ARTICLE DOI 10.52781/cmm.a183

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

Intercambio seguro de datos sensibles en ciberdefensa: una propuesta de programa de gestión desde la perspectiva de la ciencia abierta

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.

Resumen: La ciencia abierta en ciberdefensa presenta un desafío específico debido a la naturaleza restringida de los datos, lo que, a su vez, dificulta su intercambio en pro del avance tecnológico. A partir de una investigación cualitativa realizada con expertos de áreas estratégicas, se propuso crear un Programa de Gestión de Datos Sensibles (PGDS) con el objetivo de permitir el intercambio seguro de estos datos. Los resultados demuestran que la mayoría de los encuestados considera positiva la existencia del PGDS para tratar, controlar y poner a disposición los datos sensibles anonimizados. Así, el estudio concluye que la implementación del PGDS puede fomentar la investigación y el desarrollo tecnológico en el campo de la ciberdefensa, preservando la protección de datos sensibles.

Palabras clave: Ciencia abierta; Ciberdefensa; Protección de datos sensibles; Privacidad.

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

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

Received: Nov. 27, 2024
Accepted: Sept, 19, 2025

* This study, co-authored with two of the advisors, summarizes part of the results obtained from the research developed as part of the first author's master's thesis (Marinho, 2025), defended in the Graduate Program in Defense Engineering at the Military Institute of Engineering.

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

1 INTRODUCTION

Cyber defense actions are integrated into the national strategic framework and coordinated by the Ministry of Defense; it involves protecting information assets relevant to national defense. These actions also involve data collection for the production of intelligence knowledge and seek to ensure superiority within the cyber domain (Brasil, 2023).

These measures are related to the security of operations, which include, for example, incident handling and risk management. Accordingly, cybersecurity aims to ensure that information systems are capable of withstanding events that may compromise the essential requirements of information security—namely, the availability, integrity, confidentiality, and authenticity of transmitted, processed, or stored information (Brasil, 2021).

In this regard, the Brazilian National Cybersecurity Strategy highlights the importance of establishing and developing information analysis and sharing centers, encouraging the implementation of a national mechanism for reporting cybersecurity incidents (Brasil, 2025). This exchange of knowledge aims to identify, manage, and mitigate risks in a coordinated manner, promoting a more efficient approach.

A more accurate way to assess these risks is via concrete data derived from scientific research within the field of cybersecurity. Additionally, the concept of open science involves the democratization of access to research data, allowing both the scientific community and society to benefit from the information collected.

However, when dealing with sensitive data, such as network traffic and security incidents, the challenge becomes greater, as protecting this information is necessary to prevent both the exposure of data subjects and the risk of noncompliance with data protection laws. In this context, van Ravenzwaaij *et al*. (2024) highlight challenges in achieving a balance between legal compliance and scientific interests, ensuring privacy while allowing the dataset to remain as open as possible.

Also according to the authors, the scientific community's movement toward open science encourages researchers to make their data openly available for reuse. With this objective, this study sought to identify the main stages of a process capable of enabling secure sharing of sensitive data, thereby contributing to the advancement of research in cyber defense and to the development of a secure data sharing culture. No studies with a similar focus have been identified in the existing literature.

After identifying these stages, experts were consulted regarding the feasibility of creating a Sensitive Data Management Program (SDMP) as a proposal to facilitate the secure sharing of sensitive data, in compliance with current data protection and security regulations.

Within this context, the main objective of this study is to describe an SDMP designed to allow the secure sharing of data within cyber defense, aligning principles of open science with legal requirements of data protection. The guiding question is: How can we ensure the secure sharing of sensitive data in this context without compromising privacy or legal compliance?

To this end, specific objectives include reviewing the main concepts; identifying and analyzing studies related to the sharing of sensitive data to highlight existing gaps in the literature; determining, with experts, the necessary steps to structure an effective SDMP; and developing a program proposal that enables the secure sharing of data in compliance with current regulations.

