticas emergentes e suas implicações para indivíduos, organizações e governos. Utilizando uma abordagem qualitativa, os autores identificam e analisam diversas categorias de ameaças, destacando a sofisticação crescente e a diversidade dos ataques. A "tabela 1" do estudo mostra um aumento significativo no número total de ataques cibernéticos relatados, passando de 9,079 milhões de incidentes em 2015 para 20,05 milhões de incidentes em 2022, representando um aumento substancial de 121% em sete anos. Especificamente, os incidentes de intrusão fraudulenta aumentaram de 3,430 milhões em 2015 para 4,040 milhões em 2022, um aumento de 18%. Simultaneamente, os incidentes de fraude subiram de 3,439 milhões para 5,191 milhões, um aumento de 50%. O crescimento dos ataques cibernéticos pode ser atribuído aos avanços na tecnologia, aumento da conectividade, incentivos econômicos e táticas evolutivas dos cibercriminosos (Dave *et al*., 2023, p. 3). Abaixo, a figura lista o tipos de ataques mais comuns e o percentual de crescimento.

Figura 01 - Número total de ataques cibernéticos relatados (fonte: Dave et al., 2023).

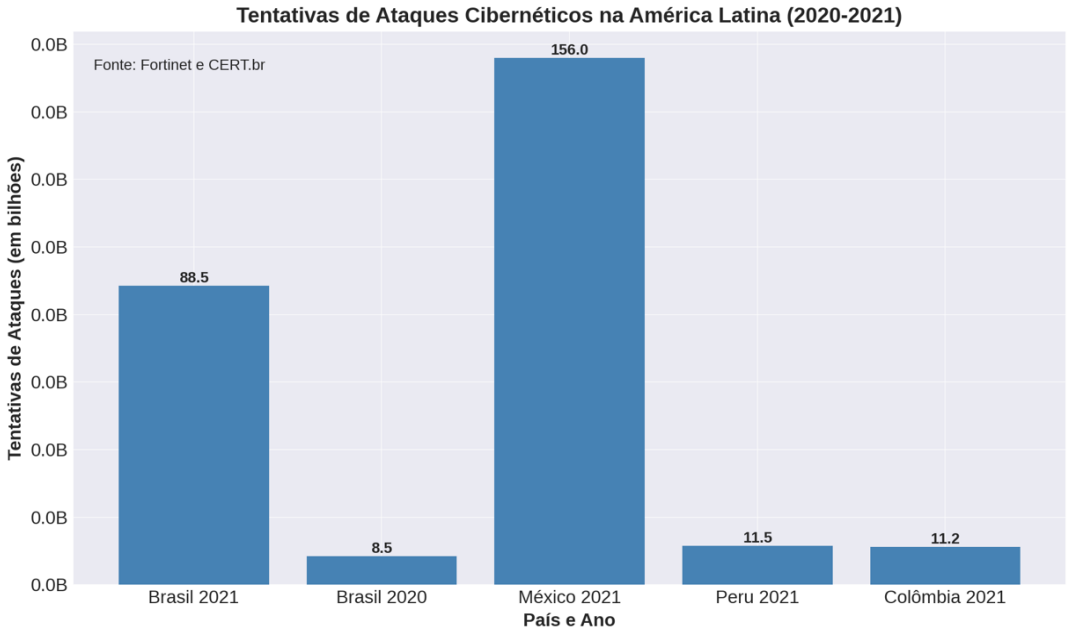
Incidents	2015	2016	2017	2018	2019	2020	2021	2022	%Increase /Source
Fraud Intrusion	3.430	3.546	3.640	3.767	3.830	3.945	4.001	4.040	18% [30]
Fraud	3.439	3.545	3.737	3.879	4.157	4.456	4.746	5.191	50% [10]
Spam	0.320	0.410	0.617	0.714	0.870	1.456	1.765	1.956	511% [32]
Denial ofService	0.367	0.544	0.676	0.754	0.945	1.276	1.382	1.568	327% [10]
Cyber Harassment	0.345	0.454	0.655	0.764	0.845	1.156	1.266	1.478	328% [32]
Vulnerabilityreports	0.310	0.515	0.614	0. 811	0.915	0.990	1.372	1.491	381% [37]
IntrusionAttempts	0.257	0.417	0.614	0.715	0.791	1.154	1.256	1.382	438% [28]
Maliciouscode	0.410	0.545	0.756	0.967	1.176	1.245	1.444	1.580	285% [37]
Contentrelated	0.201	0.375	0.576	0. 847	0.944	1.176	1.276	1.364	578% [28]
Total	**9.079**	**10.351**	**11.298**	**13.218**	**14.473**	**16.854**	**18.508**	**20.05**	

A figura acima, extraída do estudo, apresenta o aumento no número total de incidentes cibernéticos relatados entre 2015 e 2022, evidenciando um crescimento expressivo em todas as categorias analisadas. Os dados que a figura em língua inglesa nos traz é que os ataques relacionados a conteúdo lideraram o aumento percentual com 578%, seguidos por spam (511%) e tentativas de intrusão (438%). Outros incidentes, como relatórios de vulnerabilidade (381%), assédio cibernético (328%) e negação de serviço (327%), também mostraram elevações significativas. No geral, o número total de incidentes cresceu 121%, refletindo a crescente sofisticação e frequência das ameaças cibernéticas, o que reforça a necessidade de estratégias robustas de segurança da informação.

Com o aumento da sofisticação dos ataques, países como Taiwan, Estados Unidos e Espanha adotaram estratégias robustas para mitigar riscos digitais, focando na integração entre governança, inovação e colaboração entre o setor público e privado (Andreasson, 2012). Essas iniciativas refletem a crescente percepção de que a proteção cibernética precisa acompanhar o ritmo das ameaças emergentes. No Brasil, essa tendência internacional foi refletida na criação da Estratégia Nacional de Segurança Cibernética (E-Ciber), lançada em 2020 e na implementação da Lei Geral de Proteção de Dados (LGPD). Ambas as iniciativas surgiram em resposta ao aumento das ameaças no ciberespaço e foram elaboradas com base em diagnósticos e consultas públicas, estabelecendo diretrizes de governança, proteção e inovação para o país (BRASIL, 2020; Nunes; Assunção; Brustolin, 2022). Essas políticas visam promover a integração entre setores e reforçar a defesa contra os ataques cibernéticos, alinhando o Brasil às melhores práticas globais. Portanto, a implementação da E-Ciber e da LGPD representou um avanço importante, uma vez que essas políticas fornecem uma estrutura essencial para enfrentar os crescentes desafios de segurança da informação no Brasil.

O gráfico a seguir, exibe as tentativas de ataques cibernéticos registradas em 2020 e 2021 na América Latina, com ênfase em quatro países: México, Brasil, Peru e Colômbia. Os dados apontam para uma disparidade significativa entre esses países e evidenciam o expressivo crescimento das ameaças cibernéticas na região. Em 2021, o México liderou o ranking com 156 bilhões de tentativas de ataque, seguido pelo Brasil, com 88,5 bilhões, o que reflete a concentração de ataques nos dois maiores mercados digitais da América Latina. O Peru e a Colômbia apresentaram números substancialmente menores (11,5 bilhões e 11,2 bilhões, respectivamente), porém ainda relevantes no contexto regional. No caso do Brasil, observa-se um crescimento marcante em relação a 2020, quando foram registradas 8,5 bilhões de tentativas, o que representa um aumento de quase dez vezes em apenas um ano.

Gráfico 01 - Ataques na América Latina



As tentativas de ataques cibernéticos na América Latina para o ano de 2021, comparando o Brasil com outros países da região. Além disso, a comparação entre os anos de 2020 e 2021 para o Brasil destaca o aumento significativo no número de tentativas de ataques cibernéticos. Fonte Fortinet & CERT.BR

A ausência de dados de 2020 para México, Peru e Colômbia pode ser atribuída a limitações na coleta de informações em períodos anteriores ou à estratégia do relatório em enfatizar dados mais recentes. Já para o Brasil, a parceria com o CERT.br possivelmente facilitou o acesso a estatísticas detalhadas, viabilizando uma análise evolutiva mais precisa. Ademais, o destaque dado ao expressivo crescimento brasileiro ressalta a urgência de fortalecer políticas de segurança cibernética no país, que figura como um dos principais alvos na região.

Os dados refletem uma tendência crescente de ataques cada vez mais sofisticados, impulsionada pela rápida digitalização e pela ampliação do uso de tecnologias na América Latina. Conforme apontam as análises de Fortinet e CERT.br, há um aumento de métodos como ransomware e ataques direcionados, o que enfatiza a importância de medidas de defesa robustas e coordenadas.

No contexto de um mundo cada vez mais digital, onde o volume de dados sensíveis armazenados e processados pelas instituições públicas e privadas aumenta exponencialmente, a necessidade de proteger essas informações se torna crítica. No entanto, o país ainda enfrenta desafios em alcançar um nível de maturidade cibernética comparável ao de nações como os Estados Unidos e a Espanha, que possuem estratégias de segurança mais consolidadas (Andreasson, 2012). Apesar dos avanços institucionais, o Brasil ainda apresenta um nível baixo de maturidade em segurança da informação, como aponta o relatório "Revisão das Capacidades

de Segurança Cibernética do Brasil 2023" que foi realizado pelo Centro Global de Capacidade de Segurança Cibernética (GCSCC) em colaboração com a Organização dos Estados Americanos (OEA) e o Escritório de Assuntos Exteriores do Reino Unido (BRASIL, 2023). Seu objetivo foi avaliar a maturidade das capacidades de segurança cibernética do Brasil e identificar áreas onde o governo pode investir para melhorar sua segurança cibernética nacional. A avaliação, realizada entre 28 e 30 de agosto de 2023, envolveu partes interessadas de diversos setores, incluindo academia, defesa, justiça, segurança pública e empresas do setor privado, como instituições financeiras e de telecomunicações.

O relatório utilizou o Modelo de Maturidade da Capacidade de Segurança Cibernética (CMM), que divide a segurança cibernética em cinco dimensões: política e estratégia de segurança cibernética, cultura e sociedade, construção de conhecimentos, marcos legais e regulatórios e padrões e tecnologias. O relatório concluiu que, embora o Brasil tenha alcançado importantes avanços, como a implementação da E-Ciber, o nível de maturidade do país ainda apresenta desafios significativos. Outro relatório de auditoria, elaborado pelo Tribunal de Contas da União (TCU) indicou que muitas instituições públicas não adotam sequer as políticas de segurança mais básicas, resultando em ineficiências e aumento de custos (BRASIL, 2024). Além disso, a falta de alinhamento entre as políticas de segurança e as ações institucionais, agravada pelo desinteresse da alta administração, compromete a eficácia das iniciativas e deixa as instituições vulneráveis (Guimarães; Souza Neto; Lyra, 2018).

Além do ambiente público, é fundamental considerar relatórios da iniciativa privada que destacam a crescente importância da segurança da informação. A 26ª CEO Survey da Price Water House Coopers (PwC), por exemplo, é uma pesquisa global que anualmente coleta as opiniões de diretores executivos de diversas indústrias e regiões sobre questões que afetam o cenário econômico global, incluindo desafios como cibersegurança. Embora não tenha focado diretamente em políticas de segurança da informação em instituições brasileiras, o relatório revela que 33% dos diretores executivos no Brasil estão priorizando mais investimentos em segurança cibernética e privacidade de dados. Isso é uma resposta aos riscos geopolíticos e à complexidade crescente do ambiente empresarial (PwC Brasil, 2023).

Voltando à maturidade, Cordeiro (2017) indica que a maturidade da gestão da segurança da informação nas IFES está em um nível que requer melhorias significativas, especialmente nos aspectos relacionados ao comprometimento da alta gestão e à necessidade de uma cultura de segurança mais robusta. O diagnóstico da maturidade foi detalhado em diferentes domínios, como controle de acesso, gestão de ativos e segurança nas operações. Nesse sentido, Britto (2011) realizou um levantamento e diagnóstico em ministérios que fazem parte da Administração Direta

Federal (ADF), utilizando um questionário para avaliar o nível de maturidade da GovSI nessas organizações. Os resultados revelam que o nível de maturidade das instituições analisadas ainda é baixo, com muitos órgãos apresentando lacunas importantes em termos de políticas de segurança formalizadas, gestão de riscos e monitoramento. Por exemplo, 64% dos órgãos avaliados não possuem uma política formal de segurança da informação, o que reflete uma baixa conscientização e prioridade por parte da alta administração sobre a importância da segurança. Além disso, 88% não possuem um plano de continuidade de negócios, evidenciando a falta de preparo para lidar com incidentes graves que possam comprometer a operação dos serviços públicos. De forma semelhante, Guimarães, Neto e Lyra (2018) reforçam essa realidade ao apontar que, apesar de algumas melhorias nas práticas de governança de segurança da informação, o nível de maturidade na Administração Pública Federal (APF) continua aquém do desejado. As instituições ainda carecem de uma governança estruturada e integrada, o que aumenta os riscos operacionais e a ineficiência na alocação de recursos para a segurança. Esses autores sugerem que a adoção de modelos robustos de governança, pode ser um passo crucial para elevar o nível de maturidade e promover uma cultura de segurança sólida nas instituições públicas (Guimarães; Neto; Lyra, 2018).

Em face desse cenário, há oportunidades claras para aprimorar a segurança da informação na administração pública federal. A criação de um modelo de governança integrada, conforme proposto pela E-Ciber, busca unir governo, academia, setor privado e terceiro setor em uma abordagem colaborativa e efetiva (Cordeiro, 2017; BRASIL, 2020). Dessa forma, o contexto nacional se alinha às tendências internacionais, buscando fortalecer sua postura defensiva diante das ameaças digitais. Fica claro que o ambiente acadêmico brasileiro, especialmente em universidades como a Universidade de Brasília (UnB), não está imune a essas ameaças. De fato, a digitalização acelerada, impulsionada pela pandemia de Covid-19, expôs ainda mais as vulnerabilidades dessas instituições (Bou Sleiman; Gerdemann, 2021). Dados sensíveis de estudantes, registros acadêmicos, dados de pesquisa ou informações administrativas estão em risco e por isso, a adoção de políticas eficazes de segurança da informação é essencial (Ulven; Wangen, 2021; Cheng; Wang, 2022).

Nesse contexto, a aplicação de diretrizes nacionais no ambiente universitário torna-se crucial para proteger esses ativos digitais. A Política de Segurança da Informação e Comunicação (PoSIC) da UnB, criada a partir dessas diretrizes, busca alinhar as exigências legais e as melhores práticas internacionais às necessidades locais. As universidades, ao alinharem suas políticas internas com as estratégias nacionais, como a exemplo da PoSIC na UnB, podem melhor proteger seus ativos digitais e contribuir para a maturidade cibernética do país. No entanto, o sucesso dessa

política depende da adesão dos servidores técnico-administrativos e docentes, bem como da eficácia da comunicação e dos treinamentos relacionados (Cheng, Wang, 2022; Veronese; Calabrich, 2022).

Para fundamentar a abordagem, é necessário rememorar algumas definições fundamentais de "Segurança da Informação" e "Política de Segurança da Informação" para facilitar a total compreensão. A Segurança da Informação (SI) se baseia em três pilares: confidencialidade, integridade e disponibilidade. Esses princípios garantem que apenas pessoas autorizadas acessem os dados (confidencialidade), que as informações não sejam alteradas indevidamente (integridade) e que estejam sempre disponíveis quando necessário (disponibilidade) (NBR ISO 27001, 2022). Existem diversos instrumentos que auxiliam na aplicação desses princípios e este estudo foca em um deles: a política de segurança da informação. A Política de Segurança da Informação (PSI) estabelece diretrizes claras para proteger sistemas e dados, funcionando como uma "Constituição" para a organização, segundo Sêmola (2003, p. 105). Ela define regras para garantir a segurança, como autenticação e privacidade, que são essenciais para prevenir ameaças (Peltier, 2016). Como é de se esperar, a SI tornou-se prioridade nas instituições educacionais devido ao aumento das ameaças digitais, como *phishing, malware* e violações de dados (Ulven; Wangen, 2021; Cheng; Wang, 2022). Para proteger seus dados, é crucial que as instituições adotem políticas claras, promovam treinamentos e invistam em tecnologias de segurança (Ulven; Wangen, 2023). O comprometimento da administração e a capacitação contínua são cruciais para o sucesso dessas iniciativas (Cordeiro, 2017). Proteger esses dados é vital para a reputação da instituição e para a segurança dos discentes e pesquisadores. A UnB, reconhecendo a crescente importância da segurança da informação, desenvolveu políticas e processos ao longo dos anos para proteger seus ativos digitais. Esse esforço se intensificou especialmente nos últimos anos, com a digitalização dos processos acadêmicos e administrativos.

A PoSIC/UnB, define diretrizes para proteger os ativos de informação da universidade. Entre as principais ações previstas na política estão: a gestão de acessos, monitoramento de segurança, tratamento de incidentes e avaliação de vulnerabilidades. Embora a PoSIC exista na UnB, sua adesão apresenta-se como insuficiente, colocando em risco a segurança dos dados institucionais. Veronese e Mota (2023) reforçam a necessidade de uma gestão eficiente e proativa da segurança da informação. A falta de cumprimento dessas políticas pode resultar em perda de dados, danos à reputação e interrupções nas atividades acadêmicas e administrativas (Cheng *et al*, 2013; Zheng *et al*., 2023). Segundo Cheng *et al*. (2013, p. 455), a violação das políticas de segurança não só compromete a proteção dos ativos informacionais, mas também gera custos substanciais, tanto diretos quanto indiretos, como perda de negócios e necessidade de novas

medidas de segurança. Assim, a não observância dessas políticas é um problema que pode comprometer os objetivos estratégico, a viabilidade e credibilidade da instituição.

Diante dos desafios, a pesquisa foi realizada na FE-UnB com o objetivo de proporcionar uma análise detalhada e contextualizada dentro de um ambiente específico. A escolha desse local foi conveniente e permitiu que o estudo se concentrasse nas particularidades e necessidades dessa unidade acadêmica, possibilitando uma investigação mais focada e resultados mais precisos sobre as práticas e desafios relacionados à política de segurança da informação no contexto da instituição.

A FE-UnB, fundada em 1966, tem como objetivo formar profissionais para atender às demandas do sistema educacional brasileiro. Ao longo do tempo, adaptou-se a mudanças curriculares, expandiu seus programas de graduação, pós-graduação e extensão, adotando tecnologias avançadas para aprimorar a gestão e qualidade do ensino. Além disso, a faculdade contribui para debates educacionais, com foco em equidade e políticas públicas (Borges; Villar; Weller, 2018). Considerando o exposto, este estudo concentra-se na segurança da informação na FE-UnB, destacando a falta de compreensão e adesão à política como o principal problema.

A falta de treinamentos e uma cultura que não valoriza a segurança resultam em práticas arriscadas, como o uso inadequado de senhas, por exemplo (Zheng *et al*., 2023). A resistência a políticas vistas como restritivas e a falta de recursos para treinamentos agravam a situação (Ulven; Wangen, 2021; Cheng; Wang, 2022; Zheng *et al*., 2023). Com o aumento dos ataques cibernéticos e o uso crescente de tecnologia, é primordial implementar um programa de segurança eficaz para proteger dados e preservar a confiança na instituição.

A digitalização no ambiente educacional exige proteção de informações contra ameaças cibernéticas. Estudos destacam a importância da sensibilização em segurança da informação para mitigar riscos (Whitman; Mattord, 2018; Ulven; Wangen, 2021; Zheng *et al*., 2023) e a necessidade de uma cultura contínua que envolva aspectos técnicos e comportamentais (Sêmola, 2003; Tang; Li; Zhang, 2016; Vieira; Dias, 2022). A literatura reforça ainda como os treinamentos são fundamentais (Sêmola, 2003; Solms, 2016; Whitman; Mattord, 2016; Trigos; Nuno, 2021; Vieira; Dias, 2022). Investigar o nível de compreensão e adesão dos servidores da FE da UnB às políticas de segurança é imperativo para fortalecer a governança e proteger os ativos informacionais. Nesse sentido, Schneier (2015, p. 84) defende uma abordagem de segurança multicamadas, enquanto Mitnick (2011, p. 12) alerta para o papel crítico do fator humano na segurança e sugere estratégias para reduzir vulnerabilidades. Aqui, cabe fazer uma pergunta:

Qual é o nível de maturidade e conhecimento dos servidores técnico-administrativos e docentes em relação às políticas de segurança da informação da UnB?

Com esse enfoque, o objetivo principal deste estudo é analisar a implementação e a comunicação da PoSIC na UnB, bem como avaliar a adesão dos servidores técnico-administrativos e docentes às suas diretrizes. A pesquisa busca compreender como a política foi divulgada, investigando os canais de comunicação utilizados e a eficácia destes em alcançar toda a comunidade universitária. Dessa forma, o estudo pretende identificar possíveis falhas na disseminação e aplicação da PoSIC, avaliando o nível de conhecimento, a compreensão e a implementação de suas diretrizes pelos servidores da FE. Além disso, objetiva-se investigar a realização e o alcance dos treinamentos oferecidos pela UnB relacionados à PoSIC, buscando entender se esses esforços têm sido suficientes para atingir um número significativo de servidores e promover a sensibilização em segurança da informação. Pretende-se também medir o impacto da comunicação institucional na sensibilização dos servidores, verificando a existência de uma relação entre o acesso aos meios de comunicação e a adesão às práticas de segurança previstas pela política. Com essa abordagem, a pesquisa fornecerá uma visão detalhada da situação atual da PoSIC na UnB, contribuindo para um melhor entendimento e aprimoramento das práticas de segurança da informação na instituição.

2.2. PROCEDIMENTOS METODOLOGICOS

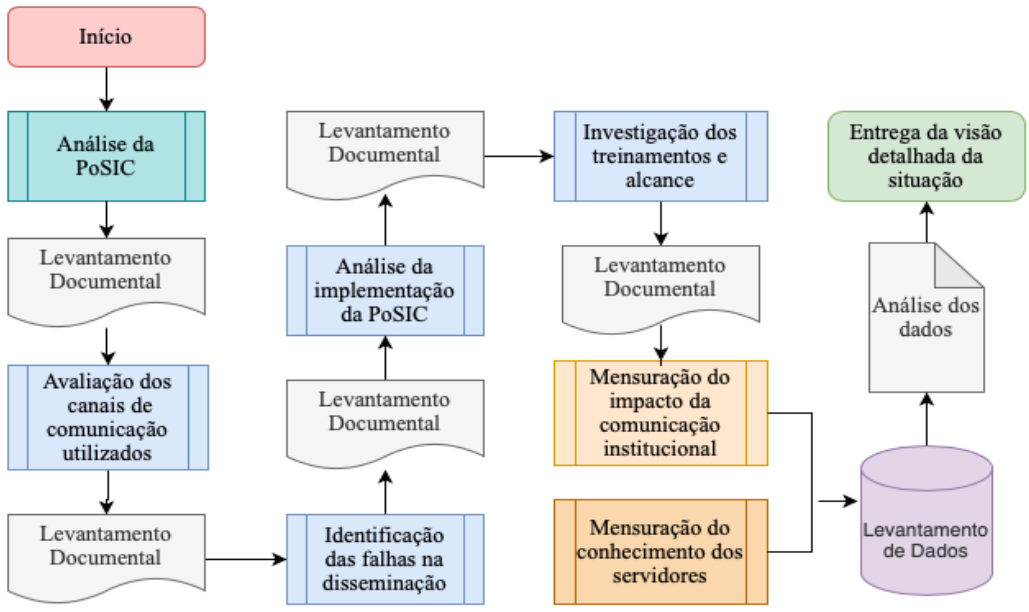
Para alcançar esses objetivos, a metodologia adotada nesta pesquisa combina pesquisa documental, que permite analisar materiais existentes, como documentos oficiais e registros (Gil, 2008), de campo, também conhecido como *survey,* para coletar dados diretamente dos servidores em seu ambiente natural (Gil, 2008) e mista, isto é, qualitativa e quantitativa para complementar a análise.

A pesquisa documental analisou registros institucionais, como protocolos de acesso à informação e comunicados oficiais, para entender a aprovação e divulgação da PoSIC. Em paralelo, a pesquisa de campo incluiu a aplicação de questionário. Após a aplicação do questionário, foram realizadas as entrevistas. Conforme Gil (2008), a pesquisa documental possibilita a obtenção de dados históricos e contemporâneos com menor custo e sem interferir diretamente no objeto de estudo, o que foi particularmente útil neste estudo que visou compreender um processo institucional. O levantamento de campo, por sua vez, foi utilizado para coletar dados por meio de questionário estruturado e entrevistas. Essa abordagem, conforme defendido por Gil (2008), permite a obtenção de dados descritivos que podem ser generalizados para uma população maior, sendo ideal para avaliar percepções e comportamentos em um ambiente específico. Ao combinar a pesquisa documental com o levantamento de campo, o estudo adotou uma metodologia que integra tanto dados qualitativos quanto quantitativos, conforme

recomenda Sampieri (2013).

Trigos e Nuno (2021) destacam a importância dessa abordagem para avaliar ações de sensibilização, combinando métodos quantitativos e qualitativos, o que permite medir o conhecimento prévio e avaliar impactos, reforçando a validade dos resultados. Creswell (2009) enfatiza a integração sinérgica entre qualitativo e quantitativo, capturando tanto dados numéricos quanto comportamentais, além de destacar o pragmatismo da metodologia, que permite adaptar os métodos às necessidades da pesquisa. Sampieri (2013) complementa, reforçando a complementaridade dos métodos para uma compreensão mais completa, com flexibilidade para ajustar a pesquisa ao contexto educacional e ao público-alvo. Portanto, a adoção da metodologia mista no estudo da Faculdade de Educação reflete uma abordagem de pesquisa abrangente e pragmática, conforme defendido por Sampieri (2013) e Creswell (2009). A metodologia envolverá a aplicação inicial de questionários para avaliar o nível atual de conhecimento e adesão às políticas de segurança da informação pelos servidores técnico-administrativos e docentes, estabelecendo uma linha de base para comparação futura. Em seguida, serão conduzidas entrevistas com uma amostra representativa de servidores para compreender suas percepções, preocupações e sugestões sobre as políticas de segurança existentes, identificando áreas específicas de melhoria. A seguir, um fluxo do processo de como a pesquisa transcorreu.

Figura 02 - Fluxo de Processo



Fonte: elaborado pelo autor.

O estudo cumpre as Resoluções CNS nº 466/2012 e nº 510/2016 e segue o Ofício Circular nº 2/2021/CONEP/SECNS/MS, garantindo a proteção e os direitos dos participantes. O consentimento livre e esclarecido foi obtido, assegurando o anonimato dos participantes e a

confidencialidade dos dados.

2.2.1. BASE DOCUMENTAL

A consulta documental, via protocolo SEI nº 23546.036316/2024-53, revelou que a PoSIC foi divulgada em um único dia, em 24 de abril de 2019, cinco meses após sua aprovação, por meio de três canais: e-mail (INFOUNB, 11184883), boletim de atos oficiais (11184916) e o no site da Secretaria de Tecnologia da Informação (STI). Entretanto, essa divulgação limitada sugere uma estratégia ineficaz, restringindo o alcance da política.

2.2.2. DESCRIÇÃO DO QUESTIONÁRIO

O questionário avaliou o conhecimento e a implementação da PoSIC/UnB entre os servidores da FE. Buscou-se entender como a política é comunicada, compreendida e aplicada na instituição. Foram avaliados o grau de conhecimento dos respondentes sobre a PoSIC/UnB, identificando falhas na disseminação e medindo o nível de sensibilização. Investigou-se a implementação prática da política no dia a dia, verificando sua integração nas operações da universidade.

Exploraram-se os canais de comunicação utilizados e a capacitação recebida, identificando lacunas que podem ser melhoradas. Coletaram-se dados sobre incidentes de segurança vivenciados, fornecendo informações sobre vulnerabilidades a serem abordadas. O questionário permitiu que os respondentes oferecessem sugestões para aprimorar a política de segurança da informação, engajando a comunidade universitária no fortalecimento das práticas de segurança.

O questionário visou diagnosticar o estado atual da política de segurança da informação na Faculdade de Educação, atuando como ferramenta de auditoria interna para identificar o conhecimento e a aplicação da política, além de reforçar a importância dos programas de sensibilização e comunicação em todos os níveis da instituição (Fowler, 2014).

