ARTIGO DOI 10.52781/cmm.a183

Compartilhamento seguro de dados sensíveis na defesa cibernética: uma proposta de programa de gestão sob a perspectiva da ciência aberta*

Secure sharing of sensitive data in cyber defense: a proposal for a management program from the open science perspective

Resumo: A ciência aberta em defesa cibernética apresenta um desafio específico devido à natureza restrita dos dados, a qual, por sua vez, dificulta que sejam compartilhados em prol do avanço tecnológico. A partir de uma pesquisa qualitativa com especialistas de áreas estratégicas, foi proposta a criação de um Programa de Gestão de Dados Sensíveis (PGDS) com o objetivo de viabilizar o compartilhamento seguro desses dados. Os resultados indicam que a maioria dos respondentes considera positiva a existência do PGDS para o tratamento, controle e disponibilização de dados sensíveis anonimizados. Dessa forma, o estudo conclui que a implementação do PGDS tem o potencial de fomentar a pesquisa e o desenvolvimento tecnológico no campo da defesa cibernética, preservando a proteção dos dados sensíveis.

Palavras-chave: Ciência aberta; Defesa cibernética; Proteção de dados sensíveis; Privacidade.

Abstract: Open science in cyber defense presents a specific challenge due to the restricted nature of data, which makes it difficult to share this data for technological advancement. Based on a qualitative survey with experts from strategic areas, the creation of a Sensitive Data Management Program (SDMP) was proposed with the aim of enabling the secure sharing of this data. The results indicate that most respondents consider the existence of the SDMP for the treatment, control, and provision of anonymized sensitive data to be positive. Thus, the study concludes that the implementation of the SDMP has the potential to promote research and technological development in the field of cyber defense, while preserving the protection of sensitive data.

Keywords: Open science; Cyber defense; Sensitive data protection; Privacy.

Isabel Cristina Sampaio Freitas Marinho
Instituto Militar de Engenharia (IME)
Rio de Janeiro, RJ, Brasil
isabel.marinho@ime.eb.br

Anderson Fernandes Pereira dos Santos
Instituto Militar de Engenharia (IME)
Rio de Janeiro, RJ, Brasil
Venturus Centro de Inovação Tecnológica
Campinas, SP, Brasil
anderson@ime.eb.br

Maria Cláudia Reis Cavalcanti
Instituto Militar de Engenharia (IME)
Rio de Janeiro, RJ, Brasil
yoko@ime.eb.br

Recebido: 27 nov. 2024
Aprovado: 19 set. 2025

* Este artigo, escrito em coautoria com dois dos orientadores, sintetiza parte dos resultados, obtidos na pesquisa desenvolvida no âmbito da dissertação de mestrado da primeira autora (Marinho, 2025), defendida no Programa de Pós-Graduação em Engenharia de Defesa do Instituto Militar de Engenharia.

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 INTRODUÇÃO

A defesa cibernética, inserida no cenário estratégico nacional de forma integrada e coordenada pelo Ministério da Defesa, envolve um conjunto de ações voltadas à proteção dos ativos de informação de interesse da defesa nacional. Essas ações também têm por finalidade a coleta de dados voltada à geração de conhecimento de inteligência e buscam assegurar superioridade no espaço cibernético (Brasil, 2023).

Essas medidas estão relacionadas com a segurança das operações, que incluem, por exemplo, o tratamento de incidentes e a gestão de riscos. Com isso, a segurança cibernética visa garantir a capacidade dos sistemas de informação em resistir a eventos que possam comprometer os requisitos essenciais da segurança da informação, sejam a disponibilidade, a integridade, a confidencialidade ou a autenticidade da informação transmitida, processada ou armazenada (Brasil, 2021).

Nesse sentido, a Estratégia Nacional de Cibersegurança destaca a importância da criação e do desenvolvimento de centros de análise e compartilhamento de informações, com estímulo à implementação de mecanismo nacional de notificação de incidentes cibernéticos (Brasil, 2025). Essa troca de conhecimentos visa identificar, gerenciar e mitigar riscos de forma coordenada, promovendo uma abordagem mais eficiente.

Uma forma de avaliação mais precisa desses riscos é por meio de dados concretos, oriundos de pesquisas científicas no contexto da segurança cibernética. Aliado a isso, o conceito de ciência aberta envolve a democratização do acesso a dados de pesquisa, permitindo que a comunidade científica e a sociedade em geral se beneficiem das informações coletadas.

No entanto, quando se trata de dados sensíveis, como os de tráfego de rede e incidentes de segurança, o desafio é maior, pois a proteção dessas informações é necessária para evitar o risco de exposição dos titulares de dados e o risco de não conformidade com as leis de proteção de dados. Nesse contexto, van Ravenzwaaij *et al*. (2024) destacam os desafios para alcançar o equilíbrio entre a conformidade legal e os interesses científicos, protegendo a privacidade e permitindo que o conjunto de dados seja tão aberto quanto possível.

Ainda segundo van Ravenzwaaij *et al*. (2024), o movimento da comunidade científica em prol da ciência aberta convida os pesquisadores a disponibilizarem seus dados abertamente para permitir o reúso. Com esse objetivo, este estudo procurou identificar as etapas principais de um processo que fosse capaz de viabilizar o compartilhamento seguro de dados sensíveis, de forma a contribuir para o avanço da pesquisa em defesa cibernética e para a criação de uma cultura de compartilhamento seguro de dados. Até onde foi possível investigar, não há na literatura levantamento com foco semelhante.

