Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas
Departamento de Administração

DANIELA ALMEIDA

CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA: ESTUDO BASEADO NA PERCEPÇÃO DE TRABALHADORES DE UMA ORGANIZAÇÃO PÚBLICA FEDERAL BRASILEIRA

Brasília – DF
2023

DANIELA ALMEIDA

CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA: ESTUDO BASEADO NA PERCEPÇÃO DE TRABALHADORES DE UMA ORGANIZAÇÃO PÚBLICA FEDERAL BRASILEIRA

Monografia apresentada ao Departamento de Administração como requisito parcial à obtenção do título de Bacharel em Administração.

Professor Orientador: Doutor Carlos André de Melo Alves

Brasília – DF

2023

DANIELA ALMEIDA

CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA: ESTUDO BASEADO NA PERCEPÇÃO DE TRABALHADORES DE UMA ORGANIZAÇÃO PÚBLICA FEDERAL BRASILEIRA

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Conclusão do Curso de Administração da Universidade de Brasília do (a) aluno (a)

Daniela Almeida

Dr. Carlos André de Melo Alves
Professor-Orientador

Dra Fabiana Freitas Mendes
Professora-Examinadora

Dr. Rafael Rabelo Nunes
Professor-Examinador

Brasília, 14 de fevereiro de 2023

Dedico este trabalho à família, base da existência e de toda a trajetória até aqui percorrida. À honrosa Organização Pública Federal que me permitiu esse intenso aprendizado.

AGRADECIMENTOS

Agradeço, preliminarmente, ao professor orientador, Dr. Carlos André de Melo Alves, pelos preciosos ensinamentos, pelas inestimáveis orientações, pela compreensão, paciência e todo apoio ao longo deste trabalho. É um privilégio ter recebido sua orientação.

Ao Diretor de Gestão Operacional e ao Coordenador Geral de Tecnologia e Gestão da Informação da Organização Pública Federal estudada, pelo patrocínio da pesquisa e pelo apoio incondicional em cada etapa.

RESUMO

O objetivo geral deste trabalho foi investigar a percepção sobre conscientização em segurança cibernética de trabalhadores de uma organização pública federal brasileira. Realizou-se pesquisa descritiva, com abordagem quantitativa. Coletaram-se dados primários com aplicação, via internet, de questionário com 13 perguntas, previamente testado e baseado no estudo de Ngoma (2019), obtendo-se a percepção de 109 trabalhadores. Subsidiariamente, consultaram-se documentos públicos da referida organização, alusivos à segurança cibernética. Trataram-se dados empregando recursos de estatística descritiva. Os principais resultados indicaram que 97,25% dos respondentes reconhecem impactos negativos das ameaças à segurança cibernética para a organização e 94,50% deles sinalizaram que a comunicação frequente dessas ameaças motiva-os a adotarem práticas online seguras. Contudo, 80,73% do total de respostas indicaram a percepção de que a organização nunca ou raramente promove treinamentos sobre segurança cibernética, e 61,47% dos respondentes indicando a percepção de que desconhecem ou não têm ciência de política formal de segurança cibernética, apesar de as fontes secundárias evidenciarem a existência de treinamento e de tal política. Este estudo pode auxiliar o aprimoramento da estratégia de conscientização em segurança cibernética da organização estudada, podendo contribuir para reflexões de gestores, acadêmicos e demais interessados na percepção sobre conscientização em segurança cibernética de organizações públicas brasileiras.

Palavras-chave: segurança cibernética, conscientização sobre segurança cibernética, organizações públicas.

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

CIS – Center for Internet Security

ENISA – European Union Agency for Cybersecurity

GSI / PR – Gabinete de Segurança Institucional da Presidência da República

IA – Inteligência Artificial

IoT – Internet das Coisas

ISO – International Standardization Organization

ITU - International Telecommunication Union

ME - Ministério da Economia

NIST - National Institute of Standards and Technology

OCDE - Organização para a Cooperação do Desenvolvimento Econômico

OEA – Organização dos Estados Americanos

PNI – Plano Nacional de Imunização

PSI - Política de Segurança da Informação

SISP – Sistema de Administração de Recursos de Tecnologia da Informação

STJ – Superior Tribunal de Justiça

TCU – Tribunal de Contas da União

TI – Tecnologia da Informação

TIC – Tecnologia da Informação e Comunicação

USB – Universal Serial Bus (porta serial universal)

SUMÁRIO

1 INTRODUÇÃO

1.1. Contextualização

A universalização do acesso à internet, a digitalização de serviços, a exponencial expansão das tecnologias digitais no dia a dia de bilhões de pessoas pelo mundo, proporcionam fácil e rápido acesso a informações, facilidades e celeridade inéditas no atendimento de diversas demandas (MAMBILLE; MBOGORO, 2020).

Entretanto, na mesma proporção, ameaças cibernéticas têm aumentado, o que acarreta no crescimento das tentativas de ataques cibernéticos, tanto em números quanto em sofisticação (ITU, 2020). O sucesso dessas empreitadas maliciosas implica na exposição de informações sensíveis, roubo de dados, perda de informações críticas e vultosos prejuízos financeiros a pessoas e a organizações (WIRTZ; WEYERER, 2017).

Para este trabalho, a expressão “conscientização em segurança cibernética” será definida conforme Ngoma (2019) como um conjunto de estratégias de educação e aculturamento de usuários dos recursos de TI, visando a disseminar conhecimento sobre as ameaças cibernéticas, os seus impactos sobre o seu dia a dia e sobre os ativos da organização e desenvolvimento de comportamento online.

A conscientização em segurança cibernética pressupõe atenção centrada nos colaboradores usuários de rede das organizações (ANDRONACHE, 2021). Contudo, o fator humano não tem sido considerado o elo mais fraco da segurança da informação, posto que o suporte da organização, por meio de informação (comunicação), também, pode estar relacionado com a exposição de entidades a ataques cibernéticos (KHANDO; et al., 2021).

A emergência de saúde pública em razão da Pandemia da COVID 19 acelerou a incorporação de tecnologias e da internet na rotina do serviço público, materializando-se a partir do emprego do trabalho remoto nas organizações públicas brasileiras, especialmente a partir de 2020. A dependência da tecnologia da informação e comunicação intensificou-se no período (ANDREASSON et al, 2021), sendo considerada para a execução das atividades nessas organizações.

Ante o contexto descrito, depreende-se que a questão de segurança cibernética nas organizações é central para a proteção dos negócios (ativos críticos) e preservação ou incremento do valor de mercado (BERKMAN et al, 2018). No

contexto das organizações públicas, trata-se de fator crítico para a preservação de ativos e informações sensíveis, essenciais à sustentação das políticas públicas e à segurança de estado (BRASIL, 2020).

No Brasil, especificamente, a transformação digital como política de estado também impulsionou, nos últimos anos, o acesso a serviços públicos digitais - com celeridade e módicos custos para os cidadãos usuários, e economia de insumos às organizações públicas. No ano de 2021 o país estava posicionado em 7º lugar na oferta de serviços digitais (BRASIL, 2021).

Na mesma proporção em que a internet e os serviços digitais permearam e estão onipresentes na vida e no trabalho, cresceu a superfície de exposição a ataques cibernéticos, sequestro de dados, roubos e vazamentos de informações (BRASIL, 2021).

Diante das ameaças cibernéticas, gestores públicos devem investir mais esforços e recursos para o enfrentamento das ameaças cibernéticas, por meio de mitigação de vulnerabilidades, aquisição de soluções de segurança, adoção de práticas de segurança cibernética, publicação de normas e diretrizes para o uso seguro dos recursos de TI (BRASIL 2020).

Considerando as organizações públicas, diversas iniciativas e ações de aprimoramento da segurança cibernética, integrantes de planos e políticas de segurança da informação aderentes às diretrizes do governo, devem ser adotadas, visando à proteção de dados, informações e ativos críticos (BRASIL, 2021). Nessa linha, a conscientização em segurança cibernética de trabalhadores do setor público é fator crítico de sucesso, reverberado entre as fontes de melhores práticas em segurança cibernética (BRASIL, 2020, 2022; ITU, 2020; CIS, 2021).

Vários métodos de conscientização em segurança cibernética foram mapeados (KHANDO et al. 2021) e a efetividade é condicionada a diversos fatores, sejam individuais, organizacionais, tecnológicos, etc. No setor público, a política de segurança da informação - PSI ganha destaque em efetividade (OEA, 2020). No âmbito do governo federal, a instituição de PSI é obrigatória por determinação do Decreto Federal nº 9.637, de 26 de dezembro de 2018.

Tendo em vista que conscientização em segurança cibernética de trabalhadores do setor público compreende diversos fatores, com diversos graus de sucesso na efetiva proteção de sistemas e informações organizacionais (NGOMA; KEEVY; RAMA, 2021; MAMBILLE; MBOGORO, 2020; NIKOLOVA, 2017), impende

compreendê-la no contexto das organizações públicas, para decisões assertivas sobre estratégias de adesão, responsabilização e conformidade em segurança da informação e comunicações.

1.2. Formulação do problema

A conscientização em segurança cibernética de trabalhadores em organizações é fator crítico de sucesso para as políticas de segurança cibernética institucional (ITU, 2020; CIS, 2021). O fator humano constitui a maior vulnerabilidade e, ao mesmo tempo, a maior fortaleza da segurança cibernética (ANDRONACHE, 2021).

As crescentes tentativas de ataque, o impacto negativo – e mesmo desastroso – dos incidentes cibernéticos e as pressões regulatórias do governo e da sociedade impõem às organizações públicas e privadas atenção, priorização e investimentos na conscientização em segurança cibernética de trabalhadores (BERKMAN et al, 2018).

Por outro lado, é relevante destacar que, é reconhecida a crescente vulnerabilidade do ambiente cibernético de uma organização em proporção inversa à experiência em tecnologia da informação dos respectivos trabalhadores (NGOMA, 2019; HANEY; JACOBS; FURMAN, 2022).

No âmbito das organizações públicas, a preocupação com as ameaças cibernéticas e os impactos de incidentes recentes – como o ataque cibernético sofrido pelo Ministério da Saúde em dezembro de 2021 – elevam, a alto grau de priorização e investimentos, as ações de conscientização dos trabalhadores dessas instituições (CIS, 2021; BRASIL, 2022).

Destaque-se que, na administração federal brasileira, já existe um arcabouço normativo robusto para incrementar e aprimorar a conscientização em segurança cibernética de trabalhadores das organizações públicas (OEA, 2020; BRASIL, 2022).

O Gabinete de Segurança Institucional - GSI/PR e o Tribunal de Contas da União - TCU também disponibilizam orientações técnicas, cartilhas de conscientização em segurança cibernética e promovem eventos para servidores e colaboradores do setor público, com o objetivo de fortalecer as iniciativas de segurança cibernética e proteção de ativos críticos (BRASIL, 2018; BRASIL, 2020).

Tendo em vista que as ameaças cibernéticas se expandem à medida que a

internet se massifica nos países (NGOMA, 2019); que, em organizações públicas e privadas, os trabalhadores constituem, ao mesmo tempo, a maior preocupação e uma das principais salvaguardas de segurança cibernética (ANDRONACHE, 2021) e que a qualificação e o conhecimento dos trabalhadores sobre práticas online seguras são indispensáveis ao incremento da conscientização em segurança cibernética (PETERSEN, 2020), existe a necessidade de estudos sobre as formas com que os trabalhadores são estimulados a práticas online seguras.

As organizações públicas, portanto, devem persistir e aumentar as medidas de segurança e conscientização de segurança cibernética dos respectivos trabalhadores. Ante ao exposto, coloca-se como problema central desta pesquisa: **Qual é a percepção sobre conscientização em segurança cibernética de trabalhadores em uma organização pública federal brasileira?**

1.3. Objetivos

1.3.1. Objetivo Geral

Investigar a percepção sobre conscientização em segurança cibernética de trabalhadores em uma organização pública federal brasileira.

1.3.2. Objetivos Específicos

- Objetivo Específico 1 (OE1): Identificar a percepção de trabalhadores em uma organização pública federal brasileira sobre as principais ameaças à segurança cibernética, com base na revisão de literatura;
- Objetivo Específico 2 (OE2): Descrever a percepção desses trabalhadores sobre conscientização em segurança cibernética, com base na revisão de literatura;
- Objetivo Específico 3 (OE3): Comparar a percepção previamente descrita sobre conscientização em segurança cibernética segundo a área de atuação do trabalhador na organização pública federal brasileira.
- Objetivo Específico 4 (OE4): Diferenciar a percepção previamente descrita de trabalhadores segundo sua experiência prévia em Tecnologia da Informação.

1.4. Justificativa

A relevância do tema proposto encontra guarida no papel estruturante das

soluções de tecnologia da informação e comunicações e serviços online setor público, que exigem proteção robusta e efetiva contra vazamentos e ataques hackers (WIRTZ; WEYERER, 2017). Ações abrangentes e multifocais, que fortaleçam a segurança cibernética, devem promover proteção de dados de forma sustentada, assegurando integridade, confiabilidade e continuidade dos serviços e dados (BRASIL, 2018).

Devido à criticidade do fator humano no sucesso de estratégias de segurança cibernética, é fundamental compreender a percepção de trabalhadores sobre o assunto, especialmente em organizações públicas, onde as mudanças estão sujeitas a ocorrer em ritmo mais lento (BACUD; MASES, 2021). Dessa forma, este trabalho busca, com os resultados obtidos, nortear estratégias de aprimoramento da segurança cibernética em organizações públicas.

Ademais, a conscientização em segurança cibernética de trabalhadores constitui fator crítico de sucesso de qualquer estratégia de proteção e continuidade dos serviços digitais (KARAGOZLU, 2020). Esse aspecto, em razão de interferências de natureza individual, social, cultural e organizacional, constitui desafio à implantação de estratégias, políticas e soluções de proteção contra ataques cibernéticos (CATOTA; MORGAN; SICKER, 2019).

Ressalte-se, que este estudo pode auxiliar o aprimoramento da estratégia de conscientização em segurança cibernética da organização estudada. O tema ainda é relativamente recente, e estudos a respeito dessa conscientização em organizações públicas são escassos (KHANDO et al. 2021), inclusive por meio de coleta da percepção de trabalhadores dessas organizações sobre esse tema (NGOMA, 2019).

Por fim, este estudo pode contribuir para a atuação de diversas esferas decisórias (KHANDO et al., 2021) e interessados. Em outras palavras, este trabalho pode contribuir para reflexões de gestores públicos, pesquisadores e demais partes interessadas na percepção sobre conscientização em segurança cibernética de organizações públicas no Brasil.

2 REVISÃO TEÓRICA

2.1 Segurança cibernética:

Karpiuk (2021) define segurança cibernética como um rol de atividades necessárias à proteção de redes e sistemas computacionais, (assim como os respectivos usuários e outras pessoas) contra ameaças cibernéticas. Adicionalmente, verifica-se convergência entre autores à ideia de proteção contra ameaças cibernéticas, assim como ao conhecimento e uso de ferramentas e demais instrumentos para a proteção de informações e dados de pessoas no ambiente cibernético (KARAGOZLU, 2020).

Segundo o Glossário de Segurança da Informação, segurança cibernética compreende o seguinte:

> ações voltadas para a segurança de operações, visando a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis (BRASIL, 2021, p. 44).

A segurança cibernética objetiva assegurar a existência e perenidade da “Sociedade da Informação de uma nação” por meio da proteção do espaço cibernético, os respectivos ativos de informação e infraestruturas críticas (BRASIL, 2010).

Iniciativas de segurança cibernética proporcionam proteção adicional a sistemas de informação de atividades que violem os atributos básicos dos dados processados: integridade, autenticidade, confidencialidade, acessibilidade. Tais iniciativas, inclusive, podem abranger a proteção de todos os ativos, inclusive pessoas (KARAGOZLU, 2020).

O escopo da segurança cibernética transcende sistemas de informação. Abrange os novos dispositivos e equipamentos eletrônicos contra as mais variadas ameaças (acesso não autorizado, desvios, fraudes, sequestro de dados, etc.); e, também, aborda as novas tecnologias, como Internet das Coisas – IoT, Inteligência Artificial – IA, entre outras (TIRUMALA; VALLURI; BABU, 2019).

O entendimento das ameaças no ambiente cibernético demanda trabalho intensivo e proporciona aprendizado contínuo. Os times de trabalhadores da segurança cibernética - e os respectivos planos de ação - devem possuir os seguintes atributos para eficácia e efetividade (PETERSEN, 2020).:

- agilidade (adaptação tempestiva às mudanças);
- flexibilidade (visando às soluções adequadas à organização);
- interoperabilidade (se possível, adoção de uma linguagem comum nas

políticas e soluções); e

- modularidade (abordagem de riscos em segurança cibernética que transcenda essa área de atuação).