2.2.2.1. Validação

O questionário utilizado foi desenvolvido com base em instrumentos já validados em estudos anteriores sobre segurança da informação e práticas de governança em instituições de ensino (Cheng *et al*., 2013; Trigos; Nuno, 2021; Zheng *et al*., 2023). Contudo, para assegurar a pertinência das perguntas ao contexto específico da UnB, o questionário passou por um processo de pré-teste com três servidores técnico-administrativos da Faculdade de Educação. Esse pré-teste serviu para identificar ambiguidades nas perguntas e adequar a linguagem ao público-alvo. Para evitar ambiguidades presentes nas opções intermediárias da escala Likert de 5 pontos aplicada

inicialmente, foram implementadas escalas ternárias e dicotômicas no questionário, tornando-as mais claras e objetivas (Sampieri et al., 2013). Adicionalmente, questões fundamentadas em psicologia social foram incorporadas (Gil, 2008), juntamente com validações concomitantes, visando aumentar a precisão das respostas. Essas questões foram elaboradas para compreender melhor as atitudes e comportamentos dos participantes em relação à segurança da informação. Introduziram-se também critérios condicionais no questionário, de modo que certas perguntas eram apresentadas apenas se as respostas anteriores fossem afirmativas. Esse método permitiu uma avaliação mais direcionada e eficaz, concentrando-se nos aspectos relevantes para cada participante e eliminando perguntas desnecessárias.

A validação do questionário, para além dos testes, foi realizada em duas etapas. Primeiramente, foi feita uma análise de conteúdo por especialistas em segurança da informação e gestão de políticas institucionais, que revisaram o instrumento para garantir que as perguntas abordassem de forma adequada as dimensões de conhecimento, aplicação e comunicação da PoSIC. Em seguida, foram conduzidas análises estatísticas preliminares, aplicando a técnica de consistência interna por meio do coeficiente 'Alfa de Cronbach', que resultou em um valor de 0,89. O Alfa de Cronbach é um indicador estatístico que mede o grau em que os itens de um instrumento estão correlacionados entre si e, portanto, se estão efetivamente medindo o mesmo constructo ou conceito. Valores desse coeficiente variam entre 0 e 1, onde valores mais próximos de 1 indicam maior consistência interna. No estudo, o coeficiente de Alfa de Cronbach obtido foi de 0,89. Esse valor é considerado excelente na literatura especializada, indicando que os itens do instrumento possuem alta consistência interna e que o instrumento é confiável para medir o que se propõe. De acordo com autores como Virla (2010), Cortina (2013) e Fowler (2014), valores de Alfa de Cronbach acima de 0,70 já são considerados adequados para pesquisas nas ciências sociais. Portanto, um valor de 0,89 reforça a validade e a confiabilidade dos dados coletados. Portanto, essa análise confirmou que o questionário apresentava consistência suficiente para medir o nível de conhecimento e adesão às práticas de segurança. O apêndice “B” detalha esse processo.

2.2.2.2. Aplicação

O questionário, baseado em um survey com 22 questões (Fowler, 2014), ficou disponível online, no endereço eletrônico: https://quest.fe.unb.br, esteve online durante 22 dias, entre o dia 23 de abril e o dia 14 de maio. O apêndice “A” apresenta o questionário na íntegra.

2.2.3. DESCRIÇÃO DAS ENTREVISTAS

Para complementar os dados quantitativos do questionário, optou-se pela realização de entrevistas semiestruturadas com servidores técnico-administrativos e docentes. A amostragem foi intencional, com o objetivo de selecionar participantes que representassem diferentes áreas de atuação e níveis hierárquicos dentro da Faculdade de Educação, assegurando a diversidade de perspectivas. O estudo realizou a análise das entrevistas utilizando a análise temática conforme descrito por Braun e Clarke (2006). Esse método permitiu identificar padrões emergentes nos dados, fornecendo percepções valiosas sobre a sensibilização e aplicação da POSIC na UnB. A análise temática é apropriada por explorar sistematicamente as percepções, conhecimentos e práticas dos entrevistados, identificando padrões e lacunas no conhecimento e na aplicação da POSIC, além de destacar necessidades de comunicação e treinamento. O roteiro de entrevista consistiu em oito perguntas principais com várias subperguntas condicionais, totalizando até 21 questões. Caso o entrevistado desconhecesse a POSIC, as perguntas tornavam-se limitadas, já que detalhes da política só poderiam ser discutidos com conhecimento prévio. O roteiro de entrevista focou em questões relacionadas ao conhecimento e à aplicação da POSIC entre os servidores. As perguntas principais abrangeram temas como a familiaridade prévia com a POSIC, a leitura e a compreensão de suas diretrizes, além da aplicação prática dessas no ambiente de trabalho. Também foram exploradas experiências de incidentes de segurança e preferências quanto à comunicação e ao treinamento sobre segurança da informação. As subperguntas foram adaptadas conforme o nível de conhecimento do entrevistado, proporcionando uma visão mais clara da eficácia da comunicação e da implementação das diretrizes da POSIC. O objetivo foi coletar dados sobre a eficácia da comunicação da POSIC e a implementação de suas diretrizes pelos servidores. A íntegra das transcrições das entrevistas está disponível para consulta no Apêndice “D”. O relatório produzido pela análise temática está disponível para consulta no Apêndice “E”.

2.2.3.1. Validação

O número de entrevistados foi determinado seguindo o critério de saturação teórica, conforme defendido por Sampieri *et al.* (2013). A saturação teórica é alcançada quando a coleta de dados adicionais não resulta em novas informações relevantes ou significativas sobre o fenômeno em investigação. Durante o processo de coleta, observou-se que, após a realização de três entrevistas, os dados obtidos começaram a apresentar recorrência e redundância nos temas e categorias emergentes. Isso indicou que o fenômeno estudado já havia sido explorado de forma suficiente e aprofundada pelos participantes selecionados (Sampieri *et al.,* 2013).

2.2.3.2. Aplicação

Foram realizadas entrevistas presenciais no dia 15 de maio de 2024, com a participação de uma docente e duas técnicas administrativas, com o objetivo de coletar dados pertinentes ao estudo. As conversas foram registradas com o auxílio de um gravador de voz digital omnidirecional, garantindo a captura integral das informações. Cada entrevista teve duração média de 10 minutos. A íntegra das transcrições das entrevistas está disponível para consulta no Apêndice D.

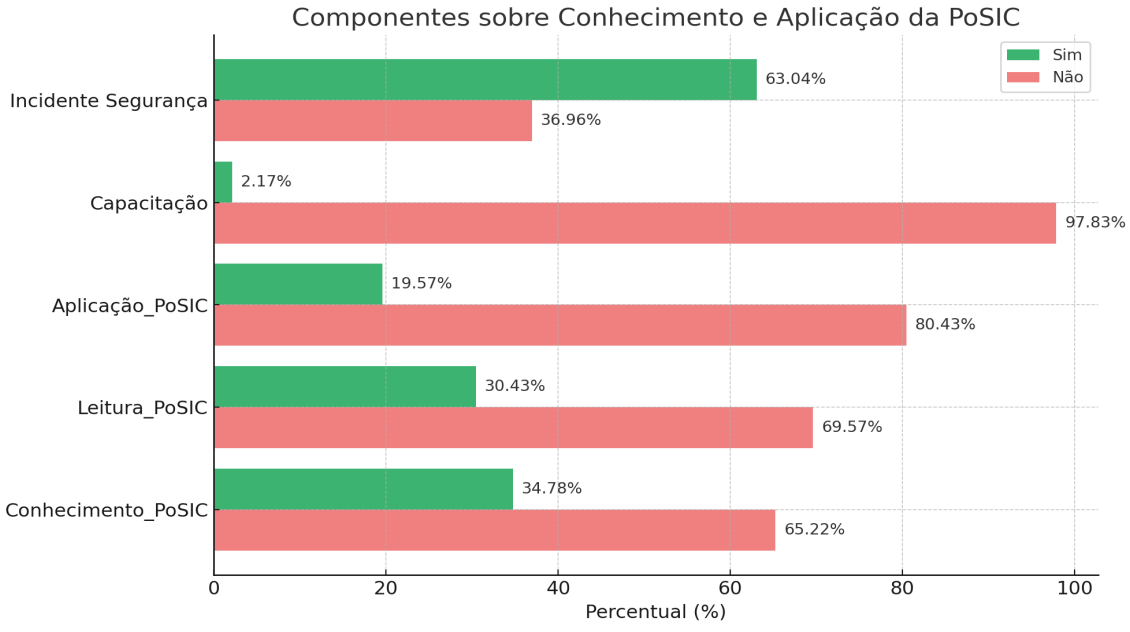
2.2.4. RESULTADOS

Nas subseções a seguir, os dados são apresentados e discutidos de forma detalhada, com foco na avaliação da comunicação e implementação da POSIC, além das percepções dos entrevistados sobre a relevância das diretrizes e a necessidade de capacitação contínua. A análise estatística complementa esses achados.

2.2.4.1. Análise Do Resultado Do Questionário

Contou com 46 respondentes, representando 36,22% da população total de 127 indivíduos (37 técnicos e 90 docentes). Dentre os participantes, 19 eram técnicos (51,35% dos técnicos) e 27 eram docentes (aproximadamente 30% dos docentes). A análise traçou o perfil dos respondentes, sua familiaridade com a POSIC/UnB e o impacto das medidas de segurança em seu ambiente de trabalho.

Gráfico 02 - Aplicação da PoSIC



Fonte: elaborado pelo autor.

Os dados revelaram uma predominância de docentes (58,70%) entre os respondentes, possivelmente indicando maior envolvimento e interesse nas questões abordadas ou influenciado pelo período de greve durante a pesquisa. A distribuição etária foi equilibrada entre 35 e 64 anos, com destaque para as faixas de 45-54 anos (32,61%) e 55-64 anos (30,43%). Houve uma ligeira predominância feminina (52,17%) em relação aos homens (45,65%). Em relação à POSIC/UnB, apenas 34,78% dos respondentes estavam cientes de sua existência, e destes poucos a leram completamente (17,39%) ou parcialmente (13,04%). A maioria não conhecia a política ou não respondeu, evidenciando falhas na comunicação e na disseminação das diretrizes de segurança. Apenas uma minoria aplicava as diretrizes frequentemente (10,87%) ou às vezes (8,70%), indicando falta de clareza ou relevância percebida no cotidiano. Além disso, 63,04% dos respondentes já sofreram algum incidente de segurança digital, mas somente 2,17% receberam treinamento específico sobre a política. As preferências para ações de sensibilização incluem comunicação por e-mail com dicas de segurança, cartilhas, folhetos e postagens em redes sociais, sugerindo que uma abordagem multimodal seria mais eficaz. A necessidade urgente de reforçar as práticas de segurança da informação na UnB é evidente, destacando a importância de aumentar o treinamento, melhorar a comunicação e garantir o acesso universal aos meios institucionais para promover uma cultura de segurança mais forte e responsiva.

2.2.4.2. Análise Do Resultado Das Entrevistas

Foram entrevistados três participantes, denominados ficticiamente como Atena, Afrodite e Perséfone, para preservar o anonimato e tornar a leitura mais amigável. Atena não estava ciente da existência da POSIC antes do questionário e não buscou conhecê-la posteriormente, o que limitou a profundidade de suas respostas e manteve a entrevista superficial, centrada em experiências gerais e preferências de treinamento. Afrodite tinha conhecimento parcial da POSIC, obtido principalmente por e-mails do STI, mas apenas leu parcialmente a política. Aplicava algumas diretrizes básicas, como evitar links maliciosos e e-mails suspeitos. Contudo, não mencionou aspectos importantes como gestão de ativos e controle de acesso, indicando lacunas significativas em seu entendimento e aplicação das diretrizes. Sua percepção de não ter enfrentado incidentes de segurança pode ser equivocada devido à falta de conhecimento sobre diferentes tipos de ataques cibernéticos, ressaltando a necessidade de treinamento contínuo. Perséfone desconhecia a POSIC antes do questionário e não buscou mais informações depois, apesar da curiosidade inicial, evidenciando falhas na disseminação eficaz da política. Demonstrou interesse em treinamentos presenciais e sugeriu a distribuição de informações por e-mail ou boletim, apontando para a necessidade de abordagens mais efetivas de comunicação. Não relatou

incidentes de segurança na UnB, mas mencionou ocorrências fora da instituição, indicando que a percepção de segurança pode ser falha sem o conhecimento adequado. As entrevistas revelaram uma falta geral de conhecimento e compreensão da POSIC entre os participantes, apontando deficiências na comunicação e treinamento dentro da universidade. Há uma necessidade urgente de melhorar a sensibilização, a educação contínua e a implementação efetiva da política para garantir a proteção dos ativos e dados sensíveis da instituição. As entrevistas com Atena, Afrodite e Perséfone complementaram os dados do questionário, reforçando a necessidade de melhorias na comunicação e implementação da POSIC na instituição. Atena desconhecia a POSIC antes do questionário e não buscou mais informações, o que limitou suas práticas de segurança. Demonstrou interesse em treinamentos híbridos, combinando palestras presenciais com atividades remotas. Afrodite, por sua vez, tinha conhecimento parcial da POSIC, obtido por informes do STI, e aplicava apenas diretrizes básicas, como evitar links maliciosos. Preferia treinamentos online, indicando a necessidade de opções flexíveis para atender às preferências dos servidores. Perséfone, também desconhecia a POSIC antes do questionário e não procurou se informar depois, embora mostrasse interesse em treinamentos presenciais. Sugeriu a distribuição de informações via e-mail ou boletim, destacando a necessidade de uma comunicação mais eficaz. As entrevistas ressaltam três aspectos cruciais para a eficácia da POSIC na UnB: conhecimento, aplicação e comunicação. A falta de conhecimento e a aplicação limitada das diretrizes evidenciam falhas na comunicação interna e na promoção da política. Para que a POSIC seja efetivamente implementada, é importante que todos os servidores estejam informados e engajados. As entrevistas evidenciam a necessidade urgente de reforçar a comunicação e promover treinamento contínuo, adotando formatos diversificados e acessíveis para aumentar o engajamento e a compreensão. Promover uma cultura de segurança da informação é vital para proteger os ativos e dados sensíveis da universidade (os apêndices “D” e "E" apresentam as entrevistas e o relatório temático na íntegra).

2.2.4.3. Análise Estatística

Os dados foram novamente analisados, desta vez utilizando o software ‘Stata’, empregando principalmente o teste do qui-quadrado para verificar associações entre variáveis categóricas (Fávero; Belfiore, 2024). A análise revelou que não há associação significativa entre perfil institucional, cargo, gênero, idade ou tempo de atuação na UnB e o conhecimento da PoSIC, indicando que fatores demográficos e profissionais não influenciam significativamente a sensibilização sobre a política de segurança. Entretanto, há uma associação significativa entre o acesso aos meios de comunicação institucionais e o conhecimento da PoSIC (Pr = 0,000),

enfatizando a importância de garantir que todos os servidores tenham acesso regular aos canais de comunicação institucionais. Além disso, identificou-se uma associação com 90% de significância entre ter sofrido um incidente de segurança e o conhecimento da PoSIC (Pr = 0,078), sugerindo que a experiência direta com problemas de segurança aumenta a conscientização sobre as políticas de segurança. Esses dados reforçam a existência de uma lacuna significativa na capacitação específica relacionada à política de segurança, evidenciando a necessidade de treinamentos e campanhas de sensibilização. Em cada etapa do processo — desde a coleta de dados até a análise dos resultados — fica claro que medidas institucionais são essenciais para garantir a adesão à política. Portanto, é imprescindível que a instituição invista em campanhas de sensibilização e treinamentos abrangentes, utilizando todos os canais de comunicação disponíveis, como e-mails e boletins eletrônicos. A eficácia dessas iniciativas será determinante para assegurar que todos os servidores estejam bem-informados e comprometidos com as diretrizes da PoSIC, fortalecendo assim a segurança institucional em sua totalidade. O apêndice “C” apresenta o relatório estatístico na íntegra.

2.3. DISCUSSÃO

Com base nos resultados obtidos, a discussão a seguir examina as consequências das deficiências na comunicação e treinamento da PoSIC, além de propor recomendações para aumentar a adesão e a eficácia das políticas de segurança da informação na instituição.

A PoSIC, conforme os Art. 4º e 45º (BRASIL, 2018a), requer ampla divulgação de suas normas e procedimentos. A restrição a e-mails e boletins pode não ser suficiente para atingir toda a comunidade universitária, necessitando de um envolvimento mais ativo (Zheng *et al*., 2023). É necessário diversificar os canais de comunicação, além de abrir espaço para feedback das unidades, melhorando a implementação da PoSIC. A falta de monitoramento da recepção e compreensão da política é uma falha significativa, comprometendo a adesão. Medir o impacto da comunicação permite ajustes e garante que a PoSIC seja uma ferramenta ativa de proteção da informação. A estratégia de comunicação precisa ser flexível para se adaptar a novas ameaças, como aponta Marciano (2006), equilibrando aspectos técnicos e humanos para garantir sua eficácia frente às mudanças. Ainda sobre a consulta (SEI nº 23546.036316/2024-53), foi informado que os treinamentos da PoSIC foram voltados exclusivamente para profissionais de Tecnologia da Informação e Comunicação (TIC), especialmente a Equipe de Prevenção e Resposta a Incidentes Cibernéticos (ETIR), sem abrangência para outros servidores. Isso pode gerar lacunas na segurança, pois usuários fora da área de TIC, frequentemente expostos a ameaças como phishing, permanecem vulneráveis. A falta de treinamentos mais amplos limita a

disseminação da cultura de segurança cibernética, essencial para que todos compreendam seu papel na proteção das informações. O Art. 41 da PoSIC atribui à STi a responsabilidade de promover essa cultura (BRASIL, 2018a) e o Comitê de Tecnologia da Informação (CTI) deve garantir os recursos necessários para essas ações (BRASIL, 2017). A PoSIC também exige divulgação contínua e treinamento para todos os usuários (BRASIL, 2018a). Embora a PoSIC preveja sanções (Art. 43), a falta de capacitação pode prejudicar a aplicação dessas medidas. Sem sensibilização adequada, a adesão é limitada, o que compromete a eficácia da política (Louzada *et al*., 2020; Zheng *et al*., 2023). Em nova consulta (SEI nº 23546.047041/2024-83), foi confirmado que não há, até o momento, um instrumento específico de capacitação sobre a PoSIC, destacando a necessidade de um programa de treinamento mais abrangente para garantir maior adesão e proteção das informações.

Em síntese, a segurança da informação em instituições educacionais é imprescindível no contexto atual de crescentes ataques cibernéticos sofisticados (Ulven; Wangen, 2021; Cheng; Wang, 2022). Como já apontado anteriormente, proteger adequadamente essas informações é vital para evitar consequências graves, como perdas financeiras, danos à reputação e comprometimento da privacidade (Perera *et al*., 2022). Além disso, falhas na implementação de medidas eficazes de cibersegurança podem resultar em interrupções significativas nas atividades educacionais e na perda de confiança. Dada a complexidade dos ativos informacionais gerenciados, é fundamental que as universidades adotem estratégias abrangentes e adaptativas de proteção de dados, combinadas com programas contínuos de sensibilização e treinamento em segurança cibernética (Zheng *et al*., 2023; Trigos; Nuno, 2021; Chai; Zolkifli, 2021).

Cordeiro (2017), Whitman e Mattord (2018), Andreasson (2012), Guimarães (2016), Marciano (2006), assim como Vieira e Dias (2022), enfatizam o papel crucial da liderança na gestão eficaz da segurança da informação. Argumentam que o envolvimento e o compromisso da alta direção são essenciais para o sucesso das políticas de segurança, garantindo a alocação de recursos e a adoção séria das medidas em todos os níveis da organização. Destacam também a necessidade de atualização contínua das políticas para refletir os avanços tecnológicos e as mudanças nas ameaças, ressaltando a importância de uma abordagem adaptativa e flexível.

Para além disso, importante rememorar que as pesquisas em segurança da informação tinham um foco predominantemente técnico, mas houve uma mudança gradual para considerar o fator humano como crucial (Marciano, 2006; Tang; Li; Zhang, 2016). Muitas vezes, esse aspecto é negligenciado pelos profissionais da área, especialmente em relação ao usuário. A sensibilização dos servidores sobre a segurança da informação torna-se indispensável, pois, mesmo com tecnologias avançadas, a falta de consciência dos riscos pode levar a grandes perdas (Chai;

Zolkifli, 2021). Estudos como os de Trigos e Nuno (2021), Vieira e Dias (2022), Cheng e Wang (2023) e Zheng *et al*. (2023) destacam que a sensibilização em segurança da informação é um pilar crucial para proteger dados sensíveis e garantir a integridade dos sistemas. Para enfrentar esses desafios, é necessário estabelecer uma cultura de segurança da informação que seja parte integrante da cultura organizacional. A literatura revisada destaca a relação entre a cultura organizacional e a gestão da segurança da informação. Organizações com uma cultura coesa são mais capazes de implementar políticas de segurança de maneira eficaz (Tang; Li; Zhang, 2016; Vieira; Dias, 2022). Há também a necessidade de um quadro claro e mensurável para detalhar a relação entre os elementos da cultura organizacional e a cultura de segurança da informação (Tang; Li; Zhang, 2016). Ao implementar uma política de segurança da informação, é crucial considerar não apenas os aspectos técnicos, mas também os recursos humanos (Marciano, 2006; Cheng *et al*., 2013; Soomro; Shah; Ahmed, 2016). O fator humano é frequentemente o ponto mais vulnerável na segurança das informações. O comprometimento e a adesão dos servidores às práticas de segurança são indispensáveis para a eficácia das políticas. Portanto, investir na sensibilização e educação dos servidores é uma estratégia fundamental para reforçar a proteção global da organização (Sêmola, 2003; Soomro; Shah; Ahmed, 2016; Tang; Li; Zhang, 2016; Vieira; Dias, 2022).

A cultura de segurança da informação é um campo multidisciplinar que envolve aspectos de ciência da computação, psicologia, sociologia, gestão empresarial e ética. Definida como a manifestação das práticas ou comportamentos de segurança da informação que evoluem a partir de valores e crenças compartilhados dentro de uma organização, a cultura de segurança é decomposta em quatro dimensões principais: conformidade, comunicação, responsabilidade e governança (Tang; Li; Zhang, 2016). O estudo desses autores utiliza a estrutura de cultura organizacional de 'Hofstede' para definir e analisar a cultura de segurança da informação, identificando como essas dimensões são afetadas pela cultura organizacional. A conformidade diz respeito ao comportamento dos servidores em relação às políticas de segurança da informação. É salutar que todos compreendam e sigam essas políticas para garantir a proteção dos dados e sistemas informáticos, minimizando riscos (Tang; Li; Zhang, 2016). A comunicação é fundamental para disseminar essas políticas, utilizando múltiplos canais como treinamentos, boletins e reuniões, promovendo uma cultura organizacional voltada à proteção da informação (Soomro; Shah; Ahmed, 2016). A responsabilidade refere-se à resposta da organização a violações das políticas de segurança. Medidas corretivas e punitivas reforçam a importância das normas e servem como aprendizado para melhoria contínua dos processos de segurança. Já a governança posiciona a segurança da informação como prioridade estratégica, integrando-a aos objetivos e

operações da organização (Tang; Li; Zhang, 2016). A sinergia entre conformidade, comunicação, responsabilidade e governança fortalece a segurança da informação, tornando-a parte intrínseca da cultura organizacional (Vieira; Dias, 2022). A segurança da informação é vista como um fenômeno social, destacando a importância do fator humano (Neto; Araújo, 2019). Mitnick e Simon (2003) e Alexandria (2009) apontam que o elemento humano é a principal causa de incidentes, destacando a necessidade de não negligenciar aspectos sociais e comportamentais. Uma cultura de segurança emerge da promoção de práticas como política de mesa limpa e uso de controles, tornando-as práticas padrão na organização (Ghonaimy; El-Hadidi; Aslan, 2002; Tang; Li; Zhang, 2016). A cultura, neste contexto, está relacionada ao comportamento organizacional em três níveis: individual, de grupo e organizacional (Vieira; Dias, 2022). Cada nível requer abordagens específicas para proteger os ativos de informação, como encorajar o relato de incidentes, apoio da gestão e implementação de políticas de segurança (Ghonaimy; El-Hadidi; Aslan, 2002; Trigos; Nuno, 2021). A implementação de processos e treinamentos eficazes em segurança cibernética, sensíveis ao contexto da organização, é indispensável para promover essa cultura (Tan Soon Chew, 2023). Um estudo recente da Revista Eletrônica de Administração (REAd) explora a relação entre cultura e segurança da informação, destacando a influência da cultura brasileira na adesão às políticas de segurança (Silveira; Lunardi; Cerqueira, 2023). A inobservância, associada ao formalismo e à flexibilidade cultural, pode levar a comportamentos que contornam regras, como o compartilhamento de senhas e acesso a conteúdos não autorizados. A discussão sobre a Cultura de Segurança da Informação (CSI) destaca sua complexidade e a necessidade de uma abordagem holística que considere aspectos técnicos, humanos e culturais. A gestão eficaz das políticas de segurança exige atenção ao elemento humano, pois o comportamento dos indivíduos pode tanto fortalecer quanto comprometer a segurança. Assim, construir uma cultura de segurança robusta requer uma abordagem integrada, promovendo compreensão e sensibilização em todos os níveis organizacionais, para fortalecer as defesas contra ameaças (Tang; Li; Zhang, 2016).

A segurança da informação em instituições de ensino superior é um desafio complexo e multidisciplinar que requer não apenas a adoção de tecnologias, mas também a sensibilização e o comprometimento de toda a comunidade acadêmica. A pesquisa realizada na FE da UnB revelou uma preocupante lacuna no conhecimento e na adesão à PoSIC, evidenciando falhas significativas na comunicação e no treinamento. Os resultados indicam que a maioria dos servidores técnico-administrativos e docentes desconhece a existência da PoSIC ou não a aplica efetivamente em suas atividades cotidianas, expondo a instituição a riscos consideráveis. Embora o acesso aos meios institucionais de comunicação e experiências pessoais com incidentes de segurança possam

aumentar a conscientização sobre a política, esses fatores isolados não são suficientes para promover uma cultura de segurança robusta. Portanto, é evidente a necessidade de investir em campanhas de sensibilização e treinamentos contínuos que alcancem todos os servidores, utilizando canais de comunicação diversos e acessíveis. Uma abordagem integrada e adaptativa é necessária para garantir o engajamento dos servidores e o alinhamento estratégico com a política de segurança da informação da UnB. A efetividade da PoSIC também depende de um compromisso ativo da alta administração, que deve assumir um papel central na promoção e reforço das práticas de segurança. Incorporar a política de segurança da informação à cultura organizacional é fundamental para que ela se torne parte intrínseca das atividades e operações da universidade. Conclui-se que, para fortalecer a segurança da informação, é necessário ir além da implementação técnica de políticas e procedimentos. Deve-se fomentar uma cultura de segurança que valorize a conformidade, a comunicação, a responsabilidade e a governança, visando criar um ambiente universitário mais seguro.

2.4. CONCLUSÃO

A segurança da informação em instituições de ensino superior configura-se como um desafio amplo que exige não apenas a adoção de tecnologias avançadas, mas também o engajamento ativo e a conscientização de toda a comunidade acadêmica. O presente estudo, realizado na FE da UnB, evidenciou uma lacuna significativa no conhecimento e na adesão à PoSIC. As falhas na comunicação institucional e a ausência de treinamentos específicos comprometem a eficácia das práticas de segurança, expondo a instituição a riscos consideráveis. Embora o acesso aos meios institucionais de comunicação e a experiência pessoal com incidentes de segurança tenham elevado a conscientização entre alguns servidores, esses fatores isolados não são suficientes para instaurar uma cultura de segurança robusta e abrangente. Torna-se, portanto, imperativo investir em estratégias que promovam a sensibilização e a capacitação contínua de todos os servidores, utilizando múltiplos canais de comunicação e treinamentos regulares. Além disso, a efetividade da PoSIC está diretamente ligada ao comprometimento da alta administração, que deve desempenhar um papel central na promoção e no reforço das práticas de segurança da informação.