Accordingly, the study first presents a theoretical review of the concepts of open science, information security, and data protection. Next, related studies are examined, followed by a detailed description of the development of the study and the methodology adopted. The results are then discussed, and finally, final considerations and suggestions for future research are presented.

2 THEORETICAL REVIEW

2.1 Open science

Open science promotes changes in the production, organization, sharing, and reuse of scientific knowledge (Costa; Shintaku, 2024). In addition to promoting scientific publications such as academic articles, it also provides access to data generated by researchers or scientists during the scientific investigation process. This includes access to methodologies, software, and the resulting outputs. Thus, open science aims to ensure the reproducibility of science and the efficient use of resources by means of collaborative practices (Sales; Coast; Shintaku, 2020).

Henning *et al*. (2019) present advantages of open data within the scope of scientific data by comparing these benefits for both science and society, serving as motivation for this study. Among advantages for science, data reuse stands out as it enables new research while reducing costs by eliminating the need to collect the same data a second time. Once collected and analyzed, such data can be used in subsequent studies from different perspectives.

Henning *et al*. (2019) indicate that all benefits providing advantages to society are related to data reuse, among which two main advantages stand out: reuse for innovation and increased competitiveness. In other words, opening data can foster the development of new products, services, and consequently, jobs, while reuse supports decision-making by ensuring that policymakers rely on evidence derived from data analysis.

However, there is a clear need for initiatives aimed at improving research related to the availability of sensitive datasets, especially regarding cyber defense. To this end, considering the possible standardization of de-identification techniques, such as anonymization and pseudonymization, may enable databases to be published without exposing the organization from which the data originated to potential vulnerabilities (Machado; Duarte Neto; Bento Filho, 2019).

2.2 Information security

Information security aims to ensure the confidentiality, integrity, and availability of information (Hintzbergen *et al.*, 2018). To protect it, it is essential to apply security controls that consider potential threats to the organization. The ABNT NBR ISO/IEC 27001:2013 standard (ABNT, 2013) defines these controls with the purpose of ensuring business continuity by addressing vulnerabilities to minimize the impact of possible incidents. This is achieved by selecting and implementing appropriate controls, including policies, processes, procedures, organizational structures, software, and hardware designed to protect information assets.

Within the cyber domain, the National Cybersecurity Strategy (Brasil, 2025) defines cyber defense as a set of actions aimed at ensuring cybersecurity of the country's strategic assets, promoting cooperation among public and private entities to enable the exchange of information for the prevention of and response to cybersecurity incidents. In turn, cybersecurity is defined as a set of measures capable of protecting the cyber domain, including tools, best practices, risk management, among others.

Concurrently, with the exponential growth of the internet, computer systems, and the ongoing evolution of communication technologies such as 5G and beyond, it is possible to reflect on the increase in cyber vulnerabilities and threats as a consequence of the greater flow of network data resulting from intensified information exchange (Oliveira, 2021).

Among the existing security solutions, Intrusion Detection Systems (IDS) stand out as technologies that help mitigate such vulnerabilities by monitoring and analyzing network data flows, thereby enabling the detection of potential attacks (Ceolin Junior *et al.*, 2023). Moreover, machine learning techniques make these detections even more robust (Cortez; Cação, 2017) as intrusion detection algorithms based on real-world data continues to be refined (Oliveira; Cavalcanti; Salles, 2017). However, this raises concerns about preserving the privacy of the individuals and organizations involved.

2.3 Data protection

In addition to the technical and administrative controls established by the ABNT NBR ISO/IEC 27001:2013 standard (ABNT, 2013), which addresses information security, and by the information security guidance issued by the Brazilian National Data Protection Agency (ANPD, 2021), Brito and Machado (2017) present strategies for tackling the issue of privacy preservation. These include data anonymization techniques for sensitive information as a potential solution, thereby enabling the availability of such data.