Boas práticas em segurança cibernética pressupõem planejamento, organização e documentação de procedimentos para gerir, manter e recuperar serviços críticos em caso de interrupção indesejada. Também é imprescindível a qualificação técnica e atualização contínua da força de trabalho (PETERSEN, 2020).

Princípios e diretrizes de segurança cibernética estão consolidados em documentos de melhores práticas ou frameworks. Quase todas as orientações se aplicam aos setores público e privado – ainda que sejam necessárias adaptações (KHANDO et al, 2021). O Quadro 1, a seguir, associa conceitos de segurança cibernética a alguns dos frameworks adotados nos setores público e privado.

Quadro 1 - Definições de Segurança Cibernética Segundo Frameworks

Framework	Definição
CIS V8	Ecossistema no espaço cibernético onde se aplicam, mensuram e monitoram os controles destinados a evitar e mitigar ameaças cibernéticas
NIST	Capacidade de proteger ou defender o uso do espaço cibernético de ataques e crimes cibernéticos
ISO 27032:2015	Proteção de privacidade, integridade e acessibilidade de informações no espaço cibernético

Fonte: elaborado pela autora a partir de CIS (2021), NIST (2019), ABNT (2015)

No enfrentamento às ameaças e crimes cibernéticos – estes últimos entendidos como crimes realizados no espaço cibernético contra ativos ou pessoas, e qualificados conforme leis locais - a segurança cibernética alia-se aos mecanismos prescritivos e normas existentes (o arcabouço legal) para tipificação e combate com o apoio da autoridade judicial (MAMBILE ; MBOGORO, 2020).

As ameaças cibernéticas, segundo o Global Security Risk (ITU, 2020) e o ENISA (2021), a cada ano se renovam, se aprimoram e são reinventadas. À medida que a tecnologia avança e permeia o dia a dia dos cidadãos, as ameaças cibernéticas ganham relevância e atenção de mitigação e enfrentamento.

Embora haja inovação entre os incidentes cibernéticos - tais como os algoritmos de aprendizagem de máquina nos *ransomwares* mais recentes (ABNT, 2015) – exemplos de ameaças reportadas por instituições governamentais estão relacionadas no Quadro 2.

Quadro 2 – Exemplos de Ameaças Cibernéticas no Setor Público

Ameaça cibernética	definição
Ransomware	Modalidade de ataque cibernético comum (ENISA, 2021; PWC, 2022), que explora vulnerabilidades. O agente invasor sequestra e criptografa o sistema da vítima (inclusive o disco rígido); posteriormente, exige resgate em dinheiro (criptomoedas) para supostamente fornecer a chave de descriptografia dos dados.
Malware	Trata-se de um software malicioso (também identificado como vírus ou Trojan) que pode capturar credenciais, roubar dados, identificar outros alvos na rede e criptografar ou destruir dados, entre outros danos. Ele infiltra-se na organização por meio de um agente invasor que explora vulnerabilidades em dispositivos de usuário final, anexos de e-mail, páginas da web, serviços em nuvem, dispositivos móveis e mídias removíveis.
Phishing	Consiste num ataque por e-mail (ou outra forma de interação por meio eletrônico) capaz de enganar o destinatário, apelando para determinado interesse em informação. Trabalhadores do setor público que não adotem cautelas ou não estejam precavidos podem abrir anexos de e-mail ou mensagens eletrônicas e ficar exposto aos efeitos desse tipo de ameaça.

Fonte: elaborado pela autora a partir de CIS (2021), (ENISA, 2021; PWC. 2022)

Entre as ameaças cibernéticas existentes na atuação das organizações públicas, ataques de *ransomware* são comuns e têm ocasionado prejuízos de bilhões de dólares a instituições públicas e privadas pelo mundo. Figura entre os tipos de ameaça mais sérios para organizações de todos os portes e para infraestruturas críticas (SYMANTEC, 2021)

Ataques de *ransomware* ocorridos apresentam repercussão - a exemplo do incidente no Tribunal de Justiça do Rio Grande do Sul em abril de 2021 (BRASIL. GSI/PR, 2022), Ministério da Saúde em 2020 (FERNANDES, 2022),

Algumas práticas de baixa maturidade em segurança cibernética - acesso remoto desprotegido, ativos e aplicativos vulneráveis, não emprego de múltiplo fator de autenticação - MFA, usuários com privilégios de acesso desnecessários, entre outros (BRASIL, 2022) podem facilitar os ataques de criminosos cibernéticos.

Quanto à ameaça de malware, está relacionada com a ausência ou insuficiência de consciência sobre segurança cibernética. O comportamento inseguro do usuário final (como clicar em links, abrir anexos, instalar software ou perfis, ou inserir unidades flash USB) aumentam as vulnerabilidades ao malware. (CIS, 2021)

As ameaças pelo *malware* foram as mais citadas por gestores e operadores de ações relativas à segurança cibernética em 2021 e 2022 (CYBEREDGE, 2022) como preocupação na gestão dos respectivos serviços. Variantes de malware são projetadas para evitar, enganar ou desabilitar as defesas. (NGOMA, 2019).

Entre as vulnerabilidades mais exploradas por *malware*s, estão navegadores sem filtro de conteúdo ou bloqueadores de pop-ups. Ausência de filtros

de spam e de ferramentas para verificação de *malware* nas soluções de correio eletrônico (CIS, 2021). A ausência de políticas de gestão de dispositivos externos (tais como discos externos USB) também expõe ativos e usuários a ataques de *malware*s.

Os ataques de *phishing* podem contribuir para a expansão de crimes cibernéticos, e para apropriação ilegal de dados confidenciais (NGOMA, 2019). Apoiados por táticas de engenharia social, atacantes miram organizações públicas com controles insuficientes de segurança (HUTTON, 2017), induzem usuários a clicarem em links que contêm arquivos maliciosos ou páginas fraudulentas.

Conforme BRASIL (2021), engenharia social é uma técnica de persuasão, empregada para que o usuário execute determinadas ações. É uma prática de má-fé de abuso de confiança dos indivíduos com o objetivo de aplicar golpes, ludibriar ou obter informações sigilosas e importantes

As vítimas de *phishing* são ludibriadas por mensagens fraudulentas, que induzem ao acesso a sites falsos e requisitam dados sensíveis. A grande dependência de usuários de redes dos serviços de correio eletrônico, torna-os vulneráveis a ataques de *phishing*. (NGOMA; KEEVY; RAMA, 2021). Nesse sentido, ENISA (2021) asseverou que a ameaça de *phishing* está no cerne dos ataques de desinformação.

Para mitigar e evitar esses ataques e incidentes cibernéticos, em geral os frameworks de segurança convergem em recomendar a conscientização de usuários em segurança cibernética. Urge fomentar o comportamento correto de trabalhadores das organizações, um manejo correto de arquivos e a identificação de links suspeitos (CIS, 2021; BRASIL, 2022).

Em razão da eficiência de alguns ataques de phishing com o uso de técnicas da engenharia social mais elaboradas, empresas líderes em segurança cibernética têm investido em soluções de conscientização para usuários por meio de simulações de *phishing*, tais como *Automated Security Awareness Program* – ASAP e *Cybersecurity Awareness Training Models* – CAT (HIJJI, 2022; NAG et al., 2022)**.**

2.2 Segurança cibernética no setor público

O aprimoramento da segurança cibernética no setor público ganhou relevância posteriormente ao início das preocupações, no setor privado (KHANDO et al, 2021). Segundo Ngoma, Keevy e Rama (2021), essa preocupação aumentou após o incidente cibernético, de grande impacto e duração de meses, contra o governo da Estônia em 2007.

O incidente, citado no parágrafo anterior, consistiu na orquestração de negação de Serviço distribuída (Distributed Denial of Service - DDoS com uso de redes de computadores infectados - botnets), que paralisou sistemas e privou milhões de cidadãos de serviços públicos dependentes da internet e de sistemas de informação, por muitas semanas (NGOMA, 2019).

A partir desse episódio, lições aprendidas foram implementadas e os governos na Europa e América do Norte aprimoraram as estratégias de segurança cibernética nas esferas estatal e privada (European Union Agency for Cybersecurity - ENISA, International Telecommunication Union - ITU, Organização para Cooperação do Desenvolvimento Econômico - OCDE, etc.) (NGOMA, 2019).

A partir do episódio do Governo da Estônia, orientações e guias foram editados e publicados para fortalecer o intercâmbio de informações e o combate às ameaças cibernéticas, tais como ENISA Threats Landscape, ITU National Cybersecurity Strategy Guide (NGOMA, 2019) e OCDE (2020).

No continente americano, Estados Unidos e Canadá foram pioneiros na implantação de programas de segurança cibernética no contexto governamental. Algumas boas práticas decorrem dessas iniciativas, tais como as diretrizes da National Initiative for Cyber Security Education - NICE (NGOMA, 2019).

A Organização dos Estados Americanos - OEA foi responsável por iniciativas e fóruns colaborativos dos governos para enfrentamento de ameaças cibernéticas, a exemplo da Estratégia Interamericana Integral para Combater as Ameaças à Segurança Cibernética (BRASIL, 2010; TIRUMALA; VALLURI; BABU, 2019).

No entanto, apesar da grande disponibilidade de orientações, diretrizes e melhores práticas de segurança cibernética, ainda persistem fragilidades nos espaços cibernéticos de organizações públicas (TIRUMALA; VALLURI; BABU, 2019). Alguns fatores peculiares ao setor público parecem dificultar a implantação efetiva da segurança cibernética (WIRTZ; WEYERER, 2017).

Em razão de interferências políticas e da estrutura burocrática, a implementação de inovações em segurança cibernética no setor público é mais lenta (BACUD; MÄSES, 2021), e esse fator pode aumentar a vulnerabilidade dos sistemas de informação institucionais a ataques cibernéticos (NGOMA; KEEVY; RAMA, 2021).

Os governos atualmente devem ser capazes de gerenciar e reduzir as vulnerabilidades e danos em incidentes cibernéticos complexos. Também, precisam tomar decisões ágeis, e escolher rapidamente alternativas de solução, ainda que com informações insuficientes (NIKOLOVA, 2017).

Diversas publicações apontaram aspectos da implantação das ações de segurança cibernética no setor público que sugerem a necessidade de reflexão. Wirtz e Weyerer (2017) evidenciaram que as organizações públicas são alvos preferenciais de ataques cibernéticos, tanto pelo valor econômico, comercial ou político dos ativos expostos quanto pelas fragilidades de controles e de conhecimento de trabalhadores dessas organizações.

Mambile e Mbogoro (2020) destacam que o desconhecimento de trabalhadores do setor público sobre práticas e normas de segurança cibernética constituem significativa vulnerabilidade. Wirtz e Weyerer (2017) apontam que os gestores e autoridades decisórias são essenciais para a gestão de segurança cibernética no setor público.

Nessa linha, Ngoma (2019) também destaca a liderança de dirigentes de organizações públicas para a implantação efetiva de iniciativas de segurança cibernética como definitiva para o sucesso. Devido ao potencial de danos de ataques bem-sucedidos, a segurança cibernética nas organizações públicas está entre as mais críticas esferas de preocupação estatal.

No Brasil, além da participação em fóruns internacionais voltados à segurança cibernética – desde 2004, quando a OEA adotou e Estratégia Interamericana Integral para Combater as Ameaças à Segurança Cibernética, – houve diversas iniciativas internas voltadas à proteção e fomento da cultura de segurança cibernética entre trabalhadores e usuários de serviços públicos (BRASIL 2010).

Como exemplo de iniciativa citada no parágrafo anterior, em 2010 o governo brasileiro assumiu a segurança cibernética como uma função estratégica do Estado e indispensável à proteção das infraestruturas críticas - energia, transportes, telecomunicações, abastecimento de água, finanças, entre outros (BRASIL 2010).

As instâncias executivas do governo brasileiro implantaram um arcabouço normativo de incentivo à cultura da segurança cibernética no poder público. Tribunal de Contas da União e Presidência da República (por meio do Gabinete de Segurança Institucional - GSI) instituíram políticas de segurança cibernética e organizaram estruturas de gerenciamento da segurança cibernética e de incidentes cibernéticos (BRASIL, 2020).

A estratégia nacional de segurança cibernética, aprovada pelo Decreto Federal nº 10.222, de 06 de fevereiro de 2020, estabelece iniciativas de melhoria do nível de segurança e maturidade de órgãos federais e estaduais em segurança cibernética – assunto que, desde 2018, tem recebido destaque e relevância perante

órgãos de controle e governo central (BRASIL, 2020).

O Relatório da OEA de Revisão da Capacidade de Cibersegurança do Brasil, de 2020, e a Estratégia de Fiscalização em Segurança da Informação e Segurança Cibernética 2020-2023 do TCU, também, evidenciam a preocupação da administração pública federal brasileira em aprimorar e elevar o grau de maturidade em segurança cibernética BRASIL, 2020).

A atuação do TCU nas orientações para aprimorar a segurança cibernética intensificou-se após os ataques de *ransomware* contra os sistemas do Superior Tribunal de Justiça - STJ em novembro de 2020 e do incidente contra o Ministério da Saúde, em dezembro de 2021, que comprometeu, entre outros, os dados do Programa Nacional de Imunização no Brasil- PNI (FERNANDES, 2021).

Uma das iniciativas foi um trabalho de auditoria no contexto de segurança ou vulnerabilidades cibernéticas dos órgãos e entidades do poder executivo federal. Esse trabalho resultou no Acórdão nº 1768/2022-Plenário, que detectou insuficiente resposta da maioria das entidades auditadas a incidentes cibernéticos (BRASIL, 2022).

As boas práticas de segurança cibernética, observadas pelo TCU e invocadas no acórdão 1768/2022 – TCU - Plenário, destacam a necessidade de consolidação da cultura da segurança cibernética - que consiste em ações e iniciativas continuadas de conscientização de trabalhadores e usuários de sistemas de informação governamentais (BRASIL, 2022).

2.3 Conscientização sobre segurança cibernética no setor público

A ocorrência de incidentes cibernéticos pode ser facilitada pelo comportamento descuidado de usuários (ANDRONACHE, 2021). Tal descuido, por sua vez, pode decorrer do desconhecimento em relação às práticas de prevenção de ataques (NGOMA, 2019; BACUD; MÄSES, 2021). Nesse contexto, as políticas e iniciativas de segurança cibernética devem priorizar a conscientização em segurança cibernética de usuários, trabalhadores e colaboradores das organizações.

Há muitas definições para conscientização em segurança cibernética; existem convergências sobre assuntos nevrálgicos, como a disseminação de conhecimento, sensibilização de usuários do espaço cibernético, treinamento e responsabilização pelo uso correto e observação de cautelas para evitar exposição da rede aos ataques cibernéticos (SHERE; NURSE; MARTIN, 2022; BACUD; MÄSES, 2021).

A conscientização em segurança cibernética pode ser entendida como um

conjunto de instrumentos voltados a influenciar o comportamento online seguro de trabalhadores (ALGAMDHI; WIN; VLAHU-GJORDIEVSKA, 2022). Também pressupõe atenção centrada nos colaboradores usuários de rede das organizações (ANDRONACHE, 2021); porém, o fator humano não tem sido considerado o elo mais fraco da segurança da informação, posto que o suporte da organização, por meio de informação (comunicação), também, pode estar relacionado com a exposição de entidades a ataques cibernéticos (KHANDO et al. 2021).

Conscientização em segurança cibernética também se compreende como o nível de apropriação, compreensão ou conhecimento de segurança cibernética quanto aos aspectos de riscos e ameaças cibernéticas e quanto às medidas de prevenção e proteção adequadas (NURSE, 2021). A conscientização sobre segurança cibernética proporciona aos usuários de TIC as informações necessárias para reconhecer ameaças cibernéticas e a forma de lidar com elas (NGOMA, 2019).

Existem várias formas de se aplicar a conscientização em segurança cibernética para trabalhadores de organizações. Nikolova (2017), Bacud e Mäses (2021) e Mambille e Mbogoro (2020) enumeram programas de treinamento formal, comunicação de normas e mecanismos de punição pelas atitudes desconformes dos usuários, soluções tecnológicas de alertas educativos, jogos virtuais “sérios” voltados ao conhecimento e lide com as ameaças e ataques, monitoramento ostensivo do uso de dispositivos no espaço cibernético corporativo, entre outros.