Após a identificação dessas etapas, buscou-se a opinião de especialistas sobre a possibilidade de criar um Programa de Gestão de Dados Sensíveis (PGDS) como uma proposta para facilitar o compartilhamento seguro de dados sensíveis, em conformidade com as normas e legislações de segurança e proteção de dados vigentes.

Nesse cenário, este trabalho tem como objetivo principal descrever um PGDS para viabilizar o compartilhamento seguro de dados no contexto da defesa cibernética, alinhando os princípios da ciência aberta com as exigências legais de proteção de dados. Para tanto, a pergunta

norteadora é: Como viabilizar o compartilhamento seguro de dados sensíveis nesse contexto sem comprometer a privacidade e a conformidade legal?

Para isso, os objetivos específicos incluem revisar os principais conceitos, levantar e analisar trabalhos relacionados ao compartilhamento de dados sensíveis, identificando lacunas existentes na literatura, identificar, com especialistas, as etapas necessárias para estruturar um PGDS eficaz e desenvolver uma proposta de programa que permita o compartilhamento seguro de dados em conformidade com normas e legislações vigentes.

Para isso, inicialmente apresenta-se a revisão teórica dos conceitos de ciência aberta, segurança da informação e proteção de dados. Em seguida, são examinados os trabalhos relacionados e depois detalhados o desenvolvimento do estudo e a metodologia adotada. Na sequência, discutem-se os resultados, e, por fim, apresentam-se as considerações finais e sugestões de trabalhos futuros.

2 REVISÃO TEÓRICA

2.1 Ciência aberta

A ciência aberta promove mudanças na produção, na organização, no compartilhamento e na reutilização do conhecimento científico (Costa; Shintaku, 2024). Com isso, além de fomentar as publicações científicas, como os artigos acadêmicos, também prevê o acesso aos dados gerados por pesquisadores ou cientistas durante o processo de investigação científica. Isso inclui o acesso às metodologias, aos softwares e aos resultados gerados. Dessa forma, a ciência aberta visa garantir a reprodutibilidade da ciência e a economia de recursos de forma colaborativa (Sales; Costa; Shintaku, 2020).

Henning *et al*. (2019) apresentam as vantagens dos dados abertos no escopo dos dados científicos por meio de um comparativo dessas vantagens tanto para a ciência como para a sociedade, servindo de motivação para este estudo. Entre as vantagens para a ciência, destaca-se a reutilização dos dados para novas pesquisas, o que reduz custos, pois elimina a necessidade de fazer a coleta desses dados uma segunda vez, haja vista que, uma vez coletados e analisados, podem ser usados em novas pesquisas sob diferentes perspectivas.

Henning *et al*. (2019) indicam que todos os benefícios que proporcionam vantagens para a sociedade estão relacionados ao reúso dos dados, dos quais destacam-se duas principais vantagens relacionadas: uma voltada ao reúso em prol da inovação e outra relacionada ao aumento da competitividade. Ou seja, abrir os dados pode ajudar na geração de novos produtos, serviços e, consequentemente, empregos, ao passo que o reúso permite o apoio à tomada de decisões, garantindo que formuladores de políticas se baseiem em evidências proporcionadas pela análise desses dados.

Contudo, observa-se a necessidade de iniciativas para a melhoria de pesquisas relacionadas à disponibilidade de conjuntos de dados sensíveis, especialmente no que tange à defesa cibernética. Para isso, considerar uma possível padronização das técnicas de desidentificação, como a anonimização e a pseudoanonimização, pode permitir que bases de dados sejam publicadas sem o risco de tornar vulnerável a organização que originou os dados (Machado; Duarte Neto; Bento Filho, 2019).

2.2 Segurança da informação

A segurança da informação tem por finalidade garantir a confidencialidade, a integridade e a disponibilidade das informações (Hintzbergen *et al.*, 2018). Para protegê-las é essencial aplicar controles de segurança, considerando as potenciais ameaças para o negócio. A norma ABNT NBR ISO/IEC 27001:2013 (ABNT, 2013) define esses controles com objetivo de garantir a continuidade dos negócios, atuando nas vulnerabilidades para minimizar os impactos de possíveis incidentes. Isso é possível por meio da escolha e implementação de controles adequados, que incluem políticas, processos, procedimentos, estruturas organizacionais, software e hardware para proteger os ativos de informação.

No âmbito do espaço cibernético, a Estratégia Nacional de Cibersegurança (Brasil, 2025) define a defesa cibernética como um conjunto de ações voltadas à segurança cibernética dos ativos estratégicos do país, promovendo a cooperação entre órgãos e entidades públicas e privadas com o objetivo de viabilizar o intercâmbio de informações para a prevenção e a resposta a incidentes cibernéticos. Por sua vez, a segurança cibernética é definida como um conjunto de medidas com capacidade de proteger o espaço cibernético, como ferramentas, melhores práticas, gestão de riscos entre outros.

Paralelamente, com o crescimento exponencial da internet, dos sistemas computacionais, da própria evolução da tecnologia de comunicação para 5G e futuras tecnologias, é possível fazer uma reflexão sobre o aumento de vulnerabilidades e ameaças cibernéticas como consequência do aumento do fluxo de dados de redes pela troca de informações (Oliveira, 2021).