Conclui-se que, para fortalecer a segurança da informação na UnB, é necessário integrar os princípios da PoSIC à cultura organizacional, fomentando a conformidade, a comunicação e a responsabilidade. Apenas com esforços coordenados e uma abordagem adaptativa será possível promover um ambiente acadêmico seguro, perseverante e confiável. Este estudo contribui para a compreensão dos desafios enfrentados na implementação de políticas de segurança da informação

em instituições de ensino superior, ressaltando a necessidade urgente de ações coordenadas para mitigar os riscos cibernéticos e elevar o nível de maturidade em segurança da informação. Recomenda-se que pesquisas futuras aprofundem a investigação sobre metodologias eficazes de treinamento e comunicação, além de mecanismos que incentivem a adesão às práticas de segurança.

3. DESENVOLVIMENTO DE UMA TECNOLOGIA SOCIAL: PROPOSTA DE UM PROGRAMA DE SENSIBILIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO (PSSI) NA FE/UNB.

3.1. INTRODUÇÃO

A crescente preocupação com a segurança da informação em instituições educacionais tem evidenciado lacunas significativas na capacitação específica relacionada às políticas de segurança. Observa-se a necessidade de abordar essas deficiências por meio de treinamentos e campanhas de sensibilização, visando desenvolver estratégias que melhorem o conhecimento e a adesão às diretrizes de segurança da informação (Cordeiro, 2017; Ulven; Wangen, 2021; Cheng; Wang, 2022; Zheng *et al*., 2023).

Neste contexto, propõe-se o desenvolvimento de um Programa de Sensibilização em Segurança da Informação (PSSI) para a Faculdade de Educação da Universidade de Brasília (FE/UnB) visando criar uma cultura organizacional de segurança da informação, capacitando os colaboradores a compreender os princípios de proteção de dados e a agir em conformidade com as políticas estabelecidas (Sikolia *et al*., 2023; Alyami *et al*. 2023; Zheng *et al*. 2023).

O PSSI busca aumentar a sensibilização dos servidores sobre os riscos associados à segurança da informação e a importância de proteger os ativos informacionais da instituição. Por meio de campanhas de sensibilização, treinamentos específicos e educação contínua, o programa pretende garantir que os servidores reconheçam ameaças comuns, compreendam as políticas de segurança e apliquem boas práticas em suas atividades diárias.

A relevância social, científica e tecnológica deste produto técnico-tecnológico reside na promoção de uma cultura de segurança que permeia todas as áreas e níveis da instituição, reduzindo o risco de violações e protegendo os ativos de informação contra ameaças internas e externas. Ademais, a implementação do PSSI na FE/UnB pode servir como modelo para outras instituições educacionais que enfrentam desafios semelhantes em relação à segurança da informação.

Ao alinhar-se com as diretrizes da Política de Segurança da Informação e Comunicações (PoSIC) da UnB e com as melhores práticas identificadas na literatura, que destacam a importância do apoio da alta direção, da relevância do conteúdo e da regularidade das atividades de treinamento, o PSSI apresenta-se como uma iniciativa imprescindível para fortalecer a governança e a proteção dos ativos informacionais. Dessa forma, contribui-se para a criação de um ambiente acadêmico mais seguro e resistente frente aos desafios cibernéticos atuais.

3.2. A PoSIC

Neste ponto, é imperativo definir à luz a constituição da PoSIC. Em 8 de novembro de 2018, a Câmara de Planejamento e Administração (CPLAD) da UnB aprovou a PoSIC, baseada no Decreto Nº 9.637, que institui a Política Nacional de Segurança da Informação. Seu objetivo é garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações da universidade (BRASIL, 2018a). Complementada pela LGPD, a PoSIC define diretrizes para proteção de dados, segurança cibernética e defesa de infraestruturas críticas (Lei Nº 13.709, 2018). A política foi elaborada conforme o artigo 15, inciso II, do Decreto Nº 9.637, seguindo normas do Gabinete de Segurança Institucional da Presidência da República (BRASIL, 2018). A PoSIC abrange a gestão de ativos, continuidade de negócios e segurança das comunicações, conforme o Plano Diretor de TIC (PDTI) da UnB (BRASIL, 2023), aplicando-se a servidores, docentes, estudantes e parceiros da universidade (BRASIL, 2018a). A Resolução Nº 004/2018 integra a PoSIC ao Projeto Político Pedagógico Institucional e ao Plano de Desenvolvimento Institucional (PDI) da UnB (BRASIL, 2018c; BRASIL, 2023). Todos os usuários devem seguir as normas da PoSIC e suas instruções complementares, alinhadas aos objetivos estratégicos e legais da Administração Pública Federal (BRASIL, 2018a). A Política de Governança de TIC (PGTIC), estabelecida pela Resolução Nº 003/2018, destaca o alinhamento estratégico, transparência e conformidade legal, assegurando que as práticas de TIC estejam de acordo com os objetivos institucionais. A gestão de riscos e planos de continuidade são fundamentais para a segurança da informação na UnB (BRASIL, 2018d). O PDI 2023-2028 reforça a PoSIC com o apoio da administração da UnB, STI e ETIR, que asseguram a execução das diretrizes de segurança (BRASIL, 2023).

O PDTIC 2023-2028 complementa o PDI ao detalhar processos e sistemas de TIC que fortalecem a segurança, com ações preventivas, monitoramento e resposta a incidentes, além de gestão de riscos e elevação da maturidade em segurança (BRASIL, 2023a). Em conjunto, o PDI e o PDTIC garantem que as iniciativas de segurança da informação sejam eficazes e monitoradas, contribuindo para o cumprimento dos objetivos da universidade (BRASIL, 2023; BRASIL, 2023a).

3.3. DESCRIÇÃO DO PRODUTO

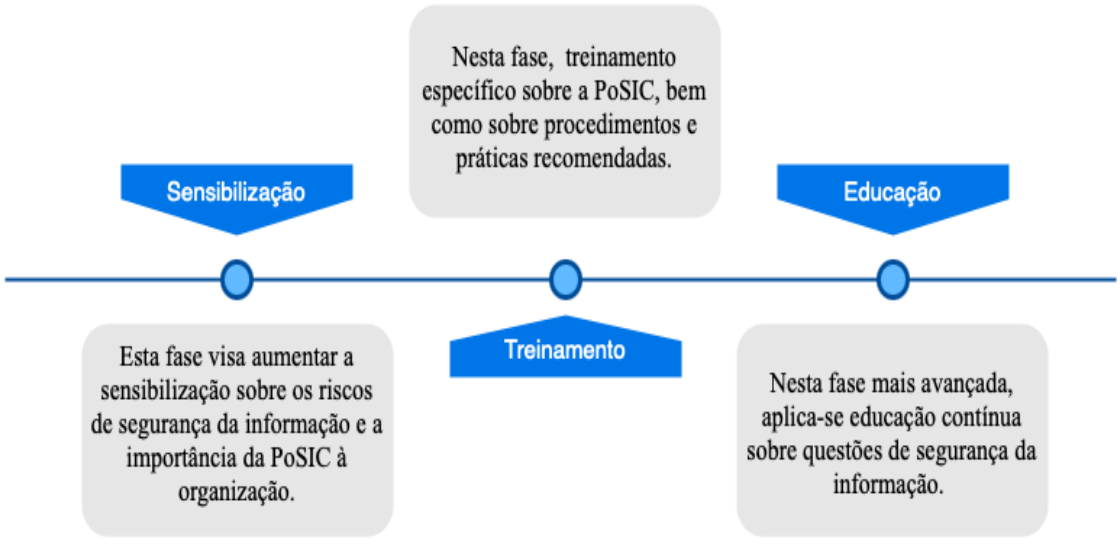
O presente trabalho resultou na elaboração de um **Programa de Sensibilização em Segurança da Informação** (PSSI) para a FE/UnB, constituindo um produto técnico-tecnológico sob a forma de tecnologia social. Esse programa surgiu a partir de uma investigação sobre a implementação da PoSIC na UnB, que evidenciou lacunas significativas no conhecimento e na

adesão dos servidores técnico-administrativos e docentes às diretrizes estabelecidas pela política.

O desenvolvimento do PSSI iniciou-se com uma pesquisa detalhada que objetivou compreender o nível de maturidade e conhecimento dos servidores em relação à PoSIC, além de identificar as principais falhas na comunicação e na implementação da política. Essa investigação culminou na elaboração de um artigo acadêmico, apresentado no primeiro capítulo, intitulado "**Avaliação da Maturidade e Adesão à Política de Segurança da Informação: Um Estudo na Faculdade de Educação da UnB**". O estudo abordou a evolução da segurança da informação no contexto das instituições de ensino superior, destacando a importância crescente desse tema diante das ameaças cibernéticas contemporâneas.

Com base nas lacunas identificadas nesse estudo, elaborou-se o PSSI, concebido para abordar as deficiências evidenciadas pela pesquisa. O programa fundamentou-se no modelo SETA (*Security Education, Training, and Awareness*), reconhecido por sua eficácia na criação de uma cultura organizacional de segurança da informação (Alyami *et al*., 2023; Sikolia *et al*., 2023; Zheng *et al*., 2023). Esse modelo proporciona uma estrutura holística que contempla as fases de sensibilização, treinamento e educação contínua, essenciais para capacitar os servidores a compreender os princípios de proteção de dados e agir em conformidade com as políticas estabelecidas.

Figura 03 - Fluxo do Modelo SETA



Fonte: elaborado pelo autor.

O PSSI foi estruturado em três fases principais: 1ª) • Sensibilização (*Awareness*): esta fase visa aumentar a sensibilização dos servidores sobre os riscos de segurança da informação e a importância de proteger os ativos de informação da organização. Isso pode incluir campanhas de

sensibilização por e-mail, cartazes informativos, boletins informativos ou workshops sobre segurança da informação. Os objetivos incluem garantir que os servidores reconheçam ameaças comuns, como *phishing*, engenharia social, uso inadequado de senhas etc. 2ª) • Treinamento (*Training*): nesta fase, os servidores recebem treinamento específico sobre as políticas de segurança da informação da organização, bem como sobre procedimentos e práticas recomendadas. O treinamento pode ser conduzido por especialistas internos ou externos e pode ser presencial ou online. Os objetivos incluem capacitar os servidores a aplicarem as políticas de segurança em suas atividades diárias, entenderem como lidar com dados sensíveis, reconhecerem sinais de possíveis violações de segurança e saberem como relatar incidentes. 3ª) • Educação (*Education*): nesta fase mais avançada, os colaboradores recebem educação contínua sobre questões de segurança da informação. Isso pode incluir cursos mais detalhados sobre tópicos específicos, *workshops* práticos ou programas de desenvolvimento profissional. Os objetivos incluem capacitar os colaboradores a desempenharem papéis mais especializados em segurança da informação, como administradores de sistemas, analistas de segurança, especialistas em resposta a incidentes etc.

3.4. BASE TEÓRICA

O desenvolvimento do PSSI considerou os referenciais teóricos e normativos relevantes, incluindo a PoSIC da UnB, o Decreto nº 9.637/2018, que institui a Política Nacional de Segurança da Informação e a Lei Geral de Proteção de Dados (LGPD). Além disso, foram consultados estudos acadêmicos e pesquisas recentes sobre segurança da informação em instituições educacionais, os quais enfatizam a importância da conscientização, do treinamento e da educação contínua dos servidores (Ulven; Wangen, 2021; Cheng; Wang, 2022; Zheng *et al*., 2023).

Ao seguir este modelo, as organizações podem criar uma cultura de segurança da informação que permeia todas as áreas e níveis da empresa, garantindo que todos os servidores compreendam e sigam as políticas de segurança estabelecidas. Isso pode ajudar a reduzir o risco de violações de segurança e proteger os ativos de informação da organização contra ameaças internas e externas (De Casanove; Leleu; Sèdes, 2022; Zheng *et al*., 2023). O SETA pode adaptar-se a diferentes níveis de conhecimento e experiência dos usuários, fornecendo sensibilização, treinamento e educação adequados à sua capacidade de compreensão. Alyami *et al*. (2024) identificam vários fatores críticos de sucesso (FCS) que são essenciais para a eficácia dos programas de SETA. Entre esses fatores estão o apoio da alta direção, a clareza e a relevância do conteúdo, bem como a regularidade e a interatividade das atividades de treinamento. Esses aspectos são fundamentais para garantir que os usuários não apenas recebam a informação, mas

também a integrem em suas práticas diárias. A pesquisa na FE-UnB reconhece a necessidade de tais elementos ao propor um programa que inclui sessões regulares de treinamento e comunicação contínua sobre as políticas de segurança da informação (Alyami *et al*., 2024).

O apoio da alta direção é um dos fatores mais críticos para o sucesso de programas SETA. Este apoio se traduz na alocação de recursos adequados, na promoção do programa e na integração das práticas de segurança na cultura organizacional. Na FE-UnB, o envolvimento dos gestores e líderes acadêmicos é crucial para a implementação eficaz do PSSI. Sem esse apoio, as iniciativas de sensibilização podem ser percebidas como secundárias ou opcionais, o que comprometeria sua eficácia (Alyami *et al*., 2024). Outro ponto crucial destacado por Alyami *et al*. (2024) é a necessidade de que o conteúdo dos programas SETA seja claro, relevante e específico para o público-alvo. Isso implica adaptar as mensagens de segurança para que sejam compreensíveis e aplicáveis às funções específicas dos servidores técnico-administrativos e docentes. A clareza e a relevância garantem que os participantes vejam o valor nas informações e estejam mais inclinados a adotar as práticas recomendadas.

Trigos e Nuno (2021) apontam que a efetividade dos programas de sensibilização depende da adequação do conteúdo à realidade dos usuários e da regularidade das atividades de treinamento. Isto corrobora com a necessidade do PSSI na FE-UnB, que é projetado para preencher as lacunas de conhecimento e fortalecer a cultura de segurança entre os servidores técnico-administrativos e docentes. Ainda segundo Trigos e Nuno (2021), campanhas regulares e dinâmicas de sensibilização têm um impacto significativo na melhoria da postura de segurança dos usuários, reduzindo comportamentos arriscados e aumentando a aderência às políticas institucionais.

Programas que incluem atividades práticas, simulações e feedback contínuo tendem a ser mais eficazes (Soomro; Shah; Ahmed, 2016). Na FE-UnB, a proposta de implementação do PSSI inclui workshops interativos, sessões de perguntas e respostas, e-mails, boletins etc. Essas estratégias não apenas educam, mas também envolvem os participantes de forma ativa, aumentando a retenção do conhecimento e a aplicação prática das diretrizes de segurança (Soomro; Shah; Ahmed, 2016; Alyami *et al*., 2024).

Em ambientes com usuários básicos, o programa pode começar com uma fase de sensibilização, apresentando conceitos fundamentais da PoSIC de forma simples e de linguagem acessível. O treinamento pode então focar em habilidades práticas básicas, como identificação de *e-mails* de *phishing* ou criação de senhas seguras, por exemplo. A educação pode ser direcionada para fornecer um entendimento mais profundo dos princípios da PoSIC, sempre mantendo a linguagem e os exemplos relevantes e compreensíveis para o público-alvo. A experiência relatada

por Trigos e Nuno (2021) demonstra que programas de sensibilização bem-estruturados resultam em uma redução significativa de incidentes de segurança da informação. Aplicando este conhecimento ao contexto da FE-UnB, espera-se que a implementação do PSSI resulte em uma melhora substancial na compreensão e adesão às práticas de segurança da informação. Isso é fundamental para criar um ambiente educacional seguro, onde os dados são protegidos e a integridade dos sistemas é mantida.

O modelo SETA tem sido implementado por diversas empresas em diferentes setores. Por exemplo, uma empresa no setor financeiro, como a JPMorgan Chase, utiliza programas SETA para educar seus colaboradores sobre práticas de segurança cibernética e reduzir riscos. No setor de infraestrutura crítica, empresas como a Duke Energy implementam treinamentos de sensibilização para proteger contra ameaças digitais. Além disso, no setor de saúde, organizações como a Mayo Clinic adotam programas SETA para garantir a segurança das informações dos pacientes e conformidade com regulamentações (Zheng *et al*., 2023).

O estudo *An Empirical Study of SETA Program Sustaining Educational Sector's Information Security vs. Information Systems Misuse* (2023), foi realizado no College of Business da City University of Hong Kong (CityU). O estudo investigou o impacto de um programa SETA na segurança da informação e no uso indevido de sistemas de informação. O estudo adota uma abordagem de pesquisa quantitativa, utilizando teoria da dissuasão e variáveis intermediárias como custo percebido e consciência de segurança da informação. A *Information Security Awareness* (ISA) ou em português "Consciência de Segurança da Informação" (CSI), no estudo, refere-se à compreensão e ao conhecimento que um indivíduo ou grupo tem sobre a importância da proteção das informações e dos dados. Os resultados indicaram que a implementação do programa SETA teve um impacto positivo na percepção de custo e na ISA dos alunos, contribuindo para a redução do comportamento de uso indevido dos sistemas de informação. Com a adoção do programa, os alunos desenvolveram uma maior compreensão dos custos associados ao uso inadequado dos sistemas de informação, o que os levou a reconsiderar suas ações antes de cometerem infrações. Além disso, o programa aumentou a sensibilização sobre a importância da segurança da informação, incentivando os alunos a adotarem práticas mais seguras. Como resultado, observou-se uma redução notável no comportamento de uso indevido dos sistemas de informação (Zheng *et al*., 2023).

Outro estudo que demonstra a eficácia da aplicação do programa SETA foi realizado por Sikolia, Biros e Zhang (2023). Este estudo investigou a eficácia dos programas SETA na mitigação de erros humanos em um cenário longitudinal. Os resultados indicaram que os programas SETA podem reduzir a susceptibilidade a ataques de phishing em 50%. Além disso,

foi observado que o conhecimento de segurança cibernética dos usuários aumentou entre 12-17% após a participação no programa. No entanto, para que essa eficácia seja mantida ao longo do tempo, é necessário implementar reforços contínuos e adaptar os programas para enfrentar a diminuição do conhecimento adquirido. Uma observação crucial é a diferença na taxa de decaimento entre conhecimentos técnicos e aplicáveis, o que indica a necessidade de abordagens específicas para cada tipo de conhecimento. os resultados deste estudo sugerem que investir em programas SETA é extremamente valioso. No entanto, eles devem estar cientes da importância de realizar treinamentos periódicos e enviar lembretes constantes para garantir que a eficácia seja mantida a longo prazo. Além disso, a compreensão de que diferentes tipos de conhecimento têm durações de retenção distintas pode ajudar a desenvolver estratégias mais eficazes para programas de treinamento contínuo. Por exemplo, conhecimentos técnicos podem requerer reforços mais frequentes, enquanto conhecimentos aplicáveis podem necessitar de abordagens diferentes para garantir sua retenção. Dessa forma, a adoção de estratégias de treinamento que considerem essas diferenças pode maximizar a eficácia dos programas SETA.

O estudo de Alyami *et al*. (2023) identificou 11 fatores críticos de sucesso para a eficácia dos programas SETA, quais sejam: engajamento da alta direção; cultura organizacional; conteúdo relevante e atualizado; métodos de treinamento eficazes; frequência e regularidade do treinamento; avaliação e feedback contínuos; integração com processos de negócio; recursos adequados; responsabilidade e *accountability*; medidas de reforço e recompensa; comunicação efetiva. Esses fatores foram mapeados ao longo das fases do ciclo de vida de um programa SETA e incluíram aspectos como a realização de uma avaliação inicial da sensibilização dos colaboradores sobre segurança, conhecimento do público-alvo para garantir a adequação do conteúdo e comunicação contínua de mensagens relevantes. A análise de entrevistas com informantes-chave revelou que esses fatores são essenciais para projetar e sustentar um programa SETA eficaz, capaz de mudar o comportamento dos colaboradores em relação à segurança da informação.

Estudos abordam diferentes aspectos da importância e eficácia dos programas SETA, convergindo em vários pontos chave:

• **Redução de Riscos de Segurança**: todos os estudos concordam que os programas SETA são fundamentais para reduzir os riscos de segurança, especialmente em termos de suscetibilidade a ataques de *phishing* e outros erros humanos (Sikolia *et al*., 2023; Alyami *et al*. 2023; Zheng *et al*. 2023);

• **Importância do Ciclo de Vida Completo**: a adoção de um modelo de ciclo de vida completo, que abrange *design*, desenvolvimento, implementação e avaliação, é crucial para a eficácia dos programas SETA. Isso assegura que todas as fases do programa são abordadas adequadamente, promovendo uma mudança de comportamento duradoura entre os colaboradores (Sikolia *et al*., 2023; Alyami *et al*. 2023; Zheng *et al*. 2023);

• **Fatores Críticos de Sucesso**: a identificação e o gerenciamento de fatores críticos de sucesso são essenciais. Elementos como a manutenção de avaliações, a construção de campanhas de sensibilização e a consideração da cultura organizacional são destacados como fundamentais para a implementação bem-sucedida de programas SETA (Alyami *et al*. 2023; Zheng *et al*. 2023);

• **Desafios na Implementação**: um desafio recorrente mencionado é a diminuição do impacto dos programas SETA ao longo do tempo. A necessidade de sessões de treinamento e sensibilização contínuas para manter o conhecimento e a vigilância dos funcionários é enfatizada como uma prática necessária para sustentar a eficácia dos programas SETA (Sikolia *et al*., 2023; Alyami *et al*. 2023; Zheng *et al*. 2023).

A análise comparativa dos estudos revela que, embora os programas SETA sejam essenciais para a segurança cibernética organizacional, sua eficácia depende de uma abordagem que abranja todo o ciclo de vida do programa, focando em fatores críticos de sucesso e na manutenção contínua do conhecimento e comportamento dos colaboradores. A implementação de práticas contínuas de treinamento e sensibilização, aliada a uma avaliação periódica, é vital para garantir a eficácia a longo prazo desses programas (Sikolia *et al*., 2023; Alyami *et al*. 2023; Zheng *et al*. 2023).

Para a implementação eficaz do PSSI, propôs-se uma parceria estratégica entre a Secretaria de Tecnologia da Informação (STI) e a Coordenadoria de Capacitação (Procap) da UnB. A STI, com sua expertise técnica, contribuiria na elaboração de conteúdos específicos, enquanto a Procap, responsável pelo desenvolvimento de competências dos servidores, atuaria como veículo ideal para disseminar as práticas essenciais de segurança. Essa colaboração é fundamental para garantir recursos adequados, promover o programa e integrar as práticas de segurança à cultura organizacional, alinhando-se aos fatores críticos de sucesso identificados por Alyami *et al*. (2023).

A Universidade de Brasília conta com a Coordenadoria de Capacitação (Procap), parte integrante da Diretoria de Capacitação, Desenvolvimento e Educação (Dcade), subordinada ao Decanato de Gestão de Pessoas (DGP). O propósito principal da Procap é oferecer uma variedade de ações de capacitação para os servidores, tanto técnico-administrativos quanto docentes. Essas ações incluem cursos nas modalidades presencial, híbrido, remoto e a distância, além de oficinas,

palestras e mestrados profissionais (BRASIL, 2016). O objetivo é promover o desenvolvimento de competências e a atualização de conhecimentos e habilidades. Os departamentos da UnB têm acesso ao Plano de Desenvolvimento de Pessoas (PDP), que permite planejar as necessidades de capacitação de cada unidade e de suas equipes (BRASIL, 2023b). A responsabilidade pela capacitação do corpo técnico, especialmente na área de tecnologia, recai sobre a Secretaria de Tecnologia da Informação (STI), que também oferece treinamentos específicos conforme as demandas identificadas pela Procap. No entanto, a STI não é responsável pela capacitação geral do corpo técnico-administrativo e docente, função esta atribuída à Procap.

Para assegurar a segurança das informações e comunicações na UnB é imperativo que a STi estabeleça uma parceria estratégica com a Procap. Esta colaboração é fundamental para uma implementação eficaz das normas e procedimentos estipulados nos Artigos 4º e 45º da PoSIC/UnB, garantindo sua ampla divulgação e compreensão entre todos os servidores.

A Procap, sendo responsável pelo desenvolvimento de competências e pela atualização de conhecimentos e habilidades através de uma variedade de ações formativas (BRASIL, 2016), posiciona-se como um veículo ideal para disseminar práticas essenciais de segurança. A STi, com sua expertise técnica, pode contribuir significativamente, trabalhando em conjunto com a Procap na elaboração de conteúdos que abordem especificidades da segurança da informação. Essa sinergia permitiria não apenas a capacitação adequada dos servidores em temas críticos, mas também a atualização constante dos currículos para refletir os avanços tecnológicos e as novas ameaças cibernéticas. Ademais, essa interação contínua facilita a identificação de lacunas de conhecimento em segurança da informação, possibilitando ajustes no Plano de Desenvolvimento de Pessoas (PDP) para incluir treinamentos especializados. Isso não só reforça a infraestrutura de segurança de dados da UnB como também promove uma cultura organizacional que valoriza a segurança da informação. Uma cultura robusta de segurança pode ser cultivada não apenas por meio de treinamentos, mas também através de campanhas de sensibilização, workshops e outros eventos promovidos em parceria, enfatizando a importância da segurança das informações no ambiente acadêmico e administrativo. Portanto, a colaboração entre a STi e a Procap é crucial não só para cumprir os requisitos da PoSIC, mas também para proteger os recursos da universidade e preparar adequadamente sua comunidade para enfrentar os desafios relacionados à segurança da informação de maneira proativa e informada.

3.5. INTERVENÇÃO

A pesquisa, já em sua concepção, manifesta uma abordagem intervencionista, que se caracteriza por propor uma ação direta ou uma intervenção com o objetivo de modificar, aprimorar ou causar um impacto significativo na situação atual. Esta característica se torna evidente mesmo que a proposta ainda se encontre em uma fase conceitual. No que diz respeito à gestão da segurança da informação na FE/UnB, a natureza intervencionista da proposta se revela por meio de diversos aspectos. A proposta estabelece o objetivo de promover uma mudança ativa, propondo um programa para aumentar a sensibilização sobre a segurança da informação e abordando práticas seguras. Tal iniciativa representa uma mudança substancial nos procedimentos atuais, evidenciando a busca por um impacto direto e efetivo. Além disso, ela possui o potencial de influenciar e modificar as políticas e práticas existentes na instituição, demonstrando que seu alcance vai além do teórico, podendo se converter em ações concretas. Hayes (2014) oferece uma visão contemporânea sobre como gerenciar mudanças nas organizações. Ele explora como as propostas de mudança, mesmo antes de sua implementação, são essenciais no processo de gestão da mudança. O foco da proposta em ações diretas como a elaboração de programas de treinamento, análise e possível modificação da cultura organizacional, reforça seu caráter intervencionista. Estas ações não são apenas teóricas, mas sim voltadas para a prática, com o intuito de causar uma mudança real e perceptível. Por fim, o propósito explícito da proposta é intervir na situação atual para melhorar a segurança da informação. Este é um elemento importante de um modelo intervencionista, que se baseia na premissa de que ações diretas são necessárias para gerar transformações significativas. Portanto, mesmo que a proposta esteja atualmente em um estágio teórico ou planejado, sua orientação para a mudança ativa e o impacto potencial nas políticas e práticas de segurança da informação na UnB a qualificam como intervencionista.

