



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS FLORIANO
CURSO TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

JOÃO RAFAEL OLIVEIRA TAVARES

**ENGENHARIA SOCIAL NO HOME OFFICE: ANÁLISE COMPARATIVA DA
PERCEPÇÃO DE VULNERABILIDADES DE ATAQUES DE PHISHING ENTRE
SERVIDORES REMOTOS E PRESENCIAIS DO INSTITUTO FEDERAL DO PIAUÍ.**

FLORIANO

2026

JOÃO RAFAEL OLIVEIRA TAVARES

ENGENHARIA SOCIAL NO HOME OFFICE: ANÁLISE COMPARATIVA DA
PERCEPÇÃO DE VULNERABILIDADES DE ATAQUES DE PHISHING ENTRE
SERVIDORES REMOTOS E PRESENCIAIS DO INSTITUTO FEDERAL DO PIAUÍ

Trabalho de Conclusão de Curso (artigo científico) apresentado como exigência parcial para obtenção do diploma do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Floriano .

Orientador: Prof. Dr. Leandro Rodrigues de Oliveira.

FLORIANO

2026

ENGENHARIA SOCIAL NO HOME OFFICE: ANÁLISE COMPARATIVA DA PERCEPÇÃO DE VULNERABILIDADES DE ATAQUES DE PHISHING ENTRE SERVIDORES REMOTOS E PRESENCIAIS DO INSTITUTO FEDERAL DO PIAUÍ

João Rafael Oliveira Tavares¹
Leandro Rodrigues de Oliveira²

RESUMO

A segurança da informação é indispensável para a sustentabilidade e a governança das organizações públicas. A migração abrupta para o *home office* expandiu a superfície de ataques cibernéticos, deslocando os servidores do perímetro de defesa corporativa tradicional. Sob a premissa de que o fator humano constitui o elo mais vulnerável, frequentemente explorado via engenharia social e *phishing*, este estudo analisou comparativamente a percepção de vulnerabilidade e o comportamento preventivo entre servidores em regime presencial (n=74) e remoto/híbrido (n=155) no Instituto Federal do Piauí (IFPI). Metodologicamente, realizou-se uma pesquisa descritivo-comparativa do tipo *survey* (N=229). Os dados foram analisados por estatística descritiva, testes não-paramétricos (Mann-Whitney, Qui-quadrado) e Teste *t* de Student. Os resultados empíricos refutaram as hipóteses de que o ambiente remoto amplia a vulnerabilidade prática ou inibe a validação social informal: ambos os grupos apresentaram elevados e homogêneos índices de acerto (>96%) em cenários comportamentais simulados (Reitoria, RH e TI). Contudo, constatou-se uma diferença estatisticamente significativa no comportamento relacionado ao uso de redes Wi-Fi públicas ($p<0,05$), com maior exposição factual dos servidores remotos. O diagnóstico revelou ainda um cenário de carência crônica de treinamento, atingindo 87,8% da amostra de forma homogênea e agnóstica ao regime de trabalho. Conclui-se que a resiliência observada decorre de uma postura defensiva intuitiva e não de maturidade digital formal, ressaltando a urgência de programas permanentes de *Security Awareness* focados na mobilidade.

Palavras-chave: Engenharia Social; Home Office; Phishing; Segurança da Informação; Percepção de Risco.

¹ Graduando em Tecnologia em Análise e Desenvolvimento de Sistemas. Instituto Federal de Educação, Ciência e Tecnologia do Piauí. joao.tavares.2020114ielm08.3101@gmail.com.

² PhD in Administration - Behavioral Strategy - Mestre em Gestão Pública, Professor Associado do IFPI, Avaliador MEC - INEP, Advogado e Contador. leandro@ifpi.edu.br leandroliveir9@gmail.com

Data de aprovação: 22/06/2026

**SOCIAL ENGINEERING IN REMOTE WORK: A COMPARATIVE ANALYSIS OF
VULNERABILITY PERCEPTION TO PHISHING ATTACKS BETWEEN REMOTE AND ON-SITE
PUBLIC SERVANTS AT THE FEDERAL INSTITUTE OF PIAUÍ**

João Rafael Oliveira Tavares¹
Leandro Rodrigues de Oliveira²

ABSTRACT

Information security is fundamental to the sustainability and governance of public organizations. The abrupt migration to remote work expanded the cyber attack surface, displacing employees from traditional corporate defense perimeters. Grounded on the premise that the human factor is the weakest link, often exploited via social engineering and phishing, this study comparatively analyzed the risk perception and preventive behavior between on-site (n=74) and remote/hybrid (n=155) public servants at the Federal Institute of Piauí (IFPI). Methodologically, a descriptive-comparative survey was conducted (N=229). Data were analyzed using descriptive statistics, non-parametric tests (Mann-Whitney, Chi-square), and Student's t-test. Empirical results refuted the hypotheses that remote environments amplify practical vulnerability or inhibit informal social validation: both groups showed high and homogeneous hit rates (>96%) in simulated behavioral scenarios (Rectorate, HR, and IT). However, a statistically significant difference was found in behaviors related to public Wi-Fi usage ($p < 0.05$), reflecting higher factual exposure among remote workers. The diagnostic also revealed a scenario of chronic lack of training, affecting 87.8% of the sample homogeneously across both work regimes. In conclusion, the observed resilience stems from an intuitive defensive stance rather than formal digital maturity, highlighting the urgent need for continuous Security Awareness programs tailored to workforce mobility.

Keywords: Social Engineering; Home Office; Phishing; Information Security; Risk Perception.

¹ Undergraduate student in Systems Analysis and Development. Federal Institute of Education, Science and Technology of Piauí. joao.tavares.2020114ielm08.3101@gmail.com.

² PhD in Administration (Behavioral Strategy), Master in Public Management, Associate Professor at IFPI, MEC - INEP Evaluator, Attorney at Law and Accountant. leandro@ifpi.edu.br leandroliveir9@gmail.com

Date of approval: June 22, 2026

1 INTRODUÇÃO

No cenário contemporâneo, a segurança da informação (SI) consolidou-se como um pilar estratégico indissociável da sustentabilidade, perenidade e governança de organizações públicas e privadas, sendo responsável direta por salvaguardar ativos críticos contra ameaças cibernéticas crescentes e acessos não autorizados (Mitnick; Simon, 2003). Historicamente pautada em soluções tecnológicas de perímetro, como criptografia de ponta, barreiras de *firewalls* e sistemas robustos de detecção de intrusão, as defesas organizacionais enfrentaram uma disrupção sem precedentes decorrente da necessidade de continuidade operacional em períodos de crise (Azan *et al.*, 2022). Esse panorama forçou uma migração em larga escala, célere e de caráter reativo para o regime de *home office* ou teletrabalho (Park *et al.*, 2023). Tal transição descentralizou o ambiente corporativo tradicional, deslocando os colaboradores para fora das redes institucionais monitoradas e expandindo significativamente a superfície de ataque das instituições (Al-ghadhban; Al-twaijry, 2024). Em suas infra estruturas domésticas, frequentemente caracterizadas pelo uso de dispositivos pessoais (*Bring Your Own Device*- BYOD) e redes Wi-Fi residenciais desprovidas de controles robustos, os indivíduos tornaram-se alvos mais expostos e acessíveis a investidas maliciosas, desafiando as Políticas de Segurança da Informação (PSI) vigentes (Koch, 2022).

Nesse novo ecossistema descentralizado, a literatura científica e a prática de mercado convergem ao apontar que o fator humano permanece como o elo mais vulnerável, imprevisível e crítico na cadeia de custódia da segurança (Mitnick; Simon, 2003). Subvertendo as barreiras tecnológicas avançadas, os atacantes têm priorizado táticas de Engenharia Social, as quais se fundamentam na manipulação psicológica, na exploração de vieses cognitivos e na quebra de expectativa de confiança para induzir os usuários a executarem ações inseguras (Hahnagy, 2018). Dentre essas táticas, o *phishing* destaca-se pela alta prevalência, sofisticação e potencial destrutivo no ambiente digital (Abuelezz *et al.*, 2025). Caracterizado pelo envio de comunicações fraudulentas estruturadas de forma precisa para mimetizar fontes legítimas e autoridades confiáveis, o *phishing* explora deliberadamente a desatenção, o medo, a curiosidade ou o senso de urgência artificialmente criado (Amaya-Gómez *et al.*, 2023). Sob a ótica da psicologia cognitiva, tais ataques

buscam sobrecarregar o processamento mental do indivíduo, forçando tomadas de decisão rápidas baseadas no Sistema 1 — heurístico, automático e intuitivo —, em detrimento da análise analítica e reflexiva propiciada pelo Sistema 2 (Kahneman, 2011). A eficácia crônica dessas investidas demonstra empiricamente que a resiliência de uma organização depende crucialmente da prontidão cognitiva e do comportamento preventivo de seus colaboradores (Souza, 2013).

Apesar do amplo reconhecimento acerca da criticidade do comportamento humano, persiste uma lacuna teórica e empírica na literatura de segurança: o entendimento de como a percepção subjetiva de risco e a vulnerabilidade prática a ataques de engenharia social variam em função do regime de trabalho do indivíduo, especialmente no âmbito da administração pública brasileira (Azan *et al.*, 2022). Estudos anteriores em instituições educacionais indicam que, mesmo em ambientes estritamente presenciais, o nível de conhecimento dos servidores sobre as PSI é baixo e a adesão às diretrizes é insatisfatória, cenário que é agravado pela carência crônica de programas de capacitação contínua e sistemática (Martins; Silva, 2021). Todavia, com a consolidação de modelos híbridos e remotos no setor público, carece-se de um diagnóstico comparativo rigoroso (Park *et al.*, 2023). Não está claro se o distanciamento físico do suporte técnico e o isolamento em *home office* reduzem a vigilância e inibem a validação social informal de ameaças eletrônicas ou se, paradoxalmente, a consciência da descentralização eleva a cautela individual dos servidores (Al-ghadhban; Al-twaijry, 2024). Diante desse cenário complexo, emerge a seguinte questão de pesquisa: **Qual a diferença na percepção de vulnerabilidade a ataques de *phishing* entre servidores do Instituto Federal do Piauí que atuam em regime de trabalho remoto e aqueles em regime presencial, e como essa percepção se reflete no nível de conhecimento sobre práticas de segurança da informação?**

A relevância desta investigação sustenta-se em dimensões institucionais, sociais, acadêmicas e práticas de forma interdependente. Sob o prisma institucional e social, as Instituições Federais de Ensino (IFES) são custodiantes fiduciárias de um vasto e sensível patrimônio informacional, que abrange dados pessoais e acadêmicos de milhares de discentes, informações funcionais de servidores e pesquisas científicas de interesse estratégico e público (Martins; Silva, 2021). Incidentes de segurança nesses ambientes geram prejuízos que transcendem as perdas financeiras, afetando a reputação institucional e violando preceitos da Lei

Geral de Proteção de Dados - LGPD (Brasil, 2018). Do ponto de vista acadêmico, a pesquisa avança sobre a literatura ao migrar de revisões teóricas amplas para um diagnóstico empírico e comparativo situado no funcionalismo público, gerando dados primários inéditos por meio de uma abordagem descritivo-comparativa estruturada (Gil, 2017; Yin, 2015). Em termos práticos, a relevância manifesta-se na oferta de subsídios baseados em evidências estatísticas para que gestores de Tecnologia da Informação possam aprimorar suas PSI e desenhar programas de treinamento personalizados (*Security Awareness*), direcionados às vulnerabilidades específicas diagnosticadas conforme a modalidade laboral (Abuelezz *et al.*, 2025; Koch, 2022).

