REVISTA MIRANTE
Daqui se vê do alto!
Câmpus Anápolis de Ciências Exatas e Tecnológicas Henrique Santillo
Universidade Estadual de Goiás

Revista Mirante, Anápolis (GO), v. 18, n. 2, p. 22-33, dez. 2025. ISSN 1981-4089

CONSCIENTIZAÇÃO DO SERVIDOR PÚBLICO ACERCA DAS LEIS E NORMAS DE SEGURANÇA DA INFORMAÇÃO NO LOCAL DE TRABALHO

RAISING PUBLIC SERVANTS' AWARENESS OF INFORMATION SECURITY LAWS AND REGULATIONS IN THE WORKPLACE

DIOGO PEDRO DA SILVA CRUZ
UEG - Universidade Estadual de Goiás, Itaberaí (GO)
diogopedro7777@gmail.com

Resumo: Com o avanço das redes de computadores, impulsionado pela internet, a sociedade enfrenta uma crescente necessidade de interconexão e demanda por informações. No contexto brasileiro, apesar da criação da Autoridade Nacional de Proteção de Dados (ANPD) após a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), ainda é insuficiente a atenção dada ao potencial das redes de computadores e às ameaças a que os usuários estão sujeitos. Este artigo investiga o nível de conscientização dos servidores públicos e colaboradores terceirizados da Secretaria de Segurança Pública do Estado de Goiás (SSP-GO) em relação às normas de segurança da informação e à LGPD. Utilizou-se uma abordagem quantitativa, por meio da aplicação de um questionário estruturado com 33 perguntas, respondido por 60 participantes. Os resultados revelam práticas inseguras, indicando baixa adesão às diretrizes básicas de segurança. Casos reais de vazamento de dados na SSP-GO corroboram os achados. A partir disso, propõe-se a implementação de ações educativas e políticas organizacionais que promovam uma cultura de proteção da informação no setor público. Conclui-se que o fortalecimento da segurança da informação exige investimento contínuo em capacitação, conscientização e governança dos dados.
Palavras-chave: Segurança da informação. Tecnologia. Proteção de dados.

Abstract: With the advance of computer networks, driven by the internet, society faces a growing need for interconnection and demand for information. In the Brazilian context, despite the creation of the National Data Protection Authority (ANPD) following the enactment of the General Personal Data Protection Act (LGPD), there is still insufficient attention paid to the potential of computer networks and the threats to which users are subject. This article investigates the level of awareness of civil servants and outsourced employees of the Goiás State Public Security Department (SSP-GO) in relation to information security standards and the LGPD. A quantitative approach was used, through the application of a structured questionnaire with 33 questions, answered by 60 participants. The results reveal insecure practices, indicating low adherence to basic security guidelines. Real cases of data leaks at SSP-GO corroborate the findings. On this basis, it is proposed to implement educational actions and organizational policies that promote a culture of information protection in the public sector. The conclusion is that strengthening information security requires continuous investment in training, awareness and data governance.
Keywords: Information security. Technology. Data protection.

Introdução

O uso crescente da tecnologia nas organizações deixou de ser um luxo e se tornou uma necessidade para a sobrevivência no mercado atual. Esse fenômeno não se deve apenas à competitividade, mas também à necessidade de atender às exigências legais estabelecidas por regulamentações específicas. O administrador público precisa incorporar ferramentas tecnológicas

Revista Mirante, Anápolis (GO), v. 18, n. 2, p. 22-33, dez. 2025. ISSN 1981-4089

para cumprir suas obrigações fiscais, administrativas e trabalhistas. Nesse contexto, especialmente após a pandemia de COVID-19, que acelerou a demanda por produtos tecnológicos, observou-se o aumento de crimes digitais como a obtenção indevida de dados, a propagação maliciosa de vírus e outros tipos de fraudes (BRITO, 2024).

Ao analisar o comportamento de servidores públicos e colaboradores terceirizados em seus locais de trabalho, verificou-se um baixo nível de conhecimento sobre as normas de segurança da informação e as leis vigentes (MOURA; PIRES, 2021). Diante dessa constatação, o objetivo deste trabalho é oferecer pressupostos para orientar e apoiar a implementação de ações que garantam a proteção da informação, a ser adaptado conforme os requisitos de cada organização, seu ramo de atuação e as leis e regulamentações pertinentes. Dessa forma, visa-se contribuir para a criação de uma cultura de proteção de dados no ambiente de trabalho.