A NBR ISO/IEC 27032:2015 entende conscientização em segurança cibernética como um conjunto de práticas de treinamento e aperfeiçoamento de funcionários e colaboradores, sobre competências voltadas à segurança no espaço cibernético - reiteradas e atualizadas, em linha com os avanços tecnológicos das ameaças e ataques. Recomendam-se conteúdos direcionados, tais como:

- conhecimento das ameaças mais recentes e as formas de ataques de engenharia social (por exemplo, como o *phishing* evoluiu de sites falsos isolados para uma combinação de Spam, *Cross site scripting* e ataques de injeção de SQL);
- esclarecimentos sobre como ataques de engenharia social podem manipular ou roubar informações individuais e corporativas, como os invasores podem se aproveitar da tendência natural humana de obedecer a pedidos feitos com autoridade (embora possam ser irreais), comportamento amigável, posando como vítima e reciprocidade, primeiro dando algo de valor ou ajuda;
- entendimento sobre qual informação precisa ser protegida e como protegê-la, conforme a política de segurança cibernética;
- orientações para relatar, denunciar ou alertar as instâncias pertinentes -

sejam as autoridades ou agências – sobre um evento suspeito ou aplicativo enganoso; e informações sobre contratos disponíveis. (ABNT, 2015)

Após expor diferentes definições sobre a expressão “conscientização em segurança cibernética”, para os fins deste estudo a referida expressão será entendida conforme citado na introdução, com base em NGOMA (2019).

A referida conscientização em segurança cibernética pode ser uma preocupação em vários níveis de governo (NGOMA, 2019; CATOTA; MORGAN; SICKER, 2019). Como uma estratégia nacional, envolve políticas públicas de educação, campanhas com usuários de serviços públicos digitais, e trilhas de qualificação para trabalhadores de organizações públicas.

Ngoma (2019) consolidou as iniciativas de países por ele indicados como líderes na conscientização em segurança cibernética: Estados Unidos, Reino Unido, Canadá e Austrália. Os propósitos desses países na implementação de políticas e iniciativas são consolidados no quadro a seguir:

Quadro 3: Propósitos Principais de Conscientização em Segurança Cibernética dos Países Líderes

Propósito	Descrição
Desenvolvimento econômico	Prevenção aos ataques e incidentes cibernéticos que acarretam prejuízos bilionários a governos e entidades estatais, bem como manter reputação positiva de estabilidade cibernética para sustentar a relevância do comércio eletrônico na economia nacional
Conhecimento e prevenção de riscos no espaço cibernético	Tem por finalidade proteger infraestruturas críticas governamentais e empresariais
Promoção de uma cultura de segurança cibernética na população	Colaboração dos usuários de serviços digitais, por meio de comportamentos corretos e da prevenção contra ataques cibernéticos

Fonte: elaborado pela autora com base em NGOMA (2019)

Segundo Ngoma (2019), os planos de ação e políticas públicas voltados à conscientização em segurança cibernética são fortalecidos nesses países líderes, que se encontram mais adiantados em níveis de maturidade e dispõem de mecanismos aprimorados de prevenção e enfrentamento de ataques cibernéticos.

Ademais, os usuários devem ter à sua disposição os canais de reporte, notificação ou denúncia de atividades suspeitas no espaço cibernético, de modo a comunicar adequada e tempestivamente potenciais ameaças ou incidentes cibernéticos. (ABNT, 2015; BRASIL, 2022).

No Brasil, a preocupação com conscientização em segurança cibernética no setor público acompanhou os debates internacionais. O Livro Verde de Segurança Cibernética no Brasil destaca o protagonismo do governo brasileiro na articulação

com outras nações para intercâmbio de informações e experiências de prevenção de ameaças e combate aos ataques e crimes cibernéticos (BRASIL, 2010).

Adicionalmente, no País o investimento em educação, qualificação e promoção da cultura de segurança cibernética é assunto de fóruns intergovernamentais. Diferentes iniciativas foram adotadas desde edição de normas até a promoção de eventos educativos em diversas esferas de governo (BRASIL, 2020).

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) desde o final dos anos 1990 editou normas, orientações e instruções voltadas à proteção e manutenção de ativos críticos de tecnologia e informação, e a conscientização em segurança cibernética sempre esteve em pauta. O Quadro 4, a seguir, consolida os atos normativos a serem observados por órgãos e entidades da administração pública no Brasil.

Quadro 4 – Base Normativa sobre Segurança Cibernética no Brasil

Identificação da norma	descrição
Decreto nº 9.637, de 26 de dezembro de 2018	Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.
Decreto nº 10.222, de 05 de fevereiro de 2020	Aprova a Estratégia Nacional de Segurança Cibernética.
Decreto nº 10.748, de 16 de julho de 2021	Institui a Rede Federal de Gestão de Incidentes Cibernéticos.
Portaria Nº 93 GSI/PR, de 18 de outubro de 2021	Aprova o Glossário de Segurança da Informação.
Instrução Normativa GSI Nº 1 - 27 de maio de 2020.	Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.
Instrução Normativa GSI Nº 4 - 26 de março de 2020	Dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G.

Fonte: adaptado de BRASIL, 2018, 2020 e 2021 (acessado em 25/08/2022)

Registre-se que as normas relacionadas no Quadro 4 contemplam referências à divulgação e conscientização de usuários de serviços públicos em segurança cibernética. Adicionalmente, a jurisprudência do TCU recomenda e determina a divulgação de melhores práticas e padrões aceitáveis de comportamento no espaço cibernético, com especial atenção aos gestores das unidades auditadas pelo referido tribunal de contas e aos trabalhadores das organizações públicas (BRASIL, 2022).

Nesse sentido, existe iniciativa do TCU indicando a divulgação da Cartilha

“Cinco controles de segurança cibernética para ontem” (BRASIL, 2022), em continuidade aos trabalhos de acompanhamento do Acórdão nº 1768/2022-TCU-Plenário, que reforça a necessidade de conscientização dos gestores públicos sobre os riscos de ataques e incidentes cibernéticos aos quais se expõem as organizações do setor público, à medida que avançam na transformação digital do país (BRASIL, 2022).

Entre os cinco controles da Cartilha – derivados do citado *framework* CIS V8 – o Controle 14 refere-se à conscientização sobre segurança e treinamento de competências. Esse controle tem o objetivo de reduzir a possibilidade de incidentes oriundos do comportamento humano, decorrentes do uso de engenharia social (CIS, 2021).

O Controle 17 refere-se a gestão de respostas a incidentes, e, também, tangencia a conscientização em segurança cibernética, pois orienta a identificar e a reconhecer ameaças e ataques para o reporte tempestivo e ações eficazes de prevenção, combate e recuperação de dados e sistemas eventualmente afetados. Esse controle é aplicável a todos os stakeholders (BRASIL, 2022).

Os desafios dos gestores de organizações públicas consistem em envolver os trabalhadores como corresponsáveis pela segurança cibernética, promovendo cultura, comportamentos e usos adequados dos recursos de tecnologia disponíveis (BRASIL, 2022). Também, é indispensável a responsabilização desses usuários pelo comportamento que apresentarem (BRASIL, 2020).

No serviço público, os trabalhadores podem ser enquadrados em diversas áreas de atuação conforme a formação e a natureza do serviço: áreas finalísticas (ou negociais), e aqueles que atuam nas áreas-meio. Enquanto os primeiros, conforme Pereira e Souza (2014), exercem atribuições diretamente relacionadas ao negócio da organização, os trabalhadores da área-meio atuam no apoio, de natureza administrativa ou atividades acessórias (BRASIL, 1967).

Atribuições gerenciais e decisórias, também, constituem possíveis recortes demográficos de trabalhadores de organizações públicas. De notar que Ngoma (2019) e Andreasson et al. (2021) estudaram gestores públicos (executivos de unidades administrativas ou gestores de TI das respectivas organizações públicas), Mambile e Mbogoro (2020) enfocaram os trabalhadores de organizações públicas, de modo geral.

Espera-se que, quanto maior a instrução, o nível gerencial, o conhecimento em administração pública do trabalhador e seu tempo de experiência em TI, maior será o grau de conscientização em segurança cibernética, mais célere e eficaz

tende a ser a aprendizagem e aplicação e maior será a colaboração para a segurança cibernética da organização pública (NGOMA, 2019; PETERSEN, 2020; ANDRONACHE, 2021).

O trabalho de Ngoma (2019) procurou captar, por meio de questionários estruturados, a percepção de trabalhadores de organizações públicas da África do Sul. O referido estudo estruturou questionário com base em revisão de literatura. O público-alvo do citado estudo foram gestores de entidades estatais do referido País, com mandato e legitimação para implantar ações de conscientização de segurança cibernética. As perguntas foram organizadas e aplicadas abrangendo as seguintes seções:

- Dados sociodemográficos dos respondentes, com informações gerais dos participantes. Foram levantados o conhecimento, habilidades e experiência em TI, os cargos dos participantes, qualificações e tempo de experiência em TI. Aplicaram-se questões de múltipla escolha e questões com escala Likert.
- Avaliação de ameaças e riscos de segurança cibernética nas organizações do setor público sul-africano. Objetivou-se obter dados sobre a conscientização da segurança cibernética e de ameaças nas organizações do setor público. Foram utilizadas perguntas de múltipla escolha, algumas das quais com escala Likert.
- Avaliação da conscientização em segurança cibernética nas organizações do setor público sul-africano. O objetivo foi compreender a efetividade de iniciativas específicas para a conscientização de segurança cibernética por parte da organização. Aplicaram-se questões de múltipla escolha e de resposta aberta para livre manifestação do entrevistado.

Uma vez que este trabalho busca captar e compreender a percepção de trabalhadores de uma organização pública – da esfera federal, com atuação e presença em todos os estados da Federação – observou-se um paralelismo entre os agentes públicos respondentes no estudo de referência e o público-alvo de organizações públicas atuantes em outros países, inclusive no Brasil.

Assim, nesta pesquisa pretende seguir linha de questões similares à do estudo da África do Sul, em razão da equivalência do objeto de estudo com o trabalho desenvolvido por Ngoma (2019) – trabalhadores de organizações públicas – e da aplicação em organizações estatais de um país em desenvolvimento, integrante do BRICS.

Neste sentido, o estudo conduzido em organizações estatais da África do Sul evidenciou que a maioria das organizações públicas lida com problemas

decorrentes de ameaças à segurança cibernética originárias do uso de internet, Constatou-se, ainda, que os gestores dessas organizações adotam alternativas para comunicar aos usuários sobre ameaças à segurança cibernética, de forma não consistente.

Ademais, Ngoma (2019) demonstrou que o treinamento de conscientização sobre segurança cibernética foi reconhecido por gestores das organizações sul africanas como instrumento relevante para minimizar o impacto das ameaças de segurança cibernética. A falta de treinamento de atualização, por outro lado, é uma preocupação de diversas organizações do setor público.

Por fim, outro achado relevante de Ngoma (2019) foi que a maioria das organizações estatais da África do sul carece de políticas formais de segurança cibernética – que acarreta na ausência de direção política e dificuldade de implementar iniciativas de segurança cibernética efetivas.

3 MÉTODOS E TÉCNICAS DE PESQUISA

3.1 Tipo e descrição geral da pesquisa

Este trabalho decorre de pesquisa do tipo descritiva. A pesquisa descritiva objetiva, primordialmente, categorizar uma população ou fenômeno de interesse, e estabelecer relações entre variáveis (GIL, 2008). Este estudo, também, adotou enfoque quantitativo, em razão da adoção de recursos estatísticos para tratamento dos dados (COLAUTO; BEUREN, 2003).

3.2 Caracterização da Organização objeto do estudo

Este estudo foi realizado em uma organização pública federal brasileira que é uma autarquia e pertence à administração indireta da União. Em suas atividades responde pela execução de políticas de estado definidas pelo poder executivo federal.

Adicionalmente, a referida organização pública integra o Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, instituído pelo Decreto nº 7579 de 11 de outubro de 2011, com o objetivo de organizar a operação, controle, supervisão e coordenação dos recursos de tecnologia da informação da administração direta, autárquica e fundacional. Ademais, a organização pública federal, em termos de gestão de TIC, está sujeita a diretrizes editadas pelo GSI / PR, inclusive quanto a segurança cibernética.

Com base em fontes secundárias utilizadas neste trabalho (Portarias e planos disponíveis no portal institucional), apurou-se que essa Organização pública federal pactuou, em 2020, o Plano de Transformação Digital com o Ministério da Economia e com a Presidência da República, com os objetivos de ampliar a oferta de serviços digitais ao cidadão, acelerar o atendimento e promover a interoperabilidade com as diversas bases de dados do governo.

Possui Política de Segurança da Informação e Comunicações atualizada e publicada e Comitê de Segurança da Informação, constituído e atuante, bem como Equipe de Gestão e Tratamento de Incidentes Cibernéticos - ETIR constituída e atuante.

A organização federal objeto do estudo faz-se presente com sede nacional e unidades físicas com diferentes níveis de autonomia administrativa, em todas as unidades da Federação.

3.3 População e Amostra

3.3.1 População

A população consiste em servidores públicos (efetivos, comissionados, cedidos) e colaboradores (trabalhadores de contratos de terceirização de serviços) que utilizam os serviços de TIC como ferramenta de trabalho, e dependem do acesso à internet para desempenhar suas funções. O Quadro 5, a seguir, mostra a composição de trabalhadores da Organização federal objeto do estudo:

Quadro 5: Composição dos Trabalhadores da Organização Federal Conforme Respectivo Vínculo

Vínculo do trabalhador	quantidade
Servidores públicos (efetivos ou comissionados)	2996
Colaboradores (terceirizados / TEDs)	1899
Total	4895

Fonte: a autora, baseada em Brasil (2022).

Do total dos servidores, 602 atuam nos órgãos da organização, e 2394 atuam nas unidades descentralizadas. Esta informação foi obtida a partir da utilização de filtros de pesquisa do Portal da Transparência da Controladoria Geral da União (BRASIL, 2022), disponível como informação pública.

As unidades da Organização caracterizadas como órgãos na respectiva estrutura regimental foram incorporadas aos filtros de pesquisa, obtendo-se o total de servidores efetivos atuantes nos órgãos da organização. Procedimento semelhante foi adotado para se obter o quantitativo de servidores atuantes nas unidades descentralizadas.

O quantitativo de trabalhadores, também, foi obtido a partir do cruzamento de dados disponíveis no portal da transparência. Tanto os trabalhadores que atuam nas atividades-fim quanto aqueles alocados em atividades-meio, de apoio técnico-operacional e administrativo, são usuários de recursos de TI.

A população que se pretende estudar abrange trabalhadores com e sem função de gestão, bem como os atuantes na área meio quanto na área fim, em razão das diretrizes e recomendações dos frameworks de segurança cibernética (BRASIL, 2022; CIS, 2021; PETERSEN, 2020).

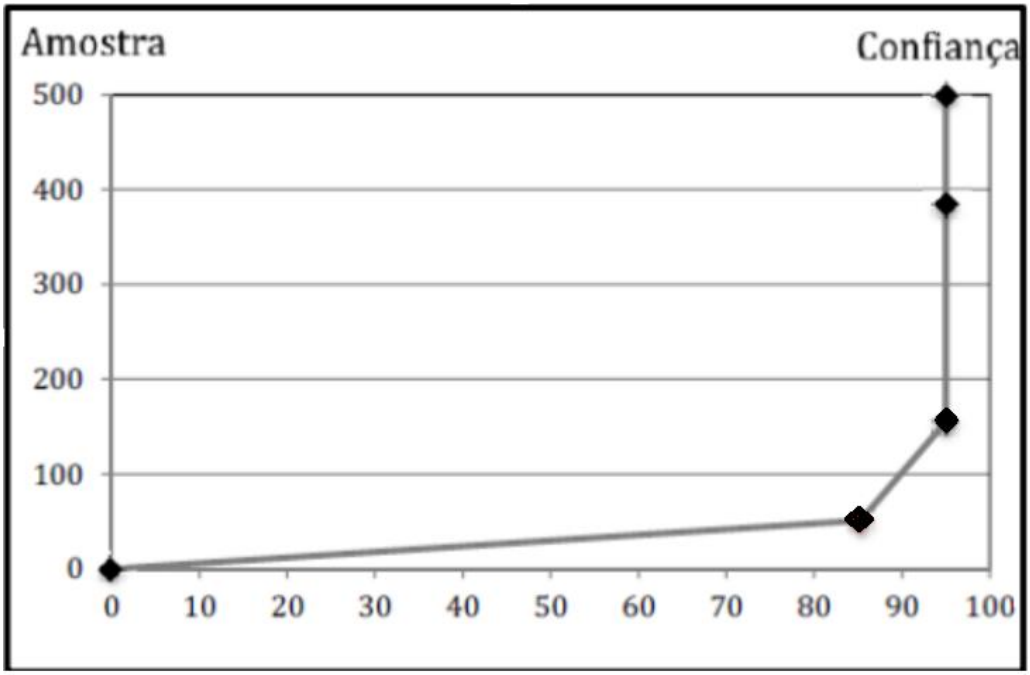
3.3.2. Amostra

Conforme Ngoma (2019), e Gil (2008), a amostra obtida é do tipo por conveniência, pois os respondentes pertencem a um conjunto de trabalhadores da organização e a adesão à pesquisa foi livre e voluntária. Para esta pesquisa, obtiveram-se 109 respondentes.