Para responder à questão formulada, o presente estudo estabelece como objetivo geral analisar comparativamente a percepção de vulnerabilidade a ataques de *phishing* entre os servidores que atuam em regime de trabalho presencial e remoto/híbrido no Instituto Federal do Piauí. Para o alcance desse propósito, definiram-se os seguintes objetivos específicos: fundamentar teoricamente os conceitos de engenharia social, *phishing* e os desafios de segurança da informação associados aos regimes de trabalho presencial e remoto; diagnosticar o nível de conhecimento conceitual e a percepção de risco frente a cenários de vulnerabilidade entre os servidores de ambos os regimes; analisar os dados coletados para identificar e testar a existência de diferenças estatisticamente significativas na postura preventiva dos grupos; e propor diretrizes estratégicas para um programa de conscientização em segurança da informação alinhado às necessidades evidenciadas pelos achados empíricos.

4 REFERENCIAL TEÓRICO

4.1 ENGENHARIA SOCIAL E A VULNERABILIDADE DO FATOR HUMANO

No ecossistema contemporâneo da Segurança da Informação (SI), os investimentos institucionais concentram-se historicamente no desenvolvimento de barreiras lógicas e tecnológicas (Santos, 2022). Tais mecanismos compreendem criptografia assimétrica, barreiras de *firewalls* de última geração e sistemas automatizados de detecção de intrusão (Rodrigues, 2022). Contudo, a sofisticação dessas defesas tecnológicas é frequentemente neutralizada quando os atacantes direcionam seus esforços para a manipulação da camada humana (Mitnick; Simon, 2003).

Sob essa perspectiva, o fator humano é catalogado na literatura como o elo mais vulnerável e imprevisível de toda a cadeia de custódia da segurança organizacional (Souza, 2022). Mitnick e Simon (2003) asseveram que o comportamento dos usuários, balizado por vulnerabilidades psicossociais, converte o indivíduo no principal vetor de incidentes ciberespaciais. Isso ocorre porque contornar um controle operacional por meio da persuasão humana demanda significativamente menos tempo e recursos do que a quebra forçada de algoritmos lógicos consolidados (Hadjnagy, 2018).

Essa exploração metódica das fragilidades comportamentais viabiliza-se por meio da Engenharia Social (Martins; Silva, 2021). A engenharia social é definida como o conjunto de táticas que utilizam a manipulação psicológica para induzir indivíduos a executarem ações inseguras (Hadjnagy, 2018). Essas ações incluem a revelação voluntária de credenciais de acesso, o fornecimento de dados sigilosos e a desativação inadvertida de defesas de rede (Souza, 2013).

Os engenheiros sociais operam subvertendo expectativas legítimas de interação e construindo pretextos fraudulentos (Mitnick; Simon, 2003). Tais pretextos cooptam o desejo inerente de cooperação, o medo da autoridade e a boa-fé dos colaboradores (Hadjnagy, 2018). Conforme preconizado pela literatura, a engenharia social ramifica-se classicamente entre abordagens baseadas em computador, que utilizam automação digital, e abordagens baseadas em interações humanas diretas, sustentadas pelo diálogo e pela criação de falsos laços de confiança (Mitnick; Simon, 2003).

4.1.1 Os ciclos de ataque

Os ataques de engenharia social não são eventos isolados ou improvisados; eles seguem um ciclo metodológico estruturado que aumenta sua probabilidade de sucesso (Al-ghadhban; Al-twaijry, 2024). O modelo clássico de Mitnick e Simon (2003) consolida o ataque em quatro fases principais: (1) Pesquisa (*Information Gathering*); (2) Desenvolvimento de confiança (*Rapport/Trust Development*); (3) Exploração (*Exploitation*), e (4) Execução e evasão (*Utilization/Goal*). Metodologias mais recentes de testes de penetração validam este ciclo, detalhando a fase de "Pesquisa" como a coleta sistemática de informações (abertas e sigilosas) sobre o alvo para aumentar a credibilidade do ataque (Al-ghadhban; Al-twaijry, 2024). A fase de "Exploração" é onde o atacante utiliza a confiança estabelecida para induzir a vítima a realizar a ação desejada, como revelar uma senha ou clicar em um link (Al-ghadhban; Al-twaijry, 2024; Mitnick; Simon, 2003).

Cada fase desse ciclo possui uma função crítica. A fase de "Pesquisa" (*Information Gathering*) é talvez a mais demorada e crucial, envolvendo *footprinting* e *reconnaissance*, onde o atacante utiliza fontes abertas (OSINT), como redes sociais e o site da própria instituição, ou até mesmo o lixo (*dumpster diving*), para construir um perfil detalhado do alvo (Mitnick; Simon, 2003; Martins; Silva, 2021). A fase de "Desenvolvimento de Confiança" (*Rapport*) é onde o pretexto (*pretext*) é estabelecido; o atacante usa a informação coletada (ex: nome de um chefe, um projeto em andamento) para criar uma narrativa crível que justifique o contato (Mitnick; Simon, 2003). A fase final, "Execução e Evasão" (*Utilization*), não se limita a obter o dado, mas inclui cobrir os rastros (*covering tracks*) para evitar a detecção imediata, garantindo a longevidade do acesso obtido e dificultando a resposta ao incidente (Al-ghadhban; Al-twaijry, 2024).

4.1.2 Meios de atuação

A engenharia social manifesta-se por diversos vetores de ataque, que podem ser classificados conforme o meio de contato com o alvo. Os principais vetores incluem: (1) Ataques baseados em computador, sendo o *e-mail* (Phishing) o mais comum, mas também incluindo pop-ups ou *malwares* (Santos, 2022; Martins; Silva, 2021); (2) Ataques baseados em telefone (*Vishing*), onde o atacante utiliza a voz

para se passar por uma figura de autoridade, como um técnico de TI ou gestor (Al-ghadhban; Al-twajiry, 2024); (3) Ataques baseados em interação humana (físicos), que envolvem contato pessoal, impersonação (como fingir ser um técnico ou fornecedor) ou observação direta (*shoulder surfing*) (Abuelezz *et al.*, 2025; Mitnick; Simon, 2003); e (4) Ataques baseados em resíduos (*dumpster diving*), que consistem na coleta de informações relevantes descartadas incorretamente, como listas telefônicas ou documentos internos (Martins; Silva, 2021; Mitnick; Simon, 2003).

É importante notar que esses vetores são raramente usados de forma isolada; ataques sofisticados frequentemente combinam múltiplos meios no que é conhecido como "ataque híbrido" ou *blended attack* (Al-ghadhban; Al-twajiry, 2024). Por exemplo, um atacante pode iniciar com *phishing* (computador) para obter o nome de um gerente, usar *dumpster diving* (resíduos) para encontrar um organograma e, em seguida, executar um ataque *vishing* (telefone) contra um subordinado, usando as informações coletadas para personificar o gerente de forma convincente (Mitnick; Simon, 2003). A escolha do vetor depende do objetivo do atacante e da resistência do alvo; o *vishing*, por exemplo, é altamente eficaz para explorar o senso de urgência e autoridade, pois a comunicação por voz adiciona pressão temporal e pistas emocionais que e-mails não possuem (Al-ghadhban; Al-twajiry, 2024; Abuelezz *et al.*, 2025).

4.2 O FENÔMENO DO *PHISHING* E VIESES DE TOMADA DE DECISÃO

Dentre as múltiplas modalidades de engenharia social mediadas por computador, o *phishing* destaca-se devido à sua alta prevalência e potencial destrutivo (Abuelezz *et al.*, 2025). Estruturalmente, o *phishing* caracteriza-se pelo envio de comunicações fraudulentas desenhadas para mimetizar marcas e autoridades legítimas (Amaya-Gómez *et al.*, 2023). O sucesso continuado dessas investidas digitais reside no uso de gatilhos psicológicos altamente persuasivos incorporados ao texto (Hadnagy, 2018). Esses gatilhos apelam intencionalmente para o medo de sanções, a curiosidade, o ganho financeiro ou o senso de urgência funcional (Amaya-Gómez *et al.*, 2023). Diante do estímulo fraudulento, o usuário é induzido a clicar em links maliciosos ou a fornecer credenciais sensíveis em páginas clonadas (Abuelezz *et al.*, 2025).

Existem variações do *phishing* que aumentam sua eficácia através da personalização obtida na fase de "Pesquisa" do ciclo de ataque (Al-ghadhban; Al-twaijry, 2024). O *Spear Phishing* é um ataque altamente direcionado a um indivíduo ou grupo específico em uma organização (ex: o setor financeiro), utilizando informações pessoais (nome, cargo, projetos) para tornar a comunicação fraudulenta extremamente convincente (Santos, 2022). Uma subcategoria é o *Whaling*, que foca especificamente em executivos de alto escalão (CEOs, Reitores), visando obter acesso privilegiado (Al-ghadhban; Al-twaijry, 2024). O *Pharming*, por sua vez, é uma técnica mais sofisticada que independe de um clique em e-mail, pois redireciona a vítima para um site falso mesmo que ela tenha digitado o endereço correto, geralmente através da manipulação de arquivos locais (*hosts*) ou do envenenamento de cache DNS – técnica em que dados legítimos de um servidor de armazenamento temporário(cache) são substituídos por informações falsas para desviar o tráfego dos usuários para páginas fraudulentas(Martins; Silva, 2021). A prevalência e a sofisticação do phishing no cenário contemporâneo estão diretamente relacionadas à profissionalização do cibercrime através do modelo de *Phishing-as-a-Service (PaaS)*. Conforme observa Souza (2022), esta modalidade permite que atacantes com baixo conhecimento técnico adquiram 'kits' prontos para aplicação de golpe que incluem páginas falsas idênticas às institucionais, infraestrutura de disparo de e-mails e até painéis de controle para monitorar as vítimas em tempo real.