Furthermore, Law No. 13,709, of August 14, 2018—the General Data Protection Law (LGPD – *Lei Geral de Proteção de Dados*) (Brasil, 2018)—establishes a legal framework for the protection of personal data in Brazil, focusing on privacy protection. However, the LGPD also encourages the processing of such data for research purposes, provided that anonymization or

pseudo-anonymization is ensured. In this context, anonymization emerges as the key technique that enables the use of data in scientific studies while minimizing the risks of exposing individuals or organizations.

Thus, the combination of security controls and the adoption of de-identification techniques contributes to balancing the advancement of open science with data protection.

3 RELATED STUDIES

The related studies are categorized into two aspects: (i) studies supporting the sharing of sensitive data, and (ii) studies that collect opinions using the Likert scale (1932), which is commonly applied for this type of survey (Feijó; Vicente; Petri, 2020).

3.1 Sharing of sensitive data

Regarding the sharing of sensitive data, several government initiatives stand out, such as the Protected Data Access Service (SEDAP – *Serviço de Acesso a Dados Protegidos*) (Serviço [...], 2022) from the National Institute for Educational Studies and Research Anísio Teixeira (INEP – *Instituto Nacional de Estudos e Pesquisas Educacionais*), and the Information Marketplace for Policy and Analysis of Cyber-risk and Trust (IMPACT) (What we do, 2019) from the U.S. Department of Homeland Security (DHS).

SEDAP provides researchers with access to protected data produced by INEP and focuses on the development of educational research. To this end, it defines minimum access requirements, covering all steps from the application process to the execution of the service, which takes place in a secure room on the service's premises.

The IMPACT program offers researchers access to data via a repository, focusing on the assessment of cyber risks, as well as the prevention, detection, and mitigation of cyber threats. However, only researchers based in the United States and other DHS-approved locations—Australia, Canada, Israel, Japan, the Netherlands, Singapore, and the United Kingdom—are eligible to request an account to access IMPACT.

Yet, in both cases, there was a lack of process mapping and architectural documentation. Such mapping could serve as a reference for best practices and enable transparency and dissemination of the methodology adopted, allowing other institutions to adopt the same approach, as evidenced by the European initiative, the International Data Spaces Association (IDSA)[1].

The IDSA proposes a decentralized approach to data sharing via data spaces, ensuring that each participating company can exchange information securely and reliably (Maranatha, 2023), and provides an architectural model for the development of compatible Data Spaces. Nevertheless, the roles prescribed by the legislation are not represented, since responsibility for compliance with the European General Data Protection Regulation (GDPR) (European Union, 2016) lies with the organization itself (Steinbuss *et al.*, 2019).

1 Available at: https://internationaldataspaces.org. Access on: 23, sept. 2025.

3.2 Measurement technique for opinion surveys

To structure the questionnaire for the opinion survey, a study was conducted to identify the most commonly used measurement techniques for this context. The study found that the Likert scale predominates as the primary measurement tool, according to Feijó, Vicente, and Petri (2020). In their article, the authors state that "attitude scales such as the Likert scale are widely used, especially for questions regarding preferences, tastes, and perceptions. The scale is known as being simple and easy to understand [...]" (Feijó; Vicente; Petri, 2020, p. 28, our translation).

The Likert scale enables the creation of a rating system that reflects different degrees of agreement with a given question. Typically represented on a five-point scale, it has the capacity to generate qualitative data. For the purposes of this study, the following options were adopted: "strongly disagree," "partially disagree," "neutral," "partially agree," and "strongly agree." This approach proved to be compatible with the evaluation needs of the study.

Several studies use the Likert scale to assess degrees of agreement or disagreement across different research contexts (Campos, 2020; Maranatha, 2023; Moreira *et al.*, 2024; Souza *et al.*, 2020), demonstrating its effectiveness in capturing opinions.

Campos (2020) examines the best practices of adherence to information security, including compliance with security standards such as ABNT NBR ISO/IEC 27002:2013, and their impact on the productivity of a public institution. The author assesses the compliance level of the Administrative Database of the Amazon Military Command of the Brazilian Army using the Likert scale. The study reveals a satisfactory level of compliance and also identifies areas requiring improvement, reinforcing the importance of information security management in mitigating adverse impacts.