3.6. PLANO DE AÇÃO E ALINHAMENTO DO PSSI

O plano de ação para o PSSI está fundamentado em modelos e normas reconhecidos internacionalmente, o que assegura uma abordagem sistemática e eficaz para sua implementação. O plano alinha-se com o Ciclo PDCA (Planejar-Fazer-Verificar-Agir), também conhecido como Ciclo de Deming, conforme descrito por Deming (2018) e que também se alinha as diretrizes estabelecidas pela norma ISO/IEC 27001, que trata dos Sistemas de Gestão de Segurança da Informação (NBR ISO 27001, 2022). No contexto do PSSI, a fase de planejamento envolve a proposição de conteúdos educacionais, campanhas de sensibilização e treinamentos práticos, baseados nas necessidades identificadas na pesquisa realizada na FE/UnB. A fase de execução corresponde à implementação dessas ações propostas, como a realização de cursos, workshops e

campanhas, iniciando em um departamento piloto. Durante a fase de verificação, os resultados seriam monitorados e avaliados por meio de questionários de avaliação, análise de impacto e coleta de feedback dos participantes, alinhando-se às recomendações de monitoramento contínuos, presentes na ISO/IEC 27001(NBR ISO 27001, 2022). A fase de ação incluiria ajustes e melhorias necessários com base nas avaliações, antes de expandir o programa para toda a instituição. Além disso, o plano de ação incorpora elementos do Modelo ADDIE (Análise, Desenho, Desenvolvimento, Implementação, Avaliação), amplamente utilizado no design instrucional para desenvolver programas educacionais eficazes, conforme discutido por Molenda (2003). Na fase de análise, realizou-se o levantamento das necessidades por meio da pesquisa com os servidores, identificando lacunas de conhecimento e percepção em relação à segurança da informação. Na fase de desenho, foram propostos os conteúdos educacionais, estratégias de ensino e métodos de avaliação alinhados com as necessidades identificadas. A fase de desenvolvimento contemplou a sugestão de criação de materiais educativos, como folhetos, vídeos e recursos gamificados, além do planejamento detalhado de cursos e workshops. A fase de implementação refere-se à execução das atividades educacionais e campanhas de sensibilização propostas, iniciando com o departamento piloto e expandindo gradualmente. Por fim, a fase de avaliação envolveria a aplicação de instrumentos para medir o impacto do programa, coleta de feedback e realização de ajustes necessários.

Ao fundamentar o plano de ação do PSSI nesses modelos e normas estabelecidos, o programa adota uma abordagem metodológica sólida que reforça sua credibilidade e aumenta a probabilidade de sucesso na implementação. Essa integração assegura que o PSSI atende às necessidades específicas da FE/UnB, ao mesmo tempo em que está alinhado com as melhores práticas globais em segurança da informação e educação corporativa. A aplicação do Ciclo PDCA facilita a melhoria contínua do programa, enquanto a aderência à ISO/IEC 27001 garante que os processos estejam alinhados com padrões internacionais de segurança. A incorporação do Modelo ADDIE assegura que os componentes educacionais sejam desenvolvidos de maneira estruturada e eficaz, maximizando o aprendizado e o engajamento dos participantes.

3.6.1. ESTRUTURA DO PLANO AÇÃO

Conteúdo Educacional

- Cursos de Segurança da Informação: desenvolver e implementar cursos online e presenciais sobre princípios de segurança da informação, ameaças cibernéticas e boas práticas.

- Materiais Educativos: criar folhetos informativos, vídeos educativos e artefatos gamificados para facilitar o aprendizado e engajamento com a PoSIC.

Campanhas de Sensibilização

- Campanhas Multimodais: implementar campanhas contínuas de sensibilização da PoSIC utilizando e-mails, boletins, redes sociais, workshops e seminários para alcançar toda a comunidade acadêmica.
- Eventos Educativos: organizar palestras e *webinars* com especialistas em segurança da informação para discutir temas relevantes e casos práticos.

Treinamento Prático

- Workshops Práticos: realizar sessões de treinamento prático focadas em áreas como o uso seguro de senhas, utilização de e-mail, gestão de ativos, reconhecimento de phishing etc. e boas práticas de segurança.
- Sessões de Reciclagem: oferecer treinamentos periódicos de reciclagem para garantir que os servidores estejam sempre atualizados sobre as melhores práticas de segurança.

Implementação

- Departamento Piloto: implementar inicialmente o programa PSSI em um departamento piloto para testar a eficácia e ajustar conforme necessário.
- Coleta de Feedback: coletar feedback dos participantes da fase piloto para identificar pontos de melhoria e adaptar o programa.
- Expansão Gradual: expandir a implementação para toda a Faculdade de Educação após ajustes com base no feedback da fase piloto.
- Comunicação Contínua: manter uma comunicação contínua sobre a importância da segurança da informação e os benefícios do programa PSSI.

Avaliação e Monitoramento

- Questionário de Avaliação: aplicar um questionário após a implementação do programa para medir mudanças no conhecimento, atitudes e comportamentos dos servidores.
- Análise de Impacto: realizar uma análise comparativa dos dados pré e pós-implementação para avaliar o impacto do programa.
- Sessões de Feedback: organizar sessões de feedback contínuo com os servidores para identificar áreas de melhoria e adaptar o programa conforme necessário.
- Monitoramento Contínuo: implementar um sistema de monitoramento contínuo para avaliar a eficácia do programa e fazer ajustes proativos.

3.6.2. CRONOGRAMA

Tabela 01 - Cronograma de Execução

Mês	Atividades
1-2	Desenvolvimento do questionário e realização das entrevistas iniciais.
3-4	Desenvolvimento do conteúdo educacional e materiais de treinamento.
5-6	Implementação da fase piloto e coleta de feedback.
7-8	Ajustes no programa e implementação total.
9-12	Avaliação contínua, aplicação do questionário pós-implementação e análise comparativa dos dados.

3.7. RELEVÂNCIA, COMPLEXIDADE E ADERÊNCIA

O PSSI desenvolvido neste trabalho configura-se como um produto técnico-tecnológico de alta complexidade. Essa complexidade é evidenciada pela profundidade teórica, abrangência metodológica e inovação que o programa representa no contexto da segurança da informação em instituições de ensino superior. A elaboração do PSSI exigiu uma integração interdisciplinar de conhecimentos em segurança da informação, gestão organizacional, cultura organizacional, psicologia social, educação e tecnologia da informação, demandando não apenas um entendimento de cada área, mas também a capacidade de correlacionar conceitos complexos para criar um programa coeso e eficaz. Além disso, o PSSI apresenta inovação e originalidade ao propor soluções para os desafios identificados na segurança da informação da FE/UnB. A criação de estratégias multimodais de comunicação e treinamento, adaptadas às preferências dos servidores, e a personalização do programa para o contexto específico da instituição destacam a originalidade e a capacidade de inovação do trabalho. A elaboração do PSSI também exigiu a compreensão aprofundada e a aplicação de marcos legais e normativos.

Quanto à aderência, o PSSI apresenta forte afinidade com a área de concentração e as linhas de atuação do Programa de Pós-Graduação em Gestão Pública da Universidade de Brasília. O programa aborda questões centrais da gestão pública, como governança da informação, gestão de políticas institucionais, *compliance* e gestão de riscos. A segurança da informação é um componente crítico para a eficiência, transparência e confiabilidade das instituições públicas, temas essenciais na gestão pública. O PSSI contribui diretamente para a melhoria das políticas públicas relacionadas à segurança da informação, propondo intervenções que fortalecem a proteção de dados e a conformidade legal. A elaboração do programa envolve a análise, avaliação e aprimoramento de políticas institucionais, alinhando-se à gestão de políticas públicas.

Além disso, o PSSI está intrinsecamente relacionado à governança e tecnologia da informação, ao propor práticas que melhoram a gestão da segurança da informação e a utilização

de tecnologias para capacitação e comunicação. O programa incorpora conceitos de governança de TI e promove a integração entre áreas técnicas e de gestão, refletindo os objetivos das linhas de pesquisa do programa de pós-graduação. O trabalho fornece soluções práticas e aplicáveis, contribuindo para a formação de gestores públicos capazes de enfrentar desafios complexos na área de segurança da informação, fortalecendo competências profissionais alinhadas aos objetivos do programa e preparando os discentes para atuar em contextos organizacionais reais.

A relevância social e o impacto na administração pública são evidentes, pois, ao abordar a segurança da informação em uma instituição pública de ensino superior, o PSSI tem impacto direto na melhoria dos serviços públicos, proteção dos dados dos cidadãos e aumento da confiança na administração pública. Isso reflete a missão do programa de contribuir para o desenvolvimento social e institucional. O trabalho exemplifica a integração entre pesquisa acadêmica e aplicação prática, característica valorizada no programa de pós-graduação, utilizando metodologias rigorosas para resolver problemas reais e demonstrando aderência aos princípios do programa ao promover a produção de conhecimento relevante e aplicável.

O programa não apenas atende aos requisitos acadêmicos, mas também oferece uma contribuição significativa para a melhoria das práticas institucionais e para o avanço do conhecimento na área. Dessa forma, o PSSI se estabelece como um modelo de excelência, alinhado às expectativas da CAPES e fortalecendo a avaliação institucional, demonstrando a capacidade de integrar teoria e prática para promover melhorias significativas na gestão pública.

3.8. TIPO DE PRODUTO TÉCNICO-TECNOLÓGICO

O PSSI enquadra-se predominantemente na categoria de Desenvolvimento de Tecnologia Social. Este enquadramento justifica-se pelo fato de o PSSI representar uma metodologia inovadora de intervenção social dentro da instituição, voltada para a promoção de mudanças comportamentais e culturais em relação à segurança da informação. Ao capacitar servidores técnico-administrativos e docentes e fomentar uma cultura organizacional mais consciente e proativa, o programa utiliza práticas educacionais e sociais para solucionar um problema organizacional de elevada relevância social.

3.9. POTENCIAL INOVADOR

O PSSI, desenvolvido neste estudo, apresenta um potencial inovador significativo, capaz de gerar valor substancial para a FE/UnB e, potencialmente, para outras instituições educacionais. A inovação do PSSI reside na criação de uma metodologia personalizada que integra conhecimentos teóricos avançados em segurança da informação com práticas adaptadas ao contexto específico da instituição, resultando em um produto tecnologicamente aprimorado em

relação aos processos anteriormente utilizados. Diferentemente de abordagens convencionais, o PSSI utiliza uma estratégia multidisciplinar que combina elementos de cultura organizacional, psicologia comportamental e metodologias ativas de aprendizagem. Essa integração permite uma intervenção mais eficaz, promovendo mudanças comportamentais e culturais entre os servidores técnico-administrativos e docentes em relação à segurança da informação. Ao propor a utilização de recursos tecnológicos inovadores, como ferramentas de gamificação, plataformas interativas ou estratégias de comunicação multimodais, espera-se aumentar o engajamento dos servidores e reforçar a assimilação dos conceitos de segurança. A inovação também se manifesta na personalização do programa, que foi elaborado com base em dados empíricos coletados especificamente na FE/UnB. A pesquisa detalhada sobre o nível de maturidade e conhecimento dos servidores em relação à PoSIC permitiu identificar lacunas e necessidades particulares da instituição. Essa customização representa um avanço significativo em relação a soluções genéricas disponíveis no mercado, oferecendo uma resposta mais alinhada com a realidade institucional e, consequentemente, mais eficaz. Além disso, o PSSI incorpora práticas educacionais inovadoras ao propor materiais e planos de treinamento originais, refletindo as últimas tendências e pesquisas em segurança da informação.

3.10. APLICABILIDADE

O PSSI, desenvolvido neste estudo, apresenta uma aplicabilidade potencial significativa na FE/UnB e em outras instituições educacionais que enfrentam desafios semelhantes em relação à segurança da informação. O PSSI foi concebido e elaborado a partir de uma investigação aprofundada sobre a implementação da PoSIC na UnB, que identificou lacunas significativas no conhecimento e na adesão dos servidores técnico-administrativos e docentes às diretrizes estabelecidas.

A aplicabilidade potencial do PSSI é elevada devido à sua estrutura modular e flexível, que permite adaptação a diferentes contextos organizacionais. O programa foi desenvolvido com base em modelos teóricos reconhecidos, o que facilita sua customização e adoção por outras unidades acadêmicas ou instituições.

A facilidade de aplicação do PSSI também é favorecida pelos planos de treinamento elaborados durante este estudo, que podem ser compartilhados e ajustados conforme as necessidades específicas de cada organização. A natureza adaptável do PSSI permite que ele seja dimensionado de acordo com as capacidades e limitações de cada instituição. Até o momento, o PSSI permanece como uma proposta de intervenção e não foi implementado na FE/UnB. Portanto, a aplicabilidade realizada ainda não pode ser avaliada em termos de facilidade ou dificuldade de

emprego, nem em relação à amplitude de sua aplicação prática. A ausência de aplicação prática significa que não há dados empíricos sobre a efetividade do programa ou sobre os desafios enfrentados durante sua implementação. Apesar disso, a elaboração detalhada do PSSI, incluindo planos de ação e estratégias de comunicação, proporciona um fundamento sólido para a futura implementação. A pesquisa realizada revelou o interesse dos servidores em participar de treinamentos e a necessidade reconhecida pela instituição de fortalecer a cultura de segurança da informação, o que indica um ambiente propício para a aplicação do programa. A próxima etapa recomendada é a apresentação do PSSI à direção da FE/UnB e aos órgãos competentes, como a STI e a Procap, para discussão e planejamento da possível implementação. Fatores como a definição de cronogramas, alocação de recursos e estabelecimento de parcerias internas serão determinantes para a concretização do programa.

3.11. IMPACTO POTENCIAL

O PSSI, apresenta não apenas soluções para os desafios específicos da FE/UnB, mas também oferece um modelo que pode ser amplamente aproveitado por outras organizações. A metodologia proposta é aplicável a diversas instituições que enfrentam desafios semelhantes em relação à segurança da informação, especialmente no contexto educacional e governamental.

Outras instituições de ensino superior, órgãos governamentais e organizações que lidam com dados sensíveis podem se beneficiar significativamente do PSSI. A estrutura modular e adaptável do programa permite que seja customizado para atender às necessidades e características específicas de diferentes ambientes organizacionais. Por exemplo, um ministério que busca aprimorar a cultura de segurança da informação pode utilizar o PSSI como base para desenvolver seu próprio programa de sensibilização, ajustando os conteúdos e estratégias de acordo com suas particularidades.

A demanda por soluções que fortaleçam a proteção de dados e promovam a conformidade com legislações como a LGPD é cada vez mais premente. O PSSI atende a essa demanda ao oferecer um programa estruturado que aborda diretamente as lacunas identificadas na cultura de segurança das organizações. Ao implementar o PSSI, as organizações podem esperar melhorias significativas na conscientização dos servidores, aumento da adesão às políticas de segurança e, consequentemente, uma redução na vulnerabilidade a ameaças cibernéticas.

Embora o PSSI ainda não tenha sido implementado na FE/UnB, a elaboração do programa já gerou impactos positivos no ambiente acadêmico. A pesquisa realizada para o desenvolvimento do PSSI aumentou a conscientização sobre a importância da segurança da informação entre os servidores que participaram do estudo. A aplicação de questionários e entrevistas semiestruturadas

proporcionou reflexões sobre práticas atuais e estimulou o interesse em treinamentos e capacitações futuras. Além disso, a disponibilização do PSSI como uma proposta detalhada pronta para implementação facilita a tomada de decisões por parte da administração da FE/UnB e de outras unidades da universidade. O programa serve como um catalisador para ações concretas na melhoria da segurança da informação, estabelecendo as bases para futuras iniciativas que podem levar a melhorias sociais e econômicas significativas, como a proteção de dados pessoais, preservação da reputação institucional e conformidade legal.

3.12. DESAFIOS

A implementação do PSSI, embora promissora, enfrenta desafios significativos que precisam ser considerados para garantir seu sucesso. Um dos principais obstáculos previstos é a possível resistência dos servidores técnico-administrativos e docentes às mudanças propostas. Essa resistência pode surgir devido ao conforto com práticas estabelecidas, falta de percepção sobre a gravidade dos riscos de segurança ou simplesmente pela sobrecarga de trabalho que dificulta a participação em treinamentos adicionais. Para mitigar esse desafio, é fundamental desenvolver estratégias de engajamento que demonstrem claramente os benefícios pessoais e institucionais da adoção de práticas seguras, além de garantir que os treinamentos sejam acessíveis e adaptados às rotinas dos colaboradores. Outro desafio importante refere-se às limitações orçamentárias que a instituição pode enfrentar. A implementação de um programa abrangente como o PSSI requer investimentos em desenvolvimento de materiais educativos, plataformas tecnológicas para treinamentos online, contratação de especialistas e possível atualização de infraestruturas tecnológicas. Em um contexto de restrições financeiras, pode ser difícil alocar os recursos necessários sem comprometer outras áreas essenciais. Para superar essa barreira, é possível explorar alternativas como o aproveitamento de recursos internos, parcerias com outras instituições ou setores governamentais, e a utilização de ferramentas gratuitas ou de código aberto que possam oferecer funcionalidades adequadas sem custos adicionais significativos. Além disso, a cultura organizacional existente pode influenciar a receptividade ao programa. Em ambientes onde a segurança da informação não é tradicionalmente priorizada, pode haver uma falta de apoio da alta administração ou uma ausência de políticas claras que reforcem a importância do tema. Nesse sentido, é crucial que a implementação do PSSI seja acompanhada por esforços de sensibilização dos gestores e líderes institucionais, destacando a segurança da informação como um componente estratégico para a instituição. A liderança pelo exemplo e o alinhamento do programa com os objetivos organizacionais podem facilitar a incorporação das novas práticas no cotidiano dos colaboradores. Por fim, a avaliação e mensuração dos resultados do PSSI

representam um desafio adicional. Sem indicadores claros de desempenho, torna-se difícil demonstrar o impacto do programa e justificar investimentos contínuos. É necessário estabelecer métricas que permitam monitorar a eficácia das ações implementadas, como o nível de participação nos treinamentos, a redução de incidentes de segurança ou a melhoria nas avaliações de conhecimento dos servidores. O feedback contínuo dos participantes também é valioso para ajustar e aprimorar o programa ao longo do tempo. Reconhecer e abordar esses desafios é fundamental para o planejamento estratégico do PSSI. Ao antecipar possíveis obstáculos e desenvolver soluções proativas, aumenta-se a probabilidade de sucesso na criação de uma cultura sólida de segurança da informação na FE/UnB. A implementação bem-sucedida do programa não apenas fortalecerá a proteção dos ativos institucionais, mas também servirá como modelo para outras organizações que buscam enfrentar desafios semelhantes, contribuindo para o avanço da segurança da informação no ambiente educacional e na administração pública em geral.

3.13. CONSIDERAÇÕES FINAIS

A segurança da informação em instituições de ensino superior apresenta desafios constantes e complexos, envolvendo não apenas a adoção de recursos tecnológicos, mas também o fortalecimento de uma cultura organizacional que priorize a proteção de dados e a continuidade de serviços. Esse cenário requer uma perspectiva multidisciplinar, na qual aspectos técnicos, gerenciais, educacionais e comportamentais são tratados de forma integrada, com ênfase na conscientização e no comprometimento de toda a comunidade acadêmica.

No presente estudo, identificou-se que a Faculdade de Educação da Universidade de Brasília (FE/UnB) enfrenta lacunas significativas na adoção e compreensão da Política de Segurança da Informação e Comunicação (PoSIC). Em especial, constatou-se que a percepção de servidores técnico-administrativos e docentes acerca da relevância das medidas de segurança encontra-se aquém do desejável. Embora a FE/UnB possua algum conhecimento sobre a proteção de dados e o uso de recursos computacionais, a ausência de treinamentos abrangentes e de canais de comunicação estruturados resulta em uma propagação incipiente das boas práticas de segurança cibernética.

A proposta do Programa de Sensibilização em Segurança da Informação (PSSI) emerge, portanto, como uma estratégia de enfrentamento das vulnerabilidades identificadas, concebida para abranger os diferentes níveis da organização. Fundamentado no modelo Security Education, Training, and Awareness (SETA), o PSSI parte da premissa de que a segurança da informação exige mais do que habilidades técnicas isoladas: demanda a construção de um senso coletivo de responsabilidade e a promoção de atitudes voltadas à prevenção de riscos. Assim, o PSSI está

estruturado sobre três pilares centrais – sensibilização, treinamento e educação continuada – que permitem abordar gradualmente as carências levantadas durante o diagnóstico situacional da FE/UnB apresentado na primeira parte deste trabalho.

A ênfase na sensibilização revela-se fundamental para criar uma mudança de comportamento de longo prazo, pois muitos incidentes de segurança derivam de ações desatentas, falta de conhecimento ou até de subestimação das ameaças cibernéticas. É no estágio da sensibilização que se inicia o processo de aproximar o público-alvo dos conceitos básicos de segurança, das implicações legais e institucionais de uma violação e dos possíveis danos não apenas à instituição, mas também ao indivíduo e à sociedade em geral. Dessa forma, busca-se despertar o interesse e o senso de urgência necessários para gerar engajamento.

O treinamento aparece como o segundo pilar do PSSI, conferindo profundidade e aplicabilidade aos conhecimentos adquiridos na fase de sensibilização. A partir de metodologias que privilegiem a aprendizagem ativa e contextualizada – como oficinas, simulações de ataques de phishing, estudos de caso e debates orientados por especialistas – busca-se capacitar os participantes a identificar e responder a incidentes de segurança, bem como a utilizar ferramentas e procedimentos de proteção de dados de maneira mais proficiente. Além disso, essa etapa enfatiza a relação entre os riscos mapeados (por exemplo, vazamento de dados, sequestro de informações, acessos não autorizados) e as práticas recomendadas (uso de senhas fortes, criptografia, backup regular, entre outras).

Por fim, a educação continuada complementa o processo de capacitação ao evitar que o conhecimento adquirido se limite a ações pontuais ou esporádicas. O dinamismo do cenário cibernético, marcado pela evolução constante das ameaças e das tecnologias de defesa, demanda uma atualização permanente das equipes que lidam com dados institucionais. Nesse sentido, a proposta do PSSI contempla a oferta periódica de novos módulos de treinamento, a disponibilização de canais de comunicação para consulta de dúvidas e o estímulo à participação em grupos de discussão e eventos de segurança da informação. A educação continuada também facilita a incorporação de procedimentos de governança, possibilitando que a instituição se mantenha alinhada às melhores práticas e às normas nacionais e internacionais referentes à proteção de dados.

A implementação do PSSI, contudo, não se mostra isenta de desafios. Um dos entraves mais recorrentes em iniciativas dessa natureza é a resistência interna: diante de agendas sobrecarregadas, alguns servidores técnico-administrativos e docentes podem encarar os treinamentos como uma obrigação adicional, nem sempre valorizada frente a outras demandas cotidianas. Ademais, restrições orçamentárias frequentemente limitam a abrangência e a

qualidade das ações de conscientização, dificultando a aquisição de plataformas de *e-learning*, a contratação de profissionais especializados ou a oferta de incentivos para participação em atividades de segurança. Nesse sentido, a necessidade de envolvimento ativo da alta administração torna-se premente, pois lideranças comprometidas ampliam a legitimidade das ações e podem viabilizar recursos, prazos e articulações para a consolidação efetiva do programa.

Apesar de ainda não ter sido formalmente implantado na FE/UnB, o PSSI já impulsionou avanços concretos no debate sobre a segurança da informação na instituição, contribuindo para o reconhecimento de que a proteção dos ativos informacionais não se resume a uma questão técnica, mas envolve diretamente a cultura organizacional. O estímulo às capacitações periódicas, ainda que incipiente, reforça a compreensão de que o comportamento humano é determinante para a eficácia de qualquer política de segurança. À medida que o PSSI for adotado integralmente, é provável que se observem melhorias substanciais no mapeamento e na mitigação de riscos, bem como na percepção individual e coletiva acerca das normas estabelecidas pela PoSIC.

Além disso, a experiência adquirida ao longo da pesquisa demonstra que o PSSI tem potencial para se tornar uma referência em outros contextos acadêmicos e institucionais. A flexibilidade no planejamento das ações – que podem ser adaptadas a diferentes públicos e realidades orçamentárias – e a ênfase na abordagem multimodal (incluindo treinamentos presenciais, materiais interativos e campanhas informativas) sugerem que o programa pode ser adaptado e replicado com êxito. Em um mundo cada vez mais dependente de dados e sistemas digitais, a capacidade de difundir boas práticas de segurança configura um imperativo não apenas para as instituições de ensino, mas para todos os segmentos que lidam com informações sensíveis.

Nesse sentido, recomenda-se que estudos futuros aprofundem a investigação acerca da eficácia de distintos métodos de capacitação, especialmente em relação ao treinamento contínuo, buscando avaliar o impacto específico de cada abordagem (por exemplo, gamificação, aprendizagem baseada em problemas, debates virtuais) na adesão às políticas de segurança. Tal aprofundamento deve ser acompanhado de métricas claras e mecanismos de avaliação que permitam aferir a evolução das práticas de segurança, identificando lacunas residuais e oportunidades de aprimoramento.

Conclui-se que o desenvolvimento de uma cultura de segurança da informação sólida requer mais do que tecnologias de ponta e normas corporativas. É imperativo que as instituições invistam na formação de pessoas comprometidas e conscientes, aptas a compreender os riscos associados aos ambientes digitais e a agir de forma proativa para reduzi-los. Nesse contexto, o PSSI representa um passo significativo rumo à resiliência institucional, pois não apenas fortalece a proteção de dados, mas também estimula a construção de valores coletivos que promovem

responsabilidade, colaboração e confiabilidade no âmbito acadêmico. Espera-se que, ao consolidar esses aprendizados, a FE/UnB e demais instituições de ensino superior ampliem sua capacidade de inovação e mantenham seus ativos informacionais devidamente protegidos, assegurando a continuidade e a excelência de suas atividades de ensino, pesquisa e extensão.

3.14. DOCUMENTOS COMPROBATÓRIOS E EVIDENCIAS

Para a validação e comprovação do desenvolvimento PSSI, foram elaborados diversos materiais que fundamentam a proposta apresentada neste estudo. Entre esses documentos, destacam-se o questionário utilizado na pesquisa de campo, o cálculo do coeficiente Alfa de Cronbach, as análises estatísticas realizadas no software 'Stata', as transcrições das entrevistas semiestruturadas realizadas com os servidores técnico-administrativos e docentes da Faculdade de Educação da UnB, bem como o gráfico resultante da pesquisa de *survey*.

Os documentos estão disponibilizados nos **Apêndices A, B, C, D e E**, e no **Anexo** deste trabalho. O **Apêndice A** apresenta o modelo do questionário aplicado, incluindo as escalas de medida e as instruções fornecidas aos participantes. **O Apêndice B** contém o cálculo do coeficiente Alfa de Cronbach, demonstrando a consistência interna do instrumento de pesquisa e validando sua confiabilidade estatística. **O Apêndice C** inclui as análises estatísticas realizadas no software Stata, que fundamentam os resultados quantitativos obtidos na pesquisa, como testes de qui-quadrado e outras análises descritivas e inferenciais. **O Apêndice D** apresenta as transcrições das entrevistas realizadas com os participantes denominados Atena, Afrodite e Perséfone, preservando o anonimato e detalhando as percepções, experiências e sugestões dos entrevistados em relação à segurança da informação na instituição. **O Apêndice E** apresenta o relatório ilustrativo resultante de uma análise temática das três entrevistas semiestruturadas. O **Anexo** contém o gráfico resultante da pesquisa de survey, ilustrando visualmente os dados coletados e facilitando a compreensão das principais tendências e padrões identificados.

Esses documentos comprovam a aplicação prática dos métodos de pesquisa utilizados no estudo e embasam teoricamente a proposta do PSSI. A disponibilização detalhada dos instrumentos de coleta de dados, das análises estatísticas e das transcrições das entrevistas demonstra a rigorosidade metodológica empregada e a transparência no processo de investigação. Além disso, evidenciam o alinhamento da proposta com as necessidades identificadas na instituição, reforçando a pertinência e a viabilidade da implementação do programa na Faculdade de Educação. A documentação detalhada também oferece subsídios para futuras pesquisas e intervenções, permitindo que outras instituições possam se beneficiar dos achados e metodologias aqui apresentados.

REFERÊNCIAS

ANDREASSON, Kim. **Cybersecurity: Public Sector Threats and Responses**. Boca Raton: CRC Press, 2012.

ASLAN, Ömer; AKTUĞ, Semih Serkant; OZKAN-OKAY, Merve; YILMAZ, Abdullah Asim; AKIN, Erdal. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. **Electronics**, v. 12, n. 1333, 2023. Disponível em: https://doi.org/10.3390/electronics12061333. Acesso em: 4 jul. 2024.

ALYAMI, Areej; SAMMON, David; NEVILLE, Karen; MAHONY, Carolanne. The critical success factors for Security Education, Training and Awareness (SETA) program effectiveness: a lifecycle model. **Information Technology & People**, v. 36, n. 8, p. 94-125, 2023. Disponível em: https://doi.org/10.1108/ITP-07-2022-0515. Acesso em: 18 jun. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 17799: **Técnicas de segurança e código de práticas para a gestão de segurança da informação**. Rio de janeiro, 2005.