A sustentação científica para a eficácia do *phishing* é explicada de forma robusta pelos modelos de psicologia cognitiva e tomada de decisão sob risco (Kahneman, 2011). De acordo com a Teoria do Processamento Dual, o cérebro humano opera por meio de dois sistemas analíticos interdependentes (Kahneman, 2011). O Sistema 1 atua de forma rápida, automática, intuitiva e com baixíssimo consumo de energia mental (Kahneman, 2011). Em contrapartida, o Sistema 2 caracteriza-se por ser lento, deliberativo, analítico e dependente de esforço concentrado (Kahneman, 2011). Os idealizadores de ataques de *phishing* projetam mensagens especificamente para forçar o processamento decisório por meio do Sistema 1 (Amaya-Gómez *et al.*, 2023). Ao se deparar com uma falsa urgência institucional, o colaborador reage de maneira heurística e imediata (Souza, 2013). Consequentemente, o indivíduo negligencia indicadores periféricos de fraude, cuja identificação demandaria a ativação reflexiva do Sistema 2 (Kahneman, 2011).

4.3 HOME OFFICE E A SOBRECARGA COGNITIVA

A transição compulsória para modelos de trabalho remotos e híbridos (*home office*) reconfigurou a infraestrutura operacional das organizações públicas (Park *et al.*, 2023). Sob a ótica da governança de TI, essa mudança descentralizou o perímetro de defesa tradicional das redes corporativas (Al-ghadhban; Al-twaijry, 2024). Dados institucionais sensíveis passaram a trafegar por redes Wi-Fi residenciais desprovidas de controles de segurança robustos (Koch, 2022). Adicionalmente, intensificou-se a utilização de dispositivos particulares para fins profissionais por meio do arranjo *Bring Your Own Device* (BYOD) (Azan *et al.*, 2022). A literatura adverte que essa fusão entre os domínios profissional e doméstico introduz variáveis ambientais que degradam a postura defensiva dos servidores (Park *et al.*, 2023).

A dinâmica do espaço residencial é caracterizada pela presença constante de ruídos contextuais e interrupções familiares (Park *et al.*, 2023). Esses fatores concorrem diretamente para a elevação da sobrecarga cognitiva e da fadiga mental do trabalhador (Azan *et al.*, 2022). Conforme evidenciado por Park *et al.* (2023), o excesso de estímulos simultâneos fragmenta a capacidade de atenção sustentada do indivíduo. Essa saturação atencional induz o servidor a adotar comportamentos operacionais automáticos para escoar suas demandas (Kahneman, 2011). O esgotamento dos recursos cognitivos no ambiente doméstico incapacita a análise crítica detalhada exigida para barrar fraudes (Azan *et al.*, 2022). Diante disso, assume-se que as pressões e dinâmicas do espaço residencial degradam diretamente a vigilância cibernética do indivíduo (Park *et al.*, 2023). Fundamentando-se nessas premissas, formula-se a seguinte hipótese:

H1: O regime de trabalho remoto reduz a capacidade do servidor de detectar e-mails de *phishing* devido às distrações e à sobrecarga cognitiva do ambiente doméstico.

4.4 PERCEPÇÃO DE RISCO E MECANISMOS DE VALIDAÇÃO SOCIAL

A percepção de risco constitui a variável mediadora central para a adoção de comportamentos preventivos em segurança (Souza, 2013). Ela compreende o julgamento subjetivo do indivíduo acerca da probabilidade e da gravidade

associadas a um incidente cibernético (Santos, 2022). Souza (2013) salienta que a percepção humana de ameaças digitais raramente acompanha o risco técnico e estatístico objetivo. É crucial distinguir a percepção de risco do risco técnico-estatístico; enquanto o risco técnico é uma probabilidade objetiva, a percepção é uma avaliação intuitiva e, muitas vezes, enviesada (Amaya-Gómez *et al.*, 2023). A literatura sobre o tema, fundamentada nos trabalhos seminais de Daniel Kahneman e Amos Tversky, demonstra que os seres humanos raramente tomam decisões de forma puramente racional, especialmente sob condições de incerteza (Azan *et al.*, 2022). Essa assimetria é ampliada pelo viés de otimismo, que leva o usuário a crer que incidentes ocorrem apenas com terceiros (Kahneman, 2011). Para romper essa inércia e ativar o Sistema 2 de análise crítica, os servidores necessitam de âncoras situacionais no ambiente de trabalho (Souza, 2013).

A Teoria da Perspectiva (*Prospect Theory*) e os estudos subsequentes sobre vieses cognitivos explicam por que a percepção de risco falha (Azan *et al.*, 2022). Daniel Kahneman (2011) postula a existência de dois modos de pensamento: o "Sistema 1", que é rápido, intuitivo, automático e emocional; e o "Sistema 2", que é lento, analítico, deliberado e exige esforço cognitivo (Azan *et al.*, 2022; Koch, 2022). Os ataques de engenharia social, incluindo o *phishing*, são deliberadamente projetados para ativar o Sistema 1, utilizando gatilhos emocionais (medo, urgência, curiosidade, autoridade) para contornar o escrutínio analítico do Sistema 2 (Koch, 2022; Abuelezz *et al.*, 2025). Quando o Sistema 1 domina, o indivíduo recorre a "atalhos mentais" (heurísticas), que, embora úteis no dia a dia, geram erros sistemáticos de julgamento (vieses) em contextos de segurança (Azan *et al.*, 2022).

Diversos vieses afetam diretamente a vulnerabilidade ao *phishing*. O "Viés de Confiança" (*Trust Bias*) pode levar um servidor a confiar em um e-mail baseado apenas em pistas superficiais de legitimidade, como logotipos institucionais ou uma assinatura de e-mail convincente (Abuelezz *et al.*, 2025). O "Viés de Otimismo" (*Optimism Bias*), comum em ambientes onde falta conscientização, é a crença de que se é menos suscetível a ataques do que os outros (Amaya-Gómez *et al.*, 2023). Estudos sobre golpes financeiros também apontam para o "Viés de Autoridade", uma tendência a obedecer cegamente a figuras percebidas como superiores (Koch, 2022), e a "Heurística da Disponibilidade", onde a percepção de risco é maior se o indivíduo se lembra de um incidente recente (Fernandes, 2025).

A percepção de risco não é inata ou estática; ela é moldada pela experiência,

pelo ambiente e, crucialmente, pelo treinamento (Azan *et al.*, 2022; Fernandes, 2025). A verdadeira conscientização em segurança (*security awareness*) não é apenas a transmissão de conhecimento (o que é *phishing*), mas o treinamento do Sistema 2 para reconhecer os gatilhos do Sistema 1 e interromper a resposta automática (Azan *et al.*, 2022). Em instituições federais onde há carência de programas de sensibilização contínuos e eficazes, o nível de conhecimento sobre as políticas de segurança é baixo, o que se reflete em uma percepção de risco inadequada e, conseqüentemente, em maior vulnerabilidade (Fernandes, 2025; Santos, 2022).

Em estrutura de trabalhos convencional (escritórios, etc), a copresença física de pares e o acesso imediato à TI estruturam uma rede de segurança coletiva (Rodrigues, 2022). Quando confrontado com uma mensagem ambígua, o servidor presencial recorre instintivamente a mecanismos de validação social informal (Azan *et al.*, 2022). Essa dinâmica permite consultar verbalmente o colega ao lado ou checar em tempo real a legitimidade do comunicado (Mitnick; Simon, 2003). Em contrapartida, o isolamento físico decorrente do *home office* elimina essas interações espontâneas de confirmação (Al-ghadhban; Al-twaijry, 2024). Sem redes informais de proteção mútua, o trabalhador remoto depende exclusivamente de seu próprio julgamento sob condições de incerteza (Azan *et al.*, 2022). O esforço logístico extra para formalizar uma consulta remota à TI desencoraja o comportamento preventivo (Al-ghadhban; Al-twaijry, 2024). Sob a premissa de que a pulverização geográfica anula as redes interpessoais de confirmação, propõe-se a seguinte hipótese:

H2: O trabalho remoto diminui o uso de mecanismos de validação social informal, aumentando a taxa de erro na identificação de ataques de engenharia social.

4.5 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO (PSI) E CONSCIENTIZAÇÃO

A governança preventiva contra investidas de engenharia social apoia-se na disseminação das Políticas de Segurança da Informação (PSI) (Santos, 2022). A PSI configura-se como o conjunto formal de diretrizes que regulam o uso aceitável dos ativos tecnológicos de uma organização (Rodrigues, 2022). No âmbito das Instituições Federais de Ensino (IFES), manter uma PSI atualizada é imperativo para

assegurar a conformidade com a Lei Geral de Proteção de Dados (LGPD) (Martins; Silva, 2021). No entanto, a mera publicação formal de normativas em repositórios internos não garante sua eficácia comportamental (Souza, 2022).

Pesquisas aplicadas ao setor público revelam um distanciamento entre as regras abstratas das PSI e o comportamento prático dos servidores (Martins; Silva, 2021). Esse fenômeno decorre diretamente da carência crônica de programas permanentes de conscientização em segurança (*Security Awareness*) (Santos, 2022). A literatura demonstra que treinamentos pontuais ou meramente burocráticos falham em mitigar a manipulação psicológica (Hahnagy, 2018). Com a consolidação estável dos regimes remotos nas autarquias, torna-se urgente o desenvolvimento de ações educacionais customizadas (Al-ghadhbhan; Al-twaijry, 2024). Tais programas devem abandonar abordagens genéricas e se estruturar a partir de diagnósticos empíricos que considerem as vulnerabilidades específicas de cada regime laboral (Martins; Silva, 2021).

5 PROCEDIMENTOS METODOLÓGICOS

5.1 MODALIDADE DE PESQUISA

O desenho desta pesquisa foi classificado, quanto aos seus objetivos, como descritivo e comparativo (Gil, 2017). A estratégia de pesquisa selecionada foi o levantamento (*survey*), pois a questão central busca identificar "qual" a diferença na percepção de vulnerabilidade e "com que frequência" (quantos) certos níveis de conhecimento ocorrem em dois grupos distintos (Yin, 2015, p. 37).

Embora esta pesquisa possa ser contextualizada em contextos empíricos (IFPI), esta estratégia, conforme definida por Yin (2015, p. 40), é mais apropriada, dado que investiga um fenômeno contemporâneo em profundidade e dentro de seu contexto real, onde os limites entre fenômeno e contexto não são claros. Como o objetivo principal deste estudo não foi explorar a *profundidade* do processo de um incidente de segurança em seu contexto (o que seria um caso), mas sim *mensurar e comparar* a percepção (a variável) entre grupos, o levantamento quantitativo foi a abordagem metodológica primária e mais adequada. A pesquisa adota, portanto, uma abordagem predominantemente quantitativa, complementada por uma pesquisa bibliográfica para o referencial teórico e caracterizando-se como pesquisa de campo, pois os dados serão coletados no ambiente natural dos participantes (GIL, 2017).

