REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

FATOR HUMANO NA SEGURANÇA DA INFORMAÇÃO: UMA REVISÃO DA LITERATURA SOBRE CONSCIENTIZAÇÃO E TREINAMENTO

THE HUMAN FACTOR IN INFORMATION SECURITY: A LITERATURE REVIEW ON AWARENESS AND TRAINING

Ciências Exatas e da Terra, Ciências Sociais Aplicadas • 26/08/2026

REGISTRO DOI: 10.70773/revistatopicos/787702118

Marcus Vinicius dos Santos Moura[1]

José Rodrigues de Farias Filho[2]

Julio Vieira Neto[3]

Ana Dias José Rodrigues de Farias Filho[4]

RESUMO

Este estudo investiga o papel determinante do fator humano na segurança da informação no contexto da Administração Pública Federal do Brasil, sob o prisma da conformidade regulatória frente às diversas leis que regem o tema, como o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais (LGPD), a criação do E-CIBER e ao Programa de Privacidade e Segurança da Informação (PPSI), entre outros. O objetivo geral deste artigo consiste em realizar uma revisão sistemática da literatura para mapear as vulnerabilidades comportamentais recorrentes, as táticas de engenharia social mais incidentes e as metodologias de conscientização e treinamento com maior eficácia cientificamente comprovada. A metodologia adotada ampara-se no protocolo internacional PRISMA 2020, executando uma busca estruturada em bases de dados de alto impacto como CAPES e Google Acadêmico, da qual resultou a seleção de dezenove artigos científicos rigorosamente selecionados e analisados. Os resultados do mapeamento apontam para a persistência de severos desvios de conduta rotineiros, tais como obsolescência no manuseio de credenciais e compartilhamento indevido de acessos, agravados pela falta de agência e pelo desconhecimento generalizado das normativas vigentes por parte do corpo de servidores. Revela-se também a prevalência do viés cognitivo de ilusão de segurança tecnológica, que desestimula posturas preventivas ativas dos indivíduos. Conclui-se que o fortalecimento da resiliência cibernética governamental requer a transição de um paradigma puramente tecnológico em direção a programas pedagógicos continuados, estruturados, baseados em simulações práticas e engajamento ativo, promovendo uma cultura de responsabilidade compartilhada.

Palavras-chave: Segurança da Informação; Fator Humano; Conscientização e Treinamento.

ABSTRACT

This study investigates the decisive role of the human factor in information security within the context of the Brazilian Federal Public Administration, from the perspective of regulatory compliance with key governing laws, such as the Internet Civil Framework (Marco Civil da Internet), the General Personal Data Protection Law (LGPD), the establishment of E-CIBER, and the Privacy and Information Security Program (PPSI), among others. The main objective of this article is to perform a systematic literature review to map recurring behavioral vulnerabilities, the most prevalent social engineering tactics, and the awareness and training methodologies with the highest scientifically proven effectiveness. The adopted methodology relies on the international PRISMA 2020 protocol, conducting a structured search in high-impact databases such as CAPES and Google Scholar, which resulted in the selection of nineteen rigorously analyzed scientific articles. The findings highlight the persistence of severe routine misconduct, such as poor credential management and improper sharing of access permissions, compounded by a lack of agency and widespread unawareness of current regulations among public servants. The results also reveal a prevalent cognitive bias, the illusion of technological security, which discourages individuals from taking active preventive measures. It is concluded that strengthening governmental cyber resilience requires shifting from a purely technological paradigm toward continuous, structured educational programs based on practical simulations and active engagement, thereby fostering a culture of shared responsibility.

Keywords: Information Security; Human Factor; Awareness and Training.

1. INTRODUÇÃO

No cenário contemporâneo, a informação consolidou-se como um dos ativos mais valiosos, estratégicos e indispensáveis para a continuidade e a eficiência operacional das organizações, especialmente no âmbito da Administração Pública Federal (APF) do Brasil. A rápida transformação digital e a disseminação das tecnologias da informação e comunicação reformularam profundamente a forma pela qual o Estado interage com a sociedade e gerencia seus processos internos. Todavia, essa hiperconectividade e dependência de infraestruturas digitais trouxeram consigo um aumento exponencial nas ameaças e vulnerabilidades cibernéticas, expondo as instituições governamentais a severos riscos de incidentes que afetam diretamente a integridade, a confidencialidade e a disponibilidade dos dados custodiados, conforme alertam Semlambo, Mfoi e Sangula (2022).

Diante deste cenário de riscos crescentes, a resposta convencional da maioria das instituições públicas e privadas tem sido concentrar seus maiores esforços e investimentos no fortalecimento de controles técnicos rígidos e barreiras tecnológicas complexas, tais como criptografia avançada, *firewalls* de nova geração e sistemas corporativos de detecção e prevenção de vírus. Contudo, como demonstram os dados empíricos de inteligência e segurança cibernética global, a dependência exclusiva de soluções tecnológicas tem se provado insuficiente para mitigar as quebras de segurança. O fator humano permanece como o vetor primário e o ponto de maior sensibilidade em qualquer ecossistema de proteção de dados, sendo frequentemente apontado como o elemento explorado para contornar os perímetros de defesa digitais mais robustos (Souza, 2022; Mitnick; Simon, 2003).