Considerando-se que as perguntas foram aplicadas a um grupo teoricamente heterogêneo de participantes – tanto em formação acadêmica quanto em experiência em tecnologia da informação - e que a pesquisa teve participação voluntária, não há garantias de que todos os segmentos da população estudada estejam representados na amostra, o que a caracteriza como não probabilística (NGOMA, 2019).

Sobre a quantidade de respondentes, Rodrigues (2014) demonstrou que o nível de confiança de 95% e erro amostral de 5% pode ser obtido com uma amostra a partir de 155 indivíduos. Em estudos que se baseiam e métricas baseadas na mediana, esses parâmetros permanecem inalterados em amostras de até 500 indivíduos. Com base no disposto na Figura 1, a amostra de 109 respondentes desta pesquisa geraria um nível de confiança de 92% e erro amostral de 8%.

Figura 1 - evolução de amostragem e nível de confiança



Fonte: Baseado em de Rodrigues (2014)

Sobre a amostra de 109 respondentes, 52 declararam atuar nos órgãos e 57, nas Unidades descentralizadas da organização pública estudada, conforme Tabela 01, a seguir.

Tabela 01 – Frequência e percentual de respondentes nos Órgãos e nas Unidades Descentralizadas.

Área de atuação	**Frequência**	**Porcentagem**
Órgãos	52	47,71%
Unidades Descentralizadas	57	52,29%
Total	109	100,00%

Fonte: a autora, a partir de dados da pesquisa.

Cumpre esclarecer que o parâmetro da Tabela 01 – denominado como área de atuação – atende a uma segmentação definida pela estrutura regimental da organização pública federal estudada, e está baseada em critério geográfico. Desta forma, órgãos são unidades localizadas na sede, enquanto unidades descentralizadas abrangem as superintendências regionais e outras unidades não localizadas na sede.

Como respostas ao grau de instrução dos respondentes, a maior parte declarou possuir pós-graduação (especialização, mestrado e doutorado) conforme a Tabela 02 seguinte.

Tabela 02 – Frequência e percentual de respondentes por grau de Instrução

Grau de instrução	Frequência	Porcentagem
Nível fundamental	1	0,92%
Nível médio	7	6,42%
Nível superior	42	38,53%
Pós-graduação	59	54,13%
Total	109	100,00%

Fonte: a autora, com base nas respostas obtidas

Em relação ao tempo de experiência em TI, a maioria dos respondentes declarou possuir experiência superior a 11 anos conforme a tabela seguinte: os outros com até 10 anos de experiência totalizam 35,78%. Mais de 92% dos resultados, que os respondentes declararam possuir grau de instrução superior ou de pós-graduação.

Ressalte-se que, para o tempo de experiência em TI, optou-se por deixar o preenchimento de acordo com a percepção do respondente sobre o que seria essa experiência, de modo que, nessa pergunta, não foi oferecida nota explicativa ou qualquer viés que norteasse a opção do participante.

Tabela 3 – Frequência e percentual de respondentes por tempo de experiência em TI

Tempo de Experiência	Frequência	Porcentagem
zero	15	13,76%
até 1	5	4,59%
1 - 5	5	4,59%
5 - 10	14	12,84%
11 ou mais	70	64,22%
Total	109	100,00%

Fonte: a autora, com base nas respostas obtidas

A revisão teórica aponta como fator crítico de sucesso na conscientização em segurança cibernética o grau de instrução dos usuários e o tempo de experiência em tecnologia da informação (NIST 2020, 2022; NGOMA, 2019). Nesse sentido, 77,06% dos respondentes do questionário declararam experiência superior

a 5 anos em Tecnologia da Informação.

3.4 Caracterização e descrição dos instrumentos de pesquisa

A obtenção dos dados foi feita por meio de aplicação de questionário estruturado, baseado na revisão teórica, especialmente no estudo de Ngoma (2019), com adequações às peculiaridades da organização pública objeto este estudo. O referido questionário encontra-se no APÊNDICE C deste trabalho.

O teor das questões formuladas levou em consideração, também, orientações do TCU (2022), do CIS (2021) e do GSI/PR (2020) de divulgação de boas práticas em segurança cibernética a todos os usuários, sem distinção de cargo ou exercício de função gerencial, posto que todos os trabalhadores constituem risco ou fator de sucesso na segurança cibernética da organização.

Todas as perguntas do questionário são de múltipla escolha, sendo que 03 (três) permitem seleção de mais de uma resposta. O questionário, em formato digital, constitui-se de 13 (treze) perguntas objetivas de múltipla escolha, 04 (quatro) das quais com emprego da escala Likert.

A escala Likert – também adotada no trabalho de Ngoma (2019) - é adequada à coleta de dados proposta porque, conforme Aguiar, Correia e Campos (2011), oferece 5 (cinco) opções de resposta, de forma descendente, em que pelo menos uma das alternativas tem valor neutro (indiferente ou não aplicável).

Do estudo original (NGOMA, 2019), optou-se por não incluir 04 (quatro) questões abertas, que não foram necessárias para atingir os objetivos propostos deste estudo.

A primeira seção de perguntas do questionário visa a obter informações gerais sobre os respondentes, relacionando-se 06 (seis) questões sobre área de atuação (unidade de exercício), formação, qualificação e experiência em TI, além de percepção sobre instrumentos organizacionais vigentes e relacionados à segurança cibernética. 03 (três) questões dessa seção tiveram emprego de escala Likert.

A segunda seção de perguntas refere-se à ameaças e riscos à segurança cibernética, contemplando 04 (quatro) perguntas de múltipla escolha, 01(uma) delas com emprego da escala Likert. A terceira seção de perguntas refere-se à conscientização sobre segurança cibernética, com 03 (três) perguntas de múltipla escolha.

Por fim, é adequado citar que o questionário foi previamente testado, e os procedimentos para esse teste prévio, que contribui para a validade do instrumento,

segue descrito na Subseção 3.5.1 deste estudo.

3.5. Procedimentos de Coleta e Análise de Dados

3.5.1. Coleta de dados

A coleta de dados constituiu-se de pesquisa bibliográfica prévia (PRODANOV; FREITAS, 2013), pesquisa documental e pesquisa de campo com aplicação de questionário. A pesquisa bibliográfica consistiu na revisão de literatura, a pesquisa documental ocorreu por meio da consulta a normas internas e documentos públicos da organização relativos à segurança cibernética. Para pesquisa de campo, utilizou-se de questionário eletrônico. A aplicação do questionário ocorreu com auxílio da ferramenta Google Forms[1].

A divulgação do questionário aos potenciais respondentes ocorreu via e-mail institucional da Assessoria de Comunicação Social da organização pública federal, mediante prévia autorização de condução do estudo, por parte da autoridade máxima da área de TI da organização pública objeto deste trabalho (APÊNDICE A).

No datas de 22/11 e 02/12/2022, respectivamente, foram enviados dois e-mails da referida assessoria aos trabalhadores da organização pública, posteriormente sendo apuradas as respostas dos trabalhadores que acessaram o referido formulário. Cautelas éticas sobre a proteção de dados foram informadas aos respondentes, com destaque para a adequação do estudo à lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais.

Nesse sentido, participantes da pesquisa receberam um termo de esclarecimento e consentimento sobre o tratamento dos dados oriundos de suas respostas. O texto de apresentação do questionário, previamente ao consentimento, foi apresentado ao respondente no mesmo link eletrônico. O conteúdo se apresenta no APÊNDICE B.

Para mitigar eventuais erros do questionário que comprometessem a efetividade e precisão dos dados, foi realizada uma rodada de validação das perguntas com um grupo qualificado de trabalhadores da organização pública objeto do estudo (BABBIE, 2020).

Segundo Alexandre e Coluci (2011), a construção (a partir de revisão de literatura) e a validação dos instrumentos de pesquisa são fatores críticos de

[1] Ferramenta gratuita de formulários eletrônicos. Disponível em: https://forms.google.com

sucesso da coleta de dados, e devem refletir as peculiaridades culturais, linguísticas e contextuais da população estudada.

Nesta pesquisa, adotou-se a validação das questões por meio de teste prévio com pequeno grupo de indivíduos, pertencentes à população avaliada. Nessa etapa, 6 (seis) trabalhadores da organização pública foram entrevistados quanto ao nível de compreensão das perguntas, validação do conteúdo e ao alcance dos objetivos desta pesquisa. Este grupo foi excluído da aplicação do questionário.

De quinze questões inicialmente propostas, duas foram retiradas com base na avaliação desses respondentes que apontaram problemas de clareza dos enunciados e de coerência com as respostas. Devido ao prazo insuficiente para reelaboração das questões e ao baixo impacto dessas informações no resultado, optou-se por retirá-las.

O questionário, mencionado na Seção 3.4 e apresentado no Apêndice C, foi disponibilizado para resposta em um intervalo de 11 dias, entre 22 de novembro e 02 de dezembro, por meio da plataforma Google Formulários. A pesquisa foi divulgada com o apoio da Assessoria de Imprensa da Organização.

O formulário foi precedido por uma mensagem de apresentação do questionário e declaração de concordância e preenchimento voluntário no Apêndice B. Nessa mensagem de apresentação, são explicitados os cuidados com a obtenção, tratamento e guarda dos dados, em conformidade com a Lei Geral de Proteção de Dados – Lei nº 13.709, de 2018 – conforme APÊNDICE B.

3.5.2. Análise de dados

Os dados primários e secundários obtidos para a realização do estudo foram analisados conforme procedimentos descritos nesta subseção. No caso dos dados secundários, procedeu-se análise documental de legislação, regulamentos nacionais, normas internas e publicadas, documentos institucionais de acesso público e compilações de boas práticas em segurança cibernética (NIST, CIS, ABNT).

Para tratar os dados primários, oriundos do questionário, os procedimentos empregados abrangeram estatística descritiva, com obtenção de mediana e moda. Todas as respostas foram organizadas em planilha com aplicação de estatística descritiva dos dados, sendo examinada para cada questão todas as respostas válidas com contagem de frequência e elaboração de percentuais. Para 03 (três) questões, apurou-se frequência de respostas válidas foi inferior a 109

respondentes.

Para o alcance do primeiro objetivo específico – “OE1: Identificar a percepção de trabalhadores em uma organização pública federal sobre as principais ameaças à segurança cibernética, com base na revisão de literatura“ citado na subseção 1.3.2 – os dados das questões 7 a 10 do APÊNDICE C foram tratados com estatística descritiva. Nessa linha, contemplaram-se a mediana (valor central no conjunto de dados ordenados) e a moda (valor observado com maior frequência).

Para o atendimento do segundo objetivo específico – “OE2: Descrever a percepção desses trabalhadores sobre conscientização em segurança cibernética, com base na revisão de literatura”, conforme subseção 1.3.2 – os dados das questões 4 a 6 do APÊNDICE C, foram tratados com estatística descritiva, também com o uso da mediana e da moda.

Para alcançar o terceiro objetivo específico – “OE3: Comparar a percepção previamente descrita sobre conscientização em segurança cibernética segundo a área em que o trabalhador atua na organização pública federal”, constante da subseção 1.3.2, foi feita tabulação cruzada da Questão 01 - área em que o trabalhador atua – com cada uma das questões citadas no parágrafo anterior do segundo objetivo específico.

Procedimento semelhante foi observado para o alcance do quarto objetivo específico - “OE4: Diferenciar a percepção previamente descrita de trabalhadores segundo sua experiência prévia em Tecnologia da Informação”, mencionado na subseção 1.3.2, usando, como base da tabulação com as questões 4 a 6 e 11 a 13 da questão 3 – intervalo, em anos, de experiência em Tecnologia da Informação.

A respostas foram exibidas em tabelas, descritas nos resultados. Os procedimentos estatísticos foram efetuados com o uso dos softwares Microsoft Excel e *Statistical Package for Social Sciences* – SPSS.

4 RESULTADOS

Este capítulo apresenta os resultados da pesquisa, e divide-se em quatro seções. A Seção 4.1 trata sobre a percepção sobre a identificação das ameaças cibernéticas, a Seção 4.2 refere-se à percepção sobre conscientização em segurança cibernética, a Seção 4.3 dispõe sobre a comparação da percepção sobre conscientização em segurança cibernética segundo a área de atuação do trabalhador, ao passo que a seção 4.4 discorre sobre a comparação da percepção sobre conscientização em segurança cibernética segundo o tempo de experiência com TI.

4.1. Percepção sobre Identificação das Ameaças Cibernéticas

Nesta seção foram levadas em consideração as respostas das questões 7 a 10 do APÊNDICE C. A Tabela 4 ilustra a percepção dos trabalhadores sobre comunicação de ameaças à segurança cibernética, referente às respostas válidas da Questão 7.

Tabela 4 – Percepção sobre comunicação de ameaças à segurança cibernética

Questão	Ameaças	Frequência	Porcentagem
7	Nenhum	63	58,33%
	Ransomware	19	17,59%
	Malware	42	38,89%
	Phishing	29	26,85%

Fonte: dados da pesquisa
Observação: 1. para cada linha, 100% corresponde a 108 respostas válidas para esta questão. 2. Resultados oriundos da questão 7, proposta no APÊNDICE C

Conforme Tabela 4, do total de 108 respostas válidas, 58,33% delas declarou não receber comunicação sobre as ameaças à segurança cibernética, ao passo que 38,89% das respostas declararam receber comunicação sobre malware. Esse resultado sugere certo predomínio na falta de comunicação sobre ameaças cibernéticas.

Os achados da Tabela 4 vão de encontro às evidências documentais (e-mails institucionais dirigidos a todos os usuários de TI e webinários) sobre a comunicação formal das ameaças cibernéticas aos trabalhadores da organização pública. Diverge, também, dos resultados obtidos no trabalho sobre organizações públicas da África do Sul (NGOMA, 2019), segundo o qual todos os respondentes afirmaram que a organização alerta sobre todas as ameaças cibernéticas listadas.

A Questão 8 do APÊNDICE C refere-se à percepção do trabalhador se a organização lembra consistentemente os usuários sobre práticas online seguras. O resultado é demonstrado na Tabela 5.

Tabela 5 – Percepção de que a organização lembra consistentemente os usuários de práticas online seguras

Questão	Respostas					Total	Mediana	Moda
	N	R	O	F	S			
8	11 10,09%	38 34,86%	36 33,03%	13 11,93%	11 10,09%	109 (100,00%)	O	R

Fonte: dados da pesquisa

Legenda: 1 N= Nunca; R = Raramente, O. = Ocasionalmente, F = Frequentemente, S = Sempre.

Observações: 1. o Percentual deve considerar o total de respostas para o item. 100,00% equivalem a 109 respostas. 2. Resultados oriundos da questão 8, proposta no APÊNDICE C

A Tabela 5 mostra 49 respondentes (44,95% do total de respostas válidas) manifestando frequência ‘nunca’ ou ‘raramente’ sobre a organização lembrar sobre práticas seguras online. A mediana apresentou o estado ‘ocasionalmente’ e a moda ‘raramente’. Somente 22,02% percebem frequentemente ou sempre a organização lembrando usuários sobre essas práticas. O resultado citado na Tabela 5 diverge do arcabouço documental obtido a respeito da organização pública – como campanhas por e-mail, webinários, prescrições disseminadas às unidades via Sistema Eletrônico de Informações (SEI) visando ao comportamento online seguro.

Em complemento, ainda sobre a Tabela 5, quando comparado aos resultados obtidos junto aos gestores da África do Sul (NGOMA, 2019), 50% dos respondentes registraram que a organização lembra ocasionalmente os usuários sobre práticas online seguras.