5.2 INSTRUMENTOS DE COLETA DE DADOS

O instrumento principal para a coleta de dados foi um questionário estruturado *online*, desenvolvido na plataforma *Google Forms* e distribuído por meios eletrônicos institucionais. O questionário foi dividido em três seções:

- (a) Perfil sociodemográfico e funcional (gênero, idade, escolaridade, tempo de serviço, regime de trabalho);
- (b) Nível de conhecimento sobre a Política de Segurança da Informação (PSI) e conceitos de *phishing* e *engenharia social*; e
- (c) Percepção de vulnerabilidade, utilizando uma escala Likert para mensurar a concordância com afirmativas sobre segurança em cenários de risco. A análise dos dados será realizada com estatística descritiva (frequências, médias) e estatística inferencial (Testes T de Student ou Mann-Whitney para

comparação de médias dos grupos; Teste Qui-quadrado para associação entre variáveis categóricas).

Para assegurar o rigor e a qualidade desta pesquisa empírica, foram adotadas as táticas de validação propostas por Yin (2015). A validade do construto (*construct validity*) foi endereçada na fase de elaboração do questionário. O instrumento passou por um pré-teste com um grupo reduzido de servidores (que não fizeram parte da amostra final) e por uma validação de face por especialistas (profissionais de TI e pesquisadores da área), garantindo que as questões medem efetivamente os construtos teóricos de "percepção de risco" e "conhecimento" (Yin, 2015). A confiabilidade (*reliability*) será buscada através da padronização dos procedimentos de coleta. Ao utilizar um questionário *online* único (*Google Forms*), garante-se que todos os participantes recebam as mesmas instruções e perguntas, e o TCLE (Termo de Consentimento Livre e Esclarecido) padroniza a introdução ao estudo, minimizando erros e vieses do pesquisador e permitindo a replicação futura do estudo (Yin, 2015).

Conforme preconiza a Carta Circular nº 1/2021-CONEP/SECNS/MS (Item 3), após a coleta de dados via *Google Forms*, o banco de dados foi imediatamente baixado (*download*) para um dispositivo eletrônico local (computador pessoal do pesquisador protegido por senha e criptografia). Imediatamente após a confirmação do download e integridade do arquivo, todos os registros foram excluídos permanentemente da plataforma virtual (nuvem) e dos servidores do Google, garantindo que as informações não permaneçam armazenadas em ambiente compartilhado online.

5.3 PARTICIPANTES DA PESQUISA

Os participantes desta pesquisa foram servidores públicos (técnicos-administrativos e docentes) em exercício em uma das maiores Instituições Federais de Ensino do Piauí: o Instituto Federal do Piauí (IFPI). A seleção da amostra foi não probabilística, por conveniência, sendo o convite para participação enviado mediante canais de comunicação oficiais das instituições.

Os critérios de inclusão são: (1) ser servidor ativo (efetivo ou em cargo comissionado) do IFPI; e (2) realizar atividades que envolvam o uso regular de computador e sistemas de informação institucionais. O critério de separação dos

grupos será a autodeclaração no questionário sobre seu regime de trabalho predominante no último ano (presencial ou remoto/híbrido).

Esta escolha amostral impacta diretamente a validade externa (*external validity*) do estudo. Yin (2015) distingue dois tipos de generalização: a "generalização estatística" (usada em levantamentos, da amostra para a população) e a "generalização analítica" (usada em estudos de caso, dos resultados para a teoria). Como este estudo é um levantamento com amostragem não probabilística, a generalização estatística para *todos* os servidores do IFPI foi devidamente feita com cautela. Contudo, os resultados permitirão uma generalização analítica robusta, onde os achados foram comparados com a teoria existente sobre percepção de risco e *home office* (conforme Objetivo 4), fornecendo subsídios valiosos e aplicáveis ao contexto específico das IFES estudadas.

5.3.1 Aspectos éticos da pesquisa

Este projeto foi submetido para avaliação e devidamente aprovado pelo Comitê de Ética em Pesquisa (CEP) da Universidade Federal do Piauí Campus Amílcar Ferreira Sobral (CEP/UFPI - CAFS), via Plataforma Brasil, sob o parecer **CAAE nº 94964725.6.0000.5660** favorável emitido antes do início da coleta de dados. Os participantes foram informados sobre os objetivos, riscos e benefícios da pesquisa na página inicial do questionário, onde acessaram o Termo de Consentimento Livre e Esclarecido (TCLE) digital, garantindo o "consentimento informado" (Yin, 2015). A participação foi inteiramente voluntária, resguardando o direito de desistência a qualquer momento. O anonimato e a confidencialidade dos dados foram rigorosamente garantidos, não tendo sido coletada nenhuma informação de identificação direta, como nome, matrícula ou endereço IP (Yin, 2015). Os riscos associados à pesquisa foram considerados mínimos, limitando-se a um possível desconforto psicológico leve ao refletir sobre a própria vulnerabilidade a golpes ou sobre o nível de conhecimento das políticas de segurança. Como benefício, os participantes contribuíram diretamente para um diagnóstico institucional que visa aprimorar a segurança da informação no IFPI.

6 RESULTADOS

6.1 PERCEPÇÃO DE RISCO E SEGURANÇA DIGITAL POR CATEGORIA FUNCIONAL

A análise inicial dos dados empíricos concentrou-se em mapear o comportamento e o julgamento subjetivo dos participantes quanto à segurança digital, tomando como referência a média geral dos riscos calculada a partir de cenários ambientais descentralizados. Ao segmentar essa percepção de segurança por categoria funcional (Docente e Técnico-Administrativo em Educação — TAE), observou-se uma rigorosa e homogênea proximidade analítica entre os grupos investigados. Os dados descritivos consolidados apontam que o corpo docente (n=126) apresentou uma média aritmética de risco percebido de 2,625, acompanhada por um desvio padrão de 0,890, estabelecendo seus limites amostrais entre o mínimo de 1,000 e o máximo de 5,000 pontos na escala lida. De forma análoga, os TAE (n=29) registraram uma média aritmética de 2,595 com desvio padrão de 0,981, flutuando entre o mínimo de 1,000 e o máximo de 4,750 pontos.

Tabela 1 – Estatística Descritiva

Cargo	Válido	Missing	Mean (arithmetic)	Std. Deviation	Minimum	Maximum
Docente	126	66	2.625	0.890	1.000	5.000
TAE	29	8	2.595	0.981	1.000	4.750

Fonte: O autor (2026)

Essa convergência de valores centrais e de dispersão indica que a percepção de vulnerabilidade a incidentes cibernéticos não é determinada pelas atribuições específicas do cargo ocupado no Instituto Federal do Piauí (IFPI). À luz dos modelos cognitivos de processamento decisório, essa igualdade sugere que os desafios logísticos e operacionais introduzidos pelo trabalho fora do perímetro organizacional tradicional afetam o julgamento e o comportamento defensivo de professores e técnicos de maneira equivalente. A rotina administrativa descentralizada equaliza a consciência situacional primária do corpo funcional, fazendo com que ambos os grupos operem sob o mesmo patamar de prontidão ou suscetibilidade interpretativa diante das ameaças digitais cotidianas.

6.2 O IMPACTO DA PERIODICIDADE DAS CAPACITAÇÕES NA PERCEPÇÃO DE SEGURANÇA

Na sequência, a investigação debruçou-se sobre a avaliação descritiva da relação existente entre a periodicidade das ações educacionais em segurança da informação e o nível de risco subjetivo manifestado pelos servidores. Os indicadores estatísticos levantados trazem evidências empíricas sobre o comportamento dinâmico e o caráter perecível do conhecimento adquirido em treinamentos institucionais. Os servidores que declararam ter passado por capacitações ou ações de sensibilização recentes, ocorridas nos últimos 12 meses (n=5), registraram uma média de percepção de segurança substancialmente superior, fixada em 3,400 pontos com desvio padrão de 1,421. Em contrapartida, os indivíduos cujo último treinamento ocorreu há mais de um ano (n=13) apresentaram uma média de 2,596 e desvio padrão de 0,899.

Tabela 2 – Relação entre o risco percebido e ações de treinamento

Ações	Valid	Missing	Mean (arithmetic)	Std. Deviation	Minimum	Maximum
Não possui treinamento	137	64	2.593	0,879	1.000	5.000
Treinamento há mais de 1 ano	13	7	2.596	0,899	1.000	4.250
Treinamento recente	5	3	3.400	1.421	1.750	5.000

Fonte: O autor (2026)

O dado mais alarmante emerge do cruzamento com o contingente que declarou não possuir qualquer histórico de treinamento formal na instituição (n=137). Este grupo majoritário exibiu uma média de 2,593 e desvio padrão de 0,879. Do ponto de vista analítico, a média dos servidores com treinamento obsoleto (há mais de um ano) converge de forma quase exata com a média dos servidores leigos que nunca receberam instrução formal (M=2,596 *versus* M=2,593). Atestando que o conhecimento em segurança da informação possui um "prazo de validade" perceptível no comportamento. Devido à volatilidade e rápida transformação do

cenário de ameaças e técnicas de engenharia social, a efetividade da instrução prévia é drasticamente reduzida com o tempo, equiparando profissionais treinados no passado a indivíduos completamente leigos e reforçando a necessidade vital de programas permanentes de capacitação continuada (*security awareness*).

6.3 ANÁLISE COMPARATIVA DO COMPORTAMENTO PREVENTIVO POR REGIME DE TRABALHO

A fim de compreender o impacto real do isolamento doméstico e do ambiente de trabalho na postura preventiva do corpo funcional, buscou-se identificar a existência de padrões divergentes de vulnerabilidade entre os servidores presenciais e remotos. Para testar se o regime laboral (presencial ou remoto/híbrido) influenciava o comportamento de segurança da informação e a percepção de risco dos servidores do IFPI, realizou-se uma análise comparativa estatística bivariada utilizando o Teste *t* de Student para amostras independentes ($N=229$; $gl=227$), a qual foi devidamente validada pelo teste não-paramétrico U de Mann-Whitney para assegurar a robustez da análise diante da distribuição dos dados. Os resultados unificados dessas análises estão estruturados na Tabela 3, apresentando os indicadores analíticos lado a lado.

Tabela 3 – Análise Comparativa da Confiança em Situações de Risco por Regime de Trabalho

(continua)

Itens de Segurança Avaliados (Escala Likert 1–5)	Média Presencial (n=74)	Média Remoto (n=155)	Estatística <i>t</i>	gl	p-valor (t)	Estatística U	p-valor (U)
Confiança ao abrir arquivo PDF anexo	3,84	3,92	-0,556	227	0,579	5489	0,571
Confiança ao clicar em link de atualização	3,22	3,31	-0,437	227	0,662	5574	0,721
Confiança ao fornecer senha do sistema	3,11	3,29	-1,239	227	0,217	5239	0,274

Tabela 3 – Análise Comparativa da Confiança em Situações de Risco por Regime de Trabalho

(conclusão)

Itens de Segurança Avaliados (Escala Likert 1–5)	Média Presencial (n=74)	Média Remoto (n=155)	Estatística t	gl	p-valor (t)	Estatística U	p-valor (U)
Confiança ao usar computador pessoal (BYOD)	3,69	3,78	-0,795	227	0,427	5435	0,499
Confiança ao usar rede Wi-Fi pública	2,12	2,48	-1,990	227	0,048	4786	0,036

Fonte: O Autor (2026).