As falhas comportamentais cotidianas no ambiente de trabalho, o desconhecimento generalizado de políticas institucionais escritas e a vulnerabilidade à manipulação psicológica por agentes maliciosos (fenômeno conhecido como engenharia social) representam brechas críticas que colocam em risco o patrimônio informacional público. Práticas informais recorrentes, como a anotação de credenciais em suportes físicos expostos, o uso indiscriminado de dispositivos de armazenamento de dados USB sem verificação e a execução involuntária de links e arquivos suspeitos em e-mails institucionais, constituem sintomas evidentes de uma cultura organizacional frágil em segurança da informação (Carneiro; Almeida, 2013; Falla; Pinto, 2024).

Esta problemática ganha ainda maior relevância sob a égide do ambiente normativo brasileiro atual, fortemente impactado pelas exigências legais de leis como o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais (LGPD) (Brasil, 2018b) e pelas diretrizes de governança estabelecidas pelo Programa de Privacidade e Segurança da Informação (PPSI) (Brasil, 2023). O PPSI, balizado pelo referencial internacional do CIS *Controls* v.8, impõe a necessidade de as instituições públicas brasileiras monitorarem e elevarem seu nível de maturidade em segurança, dedicando especial atenção à conscientização e ao treinamento dos recursos humanos, conforme preconizado no seu Controle 14. Nesse sentido, as práticas cotidianas dos servidores precisam ser investigadas e moldadas por metodologias que superem as barreiras do ensino passivo e tradicional.

Contudo, a literatura científica de segurança da informação revela-se historicamente fragmentada, com uma vasta produção concentrada em aspectos puramente técnicos, apresentando poucas evidências

sistematizadas sobre a efetividade de estratégias de mudança comportamental em servidores administrativos leigos. Diante desse vácuo teórico e prático, coloca-se a necessidade de realizar um mapeamento sistemático e integrado do estado da arte do fator humano na segurança governamental.

A presente pesquisa propõe-se a responder às seguintes questões:

1. *Quais são as principais vulnerabilidades comportamentais e táticas de engenharia social voltadas ao setor público identificadas na literatura recente?*

2. *Quais estratégias de conscientização e metodologias pedagógicas de treinamento de usuários têm demonstrado maior eficácia na redução de riscos?*

3. *De que maneira os frameworks internacionais e as legislações nacionais balizam as ações de segurança em recursos humanos?*

O objetivo geral deste artigo consiste em realizar uma revisão sistemática da literatura (RSL) sobre o fator humano na segurança da informação no setor público federal, triangulando referenciais normativos, evidências empíricas e estratégias pedagógicas para propor caminhos que permitam fortalecer as barreiras atitudinais contra os ataques cibernéticos modernos. Justifica-se este estudo pela premente necessidade de orientar gestores públicos com bases científicas para a alocação eficiente de recursos em segurança de pessoal, transformando o usuário final em um agente ativo de defesa corporativa, uma espécie de *firewall* humano.

2. REVISÃO DA LITERATURA

2.1. O Papel do Fator Humano e o Conceito de "Elo Mais Fraco"

O termo "fator humano" tem suas origens científicas na década de 1950, quando o economista Theodore Schultz formulou a teoria do capital humano, destacando o papel estratégico do indivíduo como um ativo de desenvolvimento nas organizações (Minto, 2021; Kanagusku; Gaseta, 2024). Com o advento da era digital e a ampla inserção de sistemas informatizados nas rotinas de trabalho, este conceito expandiu-se e passou a integrar de forma central as discussões sobre segurança de dados.

Historicamente, a literatura e os profissionais de Tecnologia da Informação adotaram uma visão estigmatizada e depreciativa em relação ao usuário final de sistemas, rotulando-o de forma quase unânime como "o elo mais fraco" da corrente de segurança da informação (Souza, 2022; Mitnick; Simon, 2003). Essa premissa fundamenta-se na complexidade inerente ao elemento humano, cujas ações são influenciadas por fatores subjetivos, pressões psicológicas, estresse, fadiga, vieses cognitivos e nível de alfabetização digital, tornando-o suscetível a erros processuais de difícil previsão matemática (Arif; Zulfiquar; Bhutto, 2011; Kanagusku; Gaseta, 2024).

Entretanto, autores contemporâneos têm contestado enfaticamente esse rótulo pessimista. Hoepers (2024) e Kanagusku e Gaseta (2024) argumentam que tratar o ser humano simplesmente como o elo mais fraco constitui uma falha conceitual e uma barreira para a eficácia das defesas cibernéticas. Segundo as autoras, quando adequadamente educado, treinado, valorizado e envolvido pelas lideranças corporativas, o fator humano deixa de ser uma vulnerabilidade passiva e eleva-se à condição de elo principal da

cadeia, atuando como uma sólida e proativa barreira defensiva atitudinal de segurança (Hoepers, 2024; Kanagusku; Gaseta, 2024).