BISHOP, Phillip A.; HERRON, Robert L. Use and misuse of the Likert item responses and other ordinal measures. **International Journal of Exercise Science**, v. 8, n. 3, p. 297-302, 2015. Disponível em: https://www.researchgate.net/publication/279854107_Use_and_Misuse_of_the_Likert_Item_Responses_and_Other_Ordinal_Measures. Acesso em: 4 jul. 2024.

BORGES, Lívia Freitas Fonseca; VILLAR, José Luiz; WELLER, Wivian. **FE 50 anos: 1966-2016: memória e registros da história da Faculdade de Educação da Universidade de Brasília. Brasília**: Editora Universidade de Brasília, 2018. Disponível em: https://livros.unb.br/index.php/portal/catalog/view/104/280/981. Acesso em: 1 fev. 2024.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação. **Diário Oficial da União**: seção 1, Brasília, DF, 27 dez. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm. Acesso em: 12 fev. 2024.

BRASIL. CENTRO GLOBAL DE CAPACIDADE DE SEGURANÇA CIBERNÉTICA. **Revisão das capacidades de segurança cibernética do Brasil 2023**. Brasília: GCSCC, 2023. Disponível em: https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/cmm-report-brazil-2023_final_pt.pdf/@@download/file. Acesso em: 21 out. 2024.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO (TCU). TCU identifica riscos de segurança da informação em organizações públicas federais. **Notícias**, 13 out. 2021. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-identifica-riscos-de-seguranca-da-informacao-em-organizacoes-publicas-federais.htm. Acesso em: 08 ago. 2024.

BRASIL. Lei Nº 13.709, de 14 de agosto de 2018a. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 11 fev. 2024.

BRASIL. Lei Nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. **Diário Oficial da União**: seção 1, Brasília, DF, 9 jul. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 14 fev. 2024.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Secretaria de Gestão de Pessoas e Relações do Trabalho no Serviço Público. **Instrução Normativa n° 001, de 19 de janeiro de 2016**. Dispõe sobre capacitação e desenvolvimento de servidores. Disponível em: https://dgp.unb.br/images/Documentos/CGP/resolucoes/atos-resolucoes-atualizadas/Instruo_Normativa_sobre_Capacitao_n_001-2016.pdf. Acesso em: 25 set. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Estratégia Nacional de Segurança Cibernética** – E-Ciber. Brasília: 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 04 jul. 2024.

BRASIL. Universidade de Brasília. **Resolução da Reitoria n.º 0013/2017**. Fundação Universidade de Brasília, 2017. Disponível em: https://atom.unb.br/uploads/r/fundacao-universidade-de-brasilia/3/f/9/3f9e443fd77a987ea5198ae8f17d5238418ca5aecb728efad76b714ef7fe946b/Resolucao_da_Reitoria_0013_2017.pdf. Acesso em: 1 jul. 2024.

BRASIL. Universidade de Brasília. **Instrução Normativa nº 0001/2021**. Secretaria de Tecnologia da Informação. Brasília, DF, 2021. Disponível em: https://sti.unb.br/images/Artigos/DocumentosSTI/IN_0001_2021_STI_UnB.pdf. Acesso em: 29 abr. 2024.

BRASIL. Universidade de Brasília. **Instrução Normativa nº 0002**. Secretaria de Tecnologia da Informação. Brasília, DF, 2021. Disponível em: https://sti.unb.br/images/Artigos/DocumentosSTI/Instruo_Normativa_0002.pdf. Acesso em: 27 fev. 2024.

BRASIL. Universidade de Brasília. **Plano de Desenvolvimento Institucional 2023-2028**. Brasília, DF, [data de publicação]. Disponível em: https://planejamento.unb.br/images/Central_de_Conte%C3%BAdos/PDI_UnB__2023_2028.pdf. Acesso em: 20 fev. 2024.

BRASIL. Universidade de Brasília. **Plano de Política Pedagógica Institucional**. Brasília, DF, abr. 2018c. Disponível em: https://dpo.unb.br/images/PPPIVersaoAprovadaConsuni.pdf. Acesso em: 02 abr. 2024.

BRASIL. Universidade de Brasília. **Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2023a-2028**. Brasília: UnB, 2023a. Disponível em: https://sti.unb.br/pla-pdtic. Acesso em: 31 maio 2024.

BRASIL. Universidade de Brasília. **Resolução da Câmara de Planejamento e Administração nº 004/2018**a. Disponível em: https://sti.unb.br/images/Artigos/DocumentosSTI/Resolucao_n__004_2018_PoSIC_UnB_1.pdf. Acesso em: 10 fev. 2024.

BRASIL. Universidade de Brasília. **Resolução nº 003/2018**b. Plano de Governança de Tecnologia da Informação e Comunicação (PGTIC). Brasília, DF, 2018d. Disponível em: https://sti.unb.br/images/Artigos/DocumentosSTI/Resolucao_n__003_2018_PGTIC_UnB_1.pdf . Acesso em: 27 fev. 2024.

BRASIL. Universidade de Brasília. **Guia - PDP UnB 2023**b. Decanato de Gestão de Pessoas – DGP, Diretoria de Capacitação, Desenvolvimento e Educação – Dcade, Coordenadoria de Capacitação – Procap. Disponível em: https://www.capacitacao.unb.br/images/Guia%20-%20PDP%20UnB%202023.pdf. Acesso em: 20 jun. 2024.

BRASIL. CONSELHO NACIONAL DE SAÚDE (Brasil). Comissão Nacional de Ética em Pesquisa. **Ofício Circular nº 2/2021/CONEP/SECNS/MS, de 24 de fevereiro de 2021**. Orientações para procedimentos em pesquisas com qualquer etapa em ambiente virtual. Disponível em: http://sei.saude.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&codigo_verificador=0019229910&codigo_CRC=607D08F0. Acesso em: 2 jun. 2024.

BRASIL. CONSELHO NACIONAL DE SAÚDE. **Resolução nº 466, de 12 de dezembro de 2012**. Aprova as diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos. Diário Oficial da República Federativa do Brasil, Brasília, DF, 13 jun. 2013. Disponível em: http://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf. Acesso em: 2 jun. 2024.

BRASIL. CONSELHO NACIONAL DE SAÚDE. **Resolução nº 510, de 07 de abril de 2016**. Dispõe sobre as normas aplicáveis a pesquisas em Ciências Humanas e Sociais. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 24 maio 2016. Disponível em: http://conselho.saude.gov.br/resolucoes/2016/Reso510.pdf. Acesso em: 2 jun. 2024.

BRAUN, Virginia; CLARKE, Victoria. Using thematic analysis in psychology. **Qualitative Research in Psychology**, v. 3, n. 2, p. 77-101, 2006. Disponível em: https://doi.org/10.1191/1478088706qp063oa. Acesso em: 10 mar. 2024.

BRITTO, Thiago Dalpoz e. **Maturidade da Segurança da Informação nas Instituições Públicas Brasileiras**. 2011. 160 f. Tese (Mestrado em Ciência da Informação) – Universidade Católica de Brasília, Brasília, 2011. Disponível em: https://bdtd.ucb.br:8443/jspui/handle/123456789/1331. Acesso em: 5 jul. 2024.

CHAI, Kar Yee; ZOLKIPLI, Mohamad Fadli. Review on confidentiality, integrity and availability in information security. **Journal of ICT in Education**, v. 8, n. 2, p. 34-42, 2021. Disponível em: https://doi.org/10.37134/jictie.vol8.2.4.2021. Acesso em: 29 jun. 2024.

CHEW, Tan Soon. Considerations for Developing Cybersecurity Awareness Training. **ISACA Journal**, [S.l.], v. 2, 2023. Disponível em: https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training. Acesso em: 25 fev. 2024.

CHENG, Lijiao; LI, Ying; LI, Wenli; HOLM, Eric; ZHAI, Qingguo. Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. **Computers & Security,** v. 39, p. 447-459, 2013. Disponível em: https://doi.org/10.1016/j.cose.2013.09.009. Acesso em: 14 jul. 2024.

CHENG, Eric; WANG, Tianchong. Institutional strategies for cybersecurity in higher education institutions. **Information**, v. 13, n. 192, 2022. Disponível em: https://doi.org/10.3390/info13040192. Acesso em: 23 abr. 2024.

CORDEIRO, Evandro Souza de Paula. **Fatores Críticos de Sucesso para o Aprimoramento da Maturidade da Gestão da Segurança da Informação das Instituições Federais de Ensino Superior**. 2017. 145 f. Dissertação (Mestrado em Gestão Pública) – Universidade Federal de Pernambuco, Recife, 2017. Disponível em: https://repositorio.ufpe.br/handle/123456789/24043. Acesso em: 5 jul. 2024.

CORTINA, Jose. What is Coefficient Alpha? An Examination of Theory and Applications. **Journal of Applied Psychology**, v. 78, n. 1, p. 98-104, 1993. Disponível em: https://doi.org/10.1037/0021-9010.78.1.98. Acesso em: 20 set. 2024.

CRESWELL, John. **Research Design: Qualitative, Quantitative, and Mixed Methods Approaches**. 3. ed. Thousand Oaks: SAGE Publications, 2009. Disponível em: https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf. Acesso em: 4 jun. 2024.

DAVE, Daksh; SAWHNEY, Gauransh; AGGARWAL, Pushkar; SILSWAL, Nitish; KHUT, Dhruv. The New Frontier of Cybersecurity: Emerging Threats and Innovations. **Pilani: BITS** Pilani, 2023. Disponível em: https://arxiv.org/pdf/2311.02630v1.pdf. Acesso em: 4 jul. 2024.

DE CASANOVE, Olivier; LELEU, Nicolas; SÈDES, Florence. Applying PDCA to Security, Education, Training and Awareness Programs. In: CLARKE, Nathan; FURNELL, Steven (eds.). Human Aspects of Information Security and Assurance. HAISA 2022. **IFIP Advances in Information and Communication Technology**, v. 658. Springer, Cham, 2022. Disponível em: https://doi.org/10.1007/978-3-031-12172-2_4. Acesso em: 8 jul. 2024.

DEMING, W. Edwards. **Out of the crisis**. Reedição. Cambridge, Massachusetts: MIT Press, 2018. Foreword de Kevin Edwards Cahill e Kelly L. Allan. 448 p. ISBN 9780262535946.

DENNING, Dorothy E. Stuxnet: What Has Changed?. **Future Internet**, v. 4, n. 3, p. 672-687, 2012. Disponível em: https://www.mdpi.com/1999-5903/4/3/672. Acesso em: 5 jul. 2024.

FÁVERO, Luiz Paulo; BELFIORE, Patrícia. **Manual de Análise de Dados – Estatística e Machine Learning com Excel®, SPSS®, Stata®, R® e Python®.** 2. ed. São Paulo: GEN, 2024.

FORTINET. FortiGuard Labs revela aumento de ciberataques no Brasil em 2021. **Comunicado à Imprensa**. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021. Acesso em: 14 jul. 2024.

FOXX, Chris. NHS cyber-attack: GPs and hospitals hit by ransomware. **BBC News**, 13 maio 2017. Disponível em: https://www.bbc.com/news/health-39899646. Acesso em: 5 jul. 2024.

FOWLER, Floyd. **Survey Research Methods.** 5. ed. Thousand Oaks: Sage Publications, 2014.

G1 MS. Polícia Federal deflagra operação contra-ataques cibernéticos a universidades federais em MS. **Portal de notícias G1**. Disponível em: https://g1.globo.com/ms/mato-grosso-do-sul/noticia/2022/04/28/policia-federal-deflagra-operacao-contra-ataques-ciberneticos-a-universidades-federais-em-ms.ghtml. Acesso em: 14 jul. 2024.

GIL, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social**. 6. ed. São Paulo: Atlas, 2008.

GUIMARÃES, Rogério. **Modelo de Governança de Segurança da Informação para a Administração Pública Federal.** 2016. 107 f. Dissertação (Mestrado em Gestão do Conhecimento e Tecnologia da Informação) – Universidade Católica de Brasília, Brasília, 2016. Disponível em: https://bdtd.ucb.br:8443/jspui/handle/tede/2000. Acesso em: 5 jul. 2024.

GUIMARÃES, Rogério; SOUZA NETO, João; LYRA, Maurício Rocha. Modelo de governança de segurança da informação para a administração pública federal. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 8, n. 3, p. 90-109, set./dez. 2018. Disponível em: https://periodicos.ufpb.br/index.php/pgc/article/view/34717 Acesso em: 14 out. 2024.

GHONAIMY, M. Adeeb; EL-HADIDI, Mahmoud T.; ASLAN, Heba K. (Eds.). **Security in the information society: visions and perspectives**. Boston: Kluwer Academic Publishers, 2002. Disponível em: https://link.springer.com/book/10.1007/978-0-387-35586-3. Acesso em: 15 fev. 2024.

HAYES, J. **The Theory and Practice of Change Management.** 4th ed. Palgrave Macmillan, 2014.

LASCOUMES, Pierre; LE GALÈS, Patrick. Introduction: understanding public policy through its instruments. **Governance**, v. 20, n. 1, p. 1-21, 2007. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-0491.2007.00342.x. Acesso em: 1 fev. 2024.

LASCOUMES, Pierre; SIMARD, Louis. L'action publique au prisme de ses instruments: introduction. **Revue Française de Science Politique**, v. 61, n. 1, p. 5-22, 2011. Disponível em: https://www.cairn.info/revue-francaise-de-science-politique-2011-1-page-5.htm. Acesso em: 1 mar. 2024.

LIKERT, Rensis. A technique for the measurement of attitudes. **Archives of Psychology**, v. 140, p. 1-55, 1932. Disponível em: https://legacy.voteview.com/pdf/Likert_1932.pdf. Acesso em: 08 jun. 2024.

LOUZADA, Iraciara Faria; LEAL, Johender Nascimento de Paula; SILVA, Willian Pereira da; RODRIGUES, Hugo Leonardo. A utilização do compliance como ferramenta da governança corporativa. **Cosmos Acadêmico**, v. 5, n. 1, p. 73-89, 2020.

KUNER, Christopher (ed.); BYGRAVE, Lee A. (ed.); DOCKSEY, Christopher (ed.); DRECHSLER, Laura (ed.). **The EU General Data Protection Regulation (GDPR): A Commentary**. New York: Oxford Academic, 2020. Edição online. Disponível em: https://doi.org/10.1093/oso/9780198826491.001.0001. Acesso em: 27 set. 2024.

MITNICK, Kevin David; SIMON, William L. **The Art of Deception: Controlling the Human Element of Security**. Prefácio de Steve Wozniak. Hoboken: John Wiley & Sons, 2011.

MARCIANO, João Luiz Pereira. **Segurança da Informação: uma abordagem social**. 2006. Tese (Doutorado em Ciência da Informação) – Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2006. Disponível em: http://www.realp.unb.br/jspui/bitstream/10482/1943/1/Jo%C3%A3o%20Luiz%20Pereira%20Marciano.pdf. Acesso em: 3 out. 2024., Brasília, 2006.

MASCARENHAS, Pedro Tenorio; ARAUJO, Wagner Junqueira de. **Segurança da Informação: uma visão sistêmica para implantação em organizações.** 1. ed. João Pessoa: Editora UFPB, 2019. Disponível em: https://www.editora.ufpb.br/sistema/press5/index.php/UFPB/catalog/view/209/75/905. Acesso em: 3 out. 2024.

MALWAREBYTES. Annual Threat Report. **Press Release**s, 2023a. Disponível em: https://www.malwarebytes.com/press/category/press-releases. Acesso em: 14 jul. 2024.

MALWAREBYTES. THREAT INTELLIGENCE TEAM. The 2023b State of Ransomware in Education. **Press Releases**, 2023. Disponível em: https://www.malwarebytes.com/press/2023/09/12/research-reveals-education-organizations-faced-a-daunting-84-increase-in-ransomware-attacks-over-the-past-six-months. Acesso em: 14 jul. 2024.

MEIRELLES, Fernando S.; FUNDAÇÃO GETULIO VARGAS (FGV). Panorama do uso de TI no Brasil em 2022. **Portal FGV**. Disponível em: https://portal.fgv.br/artigos/panorama-uso-ti-brasil-2022. Acesso em: 14 jul. 2024.

MOLENDA, Michael. In search of the elusive ADDIE model. **Performance Improvement**, v. 42, n. 5, p. 34-36, 2003. Disponível em: https://doi.org/10.1002/pfi.4930420508. Acesso em: 3 out. 2024.

NETO, Nelson Novaes; MADNICK, Stuart; DE PAULA, Anchises Moraes G.; BORGES, Natasha Malara. Developing a Global Data Breach Database and the Challenges Encountered. **Journal of Data and Information Quality,** v. 13, n. 1, artigo 3, p. 1-33, jan. 2021. Disponível em: https://doi.org/10.1145/3439873. Acesso em: 14 jul. 2024.

NILSEN, Richard K.; LEVY, Yair; TERRELL, Steven R.; BEYER, Dawn. A Developmental Study on Assessing the Cybersecurity Competency of Organizational Information System Users. **Journal of Cybersecurity Education, Research and Practice**, v. 2017, n. 2, Art. 2, dez. 2017. Disponível em: https://digitalcommons.kennesaw.edu/jcerp/vol2017/iss2/2. Acesso em: 18 jun. 2024.

NUNES, Israel Aono; ASSUNÇÃO, Juliana Zaniboni de; BRUSTOLIN, Vitelio. Análise estrutural das estratégias de segurança cibernética do Brasil e dos Estados Unidos. **Revista Brasileira de Estudos de Defesa**, v. 9, n. 2, p. 227-250, jul./dez. 2022. Disponível em: https://doi.org/10.26792/RBED.v9n2.2022.75246. Acesso em: 4 jul. 2024.

NYE, Joseph S. **Cyber Power**. Cambridge: Harvard Kennedy School, 2010. Disponível em: https://www.belfercenter.org/publication/cyber-power. Acesso em: 28 fev. 2024.

ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO. NBR ISO/IEC 27001: **Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos**. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/25074/nbriso-iec27001-seguranca-da-informacao-seguranca-cibernetica-e-protecao-a-privacidade-sistemas-de-gestao-da-seguranca-da-informacao-requisitos. Acesso em: 02 abr. 2024.

ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO. NBR ISO/IEC 27002: **Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação**. Disponível em: https://www.normas.com.br/visualizar/abnt-nbr-nm/21529/nbriso-iec27002-seguranca-da-informacao-seguranca-cibernetica-e-protecao-a-privacidade-controles-de-seguranca-da-informacao. Acesso em: 02 abr. 2024.

PELTIER, Thomas R. **Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management**. Boca Raton: CRC Press, 2016.

PERWEJ, Yusuf; ABBAS, Syed Qamar; DIXIT, Jai Pratap; AKHTAR, Nikhat; JAISWAL, Anurag Kumar. A Systematic Literature Review on the Cyber Security. **International Journal of Scientific Research and Management**, v. 9, n. 12, p. 669-710, 2021. DOI: 10.18535/ijsrm/v9i12.ec04. Disponível em: https://hal.science/hal-03509116. Acesso em: 5 jul. 2024.

PERERA, Srinath; JIN, Xiaohua; MAURUSHAT, Alana; OPOKU, De-Graft Joe. Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. **Informatics**, v. 9, n. 1, p. 28, 2022. Disponível em: https://doi.org/10.3390/informatics9010028. Acesso em: 1 jul. 2024.

PwC Brasil. 26ª CEO Survey: **Transformando o futuro, encarando o presente**. São Paulo: PwC Brasil, 2023. Disponível em: http://www.pwc.com.br/pesquisa-de-ceo. Acesso em: 23 out. 2024.

QUERO VIRLA, Milton. Confiabilidad y coeficiente Alpha de Cronbach. **Telos, Maracaibo**, v. 12, n. 2, p. 248-252, maio/ago. 2010. Disponível em: https://www.redalyc.org/pdf/993/99315569010.pdf. Acesso em: 20 set. 2024.

ROOT, Enoch. Evolution of security: the story of the ILOVEYOU worm. **Kaspersky Daily**, 2022. Disponível em: https://www.kaspersky.com/blog/cybersecurity-history-iloveyou/45001/. Acesso em: 4 jul. 2024.

SAMPIERI, Roberto H.; COLLADO, Carlos F.; LUCIO, María D. P B. **Metodologia de pesquisa**. Porto Alegre/RS: Grupo A, 2013. E-book. ISBN 9788565848367. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788565848367/. Acesso em: 20 mar. 2024.

SCHNEIER, Bruce. **Secrets and Lies: Digital Security in a Networked World**. Edição ilustrada. John Wiley & Sons, 2015.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Campus, 2003.

SIKOLIA, David; BIROS, David; ZHANG, Tianjian. How Effective Are SETA Programs Anyway: Learning and Forgetting in Security Awareness Training. **Journal of Cybersecurity Education, Research and Practice**, 2023. Disponível em: https://eric.ed.gov/?id=EJ1396066. Acesso em: 6 jun. 2024.

SILVEIRA, Jonas Rafael; LUNARDI, Guilherme Lerch; CERQUEIRA, Lucas Santos. Relação entre cultura e segurança da informação: como evitar falhas decorrentes do "jeitinho brasileiro"? REAd – **Revista Eletrônica de Administração**, v. 26, n. 3, p. 341-366, 2020. Disponível em: https://www.scielo.br/j/read/a/mXzJBPHSXLkxTFPBVGMhkqs/?format=pdf&lang=pt. Acesso em: 3 out. 2024.

SOOMRO, Zahoor Ahmed; SHAH, Mahmood Hussain; AHMED, Javed. Information security management needs more holistic approach: A literature review. **International Journal of Information Management**, v. 36, n. 2, p. 215-225, 2016. DOI: 10.1016/j.ijinfomgt.2015.11.009.

SOLMS, B. Van. **Information Security Governance: A Practical Development and Implementation Approach**. Wiley, 2016.

SOLOVE, Daniel J.; SCHWARTZ, Paul M. **Information Privacy Law**. New York: Wolters Kluwer, 2018.

SONICWALL CAPTURE LABS THREAT RESEARCH TEAM. 2024 **SonicWall Cyber Threat Report**. 2024. Disponível em: https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2024-cyber-threat-report.pdf. Acesso em: 14 jul. 2024.

SRINIVASAN, Suraj; PAINE, Lynn S.; GOYAL, Neeraj. **Cyber Breach at Target**. *Harvard Business School, General Management*, n. 117027-PDF-ENG, 32 p., 07 jul. 2016. Disponível em: https://hbsp.harvard.edu/product/117027-PDF-ENG. Acesso em: 5 jul. 2024.

SUBRAMANIAN, Sudeep; AGRAWAL, Udita. Nudging Our Way to Successful Information Security Awareness. **ISACA Journal**, [S.l.], n. 1, fev. 2021. Disponível em: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-1/nudging-our-way-to-successful-information-security-awareness. Acesso em: 25 fev. 2024.

TANG, Mincong; LI, Meng'gang; ZHANG, Tao. The impacts of organizational culture on information security culture: a case study. **Information Technology Management**, [S.l.], v. 17, p. 179-186, 2016. Publicado online em 18 nov. 2015. Springer Science Business Media New York, 2015. Disponível em: https://link.springer.com/article/10.1007/s10799-015-0252-2. Acesso em: 15 fev. 2024.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). Guia de Avaliação de Governança de TI. **Portal TCU**, 2023. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-publica-guia-de-avaliacao-de-governanca-de-ti-em-parceria-com-a-comunidade-internacional.htm. Acesso em: 5 jul. 2024.

TIPTON, Harold F.; KRAUSE, Micki. **Information Security Management Handbook**. 6. ed. Boca Raton: CRC Press, 2007.

TRIGOS, Maria Luciana; NUNO, Claudinei Di. O impacto de ações de sensibilização na segurança da informação. **Revista Científica Multidisciplinar Núcleo do Conhecimento**, v. 03, n. 10, p. 46-72, out. 2021. ISSN: 2448-0959. Disponível em: https://www.nucleodoconhecimento.com.br/administracao/acoes-de-conscientizacao. Acesso em: 29 fev. 2024.

ULVEN, Joachim Bjørge; WANGEN, Gaute. A systematic review of cybersecurity risks in higher education. **Future Internet**, v. 13, n. 2, p. 39, 2021. Disponível em: https://doi.org/10.3390/fi13020039. Acesso em: 29 jun. 2024.

VERONESE, Alexandre; MOTA, Júlia Gomes; LANNES, Yuri da Costa. Regulação do ciberespaço: possibilidades administrativas e judiciais com foco em aplicações de Internet. In: PINHO, Anna (org.). **Manual de Direito na Era Digital: Administrativo**. 1. ed. São Paulo: Editora Foco, 2023. p. 1-47. Disponível em: https://www.researchgate.net/publication/365051466. Acesso em: 3 out. 2024.

VIEIRA, Patrícia dos Santos; DIAS, Murillo de Oliveira. A cultura da segurança informacional na Petrobras. **International Journal of Development Research**, v. 12, n. 02, p. 53881-53886, 2022. Disponível em: http://www.journalijdr.com. Acesso em: 30 jun. 2024. DOI: 10.37118/ijdr.23992.02.2022.

WEILL, Peter; ROSS, Jeanne W. **IT Governance: How Top Performers Manage IT Decision Rights for Superior Results**. Boston: Harvard Business School Press, 2004.

WHITMAN, Michael E.; MATTORD, Herbert J. **Management of Information Security**. 6. ed. [S.l.]: Cengage Learning, 2018. ISBN 978-1337405713.

ZHENG, Binglong; TSE, Daniel; MA, Jiajing; LANG, Xuanyi; LU, Yinli. An Empirical Study of SETA Program Sustaining Educational Sector's Information Security vs. Information Systems Misuse. **Sustainability**, v. 15, p. 12669, 2023. Disponível em: https://doi.org/10.3390/su151712669. Acesso em: 26 fev. 2024.

APÊNDICES A – QUESTIONÁRIO

Prezado(a) Senhor(a),

Convidamos você a participar de uma investigação sobre a Política de Segurança da Informação e Comunicação da Universidade de Brasília (POSIC/UnB). Sua contribuição será fundamental para enriquecer nosso entendimento sobre o grau de conhecimento e a conscientização acerca das práticas de segurança da informação no âmbito da Faculdade de Educação.

Este questionário é objetivo e não demandará mais do que alguns minutos para ser preenchido. Estas informações são importantes para o contínuo desenvolvimento e refinamento das nossas estratégias de segurança da informação e comunição.

Anonimato e confidencialidade: suas respostas serão anônimas e tratadas com confidencialidade.

Declaro que fui adequadamente informado(a) sobre os objetivos e procedimentos desta pesquisa, compreendi todas as informações e estou ciente de que posso desistir a qualquer momento sem qualquer penalização. Ao prosseguir com o preenchimento do questionário, consinto voluntariamente em participar desta pesquisa e autorizo o uso dos meus dados conforme descrito.

Antecipadamente agradecemos pela sua disposição em contribuir com este relevante estudo.

Este estudo é parte integrante do Programa de Pós-Graduação em Governança e Inovação em Políticas Públicas, no âmbito do Mestrado Profissional.

Orientação: Alexandre Kehrig Veronese Aguiar Coorientação: Ludmila de Melo Souza.

Seção A: Perfil

A1.

Por favor, preencha com os seus dados:
(você não será identificado. Suas respostas serão anônimas e tratadas com confidencialidade).

Insira os três primeiros dígitos do seu CPF: ☐☐☐☐☐☐☐☐☐☐☐

A2.

Por favor, preencha com os seus dados:
(você não será identificado. Suas respostas serão anônimas e tratadas com confidencialidade).

Em qual setor você está alocado? ☐☐☐☐☐☐☐☐☐☐☐

A3. Qual o seu perfil institucional?

Servidor técnico-administrativo ☐

Servidor docente ☐

A4. Você ocupa função temporária ou função de confiança, como chefia ou cargos de direção?

Sim ☐

Não ☐

A5. Qual a sua faixa etária?

- ☐ 18-24 anos
- ☐ 25-34 anos
- ☐ 35-44 anos
- ☐ 45-54 anos
- ☐ 55-64 anos
- ☐ 65+ anos

A6. Qual o seu gênero?

- ☐ Feminino
- ☐ Masculino
- ☐ Outros

Outros

A7. Qual o seu tempo de atuação na UnB?