Souza *et al.* (2020) investigate the application of active learning methodologies and gamification in accounting education. Results obtained via the Likert scale show that these approaches increase student engagement and motivation, demonstrating the effectiveness of interactive pedagogical practices to promote meaningful learning.

Maranatha (2023) employs the Likert scale to validate the Clearing House model, proposed for the sharing of auditable data within International Data Spaces in the logistics sector, aligned with the objectives and motivations of the study. As a result, most experts consider the Clearing House a promising solution from both economic and technical perspectives.

Moreira *et al.* (2024) analyze the use of digital educational games to train students in identifying fake news via the JEDi tool. Case study results with high school, undergraduate, and graduate students demonstrate the effectiveness of JEDi as an instrument for detecting fake news in Portuguese-language news. For this purpose, the Likert scale was used to assess students' levels of agreement.

Chart 1 presents the domains and the Likert scale employed in these studies, underscoring its application across several domains to assess degrees of agreement.

Chart 1 – Use of the Likert scale across several domains

Study	Domain	Use of the Likert scale
Campos (2020)	Information security management in public agencies	5-point scale
Souza *et al.* (2020)	Education, teaching accounting with active methodologies	5-point scale
Maranatha (2023)	Auditing for data sharing in International Data Spaces	5-point scale
Moreira *et al*. (2024)	Education, use of tools to identify fake news	5-point scale
This study	Open science and cyber defense	5-point scale

Source: Prepared by the authors (2024).

4 DEVELOPMENT METHODOLOGY

An exploratory study was conducted to identify solutions addressing data management for cyber defense within the context of open science and in compliance with data protection legislation.

Given the need to access sensitive data related to cyberattacks for the development of academic research, the study initially focused on the motivation of organizations to provide concrete data to promote open science. It also addressed how such data should be managed, particularly regarding the need to recover parts of the data, once anonymized, by means of provenance information in order to deepen the research.

Since the promotion of open science within cyber defense depends not only on effective anonymization techniques but also on the commitment of the parties involved, the study sought expert opinions regarding the feasibility of a sensitive data management service aimed at enabling the secure sharing of such data.

The methodology applied in this study was preceded by a literature review, mainly using the Google Scholar database due to its broad scope. The review focused on the following topics: (i) cyber defense; (ii) open science; (iii) sensitive data protection; and (iv) research data management.

Therefore, the main points for the development of a process were analyzed and organized as questions in a survey form. Examples of questions include: Do you believe there is an opportunity to establish an SDMP? Which documents, policies, and procedures would be necessary to ensure information security and enable the SDMP? What would be motivational factors for data sharing?

In parallel, questions such as the following were considered: Who should the survey be directed to, and how? Who would qualify as experts? Which questions (and how many) should be included? These considerations aimed to collect expert opinions on the necessary steps for subsequent mapping of a sensitive data management process.

Consequently, experts were invited to consider the establishment of an SDMP, for which a qualitative study was conducted involving organizations that monitor the traffic of their respective data networks. The study was based on collecting the opinions of experts, both civilian and military, who work within cybersecurity and/or data management.

For this investigation, two surveys were created using Google Forms: one aimed at the civilian audience (available in Portuguese and English), and another aimed at the military audience. The civilian survey was distributed via direct contact, while the military survey was disseminated via an institutional channel by means of an internal Army document.

Finally, to assess the degree of agreement on the main points proposed by the SDMP, the Likert scale (1932) was used, aiming to highlight the relevance of the program and the key steps of the process attributed to it.

5 RESULTS

After distributing the surveys to collect expert opinions, 59 responses were obtained, including 40 from members of military organizations within the Defense sector and 19 from civilians, originating from the academic sector, federal public administration, industry, and services, as shown in Table 1.

Table 1 – Expert profiles

Sector	Academics	Federal Public Administration	Defense	Industry	Services
Total experts	2	2	40	2	13

Source: Prepared by the authors (2024).