A segurança da informação não pode ser alcançada de maneira duradoura sem considerar a subjetividade dos indivíduos e seus modelos mentais. Conforme postulam Carneiro e Almeida (2013), as rotinas corporativas de necessidade, busca e uso de fontes de informação eletrônica moldam as condutas preventivas. Para consolidar comportamentos de conformidade seguros, a organização precisa promover a democratização do conhecimento e facilitar a acessibilidade cognitiva às políticas de segurança vigentes, assegurando que o usuário entenda não apenas o que fazer, mas os motivos que justificam tais exigências operacionais (Carneiro; Almeida, 2013).

2.2. Táticas de Engenharia Social e a Vulnerabilidade Comportamental

A engenharia social caracteriza-se como um conjunto de métodos, técnicas e abordagens psicológicas utilizadas por cibercriminosos com o propósito de manipular, enganar e induzir pessoas a realizar ações indevidas ou a divulgar informações confidenciais de caráter pessoal ou institucional (Falla; Pinto, 2024; Tenório *et al.,* 2022). Em vez de explorar vulnerabilidades tecnológicas complexas em sistemas operacionais ou *softwares*, o engenheiro social ataca diretamente as fragilidades cognitivas do ser humano, como a ingenuidade, a confiança interpessoal, a curiosidade, a pressa e a vulnerabilidade à pressão psicológica (Tenório *et al.,* 2022).

As principais táticas de engenharia social mapeadas na literatura recente dividem-se em várias vertentes:

- *Phishing* por e-mail, que consiste no envio de mensagens eletrônicas fraudulentas contendo links ou anexos maliciosos que mimetizam comunicados de instituições legítimas;

- *Vishing* por telefone, onde o atacante usa de persuasão verbal direta para obter dados confidenciais sob pretexto de suporte técnico;

- *Baiting*, que envolve deixar mídias físicas infectadas (como unidades de dados USB) em postos de trabalho ou áreas públicas, contando com a curiosidade do usuário para inseri-las no computador institucional;

- *Shoulder Surfing*, no qual se observa de forma física direta a digitação de senhas e dados confidenciais nas telas das estações de trabalho (Falla; Pinto, 2024; Marcelino *et al.*, 2023).

Um aspecto crítico discutido na literatura moderna refere-se à aleatoriedade na escolha do alvo por parte dos atacantes. Scudere (2007) e Tenório *et al.* (2022) alertam que, contrariando a percepção de muitos servidores públicos, os incidentes de fraude cibernética em sua maioria não visam a uma instituição ou pessoa específica de maneira direcionada. Através de varreduras automatizadas, postagens de engenharia social genéricas em redes sociais e o lançamento amplo de iscas eletrônicas (*phishing*), os criminosos operam de forma aleatória, de modo que qualquer deslize atitudinal ou exposição descuidada de dados na internet torna o indivíduo, e a sua organização, vítimas em potencial de invasões cibernéticas severas (Scudere, 2007; Tenório *et al.,* 2022).

2.3. Normas e Diretrizes de Segurança da Informação Pública

A governança da segurança da informação no setor público federal brasileiro é balizada por um robusto conjunto de regulamentações nacionais e referenciais internacionais. No plano internacional, as diretrizes básicas são fornecidas pelas normas de sistemas de gestão da família ISO/IEC. A ABNT NBR ISO/IEC 27001 estabelece os requisitos mandatórios para a estruturação de um Sistema de Gestão de Segurança da Informação (SGSI), enquanto a ABNT NBR ISO/IEC 27002 oferece o código de prática com os controles operacionais para gerenciar os riscos (ABNT, 2013a; ABNT, 2013b).

Sob a perspectiva de recursos humanos e governança interna, destacam-se os requisitos de Liderança, Comprometimento e Recursos descritos no Requisito 5 e 7 da ISO/IEC 27001, bem como os Controles de Pessoas na Seção 6 da NBR ISO/IEC 27002, em especial o Controle 6.3, dedicado à conscientização, educação e treinamento em segurança da informação. Esses normativos determinam que a conscientização de pessoal deve ir além do mero treinamento formal sobre “o que fazer”, devendo motivar os colaboradores em relação ao “porquê” da importância de cada comportamento preventivo (ABNT, 2013b; Trigos; Nuno, 2021).

No espectro legal brasileiro, a proteção dos ativos informacionais de interesse estatal é regulada pelo Decreto nº 9.637, que institui a Política Nacional de Segurança da Informação (PNSI) (Brasil, 2018a), e pelo Decreto nº 10.222, que aprova a Estratégia Nacional de Segurança Cibernética (E-CIBER) (Brasil, 2020), além do Decreto nº 12.573, que atualiza a Estratégia Nacional de Cibersegurança para o período subsequente (Brasil, 2025). Adicionalmente, o Gabinete de Segurança Institucional estabelece orientações por meio da Instrução Normativa GSI/PR nº 3, regulando os processos obrigatórios para gestão de segurança nos órgãos federais (Brasil,

2021). No trato com o cidadão, o direito de acesso é norteado pela Lei de Acesso à Informação (LAI) (Brasil, 2011), cujos limites de sigilo e dever de integridade física dos registros são salvaguardados.