- ☐ 0-3 Anos
- ☐ 3-10 Anos
- ☐ 11-20 Anos
- ☐ 21+ Anos

Seção B: Política de Segurança na Faculdade de Educação

Atenção

Antes de avançarmos às questões subsequentes, cabe enfatizar a garantia de anonimato e a confidencialidade absoluta com que serão tratadas as suas respostas.

Observações derivadas de avaliações prévias sugerem que certas respostas podem não ter espelhado adequadamente a realidade, talvez por uma reticência em reconhecer lacunas de conhecimento acerca de especificidades normativas. Assim, a integridade nas respostas se faz não apenas desejável, mas crucial, para a efetiva consecução dos propósitos desta pesquisa. Reafirmamos que nada neste formulário possui o potencial de expor ou prejudicar os participantes envolvidos.

A progressão de cada resposta induzirá a formulação de uma nova questão, destinada a validar a precedente, mitigando possíveis ambiguidades. Reiteramos, portanto, a importância de respostas verídicas para a otimização e sucesso deste procedimento.

Contamos com sua contribuição.

B1. Eu estou ciente da existência da resolução Nº 004 de 2018, que institui a Política de Segurança da Informação e Comunicação da UnB (PoSIC/UnB)?

- [ ] Sim
- [ ] Não

B2. Por quais veículos de comunicação você foi informado sobre a Política de Segurança da Informação e Comunicação da UnB?

- [ ] e-mail
- [ ] Boletim, Sistema Eletrônico de Informações (SEI)
- [ ] Colega ou gestor
- [ ] Não fui informado institucionalmente
- [ ] Outros

Outros

B3. Eu já fiz a leitura da PoSIC/UnB?

- [ ] Sim
- [ ] Não

B4. **Você marcou sim para "Eu já fiz a leitura PoSIC/UnB), por favor, selecione a opção a seguir:**

- ☐ Sim, li completamente
- ☐ Sim, mas apenas parcialmente
- ☐ Não, ainda não li.

B5. **Você aplica as instruções (diretrizes) da política de segurança da informação e comunicação no seu trabalho diário?**

- ☐ Frequentemente
- ☐ Às vezes
- ☐ Nunca

B6. **Na última questão, você selecionou que "frequentemente" aplica a política. Por favor, descreva (brevemente) alguma situação em que você aplicou alguma das diretrizes da PoSIC/UnB?**

B7. **Você indicou que "às vezes" segue as instruções da política. Poderia explicar o que o levou a aplicar essas diretrizes em casos específicos? Quais fatores tornaram necessária a aplicação da política nessas situações?**

B8. **A responsabilidade de fiscalizar o cumprimento da PoSIC/UnB cabe à STI (anteriormente conhecida como CPD). O seu setor já foi submetido a alguma auditoria ou a qualquer tipo de fiscalização relacionada ao cumprimento dessa política?**

- ☐ Sim
- ☐ Não
- ☐ Não sei responder

B9. **Você recebe alguma informação sobre o conteúdo da política de segurança da informação e comunicação da UnB?**

- ☐ Sim
- ☐ Não

B10. **Por quais veículos de comunicação você recebe informações sobre o conteúdo da Política de Segurança da Informação da UnB?**

- [ ] e-mail
- [ ] Boletim, Sistema Eletrônico de Informações (SEI)
- [ ] Colega ou gestor
- [ ] Não fui informado institucionalmente
- [ ] Outros

Outros

B11. **Eu recebi capacitação específica relacionado à política de segurança da informação e comunicação da UnB?**

- [ ] Sim
- [ ] Não

B12. **Quem (pessoa ou instituição) ministrou a capacitação sobre a política de segurança da informação e comunicação da UnB, em que ano e em qual local você participou?**

B13. **Eu já sofri algum incidente de segurança digital, como vazamento de senhas, golpes online, invasões de privacidade, recebimento de e-mails suspeitos, clonagem de cartão de crédito, invasão de redes sociais, golpes por mensagens de texto, ataques de phishing, instalação de software malicioso, ligações de fraudadores ou acesso não autorizado a algum dos meus dispositivos?**

- [ ] Sim
- [ ] Não
- [ ] Não sei responder

B14. **Quais meios de conscientização você prefere para futuras ações relacionadas à política de segurança da informação e comunicação da UnB? (Você pode assinalar várias opções).**

- [ ] Palestras, workshops, minicursos
- [ ] Postagens educativas em redes sociais
- [ ] Webinars (seminário online em vídeo, gravado ou ao vivo)

e-mails com dicas de segurança ☐

Cartilhas ou folhetos ☐

Outros ☐

Outros

B15. Você tem acesso aos meios de comunicação institucional?

Sim ☐

Não ☐

Seção C: Sugestões

C1. Por favor, compartilhe quaisquer sugestões ou comentários que você tenha sobre como podemos melhorar a segurança da informação na UnB:

Agradecemos por sua contribuição.

APÊNDICES B – CÁLCULO DO COEFICIENTE ALFA DE CRONBACH

Para avaliar a consistência interna do questionário utilizado neste estudo, foi calculado o coeficiente Alfa de Cronbach, uma medida amplamente aplicada em pesquisas sociais para verificar a confiabilidade de instrumentos de coleta de dados. O cálculo foi realizado para cinco itens do questionário, que medem o nível de conhecimento e adesão à Política de Segurança da Informação e Comunicação (PoSIC) da Universidade de Brasília (UnB).

Os itens analisados foram:

- Conhecimento_PoSIC: o participante está ciente da existência da PoSIC.
- Leitura_PoSIC: o participante já fez a leitura da PoSIC.
- Aplicacão_PoSIC: o participante aplica as diretrizes da PoSIC em seu trabalho diário.
- Capacitação: o participante recebeu capacitação específica sobre a PoSIC.
- Incidente Segurança: o participante já sofreu algum incidente de segurança digital.

Procedimento de Cálculo no SPSS

O coeficiente Alfa de Cronbach foi calculado no software SPSS, utilizando os dados de 10 participantes. A seguir, o script utilizado para o cálculo:

```spss
* Importar os dados.
DATA LIST FREE / Conhecimento_PoSIC Leitura_PoSIC Aplicacao_PoSIC Capacitacao
Incidente_Seguranca.
BEGIN DATA
1 1 2 1 1
0 0 1 0 0
1 1 3 1 1
1 1 2 1 1
0 0 0 0 0
1 1 3 1 1
0 0 1 0 1
0 1 1 0 0
1 0 3 1 1
1 1 2 1 1
END DATA.

* Definir os rótulos das variáveis.
VARIABLE LABELS Conhecimento_PoSIC 'Conhecimento sobre a PoSIC'
        Leitura_PoSIC 'Leitura da PoSIC'
        Aplicacao_PoSIC 'Aplicação da PoSIC'
        Capacitacao 'Recebimento de capacitação'
        Incidente_Seguranca 'Sofreu incidente de segurança'.

* Calcular o coeficiente Alfa de Cronbach.
RELIABILITY /VARIABLES=Conhecimento_PoSIC Leitura_PoSIC Aplicacao_PoSIC Capacitacao
```

```
Incidente_Seguranca
  /SCALE('Confiabilidade') ALL
  /MODEL=ALPHA.
```

Resultados do Cálculo do Alfa de Cronbach

A tabela abaixo apresenta as estatísticas de confiabilidade obtidas no SPSS:

Estatísticas de Confiabilidade	Valor
Cronbach's Alpha	0,893
Número de Itens	5

O valor obtido para o coeficiente Alfa de Cronbach foi de 0,893, o que indica uma excelente consistência interna entre os itens do questionário. De acordo com a literatura, um Alfa de Cronbach acima de 0,8 é considerado como um indicador de boa confiabilidade, enquanto valores acima de 0,9 indicam excelente confiabilidade (CORTINA, 2013). Portanto, os resultados indicam que o questionário possui uma alta confiabilidade para medir o nível de conhecimento e adesão à PoSIC.

Estatísticas dos Itens

A tabela abaixo apresenta a média e o desvio padrão de cada item:

Item	Média	Desvio Padrão
Conhecimento_PoSIC	0,60	0,516
Leitura_PoSIC	0,60	0,516
Aplicacao_PoSIC	1,80	0,919
Capacitacao	0,60	0,516
Incidente_Seguranca	0,70	0,483

Esses resultados mostram que a variabilidade entre as respostas dos participantes foi relativamente baixa para a maioria dos itens, exceto para "Aplicacao_PoSIC", que apresentou um desvio padrão de 0,919, indicando maior dispersão nas respostas.

Conclusão

O coeficiente Alfa de Cronbach de 0,893 confirma a consistência interna do questionário, indicando que ele é confiável para medir os construtos de interesse — neste caso, o conhecimento e a adesão dos participantes à Política de Segurança da Informação e Comunicação da UnB. Essa confiabilidade é crucial para garantir que as conclusões tiradas com base nas respostas dos participantes sejam precisas e válidas. Assim, o questionário pode ser considerado adequado para prosseguir com as próximas etapas do estudo, incluindo a análise dos fatores que influenciam a adesão à PoSIC.

APÊNDICES C – ANÁLISE ESTATÍSTICA NO STATA

```
* Abrir log para armazenar a saída
log using "Resultados_Yang.smcl", replace

* Carregar os dados
use "/Base.dta", clear

* Tabelas de frequência simples
tab Perfil
tab Cargo
tab Genero
tab Idade
tab Tempo

* Teste do qui-quadrado: associação entre perfil institucional e ciência sobre a PoSIC
tab Perfil Ciencia, chi2

* Teste do qui-quadrado: associação entre cargo e ciência sobre a PoSIC
tab Cargo Ciencia, chi2

* Teste do qui-quadrado: associação entre gênero e ciência sobre a PoSIC
tab Genero Ciencia, chi2

* Teste do qui-quadrado: associação entre faixa etária e ciência sobre a PoSIC
tab Idade Ciencia, chi2

* Teste do qui-quadrado: associação entre tempo de atuação na UnB e ciência sobre a PoSIC
tab Tempo Ciencia, chi2

* Análise de correspondência entre capacitação e ciência sobre a PoSIC
ca CapacitacaoPoSIC Ciencia
cabiplot

* Teste do qui-quadrado: associação entre sofrer incidente de segurança digital e ciência sobre a
PoSIC
tab SofriIncidenteSeguranca Ciencia, chi2
ca SofriIncidenteSeguranca Ciencia
cabiplot

* Salvar os dados para futuras análises
save "/Base_Final.dta", replace

* Fechar o log
log close

name: <unnamed>

log: /RESULTADOS.smcl

log type: smcl
```

opened on: 10 Jun 2024, 16:15:29

. tab Perfil

Qual o seu perfil |

institucional? | Freq. Percent Cum.

Servidor docente | 28 59.57 59.57

Servidor técnico-administrativo | 19 40.43 100.00

Total | 47 100.00

. tab Cargo

Você ocupa |

função |

temporária |

ou função |

de |

confiança, |

como chefia |

ou cargos |

de di | Freq. Percent Cum.

Não | 34 72.34 72.34

Sim | 13 27.66 100.00

Total | 47 100.00

. tab Genero

Qual o seu |

gênero? | Freq. Percent Cum.

Feminino | 24 52.17 52.17

Masculino | 22 47.83 100.00

----------+----------------------------------

Total | 46 100.00

. tab Idade

Qual a sua |

faixa |

etária? | Freq. Percent Cum.

----------+----------------------------------

25-34 anos | 5 10.64 10.64

35-44 anos | 12 25.53 36.17

45-54 anos | 15 31.91 68.09

55-64 anos | 14 29.79 97.87

65+ anos | 1 2.13 100.00

----------+----------------------------------

Total | 47 100.00

. tab Tempo

Qual o seu |

tempo de |

atuação |

na UnB? | Freq. Percent Cum.

----------+----------------------------------

0-3 Anos | 9 19.57 19.57

11-20 Anos | 15 32.61 52.17

21+ Anos | 8 17.39 69.57

3-10 Anos | 14 30.43 100.00

----------+----------------------------------

Total | 46 100.00

. log using "/Resultados doc.smcl"

log file already open

r(604);

. log close

name: <unnamed>

log: /RESULTADOS.smcl

log type: smcl

closed on: 10 Jun 2024, 16:16:01

---

name: <unnamed>

log: /RESULTADOS.smcl

log type: smcl

opened on: 10 Jun 2024, 16:16:11

. *** A maioria dos respondentes não conhecem a PiSIC. Ou seja, 63%.

. * Teste do qui-quadrado para ver se algum perfil especí

> fico se relaciona com o resultado da ciência sobre a PoSIC.*

. tab Perfil Ciencia, chi2

| Eu estou ciente da existência

| da resolução Nº 004 de 2018,

Qual o seu perfil | que institui a Políti

institucional? | N/A Não Sim | Total

----------+---------+----------

Servidor docente | 0 19 9 | 28

Servidor técnico-admi | 1 11 7 | 19

----------+---------+----------

Total | 1 30 16 | 47

Pearson chi2(2) = 1.7231 Pr = 0.423

* O resultado demonstra que não existe uma tendência clara, isto é, o perfil institucional não é estatisticamente significante para explicar se um respondente possui ou não ciência da PoSIC. O valor de Pr é maior que 0.05 (significância de 95%) e ele deveria ser menor. Quanto mais próximo de zero melhor.

. tab Cargo Ciencia, chi2

Você |

ocupa |

função |

temporári |

a ou |

função |

de |

confiança |

, como | Eu estou ciente da existência

chefia ou | da resolução Nº 004 de 2018,

cargos de | que institui a Políti

di | N/A Não Sim | Total

----------+----------+----------

Não | 1 22 11 | 34

Sim | 0 8 5 | 13

----------+----------+----------

Total | 1 30 16 | 47

Pearson chi2(2) = 0.5002 Pr = 0.779

.* O resultado demonstra que não existe uma tendência clara, isto é, o cargo/função não é estatisticamente significante para explicar se um respondente possui ou não ciência da PoSIC. O valor de Pr é maior que 0.05 (significância de 95%) e ele deveria ser menor. Quanto mais próximo de zero, melhor.

. tab Genero Ciencia, chi2

| Eu estou ciente da

| existência da

| resolução Nº 004

| de 2018, que institui

Qual o seu | a Políti

gênero? | Não Sim | Total

----------+----------+----------

Feminino | 14 10 | 24

Masculino | 16 6 | 22

----------+----------+----------

Total | 30 16 | 46

Pearson chi2(1) = 1.0484 Pr = 0.306

* O resultado demonstra que não existe uma tendência clara, isto é, o gênero não é estatisticamente significante para explicar se um respondente possui ou não ciência da PoSIC. O valor de Pr é maior que 0.05 (significância de 95%) e ele deveria ser menor. Quanto mais próximo de zero melhor

> .

. tab Idade Ciencia, chi2

| Eu estou ciente da existência

Qual a sua | da resolução Nº 004 de 2018,

faixa | que institui a Políti

etária? | N/A Não Sim | Total

-----------+---------------------------------+----------

25-34 anos | 0 4 1 | 5

35-44 anos | 0 10 2 | 12

45-54 anos | 1 8 6 | 15

55-64 anos | 0 7 7 | 14

65+ anos | 0 1 0 | 1

-----------+---------------------------------+----------

Total | 1 30 16 | 47

Pearson chi2(8) = 6.8346 Pr = 0.555

O resultado demonstra que não existe uma tendência clara, isto é, o gênero não é estatisticamente significante para explicar se um respondente possui ou não ciência da PoSIC. O valor de Pr é maior que 0.05 (significância de 95%) e ele deveria ser menor. Quanto mais próximo de zero melhor

>

. tab Tempo Ciencia, chi2

| Eu estou ciente da

| existência da

Qual o seu | resolução Nº 004

tempo de | de 2018, que institui

atuação | a Políti

na UnB? | Não Sim | Total

-----------+----------------------+----------

0-3 Anos | 7 2 | 9

11-20 Anos | 11 4 | 15

21+ Anos | 4 4 | 8

3-10 Anos | 8 6 | 14

----------+----------+----------

Total | 30 16 | 46

Pearson chi2(3) = 2.2805 Pr = 0.516

O resultado demonstra que não existe uma tendência clara, isto é, o gênero não é estatisticamente significante para explicar se um respondente possui ou não ciência da PoSIC. O valor de Pr é maior que 0.05 (significância de 95%) e ele deveria ser menor. Quanto mais próximo de zero melhor

. *** De uma maneira geral, o perfil do respondente não está associado a saber ou não a política do ponto de vista estatístico ***

. tab VeiculosInformacao

Por quais veículos de comunicação |

você foi informado sobre a Política |

de Seguran | Freq. Percent Cum.

----------+----------

Boletim, Sistema Eletrônico de Informaç | 4 25.00 25.00

Colega ou gestor | 1 6.25 31.25

Não fui informado institucionalmente | 1 6.25 37.50

Outros | 3 18.75 56.25

e-mail | 7 43.75 100.00

----------+----------

Total | 16 100.00

. tab LeituraPoSIC

Eu já fiz |

a leitura |

da |

PoSIC/UnB? | Freq. Percent Cum.

----------+----------

N/A | 31 65.96 65.96

Não | 6 12.77 78.72

Sim | 10 21.28 100.00

----------+----------

Total | 47 100.00

. tab TipodeLeituraPoSIC

Você marcou sim para "Eu |

já fiz a leitura |

PoSIC/UnB), por favor, |

selecione a opç | Freq. Percent Cum.

----------+----------

Não, ainda não li. | 1 10.00 10.00

Sim, li completamente | 5 50.00 60.00

Sim, mas apenas parcialmente | 4 40.00 100.00

----------+----------

Total | 10 100.00

. tab AplicacaoPoSIC

Você aplica |

as |

instruções |

(diretrizes) |

da política |

de segurança |

da |

informação e | Freq. Percent Cum.

----------+----------

Frequentemente | 5 55.56 55.56

Às vezes | 4 44.44 100.00

----------+----------

Total | 9 100.00

. tab FiscalizacaoSTI

A |

responsabilidade |

de fiscalizar o |

cumprimento da |

PoSIC/UnB cabe à |

STI (anterior | Freq. Percent Cum.

------------------+-----------------------------------

Não | 4 26.67 26.67

Não sei responder | 10 66.67 93.33

Sim | 1 6.67 100.00

------------------+-----------------------------------

Total | 15 100.00

. tab ComunicacaoUnBPoSIC

Você |

recebe |

alguma |

informaçã |

o sobre o |

conteúdo |

da |

política |

de |

segurança |

da infor | Freq. Percent Cum.

------------+-----------------------------------

N/A | 32 68.09 68.09

Não | 7 14.89 82.98

Sim | 8 17.02 100.00

------------+-----------------------------------

Total | 47 100.00

. tab VeiculosComunicacaoUnB

Por quais veículos de comunicação |

você recebe informações sobre o |

conteúdo da Po | Freq. Percent Cum.

----------+----------

Boletim, Sistema Eletrônico de Informaç | 1 12.50 12.50

Colega ou gestor | 1 12.50 25.00

e-mail | 6 75.00 100.00

----------+----------

Total | 8 100.00

. tab CapacitacaoPoSIC

Eu recebi |

capacitaç |

ão |

específica |

relacionado |

à |

política |

de |

segurança |

da |

informaç | Freq. Percent Cum.

----------+----------

N/A | 32 68.09 68.09

Não | 14 29.79 97.87

Sim | 1 2.13 100.00

----------+----------

Total | 47 100.00

. ** Teste do qui-quadrado para essas duas variáveis ***

. tab CapacitacaoPoSIC Ciencia, chi2

Eu recebi |

capacitaç |

ão |

específic |

a |

relacionad |

o à |

política |

de | Eu estou ciente da existência

segurança | da resolução Nº 004 de 2018,

da | que institui a Políti

informaç | N/A Não Sim | Total

----------+----------+----------

N/A | 1 30 1 | 32

Não | 0 0 14 | 14

Sim | 0 0 1 | 1

----------+----------+----------

Total | 1 30 16 | 47

Pearson chi2(4) = 42.6855 Pr = 0.000

**** Resultados muito interessantes: existe uma associação estatisticamente significante entre ter ciência da política e ter recebido o treinamento. ****

. *** Agora e preciso entender em que sentido, por isso, vamos usar uma analise de correspondência simples

. ca CapacitacaoPoSIC Ciencia

(dimension is set to 1

)

Correspondence analysis Number of obs = 47

Pearson chi2(4) = 42.69

Prob > chi2 = 0.0000

Total inertia = 0.9082

3 active rows Number of dim. = 1

3 active columns Expl. inertia (%) = 100.00

| singular principal cumul

Dimension | value inertia chi2 percent percent

----------+----------

dim 1 | .9529969 .9082031 42.69 100.00 100.00

----------+----------

total | .9082031 42.69 100

Statistics for row and column categories in symmetric normalization

| overall | dimension_1

Categories | mass quality %inert | coord sqcorr contrib

----------+----------+----------

Capacitaca~C | |

N/A | 0.681 1.000 0.319 | 0.668 1.000 0.319

Não | 0.298 1.000 0.635 | -1.426 1.000 0.635

Sim | 0.021 1.000 0.045 | -1.426 1.000 0.045

----------+----------+----------

Ciencia | |

N/A | 0.021 1.000 0.011 | 0.701 1.000 0.011

Não | 0.638 1.000 0.329 | 0.701 1.000 0.329

Sim | 0.340 1.000 0.660 | -1.359 1.000 0.660

. cabiplot

(no plot with dimension < 2)

Como a amostra é pequena, não conseguimos gerar a relação. Mas de uma maneira geral, as pessoas que conhecem a PoSIC não receberam capacitação. Apenas um respondente recebeu capacitação, o que demonstra a necessidade de desenvolver formas de conscientização e justifica a sua intervenção e consequentemente seu produto.

. tab ComunicacaoUnBPoSIC

Você |

recebe |

alguma |

informaçã |

o sobre o |

conteúdo |

da |

política |

de |

segurança |

da infor | Freq. Percent Cum.

------------+-----------------------------------

N/A | 32 68.09 68.09

Não | 7 14.89 82.98

Sim | 8 17.02 100.00

------------+-----------------------------------

Total | 47 100.00

. tab VeiculosComunicacaoUnB

Por quais veículos de comunicação |

você recebe informações sobre o |

conteúdo da Po | Freq. Percent Cum.

--+-----------------------------------

Boletim, Sistema Eletrônico de Informaç | 1 12.50 12.50

Colega ou gestor | 1 12.50 25.00

e-mail | 6 75.00 100.00

--+-----------------------------------

Total | 8 100.00

. tab CapacitacaoPoSIC

Eu recebi |

capacitaç |

ão |

específica |

relacionado |

à |

política |

de |

segurança |

da |

informaç | Freq. Percent Cum.

------------+-----------------------------------

N/A | 32 68.09 68.09

Não | 14 29.79 97.87

Sim | 1 2.13 100.00

------------+-----------------------------------

Total | 47 100.00

. tab SofriIncidenteSeguranca

Eu já |

sofri algum |

incidente |

de |

segurança |

digital, |

como |

vazamento |

de senhas, |

golp | Freq. Percent Cum.

------------+-----------------------------------

Não | 16 35.56 35.56

Sim | 29 64.44 100.00

------------+-----------------------------------

Total | 45 100.00

. tab SofriIncidenteSeguranca Ciencia, chi2

Eu já |

sofri |

algum |

incidente |

de |

segurança | Eu estou ciente da

digital, | existência da

como | resolução Nº 004

vazamento | de 2018, que institui

de senhas, | a Políti

golp | Não Sim | Total

-----------+----------------------+----------

Não | 8 8 | 16

Sim | 22 7 | 29

-----------+----------------------+----------

Total | 30 15 | 45

Pearson chi2(1) = 3.1034 Pr = 0.078

. *** Os resultados são interessantes: em um nível de significância de 90%, exi

> ste uma associação entre ter sofrido algum incidênte e ter ciência da PoSIC.

> ****

. ca SofriIncidenteSeguranca Ciencia

Correspondence analysis Number of obs = 45

Pearson chi2(1) = 3.10

Prob > chi2 = 0.0781

Total inertia = 0.0690

2 active rows Number of dim. = 1

2 active columns Expl. inertia (%) = 100.00

| singular principal cumul

Dimension | value inertia chi2 percent percent

------------+--

dim 1 | .2626129 .0689655 3.10 100.00 100.00

------------+--

total | .0689655 3.10 100

Statistics for row and column categories in symmetric normalization

| overall | dimension_1

Categories | mass quality %inert | coord sqcorr contrib

----------+-------------------------+-------------------------

SofriIncid~a | |

Não | 0.356 1.000 0.644 | 0.690 1.000 0.644

Sim | 0.644 1.000 0.356 | -0.381 1.000 0.356

----------+-------------------------+-------------------------

Ciencia | |

Não | 0.667 1.000 0.333 | -0.362 1.000 0.333

Sim | 0.333 1.000 0.667 | 0.725 1.000 0.667

. cabiplot

(no plot with dimension < 2)

. tab SofriIncidenteSeguranca CapacitacaoPoSIC, chi2

Eu já |

sofri |

algum |

incidente |

de |

segurança |

digital, | Eu recebi capacitação

como | específica relacionado à

vazamento | política de segurança da

de senhas, | informaç

golp | N/A Não Sim | Total

-----------+---------------------------------+----------

Não | 8 7 1 | 16

Sim | 22 7 0 | 29

----------+----------------------------------+----------

Total | 30 14 1 | 45

Pearson chi2(2) = 4.1218 Pr = 0.127

. tab Ciencia AcessoMeiosComunicacaoInst

Eu estou |

ciente da |

existênci |

a da |

resoluçã |

o Nº 004 |

de 2018, |

que | Você tem acesso aos meios de

institui a | comunicação institucional?

Políti | N/A Não Sim | Total

----------+----------------------------------+----------

N/A | 1 0 0 | 1

Não | 0 1 29 | 30

Sim | 16 0 0 | 16

----------+----------------------------------+----------

Total | 17 1 29 | 47

. tab Ciencia AcessoMeiosComunicacaoInst, chi2

Eu estou |

ciente da |

existênci |

a da |

resoluçã |

o Nº 004 |

de 2018, |

que | Você tem acesso aos meios de

institui a | comunicação institucional?

Políti | N/A Não Sim | Total

----------+---------------------------------+----------

N/A | 1 0 0 | 1

Não | 0 1 29 | 30

Sim | 16 0 0 | 16

----------+---------------------------------+----------

Total | 17 1 29 | 47

Pearson chi2(4) = 47.0000 Pr = 0.000

. *** Resultado interessante: há uma associação estatísticamente significante a 99% de significância entre acesso a meios de comunicação institucionais e a ciência da PoSIC. Isso demonstra que se o respondente não acessou meios institucionais, ele dificilmente irá ter ciência da PoSIC ou fará uma capacitação. Isso demonstra a necessidade de intervenção.

. save "/Base.dta", replace

file /Base.dta saved

APÊNDICES D – ENTREVISTAS

PRIMEIRA ENTREVISTA

Nome, Atena.

Cargo? Assistente em Administração.

Você preencheu o formulário, certo? Sim.

Você estava ciente da existência da POSIX antes de responder ao questionário? Não.

Depois que preencheu o questionário, teve alguma curiosidade? Quis conhecer? Não.

*Neste momento, ocorreu uma hesitação, um possível receio de consequências negativas associadas à resposta.

Pode ser honesta. Não.

Já sofreu algum incidente de segurança? Não, aqui não.

Fora? Em outro trabalho.

Mas aqui na UNB ou fora da UNB? Fora da UNB.

E aqui na UNB? Nunca.

Na sua vida pessoal, alguma coisa? Não, em outro trabalho mesmo.

Você participaria de algum treinamento sobre a política de segurança de formação? Sim.

Como você gostaria que fosse esse treinamento? Online, presencial? Eu gosto de forma híbrida. Que fosse uma palestra presencial, mas que as atividades que fossem passadas para ser realizadas pudessem ser de forma remota. Eu gosto mais de palestra presencial.

- Finalizada a entrevista.

SEGUNDA ENTREVISTA:

Nome? Afrodite.

Setor? Secretaria de Pós-Graduação.

Cargo? Assistente em Administração.

Preencheu o questionário? Aham.

Estava ciente da POSIC antes de responder ao questionário? A gente sabe das políticas pelos informes que vêm nos e-mails, né?

Certo. Então, sim, você conhecia? Sim, sim.