Este artigo pretende também elevar o nível de conscientização sobre a preservação de dados pessoais e as práticas de segurança da informação nos órgãos e departamentos da Secretaria de Segurança Pública de Goiás (SSP-GO), com o intuito de aumentar a segurança dos sistemas críticos da SSP-GO e do Governo de Goiás no ambiente cibernético.

Segurança da informação

A segurança da informação é indispensável para resguardar os ativos informacionais das organizações, assegurando a confidencialidade, integridade e disponibilidade dos dados. De acordo com a norma ABNT NBR ISO/IEC 27002 (2022), a segurança da informação envolve a implementação de controles que garantam que as informações estejam protegidas contra acessos não autorizados, alterações indevidas e indisponibilidade, sendo assim, requer o comprometimento da alta direção e a definição de políticas claras alinhadas aos objetivos organizacionais. Enfatiza-se ainda a importância de pressupostos auxiliadores para identificar, avaliar e tratar riscos relacionados à informação, promovendo a continuidade dos negócios e a conformidade legal (ABNT, 2022).

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, estabelece diretrizes para o tratamento de dados pessoais no Brasil, aplicando-se tanto ao setor privado quanto ao público. No contexto do setor público, a LGPD impõe certas obrigações, como a necessidade

Revista Mirante, Anápolis (GO), v. 18, n. 2, p. 22-33, dez. 2025. ISSN 1981-4089

de nomear um encarregado pelo tratamento de dados e garantir a transparência nas operações que tangenciam essa atividade (BRASIL, 2018). Além disso, a norma ABNT NBR ISO/IEC 27002 fornece diretrizes para a implementação de controles de segurança da informação, complementando as exigências legais da LGPD (ABNT, 2022). A integração desses e outros princípios constitui a base para estabelecer uma cultura organizacional voltada à proteção de dados e à segurança da informação, como evidencia a Tabela 1.

Tabela 1 - Normas Técnicas de Segurança da Informação

Norma	Descrição
ABNT NBR ISSO/IEC 17.999:2005	Código de prática para gestão de segurança da informação
ABNT NBR ISO/IEC 27.001:2013	Sistema de gestão de Segurança da Informação — Requisitos
ABNT NBR ISO/IEC 27.002:2013	Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da Segurança da Informação
ABNT NBR ISO/IEC 27.005:2011	Gestão de Riscos de Segurança da Informação
ABNT NBR ISO/IEC 31.000:2018	Gestão de riscos — Princípios e diretrizes
ABNT NBR ISO/IEC 27.003:2020	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações
ABNT NBR ISO/IEC 27014:2021	Tecnologia da Informação — Técnicas de Segurança — Governança de segurança da informação
ABNT NBR ISO/IEC 27701:2019 Versão Corrigida: 2020	Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes
ABNT NBR ISO/IEC 29100:2020	Tecnologia da informação — Técnicas de segurança — Estrutura de Privacidade
ABNT NBR 16167:2020	Segurança da Informação — Diretrizes para classificação, rotulação e tratamento da informação
ISO/IEC 29134:2017	Tecnologia da informação — Técnicas de segurança — Diretrizes para avaliação do impacto na privacidade
ISO/IEC 29151:2017	Tecnologia da informação — Técnicas de segurança — Código de prática para proteção de informações de identificação pessoal

Revista Mirante, Anápolis (GO), v. 18, n. 2, p. 22-33, dez. 2025. ISSN 1981-4089

ISO/IEC 27035-1:2016	Tecnologia da informação — Técnicas de segurança — Gerenciamento de incidentes de segurança da informação — Parte 1: Princípios de gerenciamento de incidentes
ISO/IEC 27035-2:2016	Tecnologia da informação — Técnicas de segurança — Gerenciamento de incidentes de segurança da informação — Parte 2: Diretrizes para planejar e preparar a resposta a incidentes
LGPD lei 13.709 08/2018	LGPD (Lei Geral de Proteção de Dados Pessoais), foi editada em agosto de 2018 e entrou em vigor em agosto de 2020

Fonte: Elaborado pelo autor (2025).