A Tabela 6, a seguir, ilustra a percepção dos trabalhadores quanto ao alerta frequente sobre as ameaças de segurança cibernética. Tanto a moda quanto a mediana sinalizam que os respondentes concordam fortemente que alertas sobre ameaças à segurança cibernética motivam os usuários a comportamento online seguro. Adicionalmente, 103 dos 109 dos trabalhadores concordam em alguma medida com a importância dos alertas de ameaças para aprimorar a cultura de segurança cibernética, totalizando 94,50% das respostas válidas.

Tabela 6 – Percepção de que o alerta frequente sobre ameaças à segurança cibernética motiva os usuários a comportamento online seguro

Questão	*Respostas*					*Total*	*Mediana*	*Moda*
	D. T.	D. M.	Neutro	C. M.	C. F.			
9	0 0,00 %	2 1,83%	4 3,67%	32 29,36%	71 65,14%	109 (100,00%)	C. F.	C. F.

Fonte: dados da pesquisa

Legenda:1 D. T..= Discordo Totalmente; D. M. = Discordo Moderadamente, Neutro = Neutro (nem concordo, nem discordo), C. M. = Concordo Moderadamente, C. F = Concordo Fortemente.

Observações: 1. o Percentual deve considerar o total de respostas para o item. 100,00% equivalem a 109 respostas 2. Resultados oriundos da questão 9, proposta no APÊNDICE C

O resultado da Tabela 6 mostra que 65,14% dos respondentes concordam que o alerta frequente sobre ameaças à segurança cibernética motiva os usuários a comportamento online seguro. De notar que o trabalho de Ngoma (2019) mostra que 50% dos respondentes concordam fortemente com a relevância da comunicação de ameaças cibernéticas para a motivação de comportamento online seguro.

A Tabela 7 mostra a percepção dos respondentes sobre o impacto que as ameaças à segurança cibernética têm na organização, oriunda da questão 10 do APÊNDICE C.

Tabela 7 – Percepção de que as ameaças à segurança cibernética podem ter impacto negativo na organização

Questão	**Respostas**					**Total**	**Mediana**	**Moda**
	N	R	O	F	S			
10	0 0,00%	0 0,00%	3 2,75%	24 22,02%	82 75,23%	109 (100,00%)	S	S

Fonte: dados da pesquisa

Legenda: N = Nunca; R = Raramente, O = Ocasionalmente, F = Frequentemente, S = Sempre.

Observações: 1. o Percentual deve considerar o total de respostas para o item. 100,00% equivalem a 109 respostas. 2. Resultados oriundos da questão 10, proposta no APÊNDICE C

Segundo a Tabela 7, observou-se 82 respostas ‘sempre’ (75,23% do total de respostas válidas), também apontada como mediana e moda. Adicionalmente, 106 respondentes (97,25% do total de respostas válidas com ‘frequentemente’ ou ‘sempre’) reconhecem que as ameaças à segurança cibernética têm impacto negativo na organização. Este resultado converge com iniciativas de conscientização promovidas pela organização pública federal, conforme documentos consultados (central de conteúdo no portal institucional).

Por fim, quanto aos resultados da Tabela 7, em relação aos resultados obtidos junto aos gestores da África do Sul (NGOMA, 2019), percebe-se

convergência de resultados. Naquele trabalho, 100% dos respondentes reconheceram que as ameaças à segurança cibernética sempre têm impacto negativo na organização.

4.2. Percepção Sobre Conscientização em Segurança Cibernética

Para o alcance deste objetivo, analisam-se os resultados das Questões 11 a 13, relativas à percepção sobre a conscientização em segurança cibernética, complementada pelas questões 4 a 6 do APÊNDICE C. Em adição, os dados coletados, também, foram analisados à luz dos documentos que dispõem sobre a organização pública e que estabelecem diretrizes sobre segurança cibernética.

A Questão 11 tratou sobre a percepção se a organização possui política formal de segurança cibernética. Os resultados constam da Tabela 8.

Tabela 8 – Percepção se a organização possui política formal de segurança cibernética

Questão	***Respostas***			***Total***
	Não sei / desconheço	Não	sim	
11	67 61,47%	7 6,42%	35 32,11%	109 (100,00%)

Fonte: dados da pesquisa

Observações: 1. o Percentual deve considerar o total de respostas para o item. 100,00% equivalem a 109 respostas. 2. Resultados oriundos da questão 11, proposta no APÊNDICE C

O resultado da Tabela 8 demonstrou distribuição heterogênea da amostra entre as respostas, indicação a resposta “não sei / desconheço” com 61,47% do total de respondentes, contra 35 respondentes, correspondente a 32,11% do total de respostas válidas para a Questão 11, que afirmaram ter ciência de política formal de segurança cibernética.

Este resultado da Tabela 8, também, diverge da evidência documental com base em pesquisas a documentos públicos sobre a organização (portarias publicadas na imprensa oficial e no portal institucional, e-mails a todos os usuários), que evidenciam normas vigentes, atualizadas. O resultado, também, sugere necessidade de divulgação mais eficaz e efetiva dessas políticas, buscando a implantação de práticas online seguras.

Ainda sobre a Tabela 8, os resultados obtidos junto aos gestores da África do Sul (NGOMA, 2019) indicaram que 67% dos respondentes afirmaram não existir política formal de segurança cibernética, contra 33% que afirmaram existir essa política. O contexto daquele país induz que pode estar ausente a política formal, ao contrário da organização pública estudada neste trabalho.

Tendo em vista que a conscientização em segurança cibernética requer treinamento e comunicação efetivas aos usuários dos serviços e sistemas (NGOMA, 2019; NAG et. al, 2022), os resultados obtidos desta pesquisa podem ensejar oportunidade de revisão ações de treinamento sobre segurança cibernética entre os trabalhadores da organização pública respondentes do estudo.

A Questão 12 do APÊNDICE C diz respeito à percepção dos trabalhadores sobre os canais de comunicação utilizados pela organização para comunicar ameaças à segurança cibernética. Os resultados constam da Tabela 9, a seguir.

Tabela 9 – Percepção sobre os canais de comunicação pelos quais a organização comunica ameaças à segurança cibernética

Questão	Respostas	Frequência	Porcentagem
12	Não comunica ameaças à seg. cibernética	16	15,24%
	Outros	7	6,67%
	Intranet	20	19,05%
	Textos	3	2,86%
	Boletim informativo	17	16,19%
	E-mail	80	74,07%

Fonte: dados da pesquisa

Observação: 1. para cada linha, 100% correspondem a 105 respondentes validados para esta questão. 2. Resultados oriundos da questão 12, proposta no APÊNDICE C.

A Tabela 9 mostra o canal e-mail entre aqueles pelo qual a organização comunica ameaças à segurança cibernética, com 80 respostas das 105 respostas válidas (74,07% do total de respostas válidas). O canal intranet apresentou 20 respostas (19,05% do total de respostas válidas) e o boletim informativo apresentou 17 respostas (16,19% de respostas válidas). De notar que 16 respondentes (15,24% das respostas válidas) afirmaram que a organização não comunica ameaças à segurança cibernética.

No estudo de Ngoma (2019), 83% dos respondentes afirmam que as respectivas organizações em que atuavam comunicava ameaças à segurança cibernética via e-mail. Intranet foi lembrada por 67%, ao passo que newsletter (equivalente a boletim informativo) foi registrado por 33%. Nenhum respondente registrou ausência de comunicações de ameaças à segurança cibernética.

Os resultados dos respondentes na Tabela 12 que não identificam a comunicação de ameaças sugerem que pode ser necessário adotar estratégias mais efetivas de comunicação das ameaças à segurança cibernética.

A Questão 13 do APÊNDICE C refere-se à percepção sobre a frequência com que a organização pública estudada promove treinamentos sobre segurança cibernética. As respostas dos trabalhadores estão dispostas na Tabela 10.

Tabela 10 – Percepção sobre a frequência com que a organização promove treinamentos sobre segurança cibernética

Questão	Respostas					Total	Mediana	Moda
	N	R	O.	F.	S			
13	67 61,47%	21 19,27%	18 16,51%	1 0,92%	2 1,83%	109 (100,00%)	N	N

Fonte: dados da pesquisa
Legenda: N= Nunca; R = Raramente, O = Ocasionalmente, F = Frequentemente, S = Sempre
Observações: 1. o Percentual deve considerar o total de respostas para o item. 100,00% equivalem a 109 respostas. 2. Resultados oriundos da questão 12, proposta no APÊNDICE C

A Tabela 10 mostra 88 respondentes (80,73% do total de respostas válidas) percebendo que a organização nunca ou raramente promove treinamentos sobre segurança cibernética. Este resultado diverge das ações de treinamento promovidas pela organização, conforme consulta a documentos públicos (agendas divulgadas de webinários temáticos). Este fato pode sugerir necessidade de aprimorar a comunicação e o alcance dos treinamentos oferecidos.

Em relação aos resultados obtidos junto aos gestores da África do Sul (NGOMA, 2019), percebe-se divergência nos resultados da Tabela 10, uma vez que os gestores sul africanos, em sua maioria (83%), afirmaram que a organização promove treinamentos sobre segurança cibernética ocasionalmente ou frequentemente.

Sobre a Questão 4, a Tabela 11 descreve os resultados obtidos sobre a percepção do responsável pela conscientização sobre segurança cibernética.

Tabela 11 – Percepção do responsável pela conscientização sobre segurança cibernética

Questão	Respostas	Frequência	Porcentagem
4	Não sei / Desconheço	26	24,53%
	Outra	3	2,83%
	A Área de Recursos Humanos	2	1,88%
	A Área de Orçamento / Finanças	1	0,94%
	A Área de Tecnologia da Informação	72	67,92%
	A Organização	14	13,20%

Fonte: dados da pesquisa
Observações: 1. para cada linha, 100% correspondem a 106 respostas válidas para a questão. 2. Resultados oriundos da questão 4, proposta no APÊNDICE C

Conforme Tabela 11, do total de 106 respostas válidas, a área de TI foi lembrada como responsável pela conscientização em segurança cibernética em 72 delas (correspondendo a 67,92% do total de respostas válidas). Por sua vez, 26 respostas, (correspondente a 24,53% das respostas válidas) indicaram não saber quem é o responsável pela conscientização em segurança cibernética.

Os resultados obtidos ratificam a percepção da maioria dos respondentes em relação aos documentos formais da organização que a área responsável pela conscientização em segurança cibernética é a área de TI (portaria normativa publicada na imprensa oficial e no site institucional que define os papéis e responsabilidades de cada instância na conscientização em segurança cibernética).

Os respondentes do trabalho realizado com organizações públicas sul africanas (NGOMA, 2019) também destacaram o papel da área de TI na conscientização sobre segurança cibernética, com percentual de 67%. No entanto, 33% dos respondentes atribuíram à área de recursos humanos como responsável pela conscientização em segurança cibernética.

Com relação à Questão 5 do APÊNDICE C, a Tabela 12 apresenta os resultados sobre a existência de comitê interno ou externo envolvido em questões de segurança cibernética na organização.

Tabela 12 – Ciência da existência de comitê interno ou externo envolvido em questões de segurança cibernética na organização

Questão	**Respostas**					**Total**	**Mediana**	**Moda**
	F.I.	M. I.	Neutro	M. C.	F. C.			
5	27 24,77%	12 11,01%	31 28,44%	27 24,77%	12 11,01%	109 (100,00%)	Neutro	Neutro

Fonte: dados da pesquisa

Legenda: 1 F.I.= Fortemente Inconsciente; M. I. = Moderadamente Inconsciente, Neutro = Neutro (nem consciente, nem inconsciente), M. C. = Moderadamente Consciente, F. C. = Fortemente Consciente.

Observações: 1. o Percentual deve considerar o total de respostas para o item. 100,00% equivalem a 109 respostas. 2. Resultados oriundos da questão 5, proposta no APÊNDICE C

Sobre a Tabela 12, tanto a moda quanto a mediana evidenciam a percepção neutra dos respondentes quanto à ciência de um comitê envolvido em questões de segurança cibernética. Por sua vez, o total de 39 respondentes (35,78% do total de respondentes válidos) demonstram ciência no comitê envolvido em questões de segurança cibernética, ao passo que a mesma quantidade de 39 respondentes e proporção de 35,78% do total de respostas manifestou não ter ciência da existência desse comitê.

Este resultado da Tabela 12 destoa do percentual de ciência de 83% dos gestores públicos sobre comitês exclusivamente envolvidos em segurança cibernética no estudo de Ngoma (2019). O resultado, também, não se mostra compatível com o exame de documentos referentes à organização pública (portarias publicadas na imprensa oficial e no portal institucional), que indicam comitê instituído, atuante e dedicado a questões de segurança cibernética, assim como equipe de tratamento e resposta a incidentes de rede e campanhas de informação sobre as atividades dessas instâncias. Isso pode conotar reflexão sobre aprimoramento da divulgação das instâncias de segurança cibernética aos trabalhadores da organização pública estudada.

Com relação à Questão 6 do APÊNDICE C, a Tabela 13 expõe os resultados sobre conhecimento de iniciativa estratégica da organização para abordar a segurança cibernética.

Tabela 13 – Conhecimento de Iniciativa estratégica da organização para abordar a segurança cibernética

Questão	Respostas					Total	Mediana	Moda
	F.I.	M. I.	Neutro	M. C.	F. C.			
6	26 23,85%	11 10,09%	28 25,69%	29 26,61%	15 13,76%	109 (100,00%)	Neutro	M. C.

Fonte: dados da pesquisa

Legenda: F.I.= Fortemente Inconsciente; Neutro = neutro (nem consciente, nem inconsciente); M. I. = Moderadamente Inconsciente, M. C. = Moderadamente Consciente, F. C. = Fortemente Consciente.

Observações: 1. o Percentual deve considerar o total de respostas para o item. 100,00% equivalem a 109 respostas. 2. Resultados oriundos da questão 6, proposta no APÊNDICE C

Segundo Tabela 13, constata-se que 44 respondentes (40,37% do total de respostas válidas) manifestou alguma consciência do conhecimento de iniciativa estratégica da organização para abordar a segurança cibernética. Por outro lado, 37 respondentes (33,94% do total de respostas válidas) declararam alguma inconsciência do conhecimento dessa iniciativa.

O resultado na Tabela 13 destoa do grau de consciência dos gestores públicos da África do Sul relativos a iniciativas estratégicas sobre segurança cibernética, de 83% (NGOMA, 2019). Tal resultado, também, diverge da análise documental da organização pública em normas vigentes (portarias publicadas na imprensa oficial e no portal institucional) e campanhas de conscientização via e-mail a todos os usuários. Tais evidências podem conotar uma eventual necessidade de aprimorar a divulgação das estratégias sobre segurança cibernética aos

trabalhadores da organização pública brasileira em estudo.

4.3. Comparação da Percepção sobre Conscientização em Segurança Cibernética Segundo a Área de atuação do Trabalhador

Nesta seção, discorre-se sobre a percepção sobre conscientização em segurança cibernética de trabalhadores atuantes nos órgãos e a comparação com aqueles atuantes nas unidades descentralizadas. A área de atuação de cada trabalhador corresponde a órgãos ou unidades descentralizadas, foi citada na Tabela 1 da metodologia deste estudo e foi obtida com base na Questão 1 do APÊNDICE C do questionário.

Para o cumprimento desse objetivo, foi realizada tabulação cruzada de questões, relacionando a área de atuação com a percepção oriunda das respostas aos questionários para a Seção 4.2. Dessa forma, os resultados exibidos em tabelas, nesta seção, decompõem as percepções dos respondentes segundo a respectiva área de atuação.

Deve-se ressaltar que o estudo de referência (NGOMA, 2019) não realizou análise comparativa da percepção sobre conscientização em segurança cibernética dos respondentes com base na área de atuação. Neste trabalho, optou-se realizar esta comparação em razão de peculiaridades da organização pública federal estudada, tais como a presença física em todas os estados da Federação e as diferenças culturais agregadas, conforme descrito na seção 3.2.

Inicialmente, a Tabela 14 refere-se à percepção dos trabalhadores sobre a existência de política formal de segurança cibernética por área de atuação. Os resultados mostram que 57,69% dos respondentes dos órgãos e 64,91% das unidades descentralizadas não sabem ou desconhecem a existência de uma política formal de segurança cibernética.