Entre as soluções de segurança existentes, destacam-se as tecnologias de Sistemas de Detecção de Intrusão, do inglês Intrusion Detection Systems (IDS), que permitem mitigar tais vulnerabilidades por meio do monitoramento e da análise dos fluxos de dados de redes e, assim, possibilitam a detecção de ataques em potencial (Ceolin Junior *et al.,* 2023). Aliadas a isso, técnicas de aprendizado de máquina permitem que essas detecções sejam ainda mais robustas (Cortez; Cação, 2017), ao passo que se sugere o refinamento dos algoritmos de detecção de invasão por meio de dados reais (Oliveira; Cavalcanti; Salles, 2017). No entanto, surge a preocupação com a preservação da privacidade dos indivíduos e das organizações envolvidas.

2.3 Proteção de dados

Além dos controles técnicos e administrativos previstos na norma ABNT NBR ISO/IEC 27001:2013 (ABNT, 2013), que envolve a segurança das informações, e no guia orientativo sobre segurança da informação da Agência Nacional de Proteção de Dados (ANPD, 2021), Brito e Machado (2017) apresentam estratégias para o problema da preservação da privacidade, que incluem técnicas de anonimização de dados sensíveis como uma solução, possibilitando, por conseguinte, a disponibilização desses dados.

Aliada a isso, a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados [LGPD]) (Brasil, 2018), estabelece um marco legal para a proteção de dados pessoais no Brasil, tendo como foco a proteção da privacidade. Contudo, a LGPD também incentiva o tratamento desses dados para pesquisa, se garantida a anonimização ou pseudoanonimização. Nesse contexto,

a anonimização torna-se a técnica que permite o uso de dados em estudos científicos, minimizando os riscos de exposição de indivíduos ou organizações.

Assim, a combinação dos controles de segurança e a adoção de técnicas de desidentificação contribuem para o equilíbrio entre o avanço da ciência aberta e a proteção de dados.

3 TRABALHOS RELACIONADOS

Os trabalhos relacionados estão categorizados em dois aspectos: (i) trabalhos que apoiam o compartilhamento de dados sensíveis; e (ii) trabalhos que realizam o levantamento de opiniões utilizando a escala Likert (1932), comumente aplicada a esse tipo de levantamento (Feijó; Vicente; Petri, 2020).

3.1 Compartilhamento de dados sensíveis

Sobre o compartilhamento de dados sensíveis, destacam-se algumas iniciativas governamentais, como o Serviço de Acesso a Dados Protegidos (Sedap) (Serviço [...], 2022), do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), e o programa Information Marketplace for Policy and Analysis of Cyber-risk and Trust (IMPACT) (What we do, 2019), do Departamento de Segurança Interna dos Estados Unidos (U.S. Department of Homeland Security [DHS]).

O Sedap disponibiliza aos pesquisadores o acesso aos dados protegidos, que são produzidos pelo Inep, e conta com escopo voltado para o desenvolvimento de pesquisas educacionais. Para tanto, define os requisitos mínimos de acesso, desde as etapas de solicitação até execução do serviço, que ocorre em sala segura nas instalações do serviço.

O programa IMPACT oferece aos pesquisadores o acesso a dados por meio de um repositório, com escopo voltado para a avaliação de riscos cibernéticos, prevenção, detecção e mitigação de ameaças cibernéticas. Contudo, apenas pesquisadores sediados nos Estados Unidos e demais locais aprovados pelo DHS – Austrália, Canadá, Israel, Japão, Holanda, Singapura e Reino Unido – podem solicitar uma conta para acesso ao IMPACT.

Contudo, nesses dois casos, constatou-se a ausência de um mapeamento dos processos e da sua arquitetura. Isso poderia servir como referência de boas práticas e possibilitar a transparência e a disseminação da metodologia adotada, o que permitiria que outras instituições adotassem o mesmo método, como evidenciado pela iniciativa europeia International Data Spaces Association (IDSA)[1].

A IDSA propõe uma abordagem descentralizada para o compartilhamento de dados por meio de espaços de dados, assegurando que cada empresa participante possa trocar informações de forma segura e confiável (Maranatha, 2023), e disponibiliza o modelo de arquitetura para o desenvolvimento de Data Spaces compatíveis. Ainda assim, não são representados os papéis previstos na legislação, uma vez que a responsabilidade pela conformidade com o Regulamento Geral de Proteção de Dados europeu (General Data Protection Regulation [GDPR]) (União Europeia, 2016) é da própria organização (Steinbuss *et al.*, 2019).

1 Disponível em: https://internationaldataspaces.org. Acesso em: 23 set. 2025.

3.2 Técnica de medição para o levantamento de opiniões

Para estruturação do questionário para o levantamento de opiniões, foi feito um estudo para identificar as técnicas de medição mais usadas para esse contexto. Foi constatada a predominância do uso da escala Likert como meio de mensuração, de acordo com Feijó, Vicente e Petri (2020). No artigo, os autores relatam que "as escalas de atitudes como a Likert são amplamente utilizadas, principalmente nas questões de preferências, gostos e percepções. Conhecida como uma escala caracterizada como simples e de fácil entendimento [...]" (Feijó; Vicente; Petri, 2020, p. 28).