Nesse viés, estudos de caso demonstram a importância da implementação de políticas de segurança da informação no setor público. Um exemplo é o Tribunal de Contas do Estado do Amazonas (TCE-AM), que adotou um Sistema de Gestão de Segurança da Informação (SGSI) baseado na norma ABNT NBR ISO/IEC 27001. A implantação resultou em melhorias na proteção dos ativos informacionais, aumento da resiliência dos serviços e fortalecimento dos controles internos (SILVA, 2016).

O setor público brasileiro ainda enfrenta muitas dificuldades relacionados à segurança cibernética, especialmente diante do aumento de ataques que visam órgãos governamentais. Relatórios indicam que o Brasil está entre os países com maior número de crimes cibernéticos, afetando milhões de pessoas e causando prejuízos bilionários (CNseg, 2024). A pandemia de COVID-19 intensificou a dependência de sistemas digitais, expondo ainda mais as vulnerabilidades existentes nas infraestruturas governamentais (BRITO, 2024). A falta de investimentos em segurança da informação e a escassez de profissionais qualificados agravam a situação, tornando urgente a adoção de políticas de proteção informacional nesse cenário.

Metodologia

A presente pesquisa utilizou uma abordagem metodológica quantitativa de natureza descritiva, com o intuito de avaliar o nível de conhecimento e as práticas relacionadas à segurança da informação entre os servidores públicos e colaboradores terceirizados da Secretaria de Segurança Pública do Estado de Goiás (SSP-GO) e oferecer pressupostos para orientar e apoiar a

Revista Mirante, Anápolis (GO), v. 18, n. 2, p. 22-33, dez. 2025. ISSN 1981-4089

implementação de ações que garantam a proteção da informação. Para alcançar esse objetivo, foi adotado um procedimento estruturado baseado na coleta e análise de dados primários, obtidos diretamente dos participantes por meio de um formulário de pesquisa.

Inicialmente, foram elaborados cenários para o desenvolvimento do trabalho, visando estabelecer um contexto adequado para a investigação. O principal instrumento de coleta de dados consistiu em um questionário composto por 33 perguntas, cuidadosamente formuladas para abordar diversos aspectos relacionados à segurança da informação no ambiente organizacional. Este questionário foi disponibilizado aos participantes por meio da plataforma Google Forms, uma ferramenta digital que permite a criação, distribuição e gerenciamento de formulários online, facilitando assim o processo de coleta de dados.

A amostra da pesquisa foi composta por servidores públicos e colaboradores terceirizados de diversos departamentos da Secretaria de Segurança Pública de Goiás. O questionário foi disponibilizado para um total de 250 indivíduos vinculados à SSP-GO, dos quais 60 participaram voluntariamente, representando uma taxa de resposta de 24%. É importante ressaltar que, para incentivar a participação e agilizar o processo de coleta de dados, optou-se por não incluir perguntas de caráter pessoal no questionário, como informações sobre sexo, idade ou departamento específico de trabalho dos participantes.

Após a aplicação do questionário e a coleta dos dados, foi realizado um levantamento detalhado para avaliar o nível de conhecimento dos servidores públicos e colaboradores terceirizados sobre segurança da informação. Este levantamento envolveu a análise das respostas obtidas, com foco especial em aspectos como o uso de senhas, o compartilhamento de informações, o acesso a redes sociais e a percepção de segurança no ambiente de trabalho.

Os dados coletados foram organizados e analisados de forma sistemática, permitindo a identificação de padrões, tendências e áreas de vulnerabilidade no que diz respeito à segurança da informação na organização, por meio de gráficos e tabelas para facilitar a visualização e interpretação dos resultados, proporcionando uma compreensão mais clara e objetiva da situação atual.

Adicionalmente, foram coletados e analisados casos reais de vazamento de dados ocorridos na SSP-GO, reportados pela imprensa goiana, com o objetivo de contextualizar os resultados da pesquisa e demonstrar as consequências práticas das falhas de segurança da informação. Esses

Revista Mirante, Anápolis (GO), v. 18, n. 2, p. 22-33, dez. 2025. ISSN 1981-4089

casos foram documentados e incorporados à análise, fornecendo exemplos concretos dos riscos associados ao manejo inadequado de informações sensíveis. Ao final do processo de análise, os dados coletados foram apresentados aos gestores da SSP-GO em forma de gráficos e planilhas, com o objetivo de fornecer uma visão clara da situação atual em relação à segurança da informação na organização. Esses resultados serviram como base para o desenvolvimento de uma política de conscientização sobre segurança da informação para os funcionários, visando promover uma cultura de cuidado com as informações manipuladas na organização.