Tabela 14 – Percepção se a organização possui política formal de segurança cibernética por área de atuação

Área de Atuação	Respostas			Total
	Não sei / Desconheço	Não	Sim	
Órgãos	30 57,69%	3 5,77%	19 36,54%	52 100,00%
Unidades Descentralizadas	37 64,91%	4 7,02%	16 28,07%	57 100,00%

Fonte: dados da pesquisa

Observações: 1. o Percentual deve considerar o total de respostas válidas para cada grupo “área de atuação”: 100,00% para “Órgãos equivalem a 52 respostas; 100,00% para o grupo “Unidades Descentralizadas” equivalem a 57 respostas. 2. Resultados oriundos da tabulação da questão 1 com a 11, propostas no APÊNDICE C

A Tabela 15, a seguir mostra que 39 respondentes dos órgãos (78,00% dos respondentes dessa área) e 41 respondentes das unidades descentralizadas (74,55% dos respondentes de tal área) percebem o e-mail como canal de comunicação pelos quais a organização comunica ameaças à segurança cibernética.

Tabela 15 – Percepção sobre os canais de comunicação pelos quais a organização comunica ameaças à segurança cibernética por área de atuação

Área de Atuação	Respostas					
	N C	O	I	T	B I	E-mail
Órgãos	6 12,00%	5 10,00%	12 24,00%	5 10,00%	11 22,00%	39 78,00%
U D	10 18,18%	2 34,00%	8 14,55%	0 0,00%	6 10,91%	41 74,55%

Fonte: Dados da pesquisa

Legenda: U D = Unidade descentralizada; N C = Não comunica; O = outro; I = Intranet; T = Textos; B I = Boletim Informativo

Observações: 1. o Percentual deve considerar o total de respostas válidas para cada grupo “área de atuação”: 100,00% para “Órgãos equivalem a 50 respostas; 100,00% para o grupo “Unidades Descentralizadas” equivalem a 55 respostas. 2. Resultados oriundos da tabulação da questão 1 com a 12, propostas no APÊNDICE C

A Tabela 16 mostra a frequência de treinamentos em segurança cibernética promovidos pela organização, segmentados pela área de atuação do respondente. O resultado evidencia 73,08% dos trabalhadores dos órgãos e 77,72% dos trabalhadores das unidades descentralizadas afirmam que a organização nunca ou raramente promove treinamentos sobre segurança cibernética. Esse resultado pode nortear a organização na revisão da oferta de treinamentos e na divulgação dessas iniciativas entre os trabalhadores, independente da unidade em que atuem.

Tabela 16 – Percepção sobre a frequência com que a organização promove treinamentos sobre segurança cibernética por área de atuação

Área de Atuação	Respostas					Total	Mediana	Moda
	N	R	O	F	S			
Órgãos	26 50,00%	12 23,08%	12 23,08%	0 0,00%	2 3,85%	52 100,00%	N	N
U. D.	41 71,93%	91 5,79%	6 10,53%	1 1,75%	0 0,00%	57 100,00%	N	N

Fonte: dados da pesquisa

Legenda: U. D. = Unidades Descentralizadas; N = Nunca; R = Raramente, O = Ocasionalmente, F = Frequentemente; S = Sempre.

Observações: 1. o Percentual deve considerar o total de respostas válidas para cada grupo “área de atuação”: 100,00% para “Órgãos equivalem a 52 respostas; 100,00% para o grupo “Unidades Descentralizadas” equivalem a 57 respostas. 2. Resultados oriundos da tabulação da questão 1 com a 13, propostas no APÊNDICE C

A Tabela 17 exibe a tabulação cruzada da percepção dos responsáveis pela conscientização em segurança cibernética na organização, por área de atuação. Verificou-se similaridade nas respostas válidas dos respondentes lotados nos órgãos e nas unidades descentralizadas. Para “a área de tecnologia da informação”, foram verificadas 68,63% de respostas válidas para respondentes dos órgãos e 67,27% de respostas válidas para respondentes de unidades descentralizadas.

Tabela 17 – Percepção do responsável pela conscientização sobre segurança cibernética por área de atuação

Área de Atuação	Respostas					
	N S / D	O	RH	OF	TI	ORG
Órgãos	13 25,49%	0 0,00%	2 3,92%	1 1,96%	35 68,63%	7 13,73%
U. D.	13 23,64%	3 5,45%	0 0,00%	0 0,00%	37 67,27%	6 10,91%

Fonte: Dados da pesquisa

Legenda: U. D. = Unidades Descentralizadas; NS / D = Não sei / desconheço; O = Outra; RH = a área de recursos humanos; OF = a área de orçamento e finanças; TI = a área de tecnologia da informação; ORG = a organização.

Observações: 1. o Percentual deve considerar o total de respostas válidas para cada grupo “área de atuação”: 100,00% para “Órgãos equivalem a 51 respostas; 100,00% para o grupo “Unidades Descentralizadas” equivalem a 57 respostas. 2. Resultados oriundos da tabulação da questão 1 com a 4, propostas no APÊNDICE C.

A Tabela 18 compara a percepção sobre a ciência da existência de comitê envolvido com questões de segurança cibernética, segmentado por área de atuação. Verifica-se que, nos órgãos, há 18 trabalhadores que se declararam neutros em relação à existência de comitê dedicado a questões de segurança cibernética (34,62% do total de respostas válidas), enquanto 16 respondentes das unidades descentralizadas (28,07% das respostas válidas) declararam total inconsciência da existência do referido comitê.

Tabela 18 – Ciência da existência de comitê interno ou externo envolvido em questões de segurança cibernética na organização por área de atuação

Área de atuação	Respostas					Total	Mediana	Moda
	F. I.	M. I.	Neutro	M. C.	F. C.			
Órgãos	11 21,15%	2 3,85%	18 34,62%	13 25,00%	8 15,38%	52 100,00%	Neutro	Neutro
U. D.	16 28,07%	10 17,54%	13 22,81%	14 24,56%	4 7,02%	57 100,00%	Neutro	F.I

Fonte: dados da pesquisa.

Legenda: U. D. = Unidades Descentralizadas; F.I.= Fortemente Inconsciente; M. I. = Moderadamente Inconsciente, Neutro = Neutro (nem consciente, nem inconsciente); M. C. = Moderadamente Consciente, F. C. = Fortemente Consciente

Observações: 1. o Percentual deve considerar o total de respostas para cada área de atuação: 100,00% para Órgãos equivalem a 52 respostas; 100,00% para Unidades descentralizadas equivalem a 57 respostas. 2. Resultados oriundos da tabulação cruzada da questão 1 com a 5, propostas no APÊNDICE C.

Com relação às iniciativas estratégicas sobre segurança cibernética, a Tabela 19 mostra a decomposição dos resultados por área de atuação. Percebe-se que 24 trabalhadores das unidades descentralizadas (42,10% do total dessa área) declaram ciência das iniciativas estratégicas sobre segurança cibernética. Por sua vez, 20 respondentes dos órgãos (38,46% do total dessa área), também, declaram ciência das referidas iniciativas. Observe que 18 respondentes (34,62% do total dessa área) com a opção de neutralidade (“nem consciente, nem inconsciente”) verificada entre os trabalhadores dos órgãos.

Tabela 19 – Conhecimento de iniciativa estratégica da organização para abordar a segurança cibernética por área de atuação

Área de atuação	Respostas					Total	Mediana	Moda
	F. I.	M. I.	Neutro	M. C.	F. C.			
Órgãos	9 17,31%	5 9,62%	18 34,62%	8 15,38%	12 23,08%	52 100,00%	Neutro	Neutro
U. D.	17 29,82%	6 10,53%	10 17,54%	21 36,84%	3 5,26%	57 100,00%	Neutro	M. C.

Fonte: dados da pesquisa.

Legenda: U. D. = Unidades Descentralizadas; F.I.= Fortemente Inconsciente; M. I. = Moderadamente Inconsciente, Neutro = neutro (nem consciente, nem inconsciente), M. C. = Moderadamente Consciente, F. C. = Fortemente Consciente

Observações: 1. o Percentual deve considerar o total de respostas para cada área de atuação: 100,00% para Órgãos equivalem a 52 respostas; 100,00% para Unidades descentralizadas equivalem a 57 respostas. 2. Resultados oriundos da tabulação cruzada da questão 1 com a 6, propostas no APÊNDICE C.

4.4. Diferenciação da Percepção Sobre Conscientização em Segurança Cibernética Segundo Experiência Prévia em Tecnologia da Informação

Os resultados desta seção apresentam a percepção sobre conscientização em segurança cibernética de trabalhadores conforme o tempo de experiência em TI. A experiência de TI de cada trabalhador nesta seção foi segmentada em duas categorias: até 10 anos (39 respondentes, indicando 35,78% do total de respondentes) e 11 anos ou mais (70 respondentes, correspondendo 64,22% do total de respondentes), segundo informações da Tabela 3 exibida na Subseção 3.3.2 deste estudo e foi obtida com base na Questão 3 do APÊNDICE C do questionário.

Cabe ressaltar que o estudo de NGOMA (2019) não realizou análise comparativa da percepção sobre conscientização em segurança cibernética com o tempo de experiência em TI. Todos os respondentes naquele trabalho possuíam ao menos 11 anos de experiência em TI. Neste estudo, optou-se por fazer esta análise, em razão da peculiaridade da organização estudada, que possui presença no Distrito Federal e em todos os estados da Federação, e conta com diversidade de trabalhadores com experiência em TI com até 10 anos e com 11 anos ou mais, conforme descrito no parágrafo imediatamente anterior.

Inicialmente, a Tabela 20 mostra que 32 respondentes com até 10 anos de experiência em TI (82,05% do total de respondentes com essa experiência) não sabem ou desconhecem que a organização possui uma política formal de segurança cibernética. Por sua vez, 35 respondentes com 11 ou mais anos de experiência em TI (50,00% ou mais dos respondentes com tal experiência) não sabem ou desconhecem que a organização possui a referida política.

Tabela 20 – Percepção se a organização possui política formal de segurança cibernética por tempo de experiência em TI

Experiência em TI	Respostas			Total
	Não sei / Desconheço	Não	Sim	
Até 10	32 82,05%	0 0,00%	7 17,95%	39 35,78%
11 ou mais	35 50,00%	7 10,00%	28 40,00%	70 64,22%

Fonte: dados da pesquisa

Observações: 1. o Percentual deve considerar o total de respostas válidas para cada grupo “tempo de experiência em TI”: 100,00% para “até 10” equivalem a 39 respostas; 100,00% para o grupo “11 ou mais” equivalem a 70 respostas. 2. Resultados oriundos da tabulação da questão 3 com a 11, propostas no APÊNDICE C

Com relação aos canais que a organização utiliza para comunicar ameaças à segurança cibernética, a Tabela 21 mostra a segmentação das respostas conforme o tempo de experiência de TI. Nestes resultados, o canal e-mail apresenta-se com 26 respostas para respondentes com experiência até 10 anos de TI (72,22% do total de respostas para tal experiência) e 54 respostas para respondentes com 11 anos ou mais de experiência em TI (78,26% do total de respostas para essa experiência).

Tabela 21 – Percepção sobre os canais de comunicação pelos quais a organização comunica ameaças à segurança cibernética por tempo de experiência em TI

Experiência em TI (anos)	Respostas					
	N C	O	I	T	B I	E-mail
Até 10	7 19,44%	4 11,11%	7 19,44%	3 8,33%	6 16,67%	26 72,22%
11 ou mais	9 13,04%	3 4,35%	13 18,84%	0 0,00%	11 15,94%	54 78,26%

Fonte: Dados da pesquisa

Legenda: N C = Não comunica; O = outro; I = Intranet; T = Textos; B I = Boletim Informativo

Observações: 1. o Percentual deve considerar o total de respostas válidas para cada grupo “experiência em TI”: 100,00% para “até 10” equivalem a 36 respostas; 100,00% para o grupo “11 ou mais” equivalem a 69 respostas. 2. Resultados oriundos da tabulação da questão 3 com a 12, propostas no APÊNDICE C

A Tabela 22 traz a percepção se a organização promove treinamentos sobre segurança cibernética conforme o tempo de experiência em TI. A distribuição de respostas “nunca” e “raramente” apresentam 71,79% de respostas para respondentes com experiência de TI até 10 anos e 55,71% de respostas para respondentes com experiência de TI acima de 11 anos.

.

Tabela 22 – Percepção sobre a frequência com que a organização promove treinamentos sobre segurança cibernética por tempo de experiência em TI

Experiência em TI (anos)	Organização promove treinamento segurança cibernética					Total	Mediana	Moda
	N	R	O	F	S			
Até 10	28 71,79%	7 17,95%	4 10,26%	0 0,00%	0 0,00%	39 100,00%	N	N
11 ou mais	39 55,71	14 20,00%	14 20,00%	1 1,43%	2 2,86%	70 100,00%	N	N

Fonte: dados da pesquisa

Legenda: N = Nunca; R = Raramente, O = Ocasionalmente, F = Frequentemente; S = Sempre

Observações:1. o Percentual deve considerar o total de respostas válidas para cada grupo “experiência em TI”: 100,00% para “até 10” equivalem a 39 respostas; 100,00% para o grupo “11 ou mais” equivalem a 70 respostas. 2. Resultados oriundos da tabulação da questão 3 com a 13, propostas no APÊNDICE C

Com relação à percepção dos trabalhadores sobre os responsáveis pela conscientização em segurança cibernética, a Tabela 23 consolida os resultados por tempo de experiência em TI. Verifica-se que 25 respondentes com experiência de TI até 10 anos (61,10% do total de respondentes com essa experiência) e 47 respondentes com experiência em TI de 11 ou mais anos (70,15% dos respondentes válidos com essa experiência) indicaram a área de TI como responsável pela conscientização sobre segurança cibernética.

Tabela 23 – Percepção do responsável pela conscientização sobre segurança cibernética por tempo de experiência em TI

E. TI (anos)	Respostas					
	N S / D	O	RH	OF	TI	ORG
Até 10	10 25,64%	2 5,13%	0 0,00%	0 0,00%	25 61,10%	3 7,69%
11 ou mais	16 23,88%	1 1,49%	2 2,98%	1 1,49%	47 70,15%	3 5,48%

Fonte: Dados da pesquisa

Legenda: E. TI. = Experiência em tecnologia da informação; NS / D = Não sei / desconheço; O = Outra; RH = a área de recursos humanos; OF = a área de orçamento e finanças; TI = a área de tecnologia da informação; ORG = a organização.

Observações: 1. o Percentual deve considerar o total de respostas válidas para cada grupo "experiência em TI": 100,00% para "até 10" equivalem a 39 respostas; 100,00% para o grupo "11 ou mais" equivalem a 67 respostas. 2. Resultados oriundos da tabulação da questão 3 com a 4, propostas no APÊNDICE C

A Tabela 24 evidencia a tabulação cruzada que relaciona tempo de experiência em TI e ciência da existência de um comitê envolvido diretamente em questões de segurança cibernética. Os resultados evidenciam que 11 respondentes com até 10 anos de experiência em TI (23,28% do total de respondentes com essa experiência) e 28 respondentes com 11 anos ou mais de experiência em TI (40,00% do total de respondentes com essa experiência) declararam-se moderadamente ou fortemente conscientes da existência do comitê interno ou externo envolvido em questões de segurança cibernética.

Tabela 24 – Ciência da existência de comitê interno ou externo envolvido em questões de segurança cibernética na organização por tempo de experiência em TI

Experiência em TI (anos)	Respostas					Total	Mediana	Moda
	F. I.	M. I	Neutro	M. C.	F. C.			
Até 10	9 23,08%	6 15,38%	13 33,34%	8 20,51%	3 7,69%	39 100,00%	Neutro	Neutro
11 ou mais	18 25,71%	6 8,57%	18 25,71%	19 27,14%	9 12,86%	70 100,00%	Neutro	M.C.

Fonte: dados da pesquisa

Legenda: F.I.= Fortemente Inconsciente; M. I. = Moderadamente Inconsciente, Neutro = Neutro (nem consciente, nem inconsciente), M. C. = Moderadamente Consciente, F. C. = Fortemente Consciente

Observações: 1. o Percentual deve considerar o total de respostas para cada grupo de experiência em TI: 100,00% para “até 10” equivalem a 39 respostas; 100,00% para “11 ou mais” equivalem a 70 respostas. 2. Resultados oriundos da tabulação cruzada da questão 3 com a 5, propostas no APÊNDICE C.

Com relação às iniciativas estratégicas sobre segurança cibernética, a Tabela 25 mostra a decomposição dos resultados por experiência em TI. Observa-se que 13 respondentes com até 10 anos de experiência em TI (33,34% do total de respondentes com essa experiência) e 31 respondentes com 11 anos ou mais de experiência em TI (44,28% do total de respondentes com essa experiência) declararam-se moderadamente ou fortemente cientes de iniciativa estratégica da organização para abordar a segurança cibernética. De notar que a moda e a mediana das respostas segmentadas segundo experiência em TI foi a mesma, indicando neutralidade da ciência dessas iniciativas.