A escala Likert permite definir uma classificação que reflete diferentes graus de concordância para uma questão. Geralmente representada em cinco pontos, tem a capacidade de gerar dados qualitativos. Para fins deste estudo, adotou-se as opções "discordo totalmente", "discordo parcialmente", "indiferente", "concordo parcialmente" e "concordo totalmente". Dito isso, essa abordagem apresentou compatibilidade com a necessidade de avaliação esperada.

Diversos trabalhos utilizam a escala Likert para avaliar graus de concordância ou discordância em diferentes contextos de pesquisa (Campos, 2020; Maranatha, 2023; Moreira *et al.*, 2024; Souza *et al.*, 2020), demonstrando sua eficácia na captura de opiniões.

Campos (2020) aborda o cumprimento de boas práticas em segurança da informação, como a conformidade com padrões de segurança, a exemplo da ABNT NBR ISO/IEC 27002:2013, e seu impacto na produtividade de um órgão público. O autor analisa o grau de conformidade da Base Administrativa do Comando Militar da Amazônia, do Exército Brasileiro, utilizando a escala Likert. O estudo revela um nível satisfatório de conformidade e ainda identifica as áreas que requerem aprimoramento, reforçando a importância da gestão de segurança da informação para mitigar impactos adversos.

Souza *et al.* (2020) investigam a aplicação de metodologias ativas e gamificação no ensino da contabilidade. Os resultados obtidos por meio da escala Likert mostram que tais abordagens aumentam o engajamento e a motivação dos alunos, evidenciando a eficácia de práticas pedagógicas interativas para promover um aprendizado significativo.

Maranatha (2023) utiliza a escala Likert para validar o modelo Clearing House, proposto para o compartilhamento de dados auditáveis em International Data Spaces no setor logístico, alinhado aos objetivos e motivações do estudo. Como resultado, a maioria dos especialistas consideram o Clearing House uma solução promissora, tanto do ponto de vista econômico quanto do técnico.

Moreira *et al.* (2024) analisam o uso de jogos educativos digitais para treinar estudantes na identificação de fake news por meio da ferramenta JEDi. Os resultados em estudos de caso com alunos de ensino médio, de graduação e de pós-graduação demonstram a eficácia do JEDi como instrumento para detecção de fake news em notícias na língua portuguesa. Para isso, foi utilizada a escala Likert a fim de avaliar o nível de concordância dos estudantes.

O Quadro 1 apresenta os domínios e a escala Likert utilizada nesses trabalhos, destacando sua aplicação em diversos domínios para avaliação do grau de concordância.

Quadro 1 – Uso da escala Likert em diversos domínios

Trabalho	Domínio	Uso da escala Likert
Campos (2020)	Gestão de segurança da informação em órgão público	Escala de 5 pontos
Souza *et al.* (2020)	Educação, ensino de contabilidade com metodologias ativas	Escala de 5 pontos
Maranatha (2023)	Auditoria para o compartilhamento de dados em International Data Spaces	Escala de 5 pontos
Moreira *et al*. (2024)	Educação, uso de ferramenta para identificação de fake news	Escala de 5 pontos
Este artigo	Ciência aberta e defesa cibernética	Escala de 5 pontos

Fonte: Elaborado pelos autores (2024).

4 METODOLOGIA DE DESENVOLVIMENTO

Foi realizado um estudo exploratório em busca de soluções que tratam da gestão de dados para a defesa cibernética no contexto da ciência aberta e em conformidade com as legislações de proteção de dados.

Diante da necessidade de ter acesso a dados sensíveis referentes a ataques cibernéticos para o desenvolvimento de pesquisas acadêmicas, primeiramente iniciou-se um estudo preliminar acerca da motivação das organizações em ceder dados concretos para promoção da ciência aberta. Também foi abordado como deve ocorrer a gestão desses dados, especialmente em relação à necessidade de recuperar parte deles, uma vez anonimizados, por meio de dados de proveniência, a fim de aprofundar a pesquisa.

Uma vez que a promoção da ciência aberta no contexto da defesa cibernética não depende apenas de técnicas eficazes de anonimização, mas também do compromisso entre as partes envolvidas, o estudo buscou a opinião de especialistas a respeito da viabilidade de um serviço de gestão de dados sensíveis, visando o compartilhamento seguro desses dados.

A metodologia aplicada neste trabalho foi precedida por uma pesquisa bibliográfica, principalmente na base de dados Google Acadêmico, devido ao seu escopo abrangente. O levantamento focou temas como: (i) defesa cibernética; (ii) ciência aberta; (iii) proteção de dados sensíveis; e (iv) gestão de dados de pesquisa.

Dessa forma, foram analisados os pontos principais para a elaboração de um processo, que foram listados e formatados como perguntas em um formulário. Exemplos de questões incluem: Acredita na oportunidade de existir um PGDS? Quais documentos, políticas e procedimentos seriam necessários para garantir a segurança das informações e viabilizar o PGDS? Qual fator motivacional para o compartilhamento de dados?

Em paralelo, foram avaliadas questões como: Para quem e como o formulário será direcionado? Quem seriam os especialistas? Que perguntas (e quantas) devem ser listadas? Essas ponderações tiveram o objetivo de permitir o levantamento de opiniões de especialistas sobre as etapas necessárias para posterior mapeamento de um processo de gestão de dados sensíveis.