Por fim, a proteção à privacidade de dados de natureza pessoal geridos pela administração federal foi substancialmente fortalecida com a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) (Brasil, 2018b). Para assegurar a conformidade com a LGPD e mitigar incidentes de dados, a Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos instituiu o Programa de Privacidade e Segurança da Informação (PPSI) por meio da Portaria SGD/MGI nº 852/2023 (Brasil, 2023). O PPSI atua como um *framework* prático baseado nos primeiros dezoito controles técnicos prioritários do CIS *Controls* v.8, tendo como foco do nosso estudo o seu Controle 14 (Conscientização e Treinamento em Segurança da Informação), que obriga a execução de planos cíclicos de capacitação e conscientização para o corpo funcional governamental.

3. METODOLOGIA

Para atingir o objetivo proposto, este artigo adota o delineamento metodológico de uma Revisão Sistemática da Literatura (RSL), estruturada de acordo com o protocolo internacional estabelecido pelas diretrizes do PRISMA 2020 (Page *et al.,* 2021) e fundamentada operacionalmente nas cinco etapas de condução científica de revisões sistemáticas propostas por Okoli (2015). A RSL constitui um método rigoroso, transparente e reprodutível para identificar, avaliar e sintetizar a totalidade das evidências científicas pertinentes a um problema ou questão de pesquisa específica, mitigando a

introdução de vieses de seleção de literatura pelo pesquisador (Moen *et al.*, 2024; Page *et al.,* 2021).

A jornada investigativa transcorreu em etapas estruturadas. Inicialmente, definiram-se as três questões de pesquisa detalhadas no Capítulo 1. A fase subsequente consistiu no planejamento e na execução do protocolo de busca sistemática nas bases de dados, utilizando como fonte primária o portal de periódicos indexados na Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e o mecanismo de busca complementar do Google Acadêmico. As chaves de busca foram constituídas de *strings* combinando os termos do traço de interesse por meio do operador booleano 'AND', limitando o espectro de amostragem às publicações científicas revisadas por pares redigidas em português brasileiro ou inglês, no período de 2000 a 2025.

A estratégia de busca procedimental foi estruturada de forma sequencial com três *strings* de refinamento:

1. Cruzaram-se os termos “INFORMATION SECURITY” AND “AWARENESS AND TRAINING”, gerando um montante inicial de 52 artigos científicos. Aplicou-se então o filtro de atualidade de recorte temporal (entre 2021 e 2025) para captar os estudos contemporâneos sobre o tema, refinando a amostra para 20 artigos;

2. Refinou-se o espectro adicionando o termo do fator humano à chave original, utilizando a *string* “INFORMATION SECURITY” AND “HUMAN FACTOR” AND (“AWARENESS” OR “TRAINING”), o que resultou na identificação de 12 artigos;

3. Investigou-se a *string* “INFORMATION SECURITY” AND “HUMAN FACTOR” no intervalo entre 2011 e 2024, retornando 4 artigos adicionais de alta relevância. Ao final das três buscas estruturadas, obteve-se um total de 68 registros preliminarmente identificados.

Submeteu-se esse conjunto à etapa de triagem de duplicados e leitura crítica de títulos e resumos para avaliar a relevância temática face ao fator humano, resultando na eliminação de 44 registros inconsistentes ou fora do escopo. Desse processo, restaram 24 artigos elegíveis para avaliação de texto integral. Na fase de leitura na íntegra, aplicaram-se critérios de exclusão metodológicos rigorosos, resultando no descarte de 5 trabalhos:

Descartou-se o trabalho de Nader Hassan Khalifa por focar em análise técnica de implantação de sistemas ERP;

Excluiu-se o artigo de Jaffar Ahmad por estar redigido em idioma árabe, inviabilizando a precisão na tradução;

Descartaram-se dois estudos por abordarem exclusivamente subtemas comerciais específicos de prevenção de fraudes em transações de cartões de crédito;

Descartou-se uma publicação de 2005 devido à obsolescência dos conceitos tecnológicos em relação ao ambiente regulatório vigente.

Após o processo de triagem e a aplicação criteriosa das exclusões, a revisão sistemática consolidou a amostra definitiva de **19 artigos** científicos de alto impacto e 10 diretrizes normativas federais, os quais integraram as etapas de extração de dados, síntese de evidências e discussões presentes neste artigo. A representação

estruturada do fluxo metodológico PRISMA 2020 está detalhada no Quadro 1 a seguir.

Quadro 1. Fluxograma PRISMA

Etapa PRISMA	Descrição do Processo	Registros / Artigos (N)
Identificação	Registros identificados por meio de pesquisas estruturadas em bases de dados CAPES e Google Acadêmico via chaves booleanas combinadas.	68
Triagem	Registros avaliados preliminarmente com base na leitura crítica de títulos e resumos. Eliminação de duplicados e inconsistências de escopo.	24 (44 excluídos)
Elegibilidade	Artigos lidos na íntegra para verificação de aderência temática fina. Exclusão de 5 artigos após análise rigorosa (ERP, idioma árabe, foco comercial e obsolescência).	19 (5 excluídos)
Inclusão	Estudos finais incluídos para extração e síntese qualitativa de dados, triangulação analítica e discussão científica das RQs.	19 artigos selecionados

Fonte: Elaborado pelo autor (2026).