Nota: Diferenças estatisticamente significativas para $p < 0,05$ indicadas em negrito. Média das pontuações extraídas da escala Likert onde 1 representa "Muito Inseguro" e 5 "Muito Seguro". Graus de liberdade (gl) para o Teste $t = 227$; $N = 229$.

Os resultados indicam, de maneira altamente consistente entre os dois métodos analíticos, a ausência de diferenças estatisticamente significativas entre servidores presenciais e remotos nas variáveis essenciais de mitigação de risco, tais como a propensão a abrir arquivos PDF anexos ($p=0,579$), clicar em hiperlinks enviados em nome da TI ($p=0,662$), inserir credenciais em páginas institucionais ($p=0,217$) ou fazer uso de dispositivos particulares por meio de BYOD ($p=0,427$). Contudo, confirmou-se uma divergência estatisticamente significativa no item referente ao uso de redes Wi-Fi públicas e abertas, validada tanto pelo Teste t ($t(227)=-1,990$; $p=0,048$) quanto pelo teste de Mann-Whitney ($U=4786$; $p=0,036$). Esse achado evidencia que a consciência situacional ou a necessidade de conectar-se a infraestruturas de rede desprotegidas difere de forma relevante em função da modalidade laboral. Os servidores remotos/híbridos exibiram médias de confiança superiores, o que reflete uma maior exposição factual e operacional a riscos de interceptação de tráfego decorrente da própria natureza de mobilidade inerente ao regime de *home office*.

6.4 ASSOCIAÇÃO ENTRE O REGIME LABORAL E OS NÍVEIS DE TREINAMENTO

Com o objetivo de diagnosticar se a distribuição e alocação dos servidores nos diferentes níveis de treinamento em segurança da informação estava associada de forma dependente ao regime de trabalho exercido, aplicou-se o teste não-paramétrico Qui-quadrado de Independência (χ^2). Os resultados do cruzamento amostral revelaram independência estocástica entre as variáveis organizacionais, não sendo registrada nenhuma associação estatisticamente significativa entre elas, com valores fixados em $\chi^2(2, N=229)=0,185$ e um p-valor de 0,912.

A análise descritiva das tabelas de contingência desvela um cenário de carência de treinamento de caráter crônico e distribuído de forma homogênea no IFPI. A vasta maioria dos servidores integrados ao regime presencial (86,49%) e ao regime remoto/híbrido (88,39%) declarou não possuir nenhum tipo de treinamento voltado à segurança cibernética ou engenharia social. Sob a ótica absoluta (porcentagem dentro da coluna), constata-se que o contingente desprovido de capacitação inicial concentra-se massivamente no regime remoto/híbrido, o qual abarca 68,16% (n=137) do total de indivíduos sem instrução (n=201) detectados na pesquisa. Esse dado indica que a vulnerabilidade institucional decorrente da ausência de programas educacionais atinge ambos os ambientes de maneira agnóstica ao local de desempenho das funções.

Tabela 4 – Associação entre Regime de trabalho e Treinamento em Segurança

Regime de trabalho	Variáveis estatísticas	Não possui treinamento	Treinamento a mais de 1 ano	Treinamento recente	Total
Presencial	n	64.00	7.00	3.00	74.00
	% _{linha}	86.49 %	9.46 %	4.05 %	100.00 %
	% _{coluna}	31.84 %	35.00 %	37.50 %	32.31 %
Remoto/Híbrido	n	137.0	13.00	5.00	155.0
	% _{linha}	88.39 %	8.39 %	3.23 %	100.00 %
	% _{coluna}	68.16 %	65.00 %	62.50 %	67.69 %
Total	n	201.0	20.00	8.00	229.0
	% _{linha}	87.77 %	8.73 %	3.49 %	100.00 %
	% _{coluna}	100.00 %	100.00 %	100.00 %	100.00 %

Fonte: O autor(2026)

6.5 DESEMPENHO E RESILIÊNCIA PRÁTICA FRENTE A CENÁRIOS COMPORTAMENTAIS SIMULADOS

Para além do autorrelato de confiança, a pesquisa mapeou a vulnerabilidade e a prontidão prática dos servidores frente a táticas específicas de Engenharia Social. Foram estruturados três cenários simulados baseados em e-mails e contatos fraudulentos contendo gatilhos psicológicos clássicos de Autoridade, Urgência e Benefício/Curiosidade.

Tabela 5 – Panorama Geral de Desempenho nos cenários comportamentais

Cenário Simulado de Engenharia Social	Erro(n)	Erro(%)	Acerto(n)	Acerto(%)	Total(N)
E-mail da Reitoria (Direção Geral)	8	3,5%	221	96,5%	229
E-mail do Setor de RH	7	3,1%	222	96,9%	229
Equipe de suporte de TI	3	1,3%	226	98,7%	229

Fonte: O autor(2026)

O panorama geral de desempenho demonstrou um índice elevado de acertos (comportamento preventivo correto) em todas as modalidades avaliadas pela amostra global (N=229). No Cenário 1, que simulou um e-mail fraudulento em nome do Gabinete da Reitoria utilizando gatilhos de autoridade e prazo iminente para bloqueio de conta, registrou-se apenas 3,5% (n=8) de respostas impulsivas de erro, contra 96,5% (n=221) de acertos baseados na checagem por canais oficiais. No Cenário 2, pautado no pretexto de benefício financeiro e na abertura de anexo compactado sobre ressarcimento em nome do Setor de Recursos Humanos (RH), a taxa de erro limitou-se a 3,1% (n=7), enquanto os acertos atingiram 96,9% (n=222) dos respondentes. No Cenário 3, focado em uma abordagem simulada de suporte técnico falso de TI (*vishing*) alegando infecção por vírus para instalação de ferramentas de acesso remoto (TeamViewer/AnyDesk), observou-se a menor vulnerabilidade prática, com meros 1,3% (n=3) de erros e 98,7% (n=226) de comportamentos defensivos adequados.

Tabela 6 – Desempenho Prático nos Cenários Simulados por Regime de Trabalho

Cenário Simulado de Engenharia Social	Regime de Trabalho	Erro (n)	Erro (%)	Acerto (n)	Acerto (%)	Total (N)
Cenário 1: E-mail Falso da Reitoria	Presencial	2	2,70%	72	97,30%	74
	Remoto/Híbrido	6	3,87%	149	96,13%	155
Cenário 2: E-mail Falso do Setor de RH	Presencial	1	1,35%	73	98,65%	74
	Remoto/Híbrido	6	3,87%	149	96,13%	155
Cenário 3: Falso Suporte Técnico de TI	Presencial	0	0,00%	74	100,00%	74
	Remoto/Híbrido	3	1,94%	152	98,06%	155

Fonte: O autor(2026)

Para verificar se o ambiente de isolamento doméstico degradava a capacidade prática de identificação de golpes digitais, aplicou-se o teste Qui-quadrado de Independência cruzando o regime laboral e o desempenho prático dos participantes em cada um dos pretextos simulados (Tabela 4). Os resultados inferenciais indicaram, de forma unânime, a ausência de associações estatisticamente relevantes. No pretexto da Reitoria (Cenário 1), obteve-se $\chi^2(1, N=229)=0,203$ com um p-valor de 0,652, atestando equivalência comportamental exata entre quem atua fisicamente nos *campi* e quem realiza teletrabalho. No pretexto de urgência do RH (Cenário 2), o teste de independência fixou-se em $\chi^2(1, N=229)=1,073$ com $p=0,300$, comprovando que o gatilho emocional de benefício afeta as taxas de erro e acerto dos dois grupos de forma análoga. Por fim, na simulação de suporte técnico de TI (Cenário 3), as variáveis mantiveram-se independentes com $\chi^2(1, N=229)=1,451$ e $p=0,228$, reiterando que a resiliência operacional para barrar acessos remotos não autorizados independe da presença física do servidor na instituição.

Tabela 7 – Desempenho Prático nos Cenários Simulados com Base no Nível de Treinamento

Cenário Simulado de Engenharia Social	Nível de Treinamento Formal	Erro (n)	Erro (%)	Acerto (n)	Acerto (%)	Total (N)
Cenário 1: E-mail Falso da Reitoria	Não possui treinamento	8	3,98%	193	96,02%	201
	Há mais de 1 ano	0	0,00%	20	100,00%	20
	Treinamento recente	0	0,00%	8	100,00%	8
Cenário 2: E-mail Falso do Setor de RH	Não possui treinamento	7	3,48%	194	96,52%	201
	Há mais de 1 ano	0	0,00%	20	100,00%	20
	Treinamento recente	0	0,00%	8	100,00%	8
Cenário 3: Falso Suporte Técnico de TI	Não possui treinamento	2	1,00%	199	99,00%	201
	Há mais de 1 ano	1	5,00%	19	95,00%	20
	Treinamento recente	0	0,00%	8	100,00%	8

Fonte: O autor(2026)

Aprofundando o diagnóstico empírico, cruzou-se o desempenho nos cenários práticos simulados com o nível de treinamento formal dos servidores (Não possui treinamento; Há mais de 1 ano; Treinamento recente), buscando isolar a efetividade das ações educacionais em segurança da informação (Tabela 7). Os testes Qui-quadrado demonstraram que a propensão a incorrer em erro ou adotar a postura preventiva distribuiu-se de forma estocástica e semelhante entre servidores capacitados e leigos em todos os cenários testados. No e-mail fraudulento da Reitoria (Cenário 1), o teste indicou independência absoluta entre o histórico de instrução e as respostas corretas, com valores de $\chi^2(2, N=229)=1,155$ e $p=0,561$. No pretexto de atualização cadastral do RH (Cenário 2), a ausência de relevância estatística confirmou-se com $\chi^2(2, N=229)=1,006$ e $p=0,605$, revelando que a vulnerabilidade ao pretexto afetou os grupos de forma idêntica. Da mesma forma, o cenário do falso suporte de TI (Cenário 3) indicou que o treinamento prévio não determinou o padrão de respostas práticas da amostra, registrando $\chi^2(2, N=229)=2,367$ e $p=0,306$.

Em termos gerais, esses resultados evidenciam que a realização prévia de cursos ou a exposição a ações pontuais de sensibilização organizadas na instituição não se traduziram em vantagens estatísticas significativas ou diferenciais protetivos diante de simulações práticas de engenharia social desenvolvidas nesta pesquisa. A

elevada resiliência observada (índices de acerto superiores a 96% de forma homogênea) indica a vigência de uma barreira defensiva intuitiva generalizada e uniforme compartilhada pelos servidores do IFPI. Contudo, a ausência de impacto estatístico do treinamento sugere que os programas educacionais vigentes carecem de alinhamento prático e comportamental, operando de forma descolada das reações cotidianas exigidas para conter os gatilhos heurísticos de manipulação digital.