Dito isso, propôs-se aos especialistas estabelecer um Programa de Gestão de Dados Sensíveis, para o qual foi realizada uma pesquisa qualitativa considerando organizações que monitoram o tráfego de suas respectivas redes de dados. A pesquisa teve como base o levantamento de opiniões de especialistas, civis e militares, que atuam na área de segurança cibernética e/ou de gestão de dados.

Para tal investigação, foram confeccionados dois formulários na plataforma Google Forms, um voltado para o público civil (versões em português e em inglês) e outro voltado para o público militar. A divulgação para o público civil ocorreu via contato direto, enquanto para o público militar ocorreu via canal institucional, por meio de documento interno do Exército.

Por fim, para avaliar o grau de concordância sobre os principais pontos propostos pelo PGDS, foi utilizada a escala Likert (1932) com objetivo de evidenciar a relevância do programa e as principais etapas do processo a ele atribuído.

5 RESULTADOS

Após a divulgação dos formulários para o levantamento de opiniões de especialistas, foram obtidas 59 respostas, sendo 40 de integrantes de organizações militares, pertencentes ao setor de Defesa, e 19 de civis, oriundos do segmento acadêmico, da administração pública federal, da indústria e de serviços, conforme a Tabela 1.

Tabela 1 – Perfil dos especialistas

Segmento	Acadêmico	Administração Pública Federal	Defesa	Indústria	Serviços
Total de especialistas	2	2	40	2	13

Fonte: Elaborado pelos autores (2024).

Considerando a representatividade significativa do setor de Defesa nas respostas coletadas, neste artigo foram analisadas somente as opiniões de especialistas desse setor. A análise dessas opiniões pode auxiliar no desenvolvimento de melhores práticas e na colaboração interagências para mitigar riscos a infraestruturas no contexto da gestão e compartilhamento de dados sensíveis.

Como resultado, verificou-se que 92,5% dos respondentes (55% totalmente e 37,5% parcialmente) concordam com a existência de uma instituição responsável pelo PGDS que realize o tratamento, o controle e o compartilhamento de dados sensíveis anonimizados oriundos de tráfego de redes. Isso representaria uma oportunidade para a pesquisa e desenvolvimento de tecnologias voltadas à identificação de vulnerabilidade de redes.

Nesse sentido, 100% dos respondentes concordam que, para que as organizações tenham confiança ao compartilharem seus dados por meio do PGDS, a instituição que os atende deve adotar políticas como uma política de segurança da informação, política de privacidade e política de gestão de dados sensíveis e de pesquisa, visando representar o compromisso da instituição em proteger os dados, conforme evidenciado na Tabela 2.

Tabela 2 – Adoção de políticas

Políticas	Concordo totalmente	Concordo parcialmente	Indiferente	Discordo parcialmente	Discordo totalmente
Segurança da informação	85%	15%	0%	0%	0%
Privacidade	87,5%	12,5%	0%	0%	0%
Gestão de dados	95%	5%	0%	0%	0%

Fonte: Elaborado pelos autores (2024).

Conforme a Tabela 3, observa-se que a maioria dos respondentes considera essencial, para o compartilhamento de dados, a assinatura de um instrumento de parceria. Como exemplo, foram citadas a celebração de um convênio e de um termo de confidencialidade entre a organização e a instituição, detalhando todo o tratamento que deverá ser feito com o dado, em conformidade com normas, regulamentos e legislações vigentes, como a lei que promove a proteção de dados.

Tabela 3 – Necessidade de assinatura de convênio e termo de confidencialidade

Concordo totalmente	Concordo parcialmente	Indiferente	Discordo parcialmente	Discordo totalmente
85%	7,5%	2,5%	5%	0%

Fonte: Elaborado pelos autores (2024).

Para possibilitar ao pesquisador o acesso a uma instância do conjunto de dados sensíveis, resguardando, contudo, a segurança das informações, foi sugerida a entrega de três conjuntos de documentos: comprovante oficial de vínculo com instituição acadêmica, projeto de pesquisa e currículo Lattes, ORCID ou similar. A Tabela 4 apresenta o nível de concordância dos respondentes sobre a afirmação de que a apresentação de tais documentos favoreceria a segurança das informações.

Tabela 4 – Documentos comprobatórios do pesquisador

Documento	Concordo totalmente	Concordo parcialmente	Indiferente	Discordo parcialmente	Discordo totalmente
Vínculo	95%	2,5%	0%	2,5%	0%
Projeto	82,5%	12,5%	5%	0%	0%
Currículo	55%	27,5%	17,5%	0%	0%

Fonte: Elaborado pelos autores (2024).

De posse dos documentos recebidos, sugeriu-se analisar a relevância da pesquisa para a comunidade científica, considerando como critérios o risco de acesso aos dados e a conformidade com as políticas de segurança da informação, de privacidade e de gestão de dados sensíveis e de pesquisa. A Tabela 5 apresenta o nível de concordância dos respondentes sobre a afirmação de que tais análises devem ser realizadas no processo.

Tabela 5 – Análise dos documentos

Análise	Concordo totalmente	Concordo parcialmente	Indiferente	Discordo parcialmente	Discordo totalmente
Risco	57,5%	25%	12,5%	5%	0%
Conformidade	87,5%	5%	7,5%	0%	0%

Fonte: Elaborado pelos autores (2024).