4. RESULTADOS E DISCUSSÕES

4.1. RQ1: Vulnerabilidades Comportamentais e Táticas de Engenharia Social no Setor Público

A análise qualitativa e sistemática das evidências científicas selecionadas nesta revisão permitiu mapear as condutas de risco mais reincidentes no ambiente de trabalho administrativo

governamental. Em dissonância com as práticas formais exigidas nas políticas de segurança institucionais escritas, observa-se que os usuários leigos do setor público realizam sistematicamente comportamentos inseguros em suas rotinas operacionais (Souza, 2022).

A principal vulnerabilidade detectada na literatura refere-se à obsolescência crônica na gestão de credenciais de acesso individuais. De acordo com os achados de Souza (2022) e Semlambo, Mfoi e Sangula (2022), os usuários administrativos apresentam forte resistência para realizar a alteração periódica de senhas de trabalho, operando por meses ou anos sob chaves de autenticação estáticas e de baixa complexidade. Agravando essa fragilidade, é frequente a prática de compartilhamento eventual de logins pessoais com colegas de setor no pretexto de agilizar demandas burocráticas ou suprir ausências temporárias, contrariando o princípio de unicidade de acesso e as determinações das normas NBR ISO/IEC 27002 (Semlambo; Mfoi; Sangula, 2022; Souza, 2022).

Adicionalmente, os desvios comportamentais estendem-se ao manuseio físico de mídias e registros. O armazenamento inadequado de senhas (como lembretes e notas coladas em monitores, teclados e gavetas) e a negligência no descarte de rascunhos em papel contendo dados pessoais ou sigilosos expõem a instituição a riscos de acesso físico não autorizado (*dumpster diving* ou vazamento interno de mídias), conforme discutido por Souza (2022) e Falla e Pinto (2024). No espectro eletrônico, o tráfego de dados de trabalho por dispositivos móveis pessoais sem protocolos de proteção (BYOD) e o uso de redes Wi-Fi públicas desprovidas de conexões criptografadas seguras (como redes VPN) constituem

práticas corriqueiras que vulnerabilizam o perímetro tecnológico das repartições (Falla; Pinto, 2024; Kearney; Kruger, 2016).

No que tange às táticas de engenharia social, a literatura recente aponta o *phishing* por e-mail como a ferramenta mais incidente e destrutiva empregada por atacantes na atualidade (Falla; Pinto, 2024; Marcelino *et al.*, 2023). O sucesso dessas abordagens repousa na exploração das fraquezas psicossociais humanas. O atacante mimetiza com precisão as comunicações institucionais da alta gestão ou de autarquias do governo para instigar a urgência e compelir o servidor a executar arquivos anexos maliciosos ou links suspeitos que contornam o perímetro de rede (Falla; Pinto, 2024). Este comportamento impulsivo é frequentemente motivado pelo viés de neutralização e pela "ilusão de segurança tecnológica" discutida por Kearney e Kruger (2016) e Al-Diabat (2018): o usuário age de forma displicente por nutrir a crença errônea de que ferramentas automáticas (como o antivírus instalado na máquina) são integralmente suficientes para protegê-lo de qualquer ameaça digital, reduzindo sua postura vigilante de higiene cibernética (Al-Diabat, 2018; Kearney; Kruger, 2016).

4.2. RQ2: Estratégias de Conscientização e Metodologias de Treinamento Eficazes

Frente à constatação de que o fator humano constitui o ponto de maior sensibilidade nas defesas organizacionais, os estudos analisados dedicam expressiva atenção à identificação de metodologias que superem as limitações do ensino passivo tradicional. Como afirmam Trigos e Nuno (2021) e Koza (2022), as abordagens pedagógicas convencionais, baseadas estritamente na disponibilização passiva de extensas cartilhas normativas escritas

em portais institucionais ou na realização de palestras expositivas anuais puramente conceituais, apresentam baixa efetividade para gerar mudança de comportamento duradoura no indivíduo (Koza, 2022; Trigos; Nuno, 2021).

Para que as ações de conscientização e treinamento em segurança da informação (SI) sejam cientificamente efetivas, a literatura atual preconiza a adoção de metodologias de ensino continuadas, interativas e baseadas em simulações práticas que aumentem de forma empírica a autoeficácia e o engajamento dos envolvidos. Al-Diabat (2018) e Moen *et al.* (2024) destacam que treinamentos práticos que simulam incidentes reais de *phishing* por e-mail e manipulação psicológica controlada permitem ao servidor experimentar de forma direta as técnicas do atacante, gerando um aprendizado significativo por meio da vivência prática do erro (Al-Diabat, 2018; Moen *et al.*, 2024).

Seguindo essa mesma linha, a aplicação de conceitos de gamificação tem emergido como uma das ferramentas pedagógicas mais promissoras na área cibernética (Marcelino *et al.,* 2023). A incorporação de mecânicas de jogos, tais como competições saudáveis de conhecimento entre setores de uma repartição pública, atribuição de pontuações, medalhas e recompensas simbólicas para condutas seguras e simulações lúdicas de incidentes, remove o caráter punitivo e burocrático comumente associado à segurança da informação. A gamificação atua diretamente na motivação intrínseca do usuário, incentivando-o a adotar posturas ativas e consolidando hábitos de proteção no cotidiano (Marcelino *et al.,* 2023).