7 DISCUSSÃO

7.1 O IMPACTO DO AMBIENTE DE TRABALHO E A SOBRECARGA COGNITIVA (ANÁLISE DA HIPÓTESE 1)

O objetivo principal da primeira hipótese desta investigação (H1) foi aferir se o ambiente de trabalho remoto atuaria como um vetor ativo de ampliação de vulnerabilidades cibernéticas, reduzindo a eficácia da percepção de risco dos servidores em decorrência da sobrecarga cognitiva e das distrações inerentes ao espaço doméstico (Park *et al.*, 2023). Contudo, os resultados empíricos obtidos por meio do Teste t de Student e validados pelo teste não-paramétrico U de Mann-Whitney refutaram categoricamente essa suposição (Tabela 3). Ao avaliar os comportamentos preventivos essenciais dos colaboradores — expressos na propensão a abrir arquivos PDF suspeitos ($p=0,579$), clicar em links hipertextuais maliciosos ($p=0,662$) ou expor credenciais de acesso ($p=0,217$) —, constatou-se uma rigorosa e homogênea equivalência estatística entre os servidores do regime presencial e os do regime remoto/híbrido.

Essa equivalência de comportamento desafia frontalmente a literatura tradicional da segurança da informação, que frequentemente associa a descentralização geográfica à degradação da postura defensiva dos indivíduos (Martins; Silva, 2021). Autores clássicos do setor argumentam que a transição forçada para o ambiente residencial fragmenta a atenção do colaborador, deixando-o significativamente mais vulnerável a gatilhos impulsivos baseados em urgência e engenharia social (Rodrigues, 2022). No contexto dos servidores analisados no IFPI, todavia, a dispersão geográfica não se traduziu em um aumento da vulnerabilidade prática (Tabela 4).

Sob a ótica da Teoria dos Sistemas de Pensamento desenvolvida por Daniel Kahneman (2011), o erro comportamental em segurança da informação ocorre prioritariamente quando o indivíduo opera sob o Sistema 1 — caracterizado por respostas rápidas, intuitivas, automáticas e emocionais —, negligenciando os sinais periféricos de alerta que exigiria o esforço analítico e o escrutínio do Sistema 2 (Kahneman, 2011). Os resultados obtidos nas simulações práticas — onde o índice de acerto superou a marca de 96% em ambos os regimes funcionais — fornecem evidências empíricas de que o corpo funcional conseguiu engajar com sucesso o

esforço cognitivo do Sistema 2 durante a avaliação das comunicações eletrônicas organizacionais (Tabela 4). Esse achado indica que os gatilhos de sobrecarga cognitiva e os ruídos contextuais domésticos mapeados pela literatura não foram de intensidade suficiente para desativar a postura defensiva primária e a consciência situacional dos servidores em *home office* (Park *et al.*, 2023).

7.2 ISOLAMENTO FÍSICO E OS MECANISMOS DE VALIDAÇÃO SOCIAL (ANÁLISE DA HIPÓTESE 2)

A segunda hipótese deste estudo (H2) pressupunha que o isolamento físico imposto pelo teletrabalho inibiria os mecanismos de validação social informal, culminando em uma menor taxa de detecção prática de ataques de engenharia social se comparado ao ecossistema presencial corporativo (Azan *et al.*, 2022). Sob essa premissa, o ato cotidiano de consultar verbalmente um colega de sala ou acionar diretamente o suporte local de TI ao receber uma mensagem ambígua funcionaria como uma barreira protetiva coletiva (Rodrigues, 2022). No entanto, os testes Qui-quadrado de Independência aplicados sobre as três simulações comportamentais práticas — e-mail da Reitoria ($p=0,652$), e-mail do setor de Recursos Humanos ($p=0,300$) e suporte telefônico falso de TI ($p=0,228$) — também refutaram integralmente a validade da H2 (Tabela 4).

A teoria da influência e validação social postula que indivíduos inseridos em ambientes coletivos utilizam o comportamento e a opinião de seus pares como âncora psicológica para tomar decisões em situações de risco ou incerteza (Cialdini, 2012). Esperava-se, por conseguinte, que os servidores atuantes no regime presencial demonstrassem índices superiores de resiliência e menores taxas de erro devido à facilidade de compartilhamento de dúvidas em tempo real (Mitnick; Simon, 2003). No entanto, a homogeneidade estatística observada aponta que a validação informal presencial não operou como um diferencial de proteção ativa na amostra (Tabela 4). Os baixíssimos índices de erro prático cometidos de forma idêntica pelos dois grupos revelam que a capacidade de detecção de ameaças de *phishing* e engenharia social baseou-se em competências individuais e não em consultas interpessoais de perímetro (Souza, 2013). O isolamento do teletrabalho, portanto, não desamparou o servidor no que tange à sua percepção defensiva essencial (Al-ghadhban; Al-twaijry, 2024).

7.3 SÍNTESE COMPARATIVA DA PERCEPÇÃO DE VULNERABILIDADES E CONSCIENTIZAÇÃO

Ao confrontar os achados empíricos com o objetivo geral desta pesquisa, emerge um cenário de uniformidade comportamental que confronta e ressignifica as premissas convencionais da cultura de segurança da informação (Santos, 2022). O diagnóstico revelou que a dispersão espacial decorrente do teletrabalho não atuou como um catalisador de vulnerabilidades cognitivas, contrariando tendências apontadas em revisões teóricas que associam o *home office* a uma maior suscetibilidade a fraudes (Martins; Silva, 2021). Essa equivalência comportamental foi estatisticamente sustentada pelas análises inferenciais, demonstrando que a habilidade prática para desarmar os gatilhos emocionais de urgência, autoridade e benefício é independente do local onde o servidor desempenha suas funções administrativas (Tabela 4).

O diagnóstico aprofundado revelou, contudo, um paradoxo institucional crítico: essa resiliência generalizada observada nos cenários práticos não decorre de uma maturidade digital construída por ações formais de capacitação prévia (Tabela 6). O teste Qui-quadrado de independência revelou um cenário de carência crônica, severa e homogênea de treinamento em ambos os regimes funcionais, evidenciando que 86,49% dos servidores presenciais e 88,39% dos servidores remotos declararam nunca ter passado por qualquer programa de treinamento em SI na instituição (Tabela 5). À luz das teorias de *Security Awareness*, a ausência generalizada de uma política contínua de capacitação iguala o comportamento dos grupos por uma base leiga comum, sugerindo que o alto índice de acertos práticos decorre de uma postura defensiva intuitiva ou do medo generalizado de golpes digitais, e não de uma cultura de segurança formalizada (Fernandes, 2025; Santos, 2022).

A única exceção logística e de infraestrutura significativa na amostra emergiu no item referente ao uso de redes públicas de internet, o qual apresentou divergência estatística relevante tanto no Teste t ($p=0,048$) quanto no Teste U de Mann-Whitney ($p=0,036$). Esse achado reflete uma exposição factual decorrente da mobilidade e da flexibilidade espacial inerentes ao trabalho remoto (Al-ghadhban; Al-twaijry, 2024). Enquanto o servidor presencial atua resguardado pelas barreiras

lógicas do campus, o trabalhador em *home office* manifesta uma confiança superior ao acessar sistemas por redes externas, o que configura uma vulnerabilidade técnica real que demanda intervenção imediata da governança institucional (Rodrigues, 2022).

7.4 DIRETRIZES ESTRATÉGICAS PARA O PROGRAMA DE CONSCIENTIZAÇÃO DO IFPI

Diante das evidências empíricas consolidadas, a formulação de diretrizes para o programa de conscientização institucional do IFPI não deve fragmentar os servidores pelo critério geográfico de onde desempenham suas funções, mas sim unificá-los em uma matriz educacional comum (Fernandes, 2025). As intervenções devem atacar as vulnerabilidades pontuais detectadas, estruturando-se em três pilares estratégicos baseados em evidências:

- **Universalização Baseada em *Microlearning*:** Para mitigar de forma imediata o índice de 87,8% de servidores desprovidos de treinamento formal na instituição, propõe-se a implementação de módulos curtos e dinâmicos de aprendizagem (*microlearning*) distribuídos semanalmente através das plataformas e sistemas de comunicação interna oficiais, como o SUAP. O propósito desta ação é manter o Sistema 2 de Kahneman (2011) em estado de prontidão orgânica contínua, reduzindo o impacto de vieses cognitivos na rotina e combatendo os riscos de habituação que anulam a eficácia de treinamentos pontuais ou puramente burocráticos (Santos, 2022).
- **Blindagem do Perímetro Móvel:** Respondendo diretamente à vulnerabilidade estatisticamente significativa identificada no uso de conexões abertas residenciais e externas ($p < 0,05$), o programa de conscientização voltado aos servidores em regime remoto e híbrido deve estabelecer módulos práticos mandatórios sobre higiene cibernética fora do ambiente físico corporativo. As diretrizes devem focar na obrigatoriedade do uso de Redes Privadas Virtuais (VPNs institucionais), aplicação de criptografia em discos locais de dispositivos BYOD e adoção massiva de políticas de autenticação de duplo fator (2FA) para conter ataques de interceptação de tráfego e roubo de credenciais (Rodrigues, 2022).

- **Formalização de Canais de Reporte de Incidentes:** Direcionado especialmente ao ambiente físico dos *campi*, o programa de conscientização deve atuar na desconstrução da falácia da segurança baseada unicamente no perímetro físico e mitigar a dependência da validação social informal (Cialdini, 2012). As ações de treinamento devem instrumentalizar os servidores presenciais a substituírem a consulta verbal ao colega de sala pela notificação imediata e centralizada de qualquer anomalia digital eletrônica (Mitnick; Simon, 2003). A formalização do reporte junto às equipes de TI converte a desconfiança individual em inteligência coletiva de segurança, fortalecendo a resiliência ativa de toda a comunidade acadêmica (Fernandes, 2025).

CONSIDERAÇÕES FINAIS

A presente pesquisa cumpriu integralmente o seu objetivo geral ao analisar comparativamente a percepção de vulnerabilidade e a postura comportamental diante de ataques de *phishing* entre servidores públicos em regime presencial e remoto/híbrido no âmbito do Instituto Federal do Piauí (IFPI). Ao contrário do que sugere o senso comum e parcelas expressivas da literatura tradicional de segurança da informação, que frequentemente apontam o teletrabalho como um ambiente de degradação da vigilância (Martins; Silva, 2021), os achados estatísticos bivariados revelaram um comportamento rigorosamente homogêneo entre as modalidades laborais. A dispersão geográfica, o distanciamento físico da infraestrutura de suporte e as dinâmicas contextuais do ambiente doméstico não exerceram influência estatisticamente significativa na capacidade dos participantes de discernir e mitigar tentativas simuladas de engenharia social (Park *et al.*, 2023; Azan *et al.*, 2022).