Também foi questionado aos especialistas sobre a necessidade da emissão de um parecer técnico por parte da instituição gestora dos dados. Esse parecer, destinado à apreciação

da organização que compartilhou os dados com o PGDS, apresentaria a viabilidade técnica e o cumprimento de exigências para o compartilhamento seguro. Nesse caso, foram obtidas as respostas constantes da Tabela 6.

Tabela 6 – Necessidade de emissão de parecer técnico

Concordo totalmente	Concordo parcialmente	Indiferente	Discordo parcialmente	Discordo totalmente
72,5%	17,5%	10%	0%	0%

Fonte: Elaborado pelos autores (2024).

Em caso de aprovação de acesso aos dados sensíveis por parte da organização, foi sugerido que sejam assinados dois termos, buscando assegurar a proteção dos dados: novo termo de confidencialidade entre o PGDS e a organização, e termo de confidencialidade entre o PGDS e o pesquisador. A Tabela 7 apresenta o nível de concordância dos respondentes quanto à necessidade de assinatura desses termos.

Tabela 7 – Necessidade de assinatura de termos de confidencialidade

Termo	Concordo totalmente	Concordo parcialmente	Indiferente	Discordo parcialmente	Discordo totalmente
Entre PGDS e organização	77,5%	10%	7,5%	2,5%	2,5%
Entre PGDS e pesquisador	82,5%	12,5%	2,5%	0%	2,5%

Fonte: Elaborado pelos autores (2024).

Uma vez os termos firmados, a instituição assume a responsabilidade em prover o devido controle de segurança ao compartilhar os dados sensíveis diretamente com o pesquisador solicitante. Nesse contexto, os controles avaliados pelos especialistas referem-se ao acesso aos dados em ambiente seguro e por tempo determinado, com 92,5% dos respondentes concordando com essa afirmativa (82,5% totalmente e 10% parcialmente).

Por fim, buscou-se identificar motivações para que organizações compartilhem seus dados sensíveis, sendo apresentadas as seguintes sugestões: notificação sobre dados sensíveis anonimizados e publicados no repositório; recebimento de relatórios estatísticos de acesso ao conjunto de dados compartilhado; e recebimento de relatórios sobre as pesquisas realizadas com o acesso a seus dados sensíveis. A Tabela 8 apresenta a opinião dos respondentes sobre essas motivações.

Tabela 8 – Motivações para o compartilhamento de dados

Motivação	Concordo totalmente	Concordo parcialmente	Indiferente	Discordo parcialmente	Discordo totalmente
Notificação de publicação	65%	27,5%	5%	2,5%	0%
Relatórios estatísticos	62,5%	25%	12,5%	0%	0%
Relatórios de pesquisas	75,0%	25%	0%	0%	0%

Fonte: Elaborado pelos autores (2024).

Da análise dos resultados apresentados em todas as tabelas, foi possível verificar que a maioria dos especialistas consultados apresentam opinião favorável a todas as propostas apresentadas neste trabalho no tocante ao PGDS. Isso indica que sua implementação pode ser uma forma de garantir o comprometimento da instituição em termos de segurança da informação e proteção dos dados.

6 CONSIDERAÇÕES FINAIS

Os resultados demonstram o apoio dos especialistas à existência de um Programa de Gestão de Dados Sensíveis. O nível elevado de concordância, de 92,5%, sobre a importância de uma instituição responsável pelo tratamento, controle e compartilhamento de dados sensíveis anonimizados revela uma demanda por maior fundamentação nesse processo. Essa iniciativa facilitaria tanto a pesquisa quanto a inovação no desenvolvimento de novas tecnologias para a identificação de vulnerabilidades de redes.

Outro ponto de destaque é a unanimidade (100%) sobre a necessidade de adoção de políticas, como as de segurança da informação, de privacidade e de gestão de dados sensíveis, para garantir a proteção das informações e mitigar os riscos associados ao tratamento de dados sensíveis. Esse consenso entre os respondentes ressalta o papel essencial que essas políticas desempenham na criação de uma estrutura confiável e transparente, necessária para a cooperação entre as organizações e o PGDS.

Essa abordagem está alinhada com a Estratégia Nacional de Cibersegurança, que enfatiza a importância de estabelecer mecanismos de compartilhamento de informações sobre incidentes cibernéticos. No entanto, a análise crítica desse ponto sugere que a implementação dessas políticas não deve ser apenas um compromisso formal, mas deve também envolver mecanismos de auditoria e revisão contínua para garantir os resultados esperados, bem como a adoção de outras políticas ou procedimentos de segurança.

Quanto à exigência de instrumentos de parceria, os resultados indicam que a maioria dos especialistas considera essa medida significativa, demonstrando preocupação com a segurança e a conformidade legal no compartilhamento seguro dos dados. Contudo, a viabilidade dessa exigência a longo prazo pode ser questionada, pois pode adicionar complexidade ao processo, exigindo um equilíbrio entre os procedimentos administrativos e a acessibilidade.