Leu? Tem conhecimento? Plenamente, não.

Leu parcialmente? Não, eu vejo os informes do STI, vamos dizer assim.

Mas os informes do STI são direcionados à política ou são no contexto geral? Hum... Bom, algumas vezes eles indicaram, por questão de segurança, algo mais específico, vamos dizer assim. Tá. Né?

Então, é possível presumir que você já abriu a política? Você viu, tem conhecimento, não só da existência dela, como chegou a abri-la? Aham.

Fez uma leitura? Sim.

Completa, parcial? Não, parcial.

Uma leitura parcial. Ok. Aplica alguma das diretrizes? Se recorda de alguma diretriz que você aplica diariamente, frequentemente, às vezes? Bom, coisas de evitar aquelas, acessar links que você acha que sejam maliciosos, já ocorreu até um aviso específico sobre isso uma vez. Hum..., Mas outras coisas, assim, de forma geral, a gente tem que ter cuidado com as coisas que a gente recebe. Aham. Né? Ter um certo cuidado. Certo. Não acessar sites maliciosos e nem acessar links que o povo envia, às vezes, indicando, sei lá, atualizações que não existam, não sei. Eu não me recordo, mas uma vez ocorreu algo nesse sentido e houve um aviso específico do STI para não entrar no link, porque aquela pessoa que se dizia da UNB não era, na verdade. Na verdade, tinha acessado e tinha enviado para um bando de gente. Eu não me lembro direito o que era. Faz um ano, por aí.

Você lembra de alguma coisa sobre gestão de ativos? Não.

Utilização de e-mail? Hum... Em que sentido?

Orientações para utilizar o e-mail? Sim.

Alguma coisa nesse sentido? As regras de utilização, por exemplo, do e-mail? Se recorda ou não recorda? É, já li, mas, assim, coisas normais que você deve ou não deve fazer no e-mail institucional, normal.

Lembra de alguma (diretriz)? em particular? Não, não especificamente.

Já enfrentou algum incidente de segurança? Não, graças a Deus, não.

Nem aqui, nem fora? Não, é, nem aqui, nem fora.

Participaria de algum treinamento sobre a política? Sim.

Alguma preferência de treinamento online, livre, presencial? Online.

- Finalizada a entrevista.

TERCEIRA ENTREVISTA:

Nome, por favor? É, Perséfone.

Setor? Faculdade de Educação.

Cargo? Professora.

Preencheu o formulário, certo? Sim, preenchi.

Conhecia, tinha ciência da POSIC antes de responder o questionário? POSIC? O que é POSIC?

A Política de Segurança da Informação e Comunicação da Universidade. Não, não tinha informação.

Quando respondeu o questionário, presumo que não ficou claro o que era POSIC? Não, não ficou.

Teve alguma curiosidade de pesquisar o que era? Olha, no dia que eu preenchi, eu fiquei curiosa, mas depois eu não fui atrás para tentar saber melhor o que era.

Sobre comunicação e treinamento, você lembra a primeira comunicação? Lembra ter recebido algum informe sobre a política, um e-mail, alguma coisa assim? Eu acho que sim, acho que já recebi, mas não sei dizer exatamente quando que foi que eu recebi. Eu não cheguei atrás disso, não.

Participaria de algum treinamento sobre segurança? Sim, acho que é importante, né? Acho que é importante a gente conhecer melhor.

Alguma preferência? Se precipitar para a citação, se presencial, virtual? Olha, eu prefiro presencial, uma palestra, alguma coisa assim, acho que é mais interessante.

E sobre receber informações sobre a política, que e-mail você gostaria? Um e-mail, um

boletim? Sim, também acho que pode ser por e-mail ou um boletim, mas que viesse também por e-mail.

Última pergunta, já sofreu algum incidente de segurança digital? Na UNB, não. Mas fora da UNB, sim.

Fora da UNB, sim. Ok. Perfeito, é isto.

- Finalizada a entrevista.

APÊNDICES E – RELATÓRIO DA ANÁLISE TEMÁTICA

A seguir, apresento um relatório ilustrativo resultante de uma análise temática (inspirada em Braun & Clarke, 2006) das três entrevistas semiestruturadas realizadas com servidores técnico-administrativos (Atena e Afrodite) e uma docente (Perséfone). O foco da análise recai sobre o conhecimento e percepção acerca da POSIC (Política de Segurança da Informação e Comunicação), bem como experiências e preferências relativas a treinamento e incidentes de segurança da informação.

1. Introdução

O objetivo geral da pesquisa consistiu em compreender:

- O nível de conhecimento dos servidores sobre a POSIC;
- As experiências anteriores com incidentes de segurança;
- As preferências de treinamento para aprimorar o conhecimento e a aderência às diretrizes de segurança da informação.

As entrevistas foram conduzidas de modo semiestruturado, permitindo a livre expressão dos entrevistados e a exploração de temas emergentes relacionados à segurança da informação na Universidade.

2. Procedimentos Metodológicos

Participantes:

- Atena (Assistente em Administração); Afrodite (Assistente em Administração); Perséfone (Professora).
- Coleta de Dados: as entrevistas foram realizadas presencialmente ou em local acordado com cada participante, seguindo um roteiro básico de perguntas sobre o conhecimento da POSIC, vivências com incidentes e sugestões/formas de treinamento.

Análise: utilizou-se a Análise Temática baseada em Braun e Clarke (2006), em seis etapas:
1. Familiarização com os dados; 2. Geração de códigos iniciais; 3. Busca por temas; 4. Revisão dos temas; 5. Definição e nomeação dos temas; 6. Produção deste relatório.

3. Resultados e Discussão (Temas Identificados)

A partir da leitura e codificação das falas, emergiram quatro temas principais:

3.1. Conhecimento e Divulgação da POSIC:

- Desconhecimento ou conhecimento parcial:
- Em dois casos (Atena e Perséfone), houve declaração de desconhecimento prévio do termo “POSIC” antes de responder ao questionário. Perséfone chega a questionar “POSIC? O que é POSIC?”, indicando que não estava ciente do nome formal da política.

- Afrodite, por outro lado, demonstra ter alguma familiaridade com a política, embora "plenamente, não". Menciona que soube dela por meio de "informes do STI".
- Comunicação fragmentada:
- Notou-se que, quando há algum alerta de risco (por exemplo, e-mails maliciosos), o STI emite comunicados. Entretanto, não há um contato sistemático que aprofunde a POSIC, nem mecanismos que assegurem a leitura integral da política.

Reflexão: esses relatos sugerem que a comunicação atual sobre a POSIC é pontual e "reativa" (quando há incidentes iminentes). Parece faltar uma divulgação planejada e contínua que deixe claro o propósito e o conteúdo da POSIC.

3.2. Experiências com Incidentes de Segurança

- Incidentes pessoais em trabalhos anteriores:
- Atena relata não ter sofrido incidentes na atual instituição, mas menciona ter presenciado incidentes em outro local de trabalho.
- Afrodite diz nunca ter passado por um incidente de segurança, "graças a Deus, não".
- Perséfone confirma não ter sofrido na UNB, mas sim "fora da UNB".

Postura de cautela:

- Mesmo sem incidentes diretos, Afrodite demonstra atenção aos riscos ("ter um certo cuidado" ao abrir links, e-mails suspeitos).
- Perséfone reconhece a importância do tema ("acho que é importante a gente conhecer melhor").

Reflexão: embora não haja incidentes frequentes relatados no ambiente da universidade, a preocupação existe, especialmente quando há comunicação sobre ataques pontuais. A pouca vivência de incidentes pode levar à subestimação do risco, destacando a necessidade de treinamentos preventivos.

3.3. Preferências de Treinamento e Engajamento

Formato de treinamento:

- Atena prefere algo híbrido, com palestra presencial e atividades remotas.
- Afrodite opta por treinamento online, devido possivelmente à praticidade e flexibilidade.
- Perséfone demonstra preferência por formato presencial, pois julga "mais interessante" e envolvente.

Interesse em participar:

- Todas se mostraram dispostas a participar de algum tipo de capacitação. As variações aparecem apenas no formato desejado.

Reflexão: esse aspecto plural de preferências sugere que uma estratégia mista (presencial e online) poderia alcançar maior adesão. A palestra presencial favorece a interação e esclarecimentos em tempo real; já o material online atende à necessidade de flexibilidade de horários e revisões posteriores.

3.4. Práticas Cotidianas e Aplicação da POSIC

Aplicação parcial:

- Afrodite menciona ações simples, como evitar abrir links suspeitos ou sites maliciosos, mas não demonstra conhecimento formal de diretrizes específicas ("não me recordo, mas já li coisas normais…").
- Atena e Perséfone, por não conhecerem a POSIC em detalhe, não identificaram diretrizes específicas que aplicam.
- Possível receio: Atena hesita ao responder se teve curiosidade em conhecer a POSIC depois de responder ao questionário, sugerindo insegurança ou medo de parecer "desinteressada".

E-mails e avisos:

- Afrodite recorda comunicados do STI informando sobre links falsos que se passavam por e-mails oficiais da UNB. Esses avisos acabam servindo como catalisadores de práticas de segurança.

Reflexão: embora os entrevistados tenham algum "senso de cuidado" no uso do e-mail e acesso a links, há pouca internalização formal da POSIC. A política em si não está plenamente incorporada às rotinas de trabalho, reforçando a necessidade de capacitação focada na aplicação prática das diretrizes.

4. Conclusões

A análise das entrevistas evidencia:

- Baixa ou parcial familiaridade com a POSIC, mesmo entre servidores técnico-administrativos e docentes.
- Comunicação da POSIC ocorre de maneira pontual (e-mails de alerta), o que favorece a consciência reativa, mas não promove uma visão abrangente da política.
- Incidentes de segurança diretos na instituição parecem raros entre esses entrevistados, mas já houve experiências anteriores e preocupação com possíveis ataques de phishing ou invasões.
- Há disposição para treinamento, mas cada participante prefere um formato diferente

(online, presencial ou híbrido).

- As práticas de segurança existentes são, em geral, informais e motivadas por orientações pontuais, não por um conhecimento profundo da POSIC.

5. Recomendações

1. Divulgação Sistemática:
    - Criar estratégias de comunicação contínua, explicando os objetivos e as seções principais da POSIC, de modo que servidores e docentes saibam exatamente onde consultar as diretrizes e como aplicá-las.
    - Mensagens periódicas (por exemplo, “Dicas Mensais de Segurança”) podem promover engajamento.
2. Variedade de Formatos de Treinamento:
    - Oferecer palestras presenciais para quem prefere interação direta.
    - Disponibilizar plataforma online ou material em EAD para quem busca flexibilidade (como sugere Afrodite).
    - Hibridizar estratégias para maximizar a participação (como deseja Atena).
3. Exemplos Práticos e Relevantes:
    - Incluir casos reais de incidentes de segurança (mesmo externos) para alertar os servidores sobre riscos.
    - Ensinar práticas de segurança que vão além de não clicar em links suspeitos, por exemplo: gestão segura de senhas, uso correto do e-mail institucional, proteção de dados sensíveis etc.
4. Incentivo à Cultura de Segurança:
    - Fomentar um ambiente onde perguntas, dúvidas e falhas possam ser discutidas sem receio ou julgamentos, reduzindo hesitações ao abordar o tema.
    - Criar canais de suporte e resposta rápida, em que incidentes (ou suspeitas) possam ser relatados de forma segura.

6. Limitações e Perspectivas Futuras

- Escopo Amostral: o presente relatório baseia-se em rês entrevistas; amostras maiores ou mais diversificadas poderiam trazer nuances adicionais.
- Detalhamento dos Incidentes: Há pouca profundidade sobre incidentes reais. Seria oportuno investigar mais sobre experiências de outros setores ou unidades.
- Aplicação de Treinamentos Piloto: Sugere-se a implementação de um projeto-piloto de

treinamento (presencial e/ou online) e posterior avaliação de efetividade.

7. Considerações Finais

O conjunto de entrevistas reforça a importância de uma política institucional de segurança não apenas existente "no papel", mas ativa e incorporada ao cotidiano de servidores e docentes. A POSIC necessita de maior divulgação e treinamentos adaptados às realidades e preferências dos diferentes perfis de funcionários. Ao promover uma cultura de segurança mais sólida, a Universidade estará melhor preparada para prevenir e responder a possíveis incidentes, garantindo a proteção de informações e a tranquilidade de toda a comunidade acadêmica.

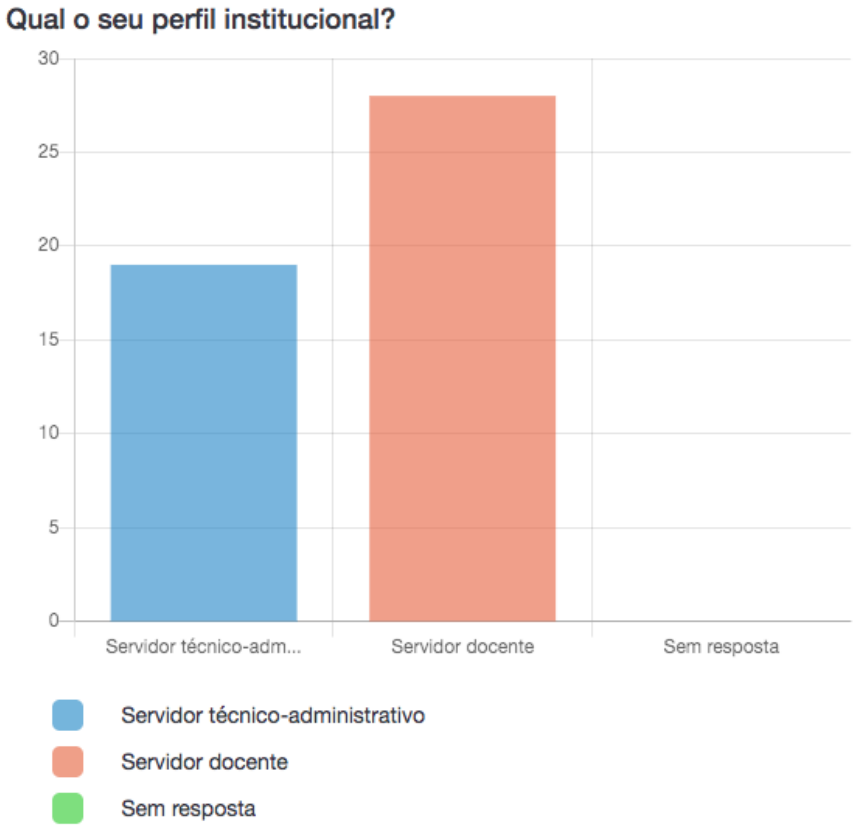
Tabela de Temas e Códigos

Tema Principal	Subtemas/Códigos	Exemplos de Falas
Conhecimento e Divulgação da POSIC	- Desconhecimento - Contato via STI - Leitura parcial	"POSIC? O que é POSIC?" "Não, plenamente, não."
Experiências com Incidentes de Segurança	- Vivência em outro emprego - Receio de phishing - Nenhum incidente	"Já sofri em outro trabalho." "Graças a Deus, nunca aqui."
Preferências de Treinamento	- Online - Presencial - Híbrido	"Eu gosto de forma híbrida." "Online." "Prefiro presencial."
Práticas Cotidianas e Aplicação da Política	- Cautela com links suspeitos - Uso do e-mail institucional - Falta de apropriação das diretrizes	"Eu vejo os informes do STI." "Não me recordo (das diretrizes)."

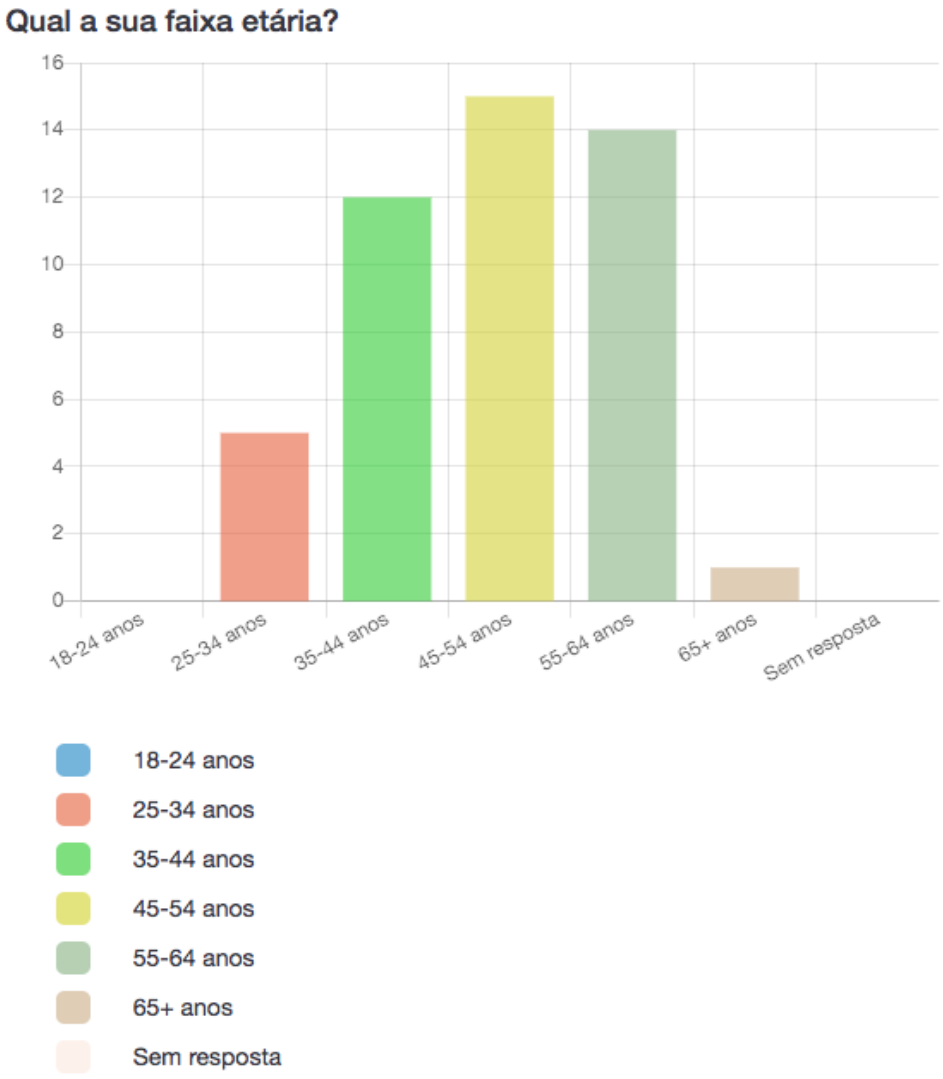
Referência principal:

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.

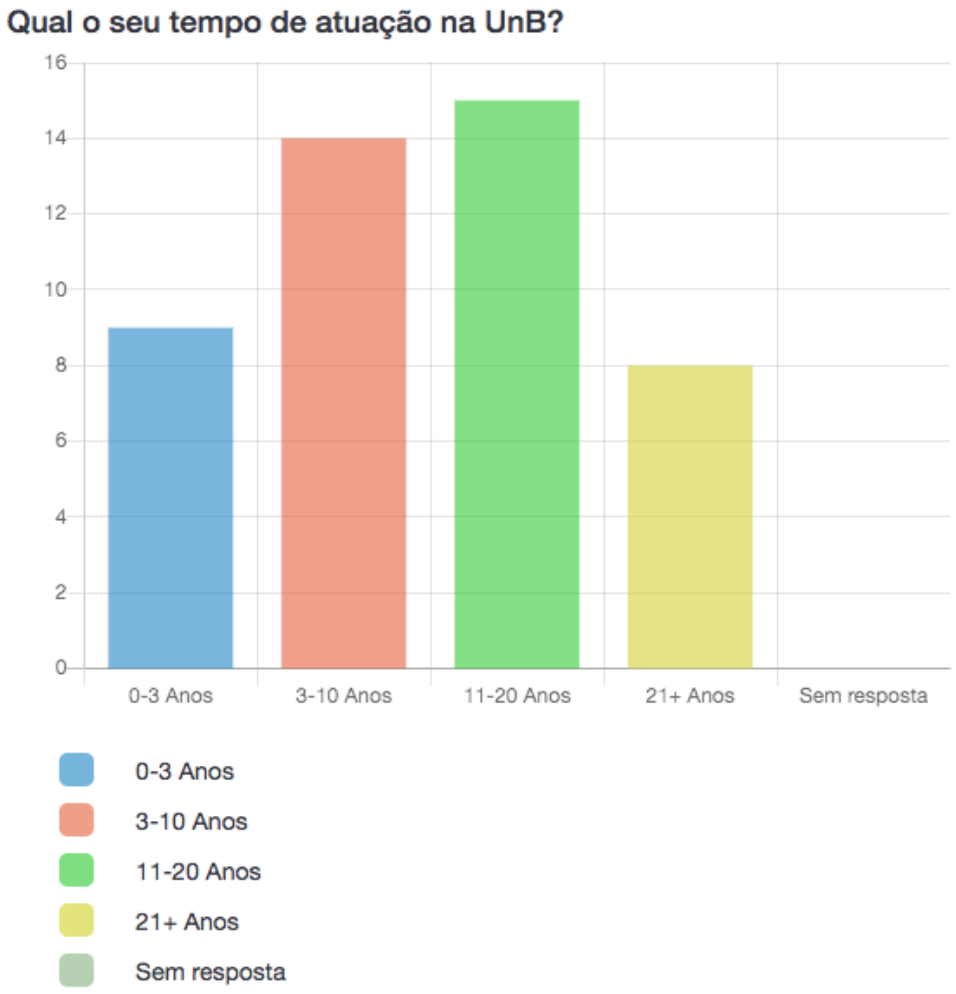
ANEXO – GRÁFICOS DO SURVEY



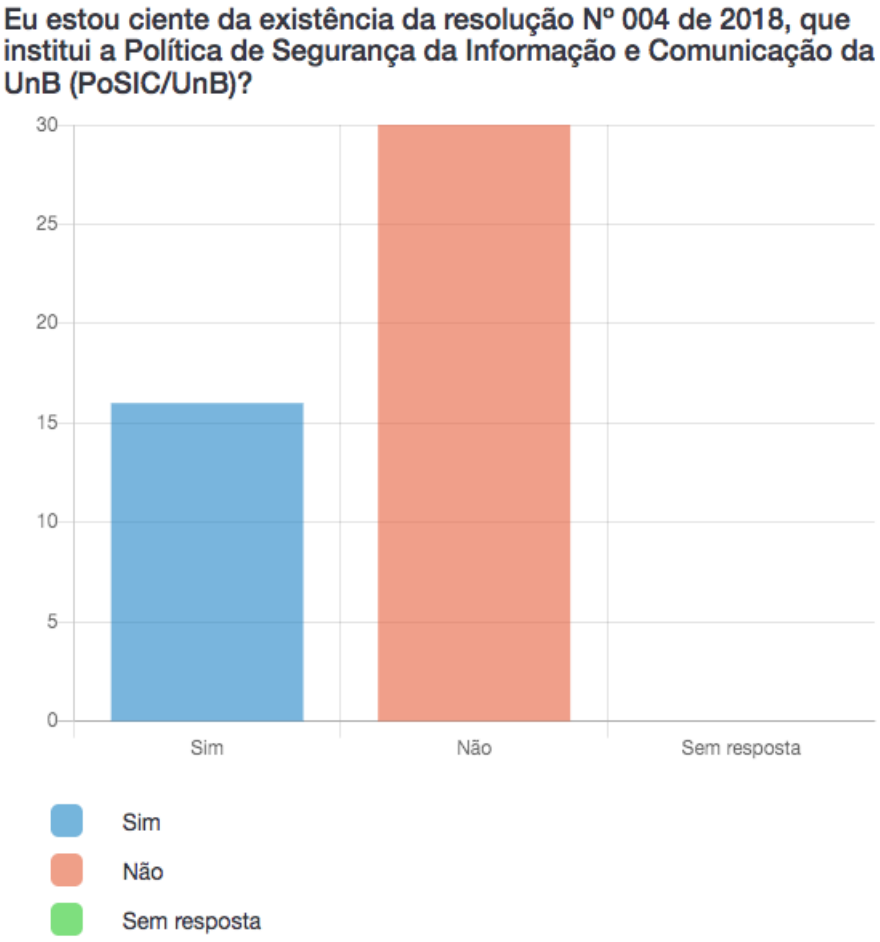
Resposta	Contagem	Percentagem
Servidor técnico-administrativo (A1)	19	40.43%
Servidor docente (A2)	28	59.57%
Sem resposta	0	0.00%



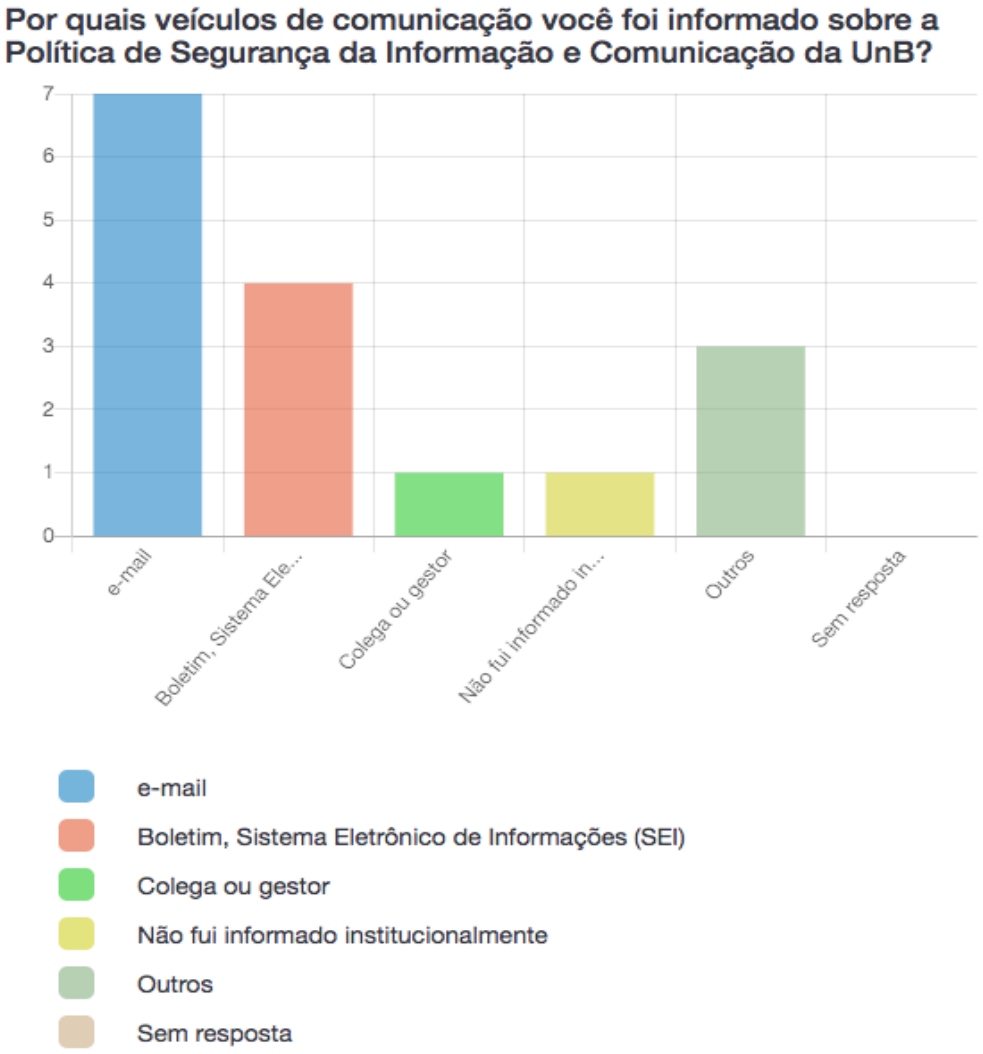
Resposta	Contagem	Percentagem
18-24 anos (A1)	0	0.00%
25-34 anos (A2)	5	10.64%
35-44 anos (A3)	12	25.53%
45-54 anos (A4)	15	31.91%
55-64 anos (A5)	14	29.79%
65+ anos (A6)	1	2.13%
Sem resposta	0	0.00%