Sendo assim, a metodologia adotada neste estudo foi fundamentada nos princípios da pesquisa aplicada, buscando não apenas identificar problemas e vulnerabilidades, mas também propor soluções práticas e viáveis para melhorar a segurança da informação. O foco na aplicabilidade dos resultados reflete o compromisso com a transformação da realidade organizacional, por meio da conscientização e capacitação dos servidores públicos e colaboradores terceirizados.

Resultados e discussão

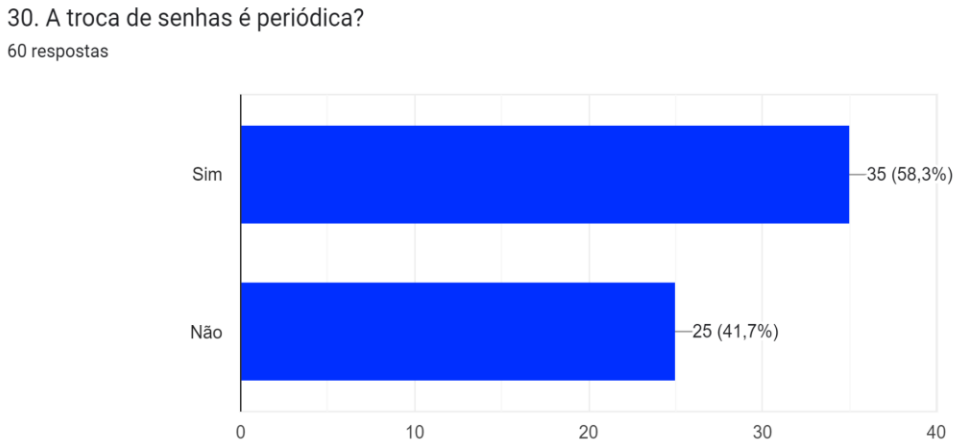
Um dos primeiros aspectos observados foi que todos os participantes da pesquisa possuem um usuário de rede na Secretaria de Segurança Pública, o que implica acesso à rede mundial de computadores. Esse dado é importante porque mostra que todos os usuários têm a capacidade de gerar e acessar uma ampla variedade de informações, aumentando assim a superfície de exposição a potenciais riscos de segurança. Além disso, constatou-se que todos os participantes também têm acesso a redes sociais, como Facebook, WhatsApp, Telegram, Instagram, YouTube e serviços de e-mail, que são importantes meios de divulgação de informações pessoais, profissionais e de localização.

Dada a Figura 1, no que diz respeito às práticas de segurança relacionadas ao uso de senhas, os resultados mostraram que apenas 58,3% dos participantes realizam a troca periódica de suas senhas. Esse percentual é preocupante, considerando que a alteração regular de senhas é uma medida básica de segurança, recomendada por especialistas e normas técnicas para reduzir o risco de acesso não autorizado a sistemas e informações. A resistência à adoção dessa prática pode estar relacionada à falta de conscientização sobre sua importância ou à percepção de que representa um

Revista Mirante, Anápolis (GO), v. 18, n. 2, p. 22-33, dez. 2025. ISSN 1981-4089

inconveniente desnecessário.