A apresentação de documentos comprobatórios por parte dos pesquisadores foi amplamente apoiada, pois representa um fator de confiança no processo de concessão de acesso a dados sensíveis. Isso reflete a preocupação com o controle e a proteção das informações. Contudo, embora esses documentos garantam a legitimidade das pesquisas, também expõem o desafio de equilibrar a segurança com a agilidade desejada, especialmente pelos pesquisadores. A necessidade de um parecer técnico e a responsabilidade da instituição em prover um ambiente seguro para o acesso aos dados também são aspectos que emergem como fundamentais para garantir a integridade do processo.

Por fim, as motivações apresentadas pelos especialistas, como a notificação sobre dados anonimizados e relatórios de pesquisas, indicam que há interesse em colaborar com a pesquisa científica, desde que sejam respeitados os requisitos de segurança da informação e privacidade. Assim, a implementação de um PGDS pode não apenas contribuir para a inovação e o avanço

da pesquisa tecnológica, mas também apoiar na criação de uma cultura de compartilhamento seguro de dados. Inclusive, os requisitos preliminares dessa implementação podem ser inferidos a partir das questões abordadas pelo formulário.

Além disso, embora os resultados sejam promissores, algumas limitações devem ser reconhecidas. Este artigo se concentrou em analisar apenas os especialistas do setor de Defesa, o que pode não refletir a diversidade de opiniões presentes em outros setores que também lidam com dados sensíveis. A análise qualitativa, baseada apenas nas opções pré-definidas da escala Likert, poderia ser aprofundada com métodos adicionais, visando captar melhor as opiniões e sugestões dos participantes.

A pesquisa também não aborda em profundidade as implicações práticas da implementação do PGDS, como a arquitetura que irá garantir a segurança tanto no armazenamento como na disponibilização dos dados anonimizados, os desafios de conformidade com a LGPD e os aspectos éticos e administrativos do compartilhamento de dados sensíveis em larga escala, temas que podem ser investigados em estudos futuros.

Os resultados mostram que as medidas propostas para o PGDS são bem aceitas pelos especialistas, ao passo que o estabelecimento de medidas técnicas e administrativas para a gestão de dados sensíveis assegura a transparência e a responsabilidade no compartilhamento seguro, promovendo uma cultura colaborativa na ciência aberta.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2013**: tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro: ABNT, 2013.

ANPD – AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo**: segurança da informação para agentes de tratamento de pequeno porte. Brasília, DF: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em: 20 out. 2024.

BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança. **Diário Oficial da União**: seção 1, Brasília, DF, p. 2, 5 ago. 2025. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-12.573-de-4-de-agosto-de-2025-646200784. Acesso em: 5 set. 2025.

BRASIL. Ministério da Defesa. **Portaria GM-MD nº 5.081, de 16 de outubro de 2023**. Aprova a Doutrina Militar de Defesa Cibernética – MD31-M-07 (2ª Edição/2023). Brasília, DF: Ministério da Defesa, 2023. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf. Acesso em: 5 set. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 19 out. 2024.

BRASIL. Portaria GSI/PR nº 93, de 18 de outubro de 2021. Aprova o glossário de segurança da informação. **Diário Oficial da União**: seção 1, Brasília, DF, p. 36, 19 out. 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370. Acesso em: 10 out. 2024.

BRITO, F. T.; MACHADO, J. C. Preservação de privacidade de dados: fundamentos, técnicas e aplicações. *In*: DELICATO, F. C.; PIRES, P. F.; SILVEIRA, I. F. (orgs.). **Jornadas de atualização em informática 2017**. Porto Alegre: Sociedade Brasileira de Computação, 2017. v. 3. p. 91-130. Disponível em: https://www.researchgate.net/profile/Felipe-Brito-4/publication/318726149_Preservacao_de_Privacidade_de_Dados_Fundamentos_Tecnicas_e_Aplicacoes/links/597a3540a6fdcc61bb05b98a/Preservacao-de-Privacidade-de-Dados-Fundamentos-Tecnicas-e-Aplicacoes.pdf. Acesso em: 20 out. 2024.

CAMPOS, G. K. D. **Análise em gestão de segurança da informação e suas consequências em órgão da administração pública federal**. 2020. Trabalho de Conclusão de Curso (Especialização em Gestão, Assessoramento e Estado-Maior) – Escola de Formação Complementar do Exército,

Salvador, 2020. Disponível em: http://bdex.eb.mil.br/jspui/handle/123456789/9396. Acesso em: 11 nov. 2023.

CEOLIN JUNIOR, T. *et al*. Correlação de alertas em um Internet Early Warning System. **Observatório de la Economía Latinoamericana**, v. 21, n. 8, p. 8196-8216, 2023. DOI: https://doi.org/10.55905/oelv21n8-023

CORTEZ, L. R. C. T.; CAÇÃO, R. F. **Workflow para descoberta de conhecimento em segurança cibernética**. 2017. Trabalho de Conclusão de Curso (Graduação em Engenharia da Computação) – Instituto Militar de Engenharia, Rio de Janeiro, 2017. Disponível em: http://www.defesacibernetica.ime.eb.br/pub/repositorio/2017-Cortez_Cacao.pdf. Acesso em: 20 out. 2024.

COSTA, M. M.; SHINTAKU, M. (orgs.). **Conferência livre Ciência Aberta no Brasil**: desafios e oportunidades. Brasília, DF: MCTI: Ibict, 2024. Disponível em: https://www.gov.br/cgu/pt-br/governo-aberto/a-ogp/planos-de-acao/6deg-plano-de-acao-brasileiro/compromisso-3/relatorio_conferencia_ibict_mcti.pdf. Acesso em: 25 out. 2024.