Adicionalmente, os programas estruturados devem ser modulares e customizados de acordo com as funções desempenhadas pelos funcionários. Oruc *et al.* (2024) demonstram, através da avaliação do programa modular "MarCy", que a capacitação em blocos temáticos e adaptados à realidade das tarefas desempenhadas pelo usuário na ponta da operação (como o descarte de dados sensíveis de RH ou o manuseio de credenciais administrativas) propicia maior fixação do conteúdo em comparação com modelos generalistas e uniformes, em consonância com as exigências pedagógicas apontadas por Amankwa (2021) e Koza (2022).

4.3. RQ3: O Alinhamento de Frameworks e Legislações em Recursos Humanos

A governança contemporânea de segurança em recursos humanos exige o perfeito alinhamento entre as melhores práticas ditadas pelos *frameworks* globais e as imposições legais das legislações nacionais. Tanjung, Nurhayati e Wibowo (2024) argumentam que a síntese de estruturas reconhecidas internacionalmente, tais como o NIST CSF 2.0, as normas NBR ISO/IEC 27001 e 27002, e os CIS *Controls* v.8, fornece um roteiro acionável para balizar as ações de proteção em ambiente governamental.

Sob o prisma das diretrizes de pessoas, o Controle 14 do CIS *Controls* v.8 estabelece 9 medidas técnicas prioritárias, entre as quais se destacam a necessidade de realizar treinamentos contínuos de competências com base nas funções, instruir a força de trabalho sobre os perigos do tráfego de dados em redes públicas inseguras e conduzir simulações estruturadas de engenharia social. Do mesmo modo, o Controle 6.3 da ABNT NBR ISO/IEC 27002 exige que as organizações definam regras claras e atualizadas sobre o uso

aceitável de recursos (Controle 5.10) e forneçam programas cíclicos de conscientização, educação e treinamento (ABNT, 2013b; Tanjung; Nurhayati; Wibowo, 2024).

No caso brasileiro, estas exortações técnicas foram revestidas de força de lei com o advento da LGPD (Brasil, 2018b), que obriga as instituições controladoras do setor público a implementarem medidas administrativas e de segurança eficazes para mitigar os riscos de vazamento ou acesso indevido a dados de terceiros. A resposta executiva do Governo Federal consolidou-se por meio do Programa de Privacidade e Segurança da Informação (PPSI) (Brasil, 2023), que adota os dezoito controles prioritários do CIS *Controls* como a métrica oficial de avaliação do nível de maturidade das instituições, balizando a conscientização de servidores como um processo obrigatório sujeito a auditorias.

Entretanto, a pesquisa de Georg *et al.* (2023) com gestores de tecnologia da informação do setor público federal revela que os desafios práticos de governança esbarram no profundo distanciamento entre o plano estratégico e o nível operacional. Embora a legislação nacional apresente elevado nível de maturidade formal por escrito, faltam orientações operacionais claras e práticas para conduzir o treinamento e mitigar a resistência de superiores à liberação de recursos específicos, limitando as políticas à mera busca de conformidade burocrática temporária frente aos órgãos de controle extremo (Benqdara, 2023; Georg *et al.,* 2023). O sucesso do alinhamento desses normativos exige, portanto, o comprometimento expresso por escrito e o apoio orçamentário prioritário das gerências e da alta gestão governamental, conforme preconizado pela ISO 27001 e corroborado empiricamente por Porche e Rahman (2023).

4.4. Discussão de Lacunas (Gap Analysis): Foco Tecnológico Vs. Negligência Educacional

O cruzamento sistemático das evidências científicas e normativas reunidas nesta revisão sistemática revela a existência de uma lacuna estrutural crônica na gestão de segurança da informação no setor público. Constata-se um descompasso acentuado na priorização estratégica: enquanto as organizações destinam vultosos recursos orçamentários à aquisição de equipamentos de rede sofisticados, licenças de sistemas de *firewall* robustos e ferramentas de criptografia forte, verifica-se uma persistente negligência orçamentária, pedagógica e analítica no que tange ao desenvolvimento do elemento humano (Souza, 2022).

De acordo com Souza (2022), Kevin Mitnick já asseverava a importância de aplicar até 40% do orçamento de segurança da informação de uma instituição em ações continuadas de educação e conscientização. Contudo, as repartições públicas federais brasileiras operam em sua grande maioria sob uma postura reativa, realizando investimentos pontuais em segurança de pessoas apenas após a ocorrência de incidentes cibernéticos graves que geram severos impactos operacionais ou reputacionais à instituição, conforme teorizado por Scudere (2007) e verificado por Georg *et al.* (2023).

Esta postura reativa fundamenta-se na dependência exclusiva de contramedidas puramente técnicas por parte dos departamentos de tecnologia da informação. Trata-se os usuários finais sob um prisma mecânico, como vetores passivos de risco a serem controlados eletronicamente, em vez de agentes ativos de segurança que precisam de agência cognitiva. Essa barreira

conceitual anula a eficácia de qualquer investimento tecnológico, uma vez que, sem a devida mudança cultural sustentada nos modelos mentais e hábitos de trabalho diários do corpo funcional leigo, os perímetros eletrônicos mais modernos serão facilmente contornados por meio de táticas psicológicas de engenharia social direcionadas à ponta operacional (Carneiro; Almeida, 2013; Hoepers, 2024; Kanagusku; Gaseta, 2024).