Tabela 25 – Percepção de ciência de iniciativa estratégica da organização para abordar a segurança cibernética por tempo de experiência em TI

Experiência em TI (anos)	Respostas					Total	Mediana	Moda
	FI	M I	Neutro	M C	F C			
Até 10	9 23,08%	6 15,38%	11 28,20%	9 23,08%	4 10,26%	39 100,00%	Neutro	Neutro
11 ou mais	17 24,28%	5 7,14%	17 24,29%	20 28,57%	11 15,71%	70 100,00%	Neutro	M. C.

Fonte: dados da pesquisa.

Legenda: F.I.= Fortemente Inconsciente; M. I. = Moderadamente Inconsciente, Neutro = neutro (nem consciente, nem inconsciente), M. C. = Moderadamente Consciente, F. C. = Fortemente Consciente

Observações: 1. o Percentual deve considerar o total de respostas para cada grupo de experiência em TI: 100,00% para “até 10” equivalem a 39 respostas; 100,00% para “11 ou mais” equivalem a 70 respostas. 2. Resultados oriundos da tabulação cruzada da questão 3 com a 6, propostas no APÊNDICE C

5 CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

Este capítulo apresenta as considerações finais a respeito desta pesquisa, cujo objetivo principal foi investigar a percepção sobre conscientização em segurança cibernética de trabalhadores em uma organização pública federal brasileira. Foi desenvolvido um estudo predominantemente quantitativo, com aplicação de questionários via formulário eletrônico disponível pela internet, complementado por exame de documentos a respeito da referida organização.

Da coleta de dados primários, obteve-se uma amostra de 109 trabalhadores da organização pública federal, integrante da administração indireta e com área de atuação em órgãos da sede no Distrito Federal e em superintendências dos estados da federação, com experiência em TI segmentada em até 10 anos e acima de 11 anos. Essa coleta de dados ocorreu por meio de questionário previamente testado, contendo 13 perguntas e baseado no estudo de Ngoma (2019). Para o tratamento dos dados, utilizou-se estatística descritiva, com aferição da mediana e moda.

O primeiro objetivo específico desta pesquisa foi identificar a percepção de trabalhadores em uma organização pública federal brasileira sobre as principais ameaças à segurança cibernética, com base na revisão de literatura. Com base nos resultados descritos na Seção 4.1, apurou-se 97,25% do total de respostas válidas com ‘frequentemente’ ou ‘sempre’ reconhecendo que as ameaças à segurança cibernética têm impacto negativo na organização. Houve 94,50% das respostas válidas concordando em alguma medida com a importância dos alertas de ameaças para aprimorar a cultura de segurança cibernética. Apurou-se que 65,14% das respostas válidas concordando que o alerta frequente sobre ameaças à segurança cibernética motiva os usuários a comportamento online seguro. 58,33% de respondentes válidos declararam não receber comunicação sobre as ameaças à segurança cibernética, embora a organização evidenciasse tal comunicação por documentos.

Adicionalmente, buscou-se alcançar o segundo objetivo específico - Descrever a percepção desses trabalhadores sobre conscientização em segurança cibernética, com base na revisão de literatura. Para 80,73% do total de respostas válidas, houve percepção que a organização nunca ou raramente promove treinamentos sobre segurança cibernética, embora exista sinalização por documentos de ações de treinamento promovidas pela organização. Constatou-se para 74,07% das respostas válidas que o canal e-mail está entre aqueles pelo qual

a organização comunica ameaças à segurança cibernética. Para 67,92% das respostas válidas, a área de TI foi lembrada como responsável pela conscientização em segurança cibernética. Houve 61,47% do total de respondentes válidos indicando que desconhecem ou não tem ciência de política formal de segurança cibernética. Tanto a moda quanto a mediana evidenciaram a percepção neutra dos respondentes quanto à ciência de um comitê envolvido em questões de segurança cibernética. Houve 40,37% do total de respostas válidas indicando alguma consciência de iniciativa estratégica da organização para abordar a segurança cibernética.

O terceiro objetivo específico - comparar a percepção previamente descrita sobre conscientização em segurança cibernética segundo a área de atuação do trabalhador na organização pública federal brasileira. Os resultados exibidos na Seção 4.3, permitiram constatar que a percepção da maioria dos respondentes nos órgãos e unidades descentralizadas é a seguinte: 1. nunca ou raramente a organização promove treinamentos sobre segurança cibernética; 2. O e-mail é o canal de comunicação pelos quais a organização comunica ameaças à segurança cibernética; 3. a área de TI é responsável pela conscientização em segurança cibernética; 4. não sabem ou desconhecem a existência de uma política formal de segurança cibernética.

Ainda com relação ao terceiro objetivo específico, houve 42,10% de respondentes válidos dos órgãos e 38,46% dos respondentes válidos das superintendências que se declararam cientes das iniciativas estratégicas de segurança cibernética da organização. Cerca de 34,62% de respondentes válidos dos órgãos declararam-se neutros em relação a existência de comitê dedicado a questões de segurança cibernética, enquanto 28,07% dos respondentes válidos de unidades descentralizadas declararam total inconsciência quanto a existência desse comitê.

O quarto objetivo específico foi diferenciar a percepção previamente descrita de trabalhadores segundo sua experiência prévia em Tecnologia da Informação. Os resultados descritos e analisados na Seção 4.4, permitiram constatar que a percepção da maioria dos respondentes com até 10 anos com experiência de TI e com 11 anos ou mais de experiência de TI: 1. nunca ou raramente a organização promove treinamentos sobre segurança cibernética; 2. O e-mail é o canal de comunicação pelos quais a organização comunica ameaças à segurança cibernética; 3. a área de TI é responsável pela conscientização em segurança cibernética.

Ainda com relação ao quarto objetivo específico, houve 82,05% dos respondentes com até 10 anos de experiência em TI e 50,00% de respondentes com 11 anos ou mais com experiência em TI que não sabem ou desconhecem que a organização possui uma política formal de segurança cibernética. houve 33,34% de respondentes válidos com até 10 anos de experiência de TI e 44,28% dos respondentes válidos com 11 anos ou mais de experiência de TI que se declararam moderadamente ou fortemente cientes de iniciativa estratégica da organização para abordar a segurança cibernética. Cerca de 23,28% de respondentes válidos com até 10 anos de experiência de TI e 40,00% dos respondentes válidos com 11 anos ou mais de experiência de TI declararam-se moderadamente ou fortemente conscientes quanto a existência de comitê interno ou externo envolvido em questões de segurança cibernética.

O atendimento aos objetivos específicos permitiu o alcance do objetivo geral do estudo. Ao investigar a percepção sobre conscientização em segurança cibernética de trabalhadores em uma organização pública federal brasileira, constatou-se que 97,25% dos respondentes reconhecem os impactos negativos das ameaças à segurança cibernética para a organização e que 94,50% desses respondentes sinalizaram que a comunicação frequente dessas ameaças motiva-os a adotarem práticas online seguras. Contudo, 80,73% do total de respostas indicaram a percepção de que a organização nunca ou raramente promove treinamentos sobre segurança cibernética e houve 61,47% do total de respondentes indicando a percepção de que desconhecem ou não tem ciência de política formal de segurança cibernética, apesar de as fontes secundárias evidenciarem a existência de treinamento e de tal política.

Os resultados obtidos, especialmente o confronto das percepções dos respondentes com evidências documentais, revelam oportunidades no sentido de sugerir à organização reflexão sobre iniciativas para o aprimoramento da conscientização em segurança cibernética. Essas iniciativas, em geral, podem ser estendidas a órgãos e a unidades descentralizadas, existindo, inclusive, possibilidade para estender tais iniciativas aos trabalhadores com experiência de TI até 10 anos e experiência superior a 11 anos. Alguns pontos para exame contemplam a divulgação de treinamento em segurança cibernética, a divulgação de iniciativas estratégicas sobre segurança cibernética, a divulgação da existência de uma política formal de segurança cibernética e de comitê que dispõe sobre o tema.

Este estudo pode auxiliar o aprimoramento da estratégia de

conscientização em segurança cibernética da organização estudada, podendo contribuir para reflexões de gestores, acadêmicos e demais partes interessadas a respeito da percepção sobre conscientização em segurança cibernética de organizações públicas no Brasil. Importante citar, contudo, que possui delimitações. A primeira delas é o tamanho da amostra não probabilística de 109 respondentes. Adicionalmente, houve questões nos resultados em que as análises das respostas válidas levaram elas a não totalizar 109 respondentes e, por conta disso, recomenda-se que as análises empreguem não apenas a contagem de frequências, mas também o exame de percentuais de respostas válidas. Os dados primários coletados dizem respeito a percepções dos respondentes e os dados secundários são fontes de evidência textual referentes ao período em que foram coletados.

Como sugestões de pesquisas futuras, pode-se conceber um ou mais estudos de caso para avaliação e aprimoramento da conscientização da segurança cibernética na organização estudada, inclusive em outros períodos de análise. É possível, também, avaliar a efetividade de soluções de mercado voltadas à conscientização em segurança cibernética por meio de estudos comparando resultados, no contexto de outras organizações da administração pública. Ademais, a revisão de literatura demonstra que pesquisas de conscientização em segurança cibernética no Brasil são escassas. Nesse sentido, sugere-se aplicação de estudos similares em outras organizações públicas de outras esferas de poder, atuantes em estados, Distrito Federal ou municípios do Brasil e do Exterior. Por fim, sugere-se estudar a percepção sobre conscientização em segurança cibernética empregando análises com recursos de estatísticas inferenciais.

REFERÊNCIAS

ABNT - Associação Brasileira de Normas Técnicas. ABNT NBR ISSO/IEC 27032:2015. Tecnologia da Informação – Técnicas de segurança – **Diretrizes para segurança cibernética**. Rio de Janeiro: ABNT, 2015. 62p.

AGUIAR, Bernardo; CORREIA, Walter; CAMPOS, Fábio. **Uso da Escala Likert na Análise de Jogos**. Arts & Design Track, Salvador, 2011. Disponível em: http://www.sbgames.org/sbgames2011/proceedings/sbgames/papers/art/short/91952.pdf. Acesso em: 13 de setembro de 2022.

ALEXANDRE, Neusa Maria Costa; COLUCI, Marina Zambon Orpinelli. **Validade de conteúdo** nos processos de construção e adaptação de instrumentos de medidas. Ciencia & saúde coletiva, v. 16, p. 3061-3068, 2011. Disponível em https://www.scielo.br/j/csc/a/5vBh8PmW5g4Nqxz3r999vrn/abstract/?lang=pt. Acesso em 14/11/2022.

ALGHAMDI, Sultan; WIN, Khin Than; VLAHU-GJORGIEVSKA, Elena. Employees' intentions toward **complying with information security controls** in Saudi Arabia's public organisations. Government Information Quarterly, v. 39, n. 4, article 101721, p. 1-18, 2022. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0740624X22000545. Acesso em 29/12/2022.

ANDREASSON, Annika; ARTMAN, Henrik; BRYNIELSSON, Joel; FRANKE, Ulrik. **A Census of Swedish Public Sector Employee Communication on Cybersecurity during the COVID-19 Pandemic**. In: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). IEEE, 2021. p. 1-8. Disponível em: https://ieeexplore.ieee.org/xpl/conhome/9478074/proceeding. Acesso em 16/06/2022.

ANDRONACHE, Alina. **Increasing Security Awareness through Lenses of Cybersecurity Culture**. Journal of Information Systems & Operations Management, v. 15, n. 1, 2021. Disponível em: https://www.researchgate.net/profile/Alina-Andronache-2/publication/353322243_Increasing_Security_Awarenesss_Through_Lenses_of_Cybersecurity_Culture/links/613c994f4e1df271062b528b/Increasing-Security-Awarenesss-Through-Lenses-of-Cybersecurity-Culture.pdf. Acesso em 22/08/2022

BABBIE, Earl R. **The practice of social research**. Cengage learning, 2020.*E-book*

BACUD, Maria Lourdes; MÄSES, Sten. **Game-Based Learning for Cybersecurity Awareness Training Programmes in the Public Sector**. In: ECEL 2021 20th European Conference on e-Learning. Academic Conferences International limited, 2021. p. 50.

BERKMAN, Henk; JONAC, Jonathan; LEEC, Gladys. **Cybersecurity awareness and market valuations**. Journal of Accounting and Public Policy, v. 37, n. 6, 2018, p. 508-526. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0278425418302370. Acesso em 06/07/2022

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde : segurança cibernética no Brasil** / Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Raphael Mandarino Junior. – Brasília: GSIPR/SE/DSIC, 2010.

_____. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em 25/08/2022.

_____. Decreto nº 10.222 de 06 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm#:~:text=DECRETO%20N%C2%BA%2010.222%2C%20DE%205,que%20lhe%20confere%20o%20art.. Acesso em 25/08/2022.

_____. Decreto-Lei nº 200, de 25 de fevereiro de 1967. Dispõe sôbre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm#view . Acesso em 16/06/2022.

_____. Presidência da República. Gabinete de Segurança Institucional. Portaria GSI/PR nº 93/2019 - Glossário de Segurança da Informação. Disponível em https://www.gov.br/gsi/pt-br/assuntos/dsic/glossario-de-seguranca-da-informacao-1. Acesso em 25/08/2022

_____. Portal da Transparência. Detalhamento de Servidores e Pensionistas. Disponível em: https://transparencia.gov.br/servidores/consulta?paginacaoSimples=true&tamanhoPagina=&offset=&direcaoOrdenacao=asc&colunasSelecionadas=detalhar%2Ctipo%2Ccpf%2Cnome%2CorgaoServidorExercicio%2CorgaoServidorLotacao%2Cmatricula%2CtipoVinculo%2Cfuncao&orgaosServidorExercicio=OR42201&ordenarPor=nome&direcao=asc. Acessado em 04/09/2022.

_____. Tribunal de Contas da União. **Estratégia de Fiscalização do TCU em segurança da informação e segurança cibernética 2020-2023**. 2021 Disponível em https://portal.tcu.gov.br/estrategia-de-fiscalizacao-do-tcu-em-seguranca-da-informacao-e-seguranca-cibernetica-2020-2023.htm. Acesso em 16/06/2022.

_____. Tribunal de Contas da União. Cinco controles de segurança cibernética para ontem / Tribunal de Contas da União. – Brasília : **TCU**, 2022. Disponível em: https://portal.tcu.gov.br/5-controles-de-seguranca-cibernetica.htm. Acesso em 14/09/2022.

CATOTA, Frankie E.; MORGAN, M. Granger; SICKER, Douglas C. **Cybersecurity education in a developing nation**: The Ecuadorian environment. Journal of Cybersecurity, v. 5, n. 1, p. tyz001, 2019. Disponível em: https://academic.oup.com/cybersecurity/article-pdf/doi/10.1093/cybsec/tyz001/28086821/tyz001.pdf. Acesso em 14/08/2022.

CENTER FOR INTERNET SECURITY. **CIS Controls TM V8**. Center for Internet Security, 2021. Disponível em https://learn.cisecurity.org/cis-controls-download. Acesso em 16/07/2022.

COLAUTO, Romualdo Douglas; BEUREN, Ilse Maria. **Coleta, análise e interpretação dos dados**. Como elaborar trabalhos monográficos em contabilidade: teoria e prática 3 (2003): 117-144.

CYBEREDGE GROUP. **2022 Cyberthreat Defense Report**. 2022. Disponível em: CyberEdge-2022-CDR-Report.pdf (cyber-edge.com). Acessado em 29 de dezembro de 2022.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. ENISA Threat Landscape 2021: April 2020 to Mid-July 2021 October, 2021 Disponível em https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021. Acesso em 16/06/2022.

FERNANDES, Aryel. **Saúde confirma ataque hacker**; Anonymous questiona versão do governo no Twitter. Disponível em: Saúde confirma ataque hacker; Anonymous questiona versão do governo (istoedinheiro.com.br). Acesso em 31/08/2022.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**. 6. ed. – São Paulo : Atlas, 2018.

HANEY, Julie; JACOBS, Jody; FURMAN, Susanne; BARRIENTOS, Fernando; . Approaches and challenges of federal **cybersecurity awareness programs**. 2022. Disponível em https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934347 Acesso em 31/08/2022.