FEIJÓ, A. M.; VICENTE, E. F. R.; PETRI, S. M. O uso das escalas Likert nas pesquisas de contabilidade. **Revista Gestão Organizacional**, Chapecó, v. 13, n. 1, p. 27-41, 2020. DOI: https://doi.org/10.22277/rgo.v13i1.5112

HENNING, P. C. *et al*. GO FAIR e os princípios FAIR: o que representam para a expansão dos dados de pesquisa no âmbito da ciência aberta. **Em Questão**, Porto Alegre, v. 25, n. 2, p. 389-412, 2019. DOI: https://doi.org/10.19132/1808-5245252.389-412

HINTZBERGEN, J. *et al*. **Fundamentos de Segurança da Informação com base na ISO 27001 e na ISO 27002**. Rio de Janeiro: Brasport, 2018.

LIKERT, R. A technique for the measurement of attitudes. **Archives of Psychology**, Nova York, n. 140, 1932. Disponível em: https://legacy.voteview.com/pdf/Likert_1932.pdf. Acesso em: 11 nov. 2023.

MACHADO, J. C.; DUARTE NETO, E. R.; BENTO FILHO, M. E. Técnicas de privacidade de dados de localização. **SBBD**, Fortaleza, p. 8, 2019. Disponível em: https://sbbd.org.br/2019/wp-content/uploads/sites/6/2019/10/To%CC%81picos-em-Gerenciamento-de-dados-e-Informacoes-2019.pdf#page=8. Acesso em: 14 out. 2024.

MARANATHA, Y. G. **Auditable data sharing in logistic data space**: design and implementation of IDS clearing house for logistic data space. 2023. Dissertação (Mestrado) – University of Twente, Enschede, 2023. Disponível em: https://essay.utwente.nl/97055/. Acesso em: 10 fev. 2024.

MARINHO, Isabel Cristina Sampaio Freitas. **Gestão de dados sensíveis no contexto da segurança cibernética**. 2025. Dissertação (Mestrado em Engenharia de Defesa) – Instituto Militar de Engenharia, Rio de Janeiro, 2025.

MOREIRA, T. O. *et al*. JEDi – a digital educational game to support student training in identifying Portuguese-written fake news: case studies in high school, undergraduate and graduate scenarios. **Education and Information Technologies**, v. 29, p. 11815-11845, 2024. DOI: https://doi.org/10.1007/s10639-023-12309-z

OLIVEIRA, Â. B. C. **A tecnologia 5G e possíveis impactos para a segurança nacional**. 2021. Trabalho de Conclusão de Curso (Especialização em Altos Estudos em Defesa) –Escola Superior de Defesa, Brasília, DF, 2021. Disponível em: https://repositorio.esg.br/handle/123456789/1519. Acesso em: 19 out. 2024.

OLIVEIRA, F. T.; CAVALCANTI, M. C.; SALLES, R. M. Towards effective reproducible botnet detection methods through scientific workflow management systems. *In*: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS (SBRC), 35., 2017, Belém. **Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2017. Disponível em: https://sol.sbc.org.br/index.php/sbrc/article/view/2678. Acesso em: 20 out. 2024.

SALES, L. F.; COSTA, M.; SHINTAKU, M. Ciência aberta, gestão de dados de pesquisa e novas possibilidades para a editoração científica. *In*: SHINTAKU, M.; SALES, L. F.; COSTA, M. (orgs.). **Tópicos sobre dados abertos para editores científicos**. Botucatu: ABEC, 2020. p. 13-21. Disponível em: https://www.abecbrasil.org.br/arquivos/Topicos_dados_abertos_editores_cientificos.pdf. Acesso em: 14 out. 2024.

SERVIÇO de Acesso a Dados Protegidos (Sedap). **Gov.br**, 3 mar. 2022. Disponível em: https://www.gov.br/inep/pt-br/areas-de-atuacao/gestao-do-conhecimento-e-estudos-educacionais/cibec/servico-de-acesso-a-dados-protegidos-sedap. Acesso em: 23 set. 2025.

SOUZA, A. N. M. *et al*. Utilização de metodologias ativas e elementos de gamificação no processo de ensino-aprendizagem da contabilidade: experiência com alunos da graduação. **Desafio online**, Campo Grande, v. 8, n. 3, 2020. Disponível em: https://desafioonline.ufms.br/index.php/deson/article/view/10317/8489. Acesso em: 11 nov. 2023.

STEINBUSS, S. *et al*. **GDPR related requirements and recommendations for the IDS reference architecture model**. Berlim: International Data Spaces Association, 2019. Disponível em: https://zenodo.org/records/5675903. Acesso em: 10 ago. 2024.

UNIÃO EUROPEIA. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016**. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General

Data Protection Regulation). França: Parlamento Europeu, 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 23 set. 2025.

VAN RAVENZWAAIJ, D. *et al*. **De-identification when making datasets FAIR: Two worked examples from the behavioral and social sciences**. [*S. l.: s. n.*], 2024. DOI: https://doi.org/10.31234/osf.io/acpm3

WHAT WE DO. **IMPACT Cyber Trust**, [*s. l.*], 2019. Disponível em: https://www.impactcybertrust.org/what. Acesso em: 23 set. 2025.