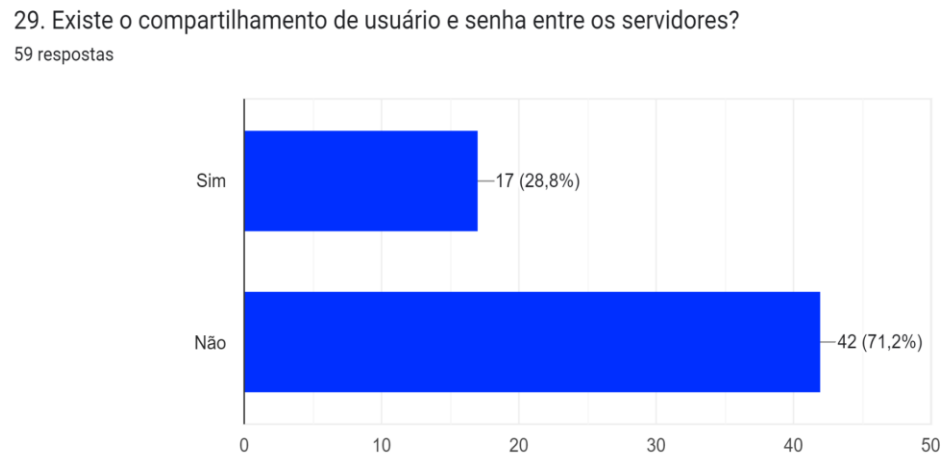
Figura 1 - Troca de senhas



Fonte: Elaborado pelo autor (2025).

Outro dado alarmante revelado pela pesquisa foi que 28,8% dos participantes compartilham suas senhas com outros usuários, como releva a Figura 2. Esta prática aumenta significativamente o risco de vazamento de dados, uma vez que compromete o princípio da responsabilidade individual pelo acesso e uso das informações. O compartilhamento de senhas dificulta a rastreabilidade das ações realizadas nos sistemas, impossibilitando a identificação precisa dos responsáveis por eventuais incidentes de segurança.

Figura 2 - Compartilhamento de senhas

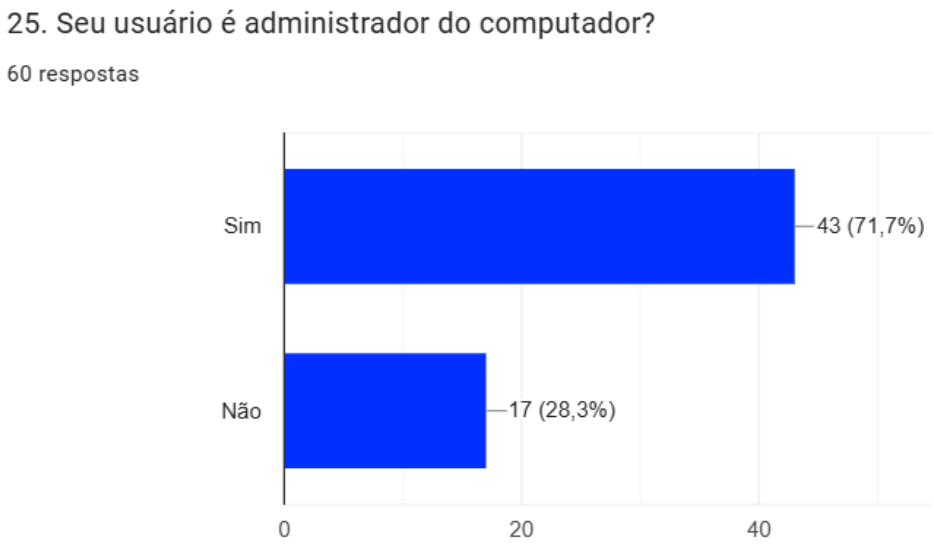


Revista Mirante, Anápolis (GO), v. 18, n. 2, p. 22-33, dez. 2025. ISSN 1981-4089

Fonte: Elaborado pelo autor (2023)

A Figura 3 aponta que 71,1% dos usuários possuem privilégios de administrador em seus computadores locais. Este elevado percentual representa um risco considerável para a segurança da rede, pois usuários com privilégios administrativos têm a capacidade de instalar softwares, modificar configurações do sistema e potencialmente comprometer a integridade e segurança do ambiente computacional como um todo. A concessão indiscriminada de privilégios administrativos contraria as boas práticas de segurança, que recomendam a aplicação do princípio do menor privilégio, segundo o qual os usuários devem ter acesso apenas aos recursos necessários para o desempenho de suas funções.

Figura 3 – Usuário administrador



Fonte: Elaborado pelo autor (2025)

Um aspecto particularmente preocupante evidenciado pelos resultados é o falso senso de segurança demonstrado pelos usuários. Embora a maioria dos servidores públicos se sinta segura ao navegar na internet em seu local de trabalho, muitos negligenciam aspectos importantes da segurança, como a troca periódica de senhas e o não compartilhamento de credenciais. Essa discrepância entre a percepção de segurança e as práticas efetivamente adotadas sugere uma lacuna de conhecimento e conscientização que precisa ser abordada por meio de programas educativos e políticas organizacionais mais rigorosas.