HIJJI, Mohammad; ALAM, Gulzar. **Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees**. Sensors, v. 22, n. 22, article 8663, p. 1-23, 2022. Disponível em: https://www.mdpi.com/1424-8220/22/22/8663. Acesso em 29/12/2022.

HUTTON, S. **Why phishing attacks are increasingly targeting the public sector** (and what you can do about it). Retrieved June, v. 14, p. 2018, 2017. Disponível em: https://gcn.com/cybersecurity/2017/10/why-phishing-attacks-are-increasingly-targeting-the-public-sector-and-what-you-can-do-about-it/304564/ . Acesso em 29/12/2022.

INTERNATIONAL TELECOMMUNICATION UNION. **Global Cybersecurity Index 2020**. ITU, 2020. 172p. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. Acesso em 15/06/2022.

KARAGOZLU, Damla. **Determination of cyber security ensuring behaviours of pre-service teachers**. Cypriot Journal of Educational Science. 15(6), p.1698-1706, 2020. Disponível em http://files.eric.ed.gov/fulltext/EJ1284571.pdf. Acesso em 17/07/2022.

KARPIUK, Mirosław. **The obligations of public entities within the national cybersecurity system**. Cybersecurity and Law, v. 4, n. 2, p. 57-72, 2021. Disponível em: https://bibliotekanauki.pl/articles/2159295.pdf . Acesso em 24/08/2022.

KHANDO, K.; GAO, S; ISLAM, S;M.; SALMAN, A. .Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & Security, v. 106, article 102267, p. 1-22. 2021. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404821000912. Acesso em 14/08/2022.

MAMBILE, Cesilia; MBOGORO, Peter**. Cybercrimes awareness, cyber laws and its practice in public sector Tanzania**. International Journal Of Advanced Technology And Engineering Exploration, v. 7, n. 68, p. 119, 2020. Disponível em https://www.proquest.com/openview/1df97c1beeb42b1ba4a4439b7ac76a0c/1?pq-origsite=gscholar&cbl=2037694. Acesso em 14/07/2022

NGOMA, Mduduzi Langalibalele. **Cybersecurity Awareness in South African Public Sector Organisations**. 2019. Dissertação de Mestrado. University of Johannesburg (South Africa).Disponível em: https://search.proquest.com/openview/01424f13f773a0b79eaaa73104fc722c/1?pg-origsite=gscholar&cbl=18750&diss=y Acesso em 15/06/2022.

_____; KEEVY, Monique; RAMA, Pranisha. **Cyber-security awareness of South African state-mandated public sector organisations**. Southern African Journal of Accountability and Auditing Research, v. 23, n. 1, p. 53-64, 2021.Disponível em https://journals.co.za/doi/abs/10.54483/sajaar.2021.23.1.4. Acesso em 16/06/2022

NAG, Abhijit Kumar BHADAURIA, Vikram S., GIBSON, Camille, NEUPANE, Ram C., CREIDER, Daniel. A Conceptual Learning Framework of **Cybersecurity Education for Military and Law Enforcement**: Workforce Development.

International Journal of Smart Education and Urban Society (IJSEUS), v. 13, n. 1, p. 1-14, 2022. Disponível em: https://www.igi-global.com/pdf.aspx?tid=309953&ptid=278264&ctid=4&oa=true&isxn=9781683183266. Acesso em 02/12/2022.

NIKOLOVA, Irena. **Best Practice for Cybersecurity Capacity Building in Bulgaria's Public Sector**. Information & Security, v. 38, p. 79-92, 2017. Disponível em https://connections-qj.org/ru/system/files/3806_cybersecurity_capacity.pdf. Acesso em 06/07/2022.

NURSE, Jason R. C. **Cybersecurity Awareness**. In: Jajodia S., Samarati P., Yung M. (eds) Encyclopedia of Cryptography, Security and Privacy. Springer, Berlin, Heidelberg,2021, p. 1-5. Disponível em: https://arxiv.org/pdf/2103.00474v1. Acesso em 14/10/2022

OEA - ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Revisão da capacidade de Cibersegurança. 2020. Disponível em: <http://www.oas.org/pt/ssm/cicte/docs/PORTRevisao-da-Capacidade-de-Ciberseguranca.pdf>. Acesso em 02/08/2022.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. Recommendation of the Council Concerning **Guidelines for the Security of Information Systems and Networks** - Towards a Culture of Security, OECD/LEGAL/0312. OECD, 2022. Disponível em https://legalinstruments.oecd.org/public/doc/116/116.en.pdf Acesso em 29/11/2022.

PEREIRA, Alexandre Pimenta Batista; SOUZA, Larissa Martins de. **Acerca da dicotomia atividade-fim e atividade-meio e suas implicações na licitude da terceirização trabalhista**. Revista de Informação Legislativa, v. 51, n. 201, p. 175-192, 2014.

PETERSEN, Rodney; SANTOS, Danielle; SMITCH, Matthew C.; WETZEL, Karen A.; WITTE, Greg. **Workforce framework for cybersecurity** (NICE framework). 2020.Disponivel em https://www.nist.gov/publications/workforce-framework-cybersecurity-nice-framework. Acesso em 02/07/2022.

PRODANOV, Cleber Cristiano; DE FREITAS, Ernani Cesar. Metodologia do trabalho científico: **métodos e técnicas da pesquisa e do trabalho acadêmico-2ª Edição**. Editora Feevale, 2013. Ebook. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=zUDsAQAAQBAJ&oi=fnd&pg=PA13&dq=prodanov%3B+freitas,+2013&ots=dc25hbz8EJ&sig=mEZp133Z-S3XJPAtdNXKFvnUD8c&redir_esc=y#v=onepage&q=prodanov%3B%20freitas%2C%202013&f=false. Acesso em: 14/10/2022.

PWC. PwC **Cyber Threats 2021**: A Year in Retrospect. PwC, 2021. Disponível em: https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf Acesso em 02/10/2022.

REIS, R. S. dos ; ALVES, C. A. M. **. Segurança Cibernética no Setor Bancário: Análise da Coautoria e da Co-Ocorrência de Palavras-Chaves em Artigos Científicos Presentes em Bases de Dados da Área de Administração**. In: IX Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade - Singep, 2021, Evento Oline. IX Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade - Singep, 2021

SAMPIERI, Roberto Hernández; COLLADO, Carlos Fernández; LUCIO, María del Pilar Baptista. **Metodologia de Pesquisa**. 5. ed. São Paulo: Mcgraw-hill, 2013.613 p.

SHERE, Anjuli RK; NURSE, Jason RC; MARTIN, Andrew. Threats to Journalists from the Consumer Internet of Things. In: 2022 International Conference on Cybersecurity, Situational Awareness and Social Media. Proceedings in Complexity. Springer 2022. Disponível em: https://kar.kent.ac.uk/94898/ Acesso em 14/10/2022

SIEGEL, Sidney. **Estatística não-paramétrica para ciências do comportamento**. 2. Porto Alegre Grupo A 2017

SYMANTEC. The Threat Landscape in 2021. White paper. Symantec, 2021. Disponível em https://symantec.drift.click/Threat_Landscape_2021_Whitepaper. Acesso em 02/05/2022.

TIRUMALA, S. S.; VALLURI, Maheswara Rao; BABU, G. **A. A survey on cybersecurity awareness concerns, practices and conceptual measures**. In: 2019 International Conference on Computer Communication and Informatics (ICCCI). IEEE. p. 1-6, 2019. Disponível em https://ieeexplore.ieee.org/xpl/conhome/8811525/proceeding. Acesso em 01/08/2022.

WIRTZ, Bernd W.; WEYERER, Jan C. **Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats**. International Journal of Public Administration, v. 40, n. 13, p. 1085-1100, 2017. Disponível em https://www.tandfonline.com/doi/full/10.1080/01900692.2016.1242614. Acesso em 14/07/2022

APÊNDICE A: Termo de Autorização

[redacted]
Coordenação-Geral de [redacted]
Divisão de Suporte Técnico [redacted]

Processo nº [redacted]
Interessado: Coordenação-Geral de [redacted], Diretoria de [redacted]

Autorização

Informo ciência do trabalho a ser realizado pela pesquisadora da Universidade de Brasília, Daniela Almeida, orientada pelo Dr. Carlos André de Melo Alves, a respeito da percepção sobre conscientização em segurança cibernética de trabalhadores em uma organização pública federal, com a finalidade de conclusão do curso de Administração.

Autorizo a realização de entrevistas, a proposição de questionários e o acesso aos documentos internos não sigilosos desta Autarquia, necessários à realização da pesquisa, a partir do segundo semestre de 2022. Adicionalmente, a pesquisadora informa que os documentos serão acessados exclusivamente para a finalidade acadêmica de subsidiar a realização do referido trabalho.

Autorizo, também, que a pesquisadora convide os trabalhadores da Autarquia a responderem questionário; em adição, a pesquisadora informa que se compromete a preservar o anonimato dos trabalhadores que aceitarem participar da pesquisa.

Por fim, a pesquisadora informa que a coleta de dados nesta pesquisa seguirá os critérios constantes no OFÍCIO CIRCULAR N.º 2/2021/CONEP/SECNS/MS, de 24 de fevereiro de 2021, que orienta a realização de procedimentos de pesquisas em qualquer etapa no ambiente virtual, estabelecendo procedimentos éticos que envolvem contato por meio do ambiente virtual, a segurança na transferência e no armazenamento de dados e ao conteúdo dos documentos tramitados.

Em tempo, após assinado, este Termo de Autorização será levado ao conhecimento da pesquisadora, por meio do seguinte endereço eletrônico, por ela informado: [redacted].

Brasília, [redacted] de 2022.

[redacted]
Diretor de [redacted]
[redacted]

logotipo Documento assinado eletronicamente por [redacted], **Diretor(a)**, em [redacted] conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

QRCode Assinatura A autenticidade deste documento pode ser conferida no site [redacted]/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador [redacted] e o código CRC [redacted].

Referência: Processo nº [redacted] SEI nº [redacted]

APÊNDICE B: MENSAGEM DE APRESENTAÇÃO DO QUESTIONÁRIO

Prezado potencial participante desta pesquisa:

Este questionário tem por objetivo avaliar a consciência atual da segurança cibernética de trabalhadores desta Autarquia Federal. Este estudo está sendo conduzido pela pesquisadora Daniela Almeida ([redacted]), como parte de sua graduação no curso Bacharelado em Administração. O título de seu estudo é Percepção da Conscientização em Segurança Cibernética de Trabalhadores de Organização Pública, sob supervisão do Professor Doutor Carlos André de Melo Alves ([redacted]).

O foco deste estudo está nos trabalhadores desta Autarquia Pública Federal, usuários de recursos de Tecnologia da Informação. Este estudo visa a beneficiar o corpo de conhecimento, pois até o momento não foi realizado estudo semelhante no Brasil. Tendo em vista a exponencial expansão da tecnologia (sobretudo após a transformação digital do governo federal) e dos incidentes cibernéticos, julga-se fundamental reunir um entendimento mais claro nesta área.

Os dados coletados para este estudo serão mantidos por um período de três anos após a conclusão do estudo. As seguintes medidas de segurança serão aplicadas aos dados coletados:

• Criptografia de informações identificáveis;

• Restrição do acesso a dados identificáveis;

• Armazenamento com segurança os dados ou documentos coletados em dispositivo protegido; e/ou

• Atribuição de um código de segurança aos dados digitais.

Os participantes receberão feedback sobre o estudo por meio de uma cópia do artigo e resultados do Trabalho de Conclusão de Curso.

Sua disposição em participar voluntariamente desta pesquisa é muito valiosa e contribui para a criação de novos conhecimentos. Esteja informado que as suas respostas são totalmente confidenciais – ou seja, os dados pessoais apenas serão do conhecimento da pesquisadora e do professor orientador. A coleta e tratamento dos dados obedecerá, no que couber, à lei nº 13.709/2018. Os resultados de todos os entrevistados serão agrupados e relatados como uma unidade, e suas respostas específicas não serão relatadas individualmente, mas usando pseudônimos.

O questionário será enviado por e-mail a todos os trabalhadores amostrados para participar da pesquisa. Os endereços de e-mail dos participantes

foram obtidos por meio de autorização formal da Autarquia.

Este questionário não deve levar mais de 15 minutos para ser preenchido.

Você é lembrado e informado por meio deste, que você não é obrigado de forma alguma a participar deste estudo. Você está participando voluntariamente e pode optar por se retirar do processo a qualquer momento, sem medo ou consequências. Você, como respondente, é lembrado e informado sobre seu direito à privacidade, confidencialidade, igualdade, justiça, dignidade humana, liberdade de escolha, liberdade de expressão, acesso à informação e acesso à comunidade científica.

Por favor, responda da forma mais aberta e franca possível às perguntas. Pede-se, ainda, que você confirme que leu e compreendeu as informações acima, e que o coletor de dados que está aplicando este questionário a você explicou adequadamente, selecionando no campo disponível abaixo.

☑ Eu, como respondente, entendo meus direitos neste processo e procedo de boa vontade e voluntariamente com o questionário:

Para qualquer dúvida sobre este questionário, entre em contato comigo em: ou alternativamente via o e-mail: [redacted]

Obrigada desde já por sua cooperação.

APÊNDICE C: QUESTIONÁRIO

Seção A: Informações Gerais

1. Qual é a área em que atua? (selecione uma opção) *

- Órgãos
- Unidades descentralizadas

* Para responder a esta pergunta, tenha como base as definições da estrutura regimental instituída pelo [redacted]

Órgãos: todas as unidades localizadas [redacted] Sede ([redacted] Diretorias, Procuradoria Federal Especializada, Auditoria Interna e Corregedoria Geral);

Unidades descentralizadas: Superintendências Regionais [redacted].

2. Qual grau de escolaridade você possui? (selecione uma opção)

- Nível fundamental
- Nível médio
- Graduação
- Pós-graduação (especialização, mestrado e doutorado)

3. Selecione o intervalo que indica seus anos de experiência com Tecnologia da Informação (selecione uma opção).

- zero
- até 1
- 1-5
- 6-10
- 11 ou mais

4. Quem, em sua organização é responsável pela conscientização sobre segurança cibernética? (selecione todas as opções aplicáveis)

- A organização
- A área de Tecnologia da Informação
- A área de Orçamento/ Finanças
- A área de Recursos Humanos
- Outra
- Não sei / desconheço

5. Você está ciente se existe um comitê interno ou externo envolvido exclusivamente em questões de segurança cibernética em sua organização? (selecione uma opção)

- Fortemente consciente
- Moderadamente consciente
- Neutro (nem consciente nem inconsciente)
- Moderadamente inconsciente
- Fortemente inconsciente

6. Você conhece alguma iniciativa estratégica em sua organização para abordar a segurança cibernética? (selecione uma opção)

- Fortemente consciente
- Moderadamente consciente
- Neutro (nem consciente nem inconsciente)
- Moderadamente inconsciente
- Fortemente inconsciente

Seção B Ameaças e riscos à segurança cibernética

7. Os usuários da sua organização são alertados sobre as seguintes ameaças à segurança cibernética? (selecione todas as opções aplicáveis)

- Phishing
- Malware
- Ransomware
- Nenhum

8. Sua organização lembra consistentemente os usuários de práticas on-line seguras? (selecione uma opção)

- Nunca
- Raramente
- Ocasionalmente
- Frequentemente
- Sempre

9. Acredito que alertar frequentemente os usuários de várias ameaças à segurança cibernética os motivará a praticarem comportamento on-line seguro. (selecione uma opção)

- Discordo totalmente
- Discordo moderadamente
- Neutro (nem concordo nem discorda)
- Concordo moderadamente
- Concordo fortemente

10. Você acredita que ameaças cibernéticas podem ter um impacto negativo na organização? (selecione uma opção)

- Nunca
- Raramente
- Ocasionalmente
- Frequentemente
- Sempre

Seção C: Conscientização sobre segurança cibernética

11. Sua organização tem uma política formal de segurança cibernética? (selecione uma opção)

- Sim
- Não

- Não sei / Desconheço

12. Sua organização comunica ameaças à segurança cibernética e, se for o caso, por meio de quais dos seguintes canais? (selecione todas as opções aplicáveis)

- E-mail
- Boletim informativo
- Textos
- Intranet
- Não comunica ameaças à segurança cibernética
- Outros

13. Sua organização promove treinamento formal de conscientização sobre segurança cibernética? (selecione uma opção)

- Nunca
- Raramente
- Ocasionalmente
- Frequentemente
- Sempre

Obrigado por participar!

Todas as informações serão tratadas como confidenciais e serão usadas apenas para produzir resultados agregados