Embora os índices de acerto nos cenários comportamentais práticos tenham sido expressivos, superando a marca de 96% de eficácia em todas as situações simuladas, o diagnóstico mapeou uma vulnerabilidade estrutural e crônica na governança da instituição. Aproximadamente 87,8% da amostra global relatou nunca ter recebido qualquer modalidade de treinamento formal ou curso de capacitação em segurança da informação ofertado pela entidade, padrão deficitário que se manteve agnóstico e independente do regime de trabalho exercido. Esse paradoxo empírico indica que a resiliência observada nas simulações não pode ser creditada a políticas institucionais estruturadas de educação digital prévia. O resultado evidencia a urgência de a administração pública transitar de uma postura reativa para o fortalecimento de políticas permanentes, obrigatórias e sistemáticas de conscientização em segurança da informação (Martins; Silva, 2021).

Nesse sentido, adverte-se que a homogeneidade comportamental e a ausência de divergências práticas entre os regimes de trabalho não devem ser interpretadas como indicativos de um ecossistema plenamente seguro ou invulnerável (Souza, 2022). Pelo contrário, a elevada concentração de servidores leigos e desprovidos de letramento formal em SI representa um fator de atenção e risco latente para a gestão estratégica (Santos, 2022). Essa vulnerabilidade é acentuada diante da constante evolução e sofisticação das técnicas de engenharia social inversa e do surgimento de ataques cirurgicamente direcionados, como o

spear phishing e o *whaling*, que exploram dados específicos e informações abertas (OSINT) sobre seus alvos para contornar defesas lógicas (Al-ghadhban; Al-twaijry, 2024; Mitnick; Simon, 2003).

Como contribuição prática e aplicada, este estudo converteu seus achados em diretrizes estratégicas para a formulação de um programa de conscientização (*Security Awareness*) baseado em evidências empíricas locais. Entre as recomendações estruturadas, destacam-se a universalização de trilhas de aprendizagem continuada no formato de *microlearning* integradas aos sistemas nativos como o SUAP, mantendo o Sistema 2 ativado na rotina de trabalho (Kahneman, 2011), além de intervenções de perímetro customizadas. Para o contingente remoto, as diretrizes enfatizam o reforço normativo sobre o uso seguro de conexões externas e a obrigatoriedade de VPNs, respondendo ao ponto de exposição estatisticamente significativa identificado no uso de redes Wi-Fi públicas ($p < 0,05$). Para o grupo presencial, as ações visam desmistificar a falsa sensação de segurança do perímetro físico e incentivar a substituição da validação social informal por canais de reporte centralizados (Cialdini, 2012).

Como limitações metodológicas desta investigação, reconhece-se a ocorrência do "efeito teto", provocado pela altíssima concentração de acertos nos cenários simulados, o que restringe a variabilidade analítica e pode mascarar nuances comportamentais sutis. Adicionalmente, pontua-se o potencial viés gerado pelo Efeito Hawthorne, fenômeno no qual os participantes elevam artificialmente seus níveis de atenção e vigilância analítica simplesmente por estarem cientes de sua integração a uma pesquisa acadêmica de campo (Yin, 2015). Outra limitação reside na natureza declaratória de parte do questionário baseado na escala Likert, que mensura a intenção de comportamento e a confiança subjetiva, e não necessariamente a reação físico-motora do indivíduo diante do ataque real (Souza, 2013).

Diante dessas limitações e das lacunas teóricas identificadas, propõe-se uma agenda robusta de pesquisa para o avanço da literatura de comportamento em segurança da informação. Primeiramente, recomenda-se a realização de estudos experimentais de campo com desenhos metodológicos não declaratórios, executando campanhas de *phishing* simulado ativo e surpresa integradas à rotina invisível do trabalho institucional, sem aviso prévio, permitindo mensurar a taxa real de cliques e o comportamento orgânico desarmado dos servidores (Mitnick; Simon,

2003). Em segundo lugar, a literatura deve avançar urgentemente na investigação do impacto da Inteligência Artificial (IA) generativa na eficácia da engenharia social. Sugere-se que futuras pesquisas avaliem como ferramentas de IA utilizadas por atacantes para eliminar erros gramaticais e automatizar pretextos hiper-personalizados afetam os atalhos mentais do Sistema 1 (Kahneman, 2011), testando se os elevados índices de acerto observados neste estudo mantêm-se estáveis face a uma indústria global de fraudes customizadas e automatizadas (Souza, 2022). Espera-se, por fim, que o diagnóstico gerado por este estudo forneça subsídios metodológicos e conceituais para o aprimoramento de políticas públicas de segurança da informação no IFPI e em outras Instituições Federais de Ensino, fortalecendo a cultura de resiliência e maturidade digital de forma sustentável.

REFERÊNCIAS

- ABUELEZZ, Israa et al. How demographic and appearance cues of a potential social engineer influence trust perception and risk-taking among targets? **Information and Computer Security**, v. 33, n. 3, p. 320-343, 2025.
- AL-GHADHBAN, Abdullah; AL-TWAIJRY, Najd. A comparative analysis of social engineering penetration testing methodologies. **Journal of Information Security and Cybercrimes Research (JISCR)**, v. 7, n. 1, p. 119-137, 2024.
- AMAYA-GÓMEZ, Rafael et al. An analysis of engineering students' risk perception to support process safety learning process. **Education for Chemical Engineers**, v. 42, p. 7-19, 2023.
- AZAN, Wilfrid et al. Increased remote work: **Information security awareness, knowledge and Uncertainty**. In: ECIS (Pre ECIS), AIS, on line (canada France), Canada, 2022.
- CIALDINI, Robert B. **As armas da persuasão**: como influenciar e não se deixar influenciar. Tradução de Ivo Korytowski. Rio de Janeiro: Sextante, 2012.
- FERNANDES, Rodrigo Ildson Lima. **da sensibilização à proteção: aplicação da política de segurança da informação, um estudo de caso na unb**. Dissertação (Mestrado em Governança e Inovação em Políticas Públicas) – Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas, Universidade de Brasília, Brasília, 2025.
- GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 6. ed. São Paulo: Atlas, 2017.
- HADNAGY, Christopher. **Social Engineering: The Science of Human Hacking**. 2. ed. Indianapolis: John Wiley & Sons, 2018.
- INSTITUTO FEDERAL DO PIAUÍ (IFPI). **Comitê de Ética em Pesquisa com Seres Humanos (CEP/IFPI)**. Disponível em: <https://www.ifpi.edu.br/cep>. Acesso em: 05 nov. 2025.
- KAHNEMAN, Daniel. **Rápido e devagar**: duas formas de pensar. Rio de Janeiro: Objetiva, 2011.
- KOCH, Gustavo Duarte Waltereith. **Perfil de vítimas de golpes em uma instituição financeira**. Trabalho de Conclusão de Curso (Bacharelado em Administração) – Escola de Administração, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2022.
- MARTINS, Ronaldo Rodrigues; SILVA, João Vitor Fonseca Duarte. Estratégias de defesa contra engenharia social em ambientes de trabalho home office. **Revista Interface Tecnológica**, v. 18, n. 2, 2021.
- MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**: lições de um hacker sobre segurança da informação. São Paulo: Pearson Education do Brasil, 2003.

PARK, Sang Hee. Relationship between indoor noise perception and remote work during the COVID-19 pandemic. **PLoS ONE**, v. 18, n. 6, p. e0286481, 2023.

RODRIGUES, Bruno Ramos. **um estudo para identificar os desafios enfrentados pelas organizações com relação a segurança da informação no ambiente de home office**. Monografia (Graduação em Engenharia de Software) – Instituto de Ciências Exatas e Tecnologia, Universidade Federal do Amazonas, Itacoatiara, 2022.

SANTOS, Maiara de Castro. **Engenharia Social e Técnicas de Defesas: uma abordagem no nível de conhecimento e de conscientização de usuários de dispositivos de Internet das Coisas**. Dissertação (Mestrado em Ciência da Computação) – Centro de Ciências Exatas e Tecnologia, Universidade Federal de Sergipe, São Cristóvão, 2022.

SOUZA, Diego dos Santos. **Engenharia Social: Explorando o elo mais fraco da Segurança da Informação**. 2013. 59 f. Monografia (Bacharelado em Informática) – Centro Universitário Carioca, Rio de Janeiro, 2013.

SOUZA, Tiago Oliveira de. **Transformação Digital e Suas Implicações na Vulnerabilidade das Organizações: Uma Revisão Sistemática da Literatura**. 2022. 67 f. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) – Centro de Informática, Universidade Federal de Pernambuco, Recife, 2022

YIN, Robert K. **Estudo de Caso: Planejamento e Métodos**. 5. ed. Porto Alegre: Bookman, 2015.

APÊNDICE A – TCLE

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

Título da Pesquisa: Engenharia Social no Home Office: Análise Comparativa da Percepção de Vulnerabilidades de Ataques de Phishing entre Servidores Remotos e Presenciais do Instituto Federal do Piauí.

1. CONVITE

Você está sendo convidado(a) a participar da pesquisa acima citada. Este estudo é um Trabalho de Conclusão de Curso (TCC) do curso de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal do Piauí (IFPI) – Campus Floriano. A sua participação é voluntária, o que significa que você tem total liberdade para decidir se quer ou não participar, sem qualquer prejuízo.

2. OBJETIVOS E JUSTIFICATIVA

Esta pesquisa tem como objetivo entender e comparar como os servidores que trabalham presencialmente e aqueles que trabalham em regime remoto (home office) percebem os riscos de ataques cibernéticos, especificamente o phishing (e-mails ou mensagens falsas que tentam roubar dados). A justificativa para este estudo é a necessidade de proteger melhor as informações da nossa instituição e dos próprios servidores, identificando quais grupos precisam de mais apoio ou treinamento em segurança.

3. PROCEDIMENTOS

Caso aceite participar, pediremos que você responda a um questionário online.

- **O que farei?** Você responderá perguntas sobre seu perfil (tempo de serviço, regime de trabalho), seu conhecimento sobre segurança e como você agiria em situações hipotéticas de recebimento de e-mails suspeitos.

- **Quanto tempo leva?** O tempo estimado para preenchimento é de 10 a 15 minutos.

- **Onde?** O questionário pode ser respondido de qualquer computador ou dispositivo com acesso à internet, no local de sua preferência.

4. RISCOS E BENEFÍCIOS

Toda pesquisa envolve riscos, mesmo que mínimos.

- **Riscos:** A participação pode gerar um leve cansaço visual ou desconforto psicológico ao refletir sobre suas próprias vulnerabilidades a golpes digitais.

- **Como contornar os riscos:** Para minimizar o cansaço, você pode pausar o preenchimento a qualquer momento. Caso sinta desconforto, você tem o direito de interromper a pesquisa imediatamente sem penalidades.

- **Benefícios:** Embora não haja benefícios financeiros diretos para você, sua participação ajudará o IFPI a desenvolver programas de treinamento mais eficazes e políticas de segurança melhores, protegendo os dados de toda a comunidade acadêmica.