Os resultados da pesquisa foram corroborados por casos concretos de vazamento de dados ocorridos na SSP-GO, reportados pela imprensa local, como mostra a Figura 4. Um dos principais

Revista Mirante, Anápolis (GO), v. 18, n. 2, p. 22-33, dez. 2025. ISSN 1981-4089

exemplos envolveu um suspeito que utilizou seu cargo de influência para obter informações de um servidor público da SSP-GO sobre um registro de atendimento prestado a uma vítima dias antes de uma tentativa de homicídio. O suspeito conseguiu acessar os dados utilizando o login de um delegado, cujas credenciais havia adquirido nas redes sociais. Com essas informações, ele entrou em contato com as vítimas e solicitou dinheiro em troca de informações sobre veículos furtados ou roubados. Este incidente ilustra claramente como a falta de práticas adequadas de segurança, como a troca periódica de senhas, pode resultar em consequências graves, incluindo a exploração criminosa de informações sensíveis.

Figura 4 - Casos de vazamento de dados na SSP-GO

Fonte: Pacheco (2021), Oliveira (2022) e Resende (2017)

Revista Mirante, Anápolis (GO), v. 18, n. 2, p. 22-33, dez. 2025. ISSN 1981-4089

As reportagens mostram que o problema de manuseio inadequado dos dados não é recente na organização, sendo uma questão persistente ao longo dos anos. Esta constatação reforça a necessidade urgente de medidas corretivas e preventivas para melhorar a segurança da informação na SSP-GO.

Considerações finais

Este artigo teve como objetivo principal oferecer pressupostos para orientar e apoiar a implementação de ações que garantam a proteção da informação, a partir da análise do nível de conscientização dos servidores públicos e colaboradores terceirizados da SSP-GO, destacando as ameaças e vulnerabilidades mais significativas, bem como as estratégias que podem ser implementadas para proteger os sistemas de informação.

As informações levantadas pela pesquisa, juntamente com os casos documentados de vazamento de dados, foram fundamentais para a elaboração de um projeto de conscientização sobre o uso adequado de dados pelos servidores da Secretaria de Segurança Pública do Estado de Goiás. O projeto contém procedimentos básicos para a segurança da informação e visa implementar uma cultura de cuidado com os dados manipulados pelos servidores públicos, de forma similar às campanhas de conscientização sobre o uso racional da água, da energia e o descarte adequado de lixo.

Os resultados da pesquisa evidenciaram a necessidade de uma abordagem mais rigorosa e sistemática para a segurança da informação na organização em questão, incluindo a implementação de políticas mais eficazes, a realização de programas de conscientização e treinamento e a adoção de medidas técnicas para proteger os sistemas e dados da organização contra ameaças internas e externas. A transformação da cultura organizacional em relação à segurança da informação é um grande desafio, mas essencial para garantir a proteção adequada dos dados sensíveis manipulados pela SSP-GO.

A principal contribuição teórica do trabalho está na articulação entre as diretrizes legais, como a LGPD e os padrões técnicos estabelecidos pelas normas ISO/IEC, possibilitando uma compreensão integrada dos marcos normativos que devem nortear a segurança da informação no setor público. No campo empírico, os dados coletados por meio de questionário revelaram

Revista Mirante, Anápolis (GO), v. 18, n. 2, p. 22-33, dez. 2025. ISSN 1981-4089

fragilidades importantes — como o compartilhamento de senhas, o uso inadequado de privilégios administrativos e a desconexão entre a percepção de segurança e as práticas reais —, o que oferece um panorama das deficiências existentes na SSP-GO. A contribuição metodológica reside na construção e aplicação de um instrumento de pesquisa que pode ser replicado em outras instituições públicas como ferramenta diagnóstica para subsidiar planos de ação voltados à segurança da informação.

Este estudo, entretanto, apresenta algumas limitações. A amostra, composta por 60 respondentes, restringe a generalização dos resultados, além da ausência de dados sociodemográficos que poderiam contribuir para análises mais aprofundadas, como possíveis relações entre perfil dos participantes e comportamentos de risco.