Assim sendo, a principal lacuna da literatura e da prática organizacional cibernética reside na escassez de estudos científicos e de metodologias empíricas robustas que avaliem o impacto de longo prazo de programas de treinamento em Segurança da Informação no ambiente público. É fundamental desenhar estratégias contínuas de conscientização que considerem o binômio do esforço do usuário frente à conformidade das políticas vigentes, integrando os fatores humanos, os processos administrativos e as ferramentas técnicas de forma equilibrada para atingir uma gestão de segurança informacional efetiva e sustentável na esfera do governo federal (Carneiro; Almeida, 2013; Hoepers, 2024; Kanagusku; Gaseta, 2024).

5. CONCLUSÃO/CONSIDERAÇÕES FINAIS

A realização desta revisão sistemática da literatura permitiu consolidar um panorama científico robusto e atualizado sobre o papel crítico do fator humano na segurança da informação governamental. O estudo respondeu às três questões de pesquisa propostas: mapearam-se as vulnerabilidades comportamentais mais comuns, centradas na displicência e obsolescência da gestão cotidiana de senhas de trabalho e no desconhecimento das normas internas, e confirmou-se o phishing por e-mail como a tática de

engenharia social mais recorrente e lesiva nas repartições públicas. Revelou-se, ainda, o severo impacto do viés de ilusão tecnológica de segurança, que reduz a proatividade preventiva dos servidores governamentais.

No aspecto estratégico, o artigo alcançou seu objetivo geral ao demonstrar que metodologias de ensino continuadas, baseadas em simulações interativas, capacitações modulares customizadas às tarefas dos setores e o uso de gamificação de aprendizagem possuem eficácia científica superior para quebrar a resistência comportamental à mudança de hábitos. Esses planos pedagógicos encontram amparo e exigência explícita em um robusto arcabouço normativo governamental e internacional, representado de forma integrada pelas diretrizes da NBR ISO/IEC 27002, do CIS *Controls*, da LGPD e do PPSI.

Como principal contribuição teórica, o trabalho contribui com a literatura sobre o tema ao estruturar um referencial qualitativo sólido e transpor a estigmatização convencional do usuário como “elo mais fraco”, fundamentando estatisticamente a necessidade de torná-lo a barreira ativa principal de defesa da organização. No plano prático e de gestão, a pesquisa entrega aos gestores federais um roteiro estruturado com bases científicas para a tomada de decisões organizacionais e alocação orçamentária eficiente, justificando o direcionamento de recursos para programas pedagógicos dinâmicos em recursos humanos para mitigar as falhas de rede.

Por fim, reconhecem-se as limitações deste artigo com relação ao escopo das bases de dados eletrônicas pesquisadas (CAPES e Google Acadêmico) e à exclusão voluntária de literatura cinzenta informal. Como caminhos para investigações futuras, sugere-se a

concepção de estudos longitudinais de acompanhamento empírico para mensurar de forma analítica e estatística a redução de chamados de suporte técnico, infecções de *malware* e vazamentos de credenciais após a aplicação sistemática de metodologias gamificadas e interativas de conscientização nos diferentes setores da administração pública.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2013a.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013b.

AL-DIABAT, Mofleh. Investigating the Determinants of College Students Information Security Behavior Using a Validated Multiple Regression Models. International Journal of Computer Science and Information Technology, v. 10, n. 6, p. 81-96, 2018.

AMANKWA, E. Relevance of Cybersecurity Education at Pedagogy Levels in Schools. Journal of Information Security, v. 12, p. 240-255, 2021.

ARIF, Mohammad; ZULFIQUAR, S.; BHUTTO, A. What Matters Most Among Human Factors to Comply With Organization's Information Security Policy. Journal of Information Security and Assurance, v. 4, n. 2, p. 110-125, 2011.

ASSEFA, A.; TENSAYE, T. Factors influencing information security compliance. Computers & Security, v. 102, p. 1-15, 2021.

BENQDARA, S. The Need for Effective Information Security Awareness in Private Financial Company: Case from Libya. International Journal of Computer Applications, v. 184, n. 51, p. 12-25, 2023.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética (E-CIBER). Brasília, DF: Presidência da República, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 8 ago. 2026.

BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12573.htm. Acesso em: 8 ago. 2026.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Institui diretrizes relativas à política de segurança da informação na Administração Pública Federal. Brasília, DF: Presidência da República, 2000. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d3505.htm. Acesso em: 8 ago. 2026.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação. Brasília, DF: Presidência da República, 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm. Acesso em: 8 ago. 2026.

BRASIL. Gabinete de Segurança Institucional. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021. Aprova os processos obrigatórios relacionados à gestão de segurança da informação. Diário Oficial da União, Brasília, DF, Seção 1, p. 15, 31 Maio 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172. Acesso em: 8 ago. 2026.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o direito constitucional de acesso às informações públicas. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 8 ago. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 8 ago. 2026.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 852, de 28 de março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação (PPSI). Diário Oficial da União, Brasília, DF, Seção 1, p. 92, 29 mar. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908. Acesso em: 8 ago. 2026.

BRASIL. Tribunal de Contas da União. Boas práticas em segurança da informação. 4. ed. Brasília, DF: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012. 103 p.