Considering the significant representation of the Defense sector among the collected responses, this study focuses exclusively on analyzing the opinions of experts from this sector. Analyzing these insights may contribute to the development of best practices and interagency collaboration to mitigate risks to infrastructures in the context of sensitive data management and sharing.

As a result, it was found that 92.5% of respondents (55% totally and 37.5% partially) agreed with the establishment of an institution responsible for the SDMP, which would handle, control, and share anonymized sensitive data originating from network traffic. This would represent an opportunity for research and the development of technologies towards identifying network vulnerabilities.

In this regard, 100% of respondents agreed that, for organizations to have confidence when sharing their data via the SDMP, the institution responsible must adopt policies such as an information security policy, a privacy policy, and a sensitive and research data management policy. These measures show the institution's commitment to data protection, as shown in Table 2.

Table 2 – Adoption of policies

Policies	Strongly agree	Partially agree	Neutral	Partially disagree	Strongly disagree
Information security	85%	15%	0%	0%	0%
Privacy	87.5%	12.5%	0%	0%	0%
Data management	95%	5%	0%	0%	0%

Source: Prepared by the authors (2024).

Table 3 shows that most respondents consider it essential to sign a partnership instrument for data sharing. Examples mentioned include the establishment of an agreement or a confidentiality term between the organization and the institution, detailing all data processing procedures in accordance with current standards, regulations, and legislation, such as the data protection law.

Table 3 – Need to sign an agreement or confidentiality term

Strongly agree	Partially agree	Neutral	Partially disagree	Strongly disagree
85%	7.5%	2.5%	5%	0%

Source: Prepared by the authors (2024).

To allow researchers to access an instance of the sensitive dataset while safeguarding information security, the submission of three sets of documents was suggested: official proof of affiliation with an academic institution, a research project, and a Lattes, ORCID, or similar academic resumé. Table 4 presents respondents' level of agreement with the statement that the submission of such documents would enhance information security.

Table 4 – Researchers' corroborating documents

Document	Strongly agree	Partially agree	Neutral	Partially disagree	Strongly disagree
Affiliation	95%	2.5%	0%	2.5%	0%
Project	82.5%	12.5%	5%	0%	0%
Resumé	55%	27.5%	17.5%	0%	0%

Source: Prepared by the authors (2024).

Upon receiving the documents, it was suggested to analyze the relevance of the research to the scientific community, considering as criteria the risk associated with data access and compliance with information security, privacy, and sensitive and research data management policies. Table 5 shows respondents' level of agreement with the statement that such analyses should be conducted in the process.

Table 5 – Document analysis

Analysis	Strongly agree	Partially agree	Neutral	Partially disagree	Strongly disagree
Risk	57.5%	25%	12.5%	5%	0%
Compliance	87.5%	5%	7.5%	0%	0%

Source: Prepared by the authors (2024).

Experts were also asked about the need for a technical report to be issued by the data management institution. This report, intended to be reviewed by the organization that shared the

data with the SDMP, would present the technical feasibility and compliance with requirements for secure data sharing. The responses obtained are shown in Table 6.

Table 6 – Need to issue a technical report

Strongly agree	Partially agree	Neutral	Partially disagree	Strongly disagree
72.%	17.5%	10%	0%	0%

Source: Prepared by the authors (2024).

In case the organization approves access to sensitive data, it was suggested that two agreements be signed to ensure data protection: a new confidentiality agreement between the SDMP and the organization, and another between the SDMP and the researcher. Table 7 presents respondents' level of agreement regarding the need to sign these documents.

Table 7 – Need to sign confidentiality agreements

Agreement	Strongly agree	Partially agree	Neutral	Partially disagree	Strongly disagree
Between the SDMP and the organization	77.5%	10%	7.5%	2.5%	2.5%
Between the SDMP and the researcher	82.5%	12.5%	2.5%	0%	2.5%

Source: Prepared by the authors (2024).