Para pesquisas futuras, recomenda-se ampliar o escopo do estudo para outras secretarias e órgãos públicos, além de incorporar métodos qualitativos, como entrevistas e grupos focais, que possam captar nuances comportamentais e culturais não detectadas por questionários. Também seria pertinente investigar o impacto de programas de capacitação e campanhas de conscientização em segurança da informação, avaliando sua efetividade por meio de estudos longitudinais.

Por fim, conclui-se que a construção de uma cultura organizacional voltada à segurança da informação exige ações envolvendo capacitação, políticas claras e tecnologia, sendo um desafio prioritário diante da crescente exposição das instituições públicas a riscos cibernéticos. A conscientização dos servidores, somada à implementação de práticas e normas adequadas, é indispensável para garantir a integridade, a confidencialidade e a disponibilidade dos dados.

Referências

ABNT. NBR ISO/IEC 17799:2005 – Tecnologia da informação – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

ABNT. NBR ISO/IEC 27002:2022 – Tecnologia da informação – Segurança da informação, cibersegurança e proteção à privacidade – Controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 1, 15 ago. 2018.

BRITO, Flávia. Segurança cibernética no Brasil: desafios e necessidades urgentes de ação. ABES, 31 dez. 2024. Disponível em: https://abes.com.br/seguranca-cibernetica-no-brasil-desafios-e-necessidades-urgentes-de-acao. Acesso em: 01 de maio de 2025.

CAMPOS, P. Segurança da informação: normas e certificações. 2007. Disponível em: https://www.infowester.com/seginfo.php. Acesso em: 10 de maio de 2024.

CNSEG. Desafios e soluções no combate aos crimes cibernéticos: a visão do mercado de seguros em debate. 2024. Disponível em: https://www.cnseg.org.br/noticias/desafios-e-solucoes-no-combate-aos-crimes-ciberneticos-a-visao-do-mercado-de-seguros-em-debate. Acesso em: 01 de maio de 2025.

GALVÃO, Daniel. A importância da segurança da informação para as organizações. 2015. Disponível em: https://www.infowester.com/seginfoimportancia.php. Acesso em: 10 de maio de 2024.

MOURA, Vívian da Silva; PIRES, Sandro Roberto. Os desafios da segurança cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. Revista Eletrônica de Administração e Turismo – ReAT, Ilhéus, v. 15, n. 2, p. 63-84, maio/ago. 2021. Disponível em: https://periodicos.uesc.br/index.php/reat/article/view/3899. Acesso em: 05 de maio de 2025.

OLIVEIRA, Danielle. Vídeo mostra quando homem invade farmácia e atira contra idoso, em Goiânia. G1, 27 jun. 2022. Disponível em: https://g1.globo.com/go/goias/noticia/2022/06/27/video-mostra-quando-homem-invade-farmacia-e-atira-contra-idoso-em-goiania.ghtml. Acesso em: 2 jul. 2025.

PACHECO, Lorena. PCGO é acionada para abrir procedimento administrativo após vazamento de ofício com demanda de efetivo. Correio Braziliense – Blog Papo de Concurseiro, 8 fev. 2021. Disponível em: https://blogs.correiobraziliense.com.br/papodeconcurseiro/pcgo-e-acionada-para-abrir-procedimento-administrativo-apos-vazamento-de-oficio-com-demanda-de-efetivo/. Acesso em: 2 jul. 2025.

RESENDE, Paula. Homem é preso suspeito de extorquir vítimas de roubos após acessar banco de dados do governo de Goiás. G1, 14 dez. 2017. Disponível em: https://g1.globo.com/go/goias/noticia/homem-e-preso-suspeito-de-extorquir-vitimas-de-roubos-apos-acessar-banco-de-dados-do-governo-de-goias.ghtml. Acesso em: 2 jul. 2025.

SILVA, Flávia Estélia. Implantação da segurança na gestão da informação na administração pública: um estudo de caso no Tribunal de Contas do Estado do Amazonas. Revista do Serviço Público, Brasília, v. 67, n. 1, p. 109-130, jan./mar. 2016. Disponível em: https://repositorio.enap.gov.br/handle/1/2922. Acesso em: 10 de maio de 2025.