Resposta	Contagem	Percentagem
0-3 Anos (A2)	9	19.57%
3-10 Anos (A3)	14	30.43%
11-20 Anos (A4)	15	32.61%
21+ Anos (A5)	8	17.39%
Sem resposta	0	0.00%

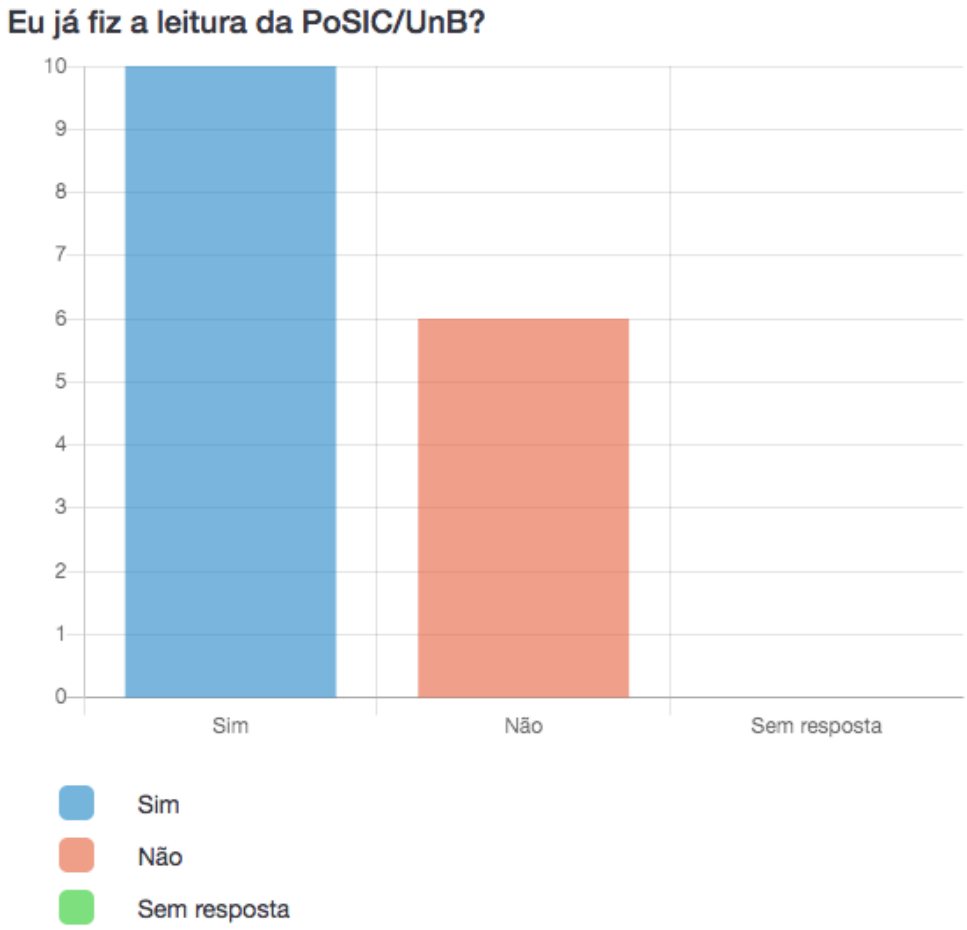


Resposta	Contagem	Percentagem
Sim (Y)	16	34.78%
Não (N)	30	65.22%
Sem resposta	0	0.00%

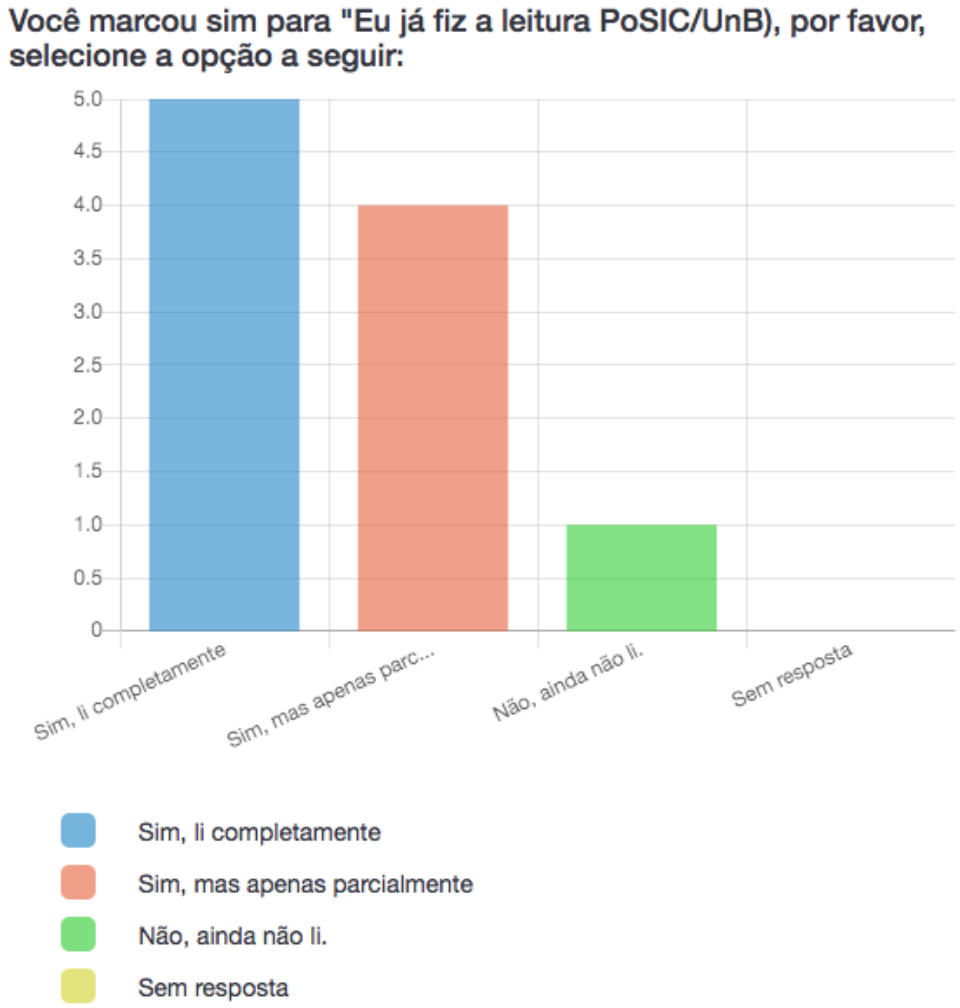


Resposta	Contagem	Percentagem
e-mail (A1)	7	43.75%
Boletim, Sistema Eletrônico de Informações (SEI) (A2)	4	25.00%
Colega ou gestor (A3)	1	6.25%
Não fui informado institucionalmente (A5)	1	6.25%
Outros	3	18.75%
Sem resposta	0	0.00%

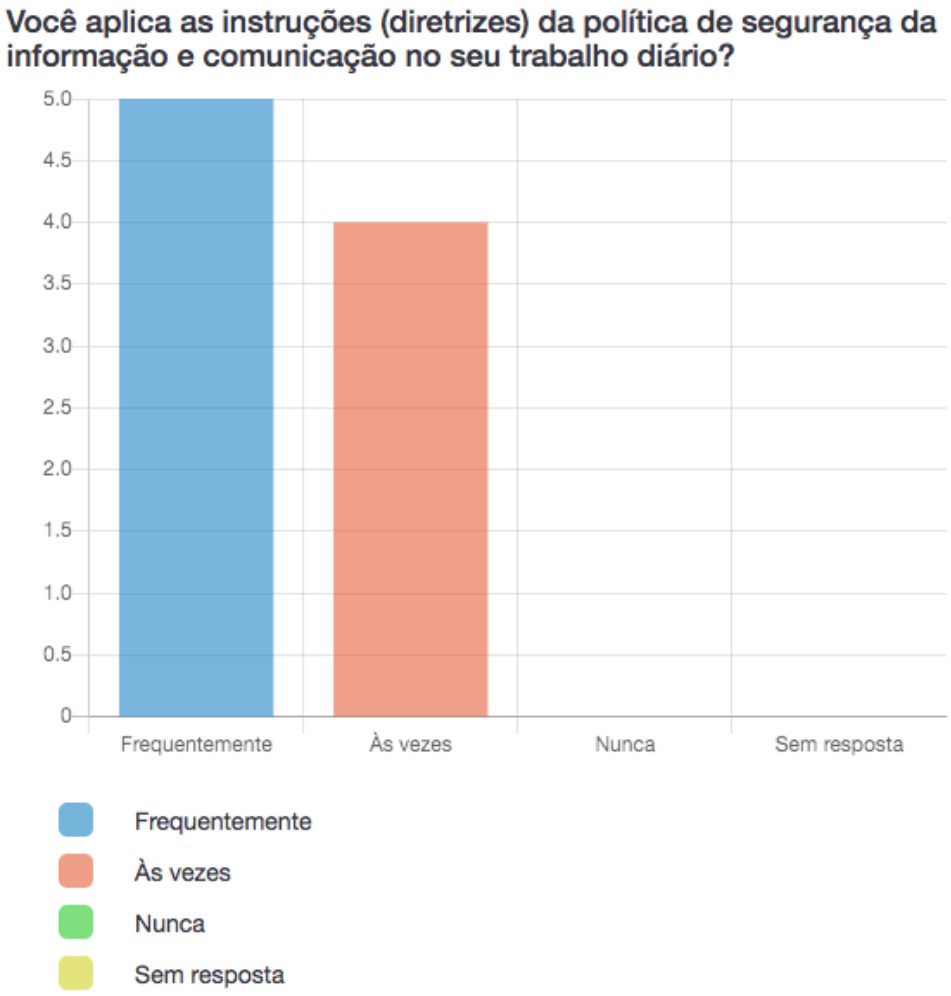
ID	Resposta
10	Boletim de Atos Oficiais da UnB
29	site



Resposta	Contagem	Percentagem
Sim (Y)	10	62.50%
Não (N)	6	37.50%
Sem resposta	0	0.00%



Resposta	Contagem	Percentagem
Sim, li completamente (A1)	5	50.00%
Sim, mas apenas parcialmente (A2)	4	40.00%
Não, ainda não li. (A3)	1	10.00%
Sem resposta	0	0.00%



Resumo de Diretriz02

Na última questão, você selecionou que "frequentemente" aplica a política. Por favor, descreva (brevemente) alguma situação em que você aplicou alguma das diretrizes da PoSIC/UnB?

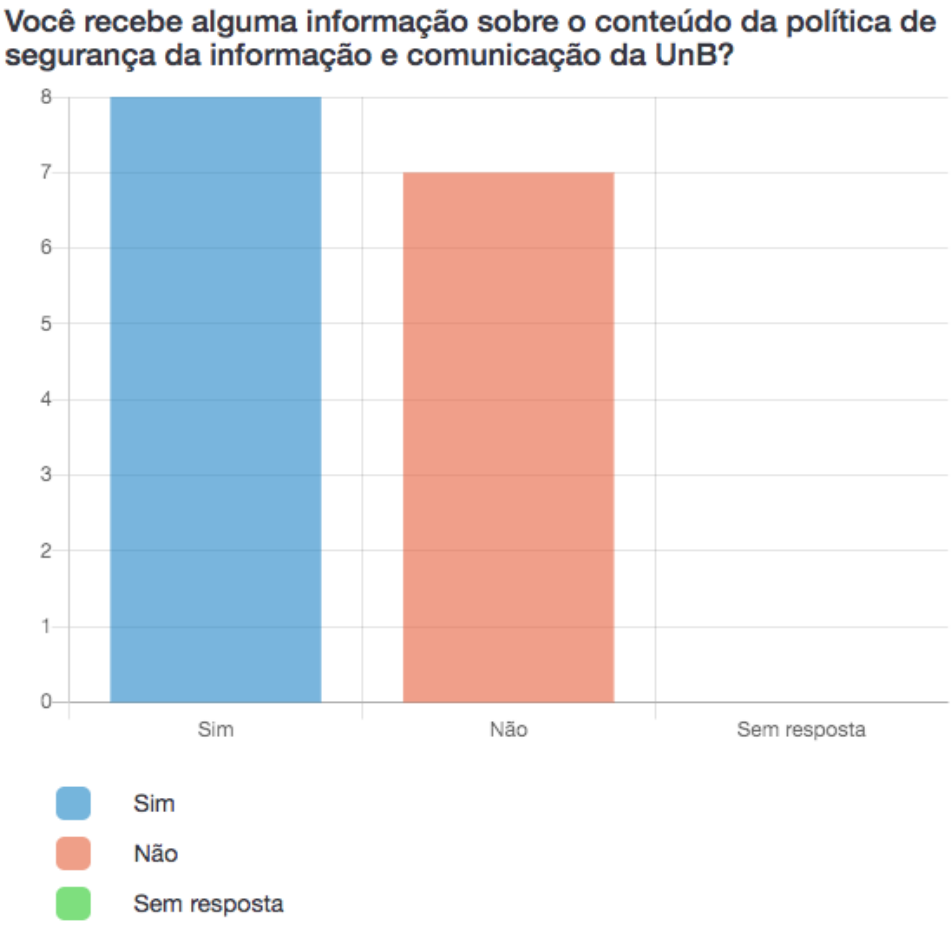
Resposta	Contagem	Percentagem
Resposta	4	100.00%
Sem resposta	0	0.00%

ID	Resposta
7	Utilização de autenticação forte, através de senhas seguras para acesso a sistemas importantes.
10	Apesar de não me enquadrar como gestor de informação trabalhar com isso, ao mencionar o "frequentemente" sobre utilização de Política de Segurança, estou me referindo a uma série de ações, como ao me logar em algum sistema da UnB de qualquer máquida, após sua utilização, me desconecto, além de não armazenar senhas nos browses ao acessar, por exemplo.
42	Melhorar mais trabalho
48	Acesso à internet, aos dados (arquivos), ao e-mail da UnB e aos sistemas para fins institucionais.

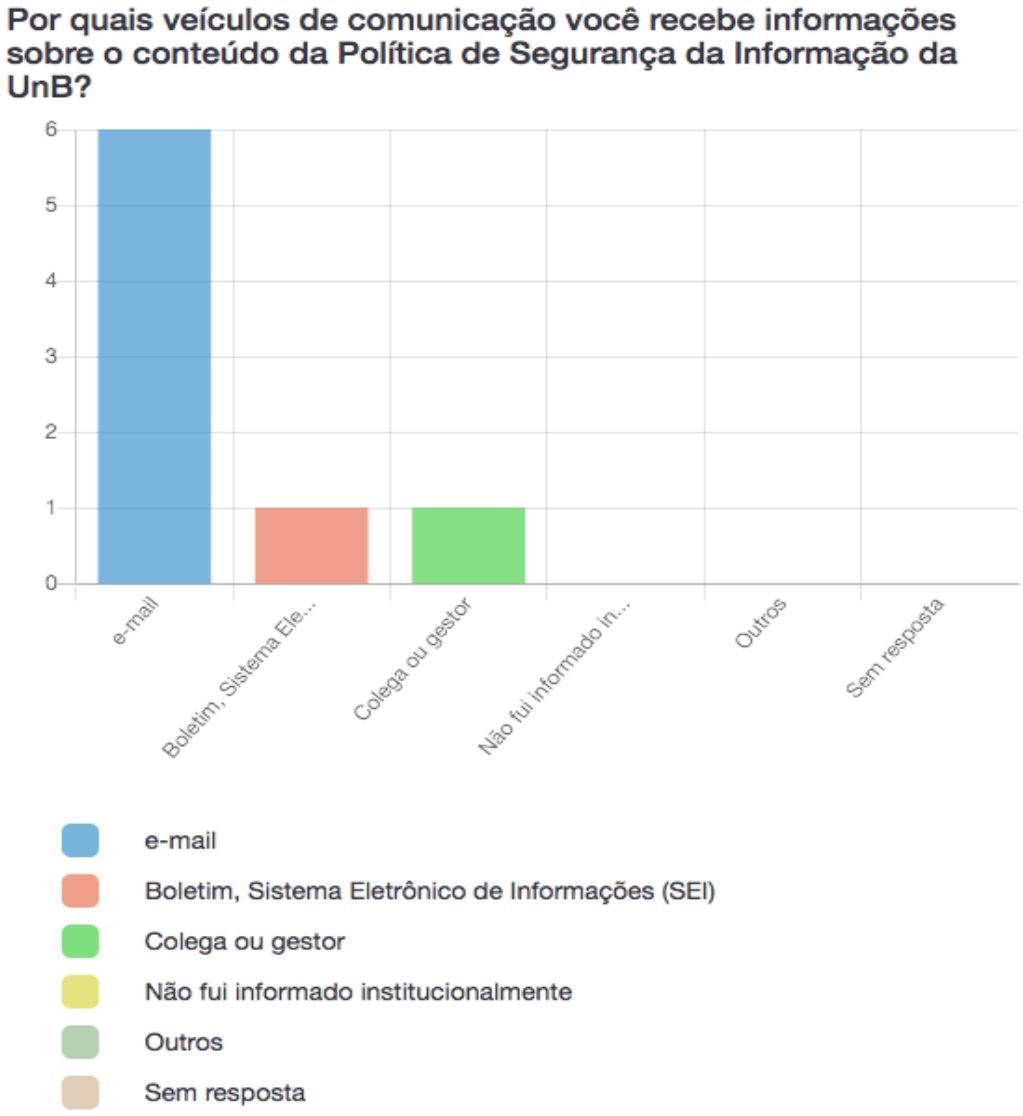
Você indicou que "às vezes" segue as instruções da política. Poderia explicar o que o levou a aplicar essas diretrizes em casos específicos? Quais fatores tornaram necessária a aplicação da política nessas situações?

Resposta	Contagem	Percentagem
Resposta	4	100.00%
Sem resposta	0	0.00%

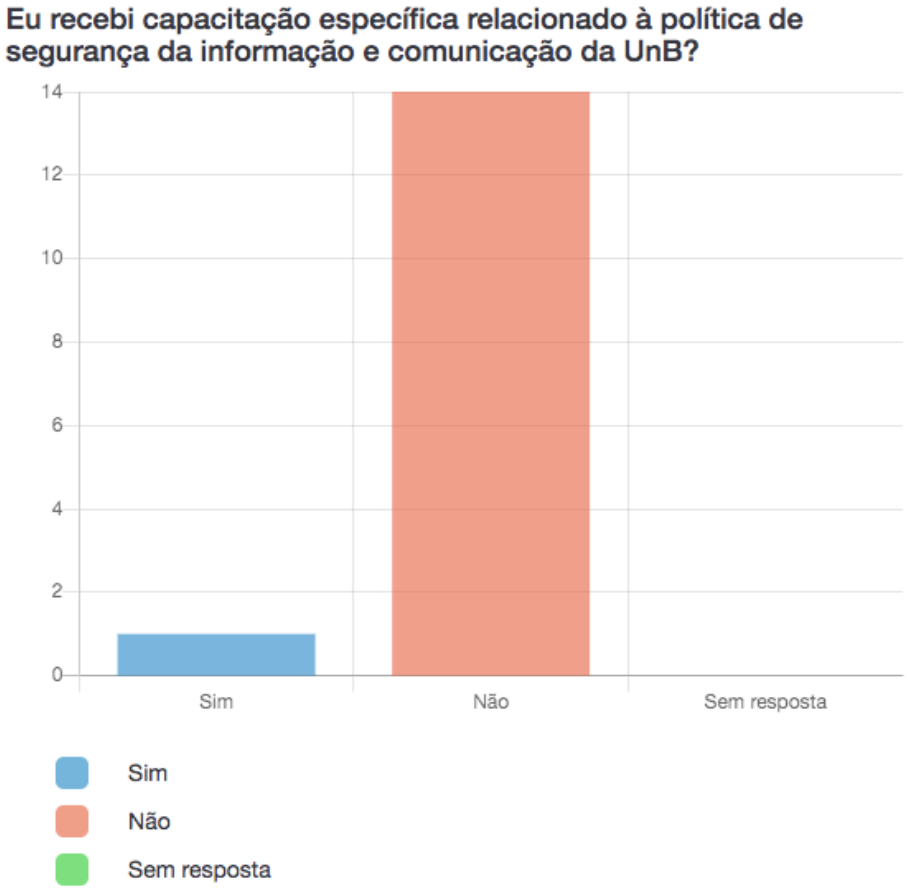
ID	Resposta
13	A Política de Segurança da Informação deverá ser mantida em pleno alinhamento ao Projeto Político Pedagógico - PPP. Assim, conhecedor do PPP, busco estar dentro das normas.
20	Tomei conhecimento sobre a Resolução em questão quando entrei na coordenação do CEDUC. Apesar de ser um tipo de gestão de informação um pouco diversa do que ocorre em outras unidades, eu marquei “as vezes” na pergunta anterior porque sempre me pego pensando que não tenho operado, seja na coordenação do CEDUC ou da própria coordenação do curso de Pedagogia EaD dentro dos princípios, principalmente quando penso no acesso para realização de tarefas e em como posso garantir que processos ou sistemas de acesso à documentação possam ser recuperados caso ocorra algum imprevisto. Em ambas as coordenações indicadas, de modo diferente, tenho que pensar em como tem sido feita a proteção de dados, o que deve ser disponibilizado ou o que tem que ser permeado pela confidencialidade. E isso significa atentar-se para o que tem sido caracterizado por Gestão de Riscos e também de Conformidade. Não sei se minha reflexão caminha na direção correta, penso que tal tema e Resolução deveria sempre ser debatidos com pessoas que assumem cargos de gestão, retomados sempre que ocorrerem mudanças de gestores. Eu confesso que o pouco do conhecimento que tive foi procurando muito nas orientações da UnB. E também marquei as vezes porque, estando em comissões para a organização do PPP do Programa de Pós-Graduação da Faculdade de Educação, tanto na comissão do Acadêmico (PPGE) quanto na do Profissional (PPGE-MP), tenho feito a reflexão das informações à luz do Plano de Desenvolvimento Institucional da UnB (PDI).
26	Quanto a negociações via nete.
38	Tempo.



Resposta	Contagem	Percentagem
Sim (Y)	8	53.33%
Não (N)	7	46.67%
Sem resposta	0	0.00%

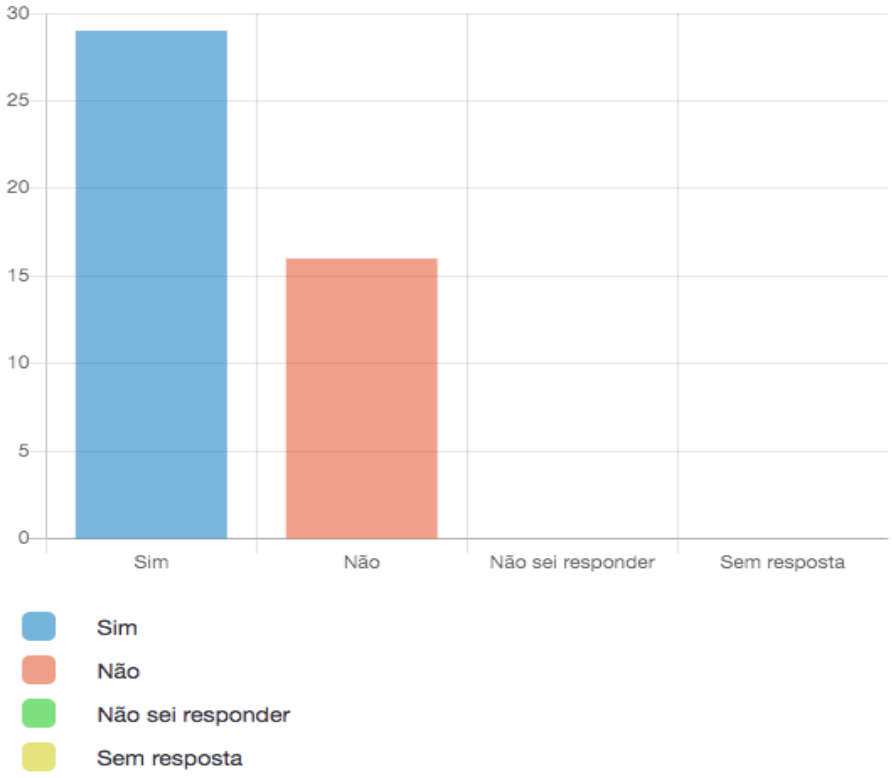


Resposta	Contagem	Percentagem
e-mail (A1)	6	75.00%
Boletim, Sistema Eletrônico de Informações (SEI) (A2)	1	12.50%
Colega ou gestor (A3)	1	12.50%
Não fui informado institucionalmente (A4)	0	0.00%
Outros	0	0.00%
Sem resposta	0	0.00%



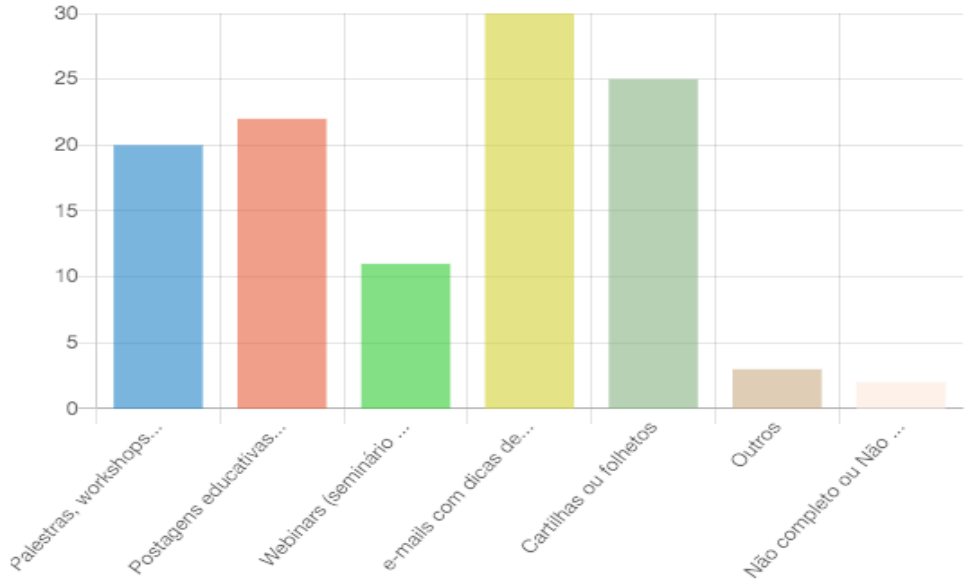
Resposta	Contagem	Percentagem
Sim (Y)	1	6.67%
Não (N)	14	93.33%
Sem resposta	0	0.00%

Eu já sofri algum incidente de segurança digital, como vazamento de senhas, golpes online, invasões de privacidade, recebimento de e-mails suspeitos, clonagem de cartão de crédito, invasão de redes sociais, golpes por mensagens de texto, ataques de phishing, instalação de software malicioso, ligações de fraudadores ou acesso não autorizado a algum dos meus dispositivos?



Resposta	Contagem	Percentagem
Sim (A1)	29	64.44%
Não (A2)	16	35.56%
Não sei responder (A3)	0	0.00%
Sem resposta	0	0.00%

Quais meios de conscientização você prefere para futuras ações relacionadas à política de segurança da informação e comunicação da UnB? (Você pode assinalar várias opções).



- Palestras, workshops, minicursos
- Postagens educativas em redes sociais
- Webinars (seminário online em vídeo, gravado ou ao vivo)
- e-mails com dicas de segurança
- Cartilhas ou folhetos
- Outros
- Não completo ou Não à mostra

Resposta	Contagem	Percentagem
Palestras, workshops, minicursos (SQ001)	20	44.44%
Postagens educativas em redes sociais (SQ002)	22	48.89%
Webinars (seminário online em vídeo, gravado ou ao vivo) (SQ004)	11	24.44%
e-mails com dicas de segurança (SQ005)	30	66.67%
Cartilhas ou folhetos (SQ006)	25	55.56%
Outros	3	6.67%

ID	Resposta
8	aplicativos de autoaprendizagem que orientem o usuário a aprimorar suas estratégias de segurança.
10	Contato dos profissionais do setor em reuniões de colegiados (departamento, conselhos, pós-grauação, etc.), para maiores esclarecimentos e conscientização.
16	Mecanismos rápidos, dinâmicos, assíncronas e privipakmente organizado em algum site ou repositório que possam ser facilmente encontrados.