Once the agreements are signed, the institution assumes responsibility for providing appropriate security controls when sharing sensitive data directly with the requesting researcher. In this context, the controls evaluated by the experts refer to access to data in a secure environment and for a limited period, with 92.5% of respondents agreeing with this statement (82.5% totally and 10% partially).

Finally, the study sought to identify motivations for organizations to share their sensitive data. The following suggestions were presented: notification about anonymized sensitive data published in the repository; receipt of statistical reports on access to the shared dataset; and receipt of reports on the research conducted using their sensitive data. Table 8 presents respondents' opinions on these motivations.

Table 8 – Motivations for data sharing

Motivation	Strongly agree	Partially agree	Neutral	Partially disagree	Strongly disagree
Notification of publication	65%	27.5%	5%	2.5%	0%
Statistical reports	62.5%	25%	12.5%	0%	0%
Research reports	75.0%	25%	0%	0%	0%

Source: Prepared by the authors (2024).

From the analysis of the results presented, it was observed that most of the consulted experts expressed favorable opinions regarding all proposals presented in this study concerning the SDMP. This indicates that its implementation may be effective to ensure institutional commitment to information security and data protection.

6 FINAL CONSIDERATIONS

The results show the experts' support for the establishment of an SDMP. The high level of agreement (92.5%) on the importance of an institution responsible for the processing, control, and sharing of anonymized sensitive data reveals a demand for stronger foundations in this process. This initiative would facilitate both research and innovation in the development of new technologies for identifying network vulnerabilities.

Another highlight is the unanimity (100%) on the need to adopt policies—such as for information security, privacy, and sensitive data management—to ensure information protection and mitigate risks associated with sensitive data processing. This consensus among respondents underscores the essential role these policies play in creating a reliable and transparent framework necessary for cooperation between organizations and the SDMP.

This approach aligns with the National Cybersecurity Strategy, which emphasizes the importance of establishing mechanisms for sharing information on cybersecurity incidents. However, a critical analysis of this point suggests that the implementation of such policies should not only be a formal commitment but should also involve auditing and continuous review mechanisms to ensure the expected outcomes, as well as the adoption of additional security policies and procedures.

Regarding the requirement for partnership instruments, the results indicate that most experts consider this measure significant, demonstrating concern for security and legal compliance in the secure sharing of data. However, the long-term feasibility of this requirement may be questioned, as it can add complexity to the process, requiring a balance between administrative procedures and accessibility.

The submission of corroborating documents by researchers was widely supported, as it represents a trust factor in the process of granting access to sensitive data. This reflects concern for information control and protection. However, although these documents guarantee the legitimacy of research, they also emphasize the challenge of balancing security with the agility desired by researchers. The need for a technical report and the institution's responsibility to provide a secure environment for data access also emerge as fundamental aspects to ensure the integrity of the process.

Finally, the motivations presented by the experts—including notifications about anonymized data and research reports—indicate an interest in collaborating with scientific research, provided that information security and privacy requirements are respected. Thus, the implementation of an SDMP could not only contribute to innovation and the

advancement of technological research but also foster a culture of secure data sharing. Moreover, the preliminary requirements for such implementation can be inferred from the issues addressed in the survey.

Additionally, while the results are promising, certain limitations must be acknowledged. This study focused exclusively on experts from the Defense sector, which may not reflect the diversity of perspectives present in other sectors that also handle sensitive data. The qualitative analysis, based solely on predefined Likert scale options, could be further enhanced with additional methods aimed at capturing participants' opinions and suggestions more comprehensively.

This study also does not explore in depth the practical implications of implementing the SDMP, such as the architecture required to ensure security in both the storage and provision of anonymized data, challenges of compliance with the LGPD, and ethical and administrative aspects of large-scale sensitive data sharing—topics that can be further investigated in future studies.

The results show that the measures proposed for the SMDP are well accepted by experts, while the establishment of technical and administrative measures for sensitive data management ensures transparency and accountability in secure data sharing, promoting a collaborative culture in open science.

REFERENCES

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.