CARNEIRO, Luciana Emirena Santos; ALMEIDA, Maurício Barcellos. Gestão da Informação e do Conhecimento no âmbito das práticas de Segurança da Informação: o fator humano nas organizações.

Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação, v. 18, n. 37, p. 175-202, 2013.

CLAVIJO MESA, Maria Valentina; PATINO-RODRIGUEZ, Carmen Elena; GUEVARA CARAZAS, Fernando Jesus. Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains. Information, v. 15, n. 11, p. 710-735, 2024.

FALLA, Diego Augusto Aparecido; PINTO, Giuliano Scombatti. Engenharia social e a importância da cibersegurança na atualidade. Revista Interface Tecnológica, v. 20, n. 2, p. 77-89, 2024.

GEORG, Marcus Aurélio Carvalho; RODRIGUES, Walisson Magno Silva; ALVES, Carlos André de Melo; JÚNIOR, Aldery Silveira; NUNES, Rafael Rabelo. Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, v. E54, p. 602-616, 2023.

HOEPERS, Cristine. A Importância dos Fatores Humanos para a Cibersegurança. Computação Brasil, n. 52, p. 61-66, 2024.

KANAGUSKU, Ana Rita Akayama; GASETA, Edson Roberto. O Mito do Elo Mais Fraco: Fator Humano na Segurança da Informação. Journal of Technology & Information, v. 5, n. 1, p. 1-21, 2024.

KEARNEY, W. D.; KRUGER, H. A. Can perceptual differences account for enigmatic information security behaviour in an organisation? Computers and Security, v. 61, p. 46-58, 2016.

KIM, L. Cybersecurity awareness - Protecting data and patients. Journal of Healthcare Information Management, v. 31, p. 12-25, 2017.

KOZA, J. Information Security Awareness and Training as a Holistic Key Factor. Journal of Cybersecurity and Privacy, v. 2, p. 144-159, 2022.

MARCELINO, Cássio Campos; OLIVEIRA, Jirlaine Fonseca de; CAZORLA, João Carlos; MISAGHI, Mehran. Programa de conscientização como estratégia para combater ataques de engenharia social no ambiente corporativo. Revista Foco, v. 16, n. 11, p. 1-15, 2023.

MOCI, E. Cybersecurity Awareness in Albania. International Journal of Cyber Criminology, v. 15, p. 45-58, 2021.

MOEN, H. et al. Survey-based analysis of cybersecurity awareness of Turkish seafarers. Maritime Policy & Management, v. 51, p. 189-204, 2024.

OMOYIOLA, B.; MCKEEBY, T. Strategies For Implementing Cybersecurity Policies in Organizations. Journal of Information Management, v. 36, p. 215-236, 2023.

ORUC, Aybars; CHOWDHURY, Nabin; GKIULOS, Vasileios. A modular cyber security training programme for the maritime domain. International Journal of Information Security, v. 23, n. 2, p. 1477-1512, 2024.

PORCHE, J.; RAHMAN, S. Security Culture, Top Management, and Training on Security Effectiveness: A Correlational Study Without CISSP Participants. International Journal of Computer Networks and Communications, v. 15, n. 2, p. 81-104, 2023.

SEMLAMBO, A. A.; MFOI, D. M.; SANGULA, Y. Information Systems Security Threats and Vulnerabilities: A Case of the Institute of

Accountancy Arusha (IAA). Journal of Computer and Communications, v. 10, n. 11, p. 29-43, 2022.

SOUZA, Fábio. Usuário, o elo mais fraco da segurança da informação. Revista Scientia Alpha, p. 2-15, 2022.

TANJUNG, Dio Febrilian; NURHAYATI, Oky Dwi; WIBOWO, Adi. Design Information Security in Electronic-Based Government Systems Using NIST CSF 2.0, ISO/IEC 27001:2022 and CIS Control. International Journal of Innovative Science and Research Technology, p. 523-530, 2024.

TENÓRIO ABS JUNIOR, José; BARCAROLI, Velcir; HABITZREITER, Taiane Tais; KLOH, Gustavo Minuzzi; FRANCESCHI, Ilvacir. Engenharia social e a aleatoriedade na escolha do alvo. Revista Conexão, n. 10, p. 550-568, 2022.

TRIGOS, M. L.; NUNO, C. D. O impacto de ações de conscientização na segurança da informação. Revista Científica Multidisciplinar Núcleo do Conhecimento, v. 3, n. 10, p. 46-72, 2021.

WHITE, Garry L.; HEWITT, Barbara; KRUCK, S. E. Incorporating Global Information Security and Assurance in I.S. Education. Journal of Information Systems Education, v. 24, p. 115-128, 2013.

---

[1] Mestrando em Sistemas de Gestão, Universidade Federal Fluminense (UFF). E-mail: acesse o artigo original para visualizar o e-mail

[2] D.Sc. em Universidade Federal Fluminense (UFF). E-mail: acesse o artigo original para visualizar o e-mail

[3] D.Sc. em Universidade Federal Fluminense (UFF). E-mail: acesse o artigo original para visualizar o e-mail

[4] D.Sc. em Universidade Federal Fluminense (UFF). E-mail: acesse o artigo original para visualizar o e-mail