5. SIGILO E PRIVACIDADE

Garantimos o total sigilo das suas informações. O questionário não solicitará seu nome, matrícula, e-mail ou endereço IP. Os dados serão analisados apenas em conjunto (estatisticamente) e divulgados em trabalhos acadêmicos sem jamais identificar quem participou.

6. ARMAZENAMENTO E DESCARTE

Para garantir sua privacidade e segurança, os dados coletados na plataforma online serão imediatamente baixados para um computador local sob a guarda do pesquisador e, em seguida, apagados definitivamente da internet (nuvem/plataforma virtual). Os arquivos locais serão mantidos por um período mínimo de 5 (cinco) anos, conforme a Resolução CNS nº 466/2012, em dispositivo protegido por senha..

7. CUSTOS, RESSARCIMENTO E INDENIZAÇÃO

- **Custos:** Você não terá nenhum custo para participar desta pesquisa.
- **Ressarcimento:** Como a pesquisa é online e respondida conforme sua conveniência, não estão previstas despesas. No entanto, é seu direito garantido ser ressarcido caso tenha alguma despesa decorrente diretamente da participação na pesquisa.
- **Indenização:** É garantido o seu direito de pleitear indenização diante de eventuais danos comprovados decorrentes da sua participação na pesquisa.

8. DESISTÊNCIA

Você tem plena liberdade para recusar-se a participar ou retirar seu consentimento em qualquer fase da pesquisa, sem necessidade de justificativa e sem qualquer penalidade ou prejuízo às suas atividades na instituição.

9. CONTATOS

Em caso de dúvidas sobre a pesquisa, você pode entrar em contato com os pesquisadores a qualquer momento:

- **Pesquisador Responsável:** João Rafael Oliveira Tavares

o Telefone: (88) 99212-6212

o E-mail: joao.tavares.2020114ielm08.3101@gmail.com

- **Pesquisador Orientador:** Prof. Dr. Leandro Rodrigues de Oliveira

o E-mail: leandro@ifpi.edu.br

Para dúvidas sobre **seus direitos como participante de pesquisa**, ou sobre questões éticas, você pode contatar o **Comitê de Ética em Pesquisa (CEP) do IFPI**:

- **Endereço:** Reitoria do Instituto Federal do Piauí. Av. Presidente Jânio Quadros, nº 330, Santa Isabel, sala 3, CEP: 64053-390, Teresina–PI.

- **Telefone:** (86) 3131-1441

- **E-mail:** cep@ifpi.edu.br

- **Horário de Atendimento:** Segunda a Sexta, das 08h às 12h e das 14h às 18h.

10. CONSENTIMENTO PÓS-ESCLARECIDO

O participante receberá uma via deste Termo de Consentimento Livre e Esclarecido assinada pelo pesquisador, e o pesquisador arquivará a outra via assinada pelo participante (ou registro eletrônico equivalente).

Diante do exposto, declaro que fui devidamente esclarecido(a) sobre os objetivos, procedimentos, riscos e benefícios da pesquisa, e concordo em participar voluntariamente.

Local, Data.

Assinatura do Participante de Pesquisa

João Rafael Oliveira Tavares (Pesquisador) CPF: 099.963.323-65

Prof. Dr. Leandro Rodrigues de Oliveira (Orientador) CPF: 042.091.603-26

APÊNDICE B – QUESTIONÁRIO

SEÇÃO 1: PERFIL FUNCIONAL E REGIME DE TRABALHO

(Objetivo: Coletar as variáveis de controle e a variável independente principal)

1.1. Cargo: () Docente () Técnico-Administrativo em Educação

1.2. Nível de Escolaridade: () Ensino Médio/Técnico () Graduação () Especialização () Mestrado () Doutorado

1.3. Tempo de Serviço na Instituição: () Menos de 1 ano () 1 a 5 anos () 6 a 10 anos () 11 a 20 anos () Mais de 20 anos

1.4. Faixa Etária: () Até 30 anos () 31 a 40 anos () 41 a 50 anos () 51 a 60 anos () Mais de 60 anos

1.5. (Questão-Chave) Qual seu regime de trabalho predominante nos últimos 12 meses? () **Presencial:** Realizo minhas atividades majoritariamente (ou 100%) nas dependências físicas da instituição. () **Remoto/Híbrido (Home Office):** Realizo minhas atividades majoritariamente (ou 100%) da minha residência ou fora da instituição.

SEÇÃO 2: CONHECIMENTO EM SEGURANÇA DA INFORMAÇÃO (SI)

(Baseado em: Fernandes, 2025; Santos, 2022. Mede o nível de conscientização formal)

2.1. Você conhece a Política de Segurança da Informação (PSI) da sua instituição? () Sim, li e conheço os detalhes. () Sim, já ouvi falar, mas não conheço os detalhes. () Não conheço.

2.2. Você já recebeu algum treinamento formal (curso, palestra, e-mail informativo) sobre Segurança da Informação ou Phishing oferecido pela sua instituição? () Sim, nos últimos 12 meses. () Sim, mas há mais de 1 ano. () Não, nunca recebi.

2.3. Em sua opinião, qual a melhor definição para "Phishing"? () Um vírus de computador que deixa a máquina lenta. () Um tipo de e-mail ou mensagem

fraudulenta que tenta roubar dados pessoais (senhas, CPF). () Um sistema de proteção de rede usado pela instituição (firewall). () Não sei definir.

2.4. Em sua opinião, qual a melhor definição para "Engenharia Social"? ()

Análise de comportamento de usuários para aprimorar a usabilidade e conexão com os serviços da instituição. () Método de persuasão utilizado pela equipe de TI para promover o engajamento no cumprimento das políticas de segurança. () Técnica de manipulação psicológica para enganar pessoas e obter informações. () Não sei definir.

SEÇÃO 3: PERCEPÇÃO DE RISCO E AMBIENTE DE TRABALHO

(Baseado em: Martins; Silva, 2021; Azan et al., 2022. Mede a percepção do risco em diferentes contextos. Use Escala Likert de 5 pontos)

Instrução: Indique seu nível de CONFIANÇA ao realizar as seguintes ações, sendo 1 (Muito Inseguro) e 5 (Muito Seguro).

Ação	1 - Muito Inseguro	2 - Inseguro	3 - Neutro	4 - Seguro	5 - Muito Seguro
3.1. Abrir um arquivo PDF/Word anexo em um e-mail de um colega de trabalho.	()	()	()	()	()
3.2. Clicar em um link enviado pelo setor de TI para "atualização cadastral".	()	()	()	()	()
3.3. Inserir sua senha do sistema institucional (ex: SUAP/SIGAA) em uma página que parece ser a oficial.	()	()	()	()	()

3.4. Usar o computador pessoal (e não o da instituição) para acessar o e-mail e sistemas institucionais. (Baseado em Martins; Silva, 2021)	()	()	()	()	()
3.5. Acessar os sistemas institucionais usando uma rede Wi-Fi pública (ex: aeroporto, café).	()	()	()	()	()

SEÇÃO 4: CENÁRIOS COMPORTAMENTAIS (ANÁLISE DE GATILHOS)

(Baseado em: Kahneman, 2011; Mitnick, 2003; Koch, 2022. Testa o Sistema 1 (impulso) vs. Sistema 2 (análise) usando gatilhos de Autoridade, Urgência e Benefício)

Instrução: Imagine as seguintes situações e marque a ação que você provavelmente tomaria.

4.1. Cenário 1 (Gatilho: Autoridade + Urgência) Você recebe um e-mail que aparenta ser do Gabinete da Reitoria (ou Direção-Geral). O título é "URGENTE: Verificação de Segurança Obrigatória" e o texto informa que sua conta será bloqueada em 2 horas se você não validar suas credenciais no link fornecido. O que você faz?

() Clico no link e insiro minha senha para não ser bloqueado.

() Respondo ao e-mail pedindo mais informações.

() Ignoro o e-mail, pois deve ser falso.

() Entro em contato com o setor de TI por outro canal (telefone, site oficial) para verificar a legitimidade antes de tomar qualquer ação.

4.2. Cenário 2 (Gatilho: Benefício/Curiosidade) Você recebe um e-mail do setor de RH/Gestão de Pessoas com o título "Erro no Pagamento: Veja os valores a serem ressarcidos". O e-mail pede que você abra a planilha anexa (ex: "Ressarcimento.zip") para conferir os valores. O que você faz?

- () Abro o anexo imediatamente para verificar os valores.
- () Respondo ao e-mail perguntando sobre o que se trata.
- () Apago o e-mail; sei que o RH não envia esse tipo de anexo.
- () Entro em contato com o setor de RH/Pagamento por outro canal (telefone, site oficial) para verificar a veracidade da informação.

4.3. Cenário 3 (Gatilho: Suporte Técnico/Vishing - Foco no Home Office) Você está em *home office* e recebe um telefonema (ou mensagem de WhatsApp) de alguém que se identifica como "Suporte Técnico da TI". A pessoa informa que identificou um "vírus" em sua conexão e precisa que você instale um programa de acesso remoto (ex: TeamViewer, AnyDesk) e informe o código de acesso para que ela possa "limpar" sua máquina. O que você faz?

- () Instalo o programa e informo o código; afinal, preciso que o computador funcione.
- () Desligo a ligação e ignoro; se fosse importante, eles mandariam um e-mail.
- () Pego o nome completo e o ramal da pessoa e digo que vou ligar de volta para o número oficial da TI para confirmar.
- () Nego o acesso e reporto o número de telefone ao setor de TI como tentativa de golpe.

SEÇÃO 5: AMBIENTE REMOTO E TREINAMENTO

(Focada apenas nos respondentes que marcaram "Remoto/Híbrido" na Questão 1.6.

Baseado em Azan et al., 2022 e Park et al., 2023)

As perguntas a seguir são apenas para quem está em regime de trabalho remoto ou híbrido.

Instrução: Indique seu grau de concordância com as frases abaixo (1-Discordo Totalmente; 5-Concordo Totalmente).

Frase	1 - Discordo Totalmente	2 - Discordo	3 - Neutro	4 - Concordo	5 - Concordo Totalmente
5.1. Sinto-me mais distraído (ex: interrupções, ruídos domésticos) ao analisar e-mails em casa do que no ambiente presencial. (Baseado em Park <i>et al.</i> , 2023)	()	()	()	()	()
5.2. Sinto-me mais inseguro ou incerto sobre como agir ao receber um e-mail suspeito quando estou em casa. (Baseado em Azan <i>et al.</i> , 2022)	()	()	()	()	()
5.3. Considero mais difícil ou demorado obter ajuda do suporte de TI quando estou em home office.	()	()	()	()	()
5.4. Acredito que estou mais vulnerável a ataques cibernéticos trabalhando em casa do que no escritório.	()	()	()	()	()

Agradecimento

"Obrigado pela sua participação! Suas respostas anônimas são fundamentais para o desenvolvimento desta pesquisa e para a melhoria da segurança da informação em nossa instituição."