ARTÍCULO DOI 10.52781/cmm.a183

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

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

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.

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

Recibido: 27 nov. 2024
Aprobado: 19 sep. 2025

* Este artículo, escrito en coautoría con dos de los tutores, resume parte de los resultados obtenidos en la investigación desarrollada en el ámbito de la disertación de maestría de la primera autora (Marinho, 2025), defendida en el Programa de Postgrado en Ingeniería de Defensa del Instituto Militar de Ingeniería.

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

1 INTRODUCCIÓN

La ciberdefensa, introducida en el escenario estratégico nacional de forma integrada y coordinada por el Ministerio de Defensa, comprende un conjunto de acciones centradas en proteger los activos de información de interés de la defensa nacional. Estas acciones también tienen el objetivo de recopilar datos para generar conocimiento de inteligencia y buscan asegurar superioridad en el ciberespacio (Brasil, 2023).

Estas medidas están relacionadas con la seguridad de las operaciones, que incluyen, por ejemplo, el tratamiento de incidentes y la gestión de riesgos. Con eso, la ciberseguridad busca garantizar la capacidad de los sistemas de información para resistir eventos que puedan comprometer los requisitos esenciales de la seguridad de la información, ya sean la disponibilidad, la integridad, la confidencialidad o la autenticidad de la información transmitida, procesada o almacenada (Brasil, 2021).

En este sentido, la Estrategia Nacional de Ciberseguridad resalta la importancia de crear y desarrollar centros de análisis e intercambio de información, fomentando la implementación de un mecanismo nacional de notificación de ciberincidentes (Brasil, 2025). Este intercambio de conocimientos busca identificar, gestionar y mitigar los riesgos de forma coordinada, lo que promueve un enfoque más eficiente.

Una forma más precisa de evaluar estos riesgos es a través de datos concretos, provenientes de investigaciones científicas en el contexto de la ciberseguridad. Asimismo, el concepto de ciencia abierta implica la democratización del acceso a datos de investigación, lo que permite a la comunidad científica y a la sociedad en general beneficiarse de la información recopilada.

Sin embargo, cuando se trata de datos sensibles, como los de tráfico de red e incidentes de seguridad, el desafío es más complejo, visto que es necesario proteger esta información para evitar el riesgo de exponer a los titulares de los datos y el riesgo de incumplimiento de las leyes de protección de datos. En este contexto, van Ravenzwaaij *et al*. (2024) resaltan los desafíos para lograr el equilibrio entre el cumplimiento legal y los intereses científicos, protegiendo la privacidad y permitiendo que el conjunto de datos sea tan abierto como sea posible.

Además, van Ravenzwaaij *et al*. (2024) también afirman que el movimiento de la comunidad científica en pro de la ciencia abierta invita a los investigadores a poner sus datos a disposición de forma abierta para permitir su reutilización. Con este objetivo, este estudio buscó identificar las etapas principales de un proceso que permitiera el intercambio seguro de datos sensibles, para contribuir al avance de la investigación en ciberdefensa y para crear una cultura de intercambio seguro de datos. Hasta donde se pudo investigar, no existe en la literatura un estudio con un enfoque similar.

Tras identificar estas etapas, se buscó la opinión de expertos respecto a la posibilidad de crear un Programa de Gestión de Datos Sensibles (PGDS) como una propuesta para facilitar el intercambio seguro de datos sensibles, de conformidad con las normas y legislaciones vigentes de seguridad y protección de datos.

En este escenario, el principal objetivo de este trabajo es describir un PGDS que permita el intercambio seguro de datos en el contexto de la ciberdefensa, alineando los principios de la ciencia abierta con los requisitos legales de protección de datos. Para ello, la pregunta orientadora es:

¿Cómo hacer viable el intercambio seguro de datos sensibles en este contexto sin comprometer la privacidad y el cumplimiento legal?

Para hacerlo, los objetivos específicos incluyen revisar los principales conceptos, identificar y analizar trabajos relacionados con el intercambio de datos sensibles, identificando brechas existentes en la literatura, identificar, con la ayuda de expertos, las etapas necesarias para estructurar un PGDS eficaz y desarrollar una propuesta de programa que permita el intercambio seguro de datos de conformidad con las normas y legislaciones vigentes.

Para eso, primeramente se presenta la revisión teórica de los conceptos de ciencia abierta, seguridad de la información y protección de datos. A continuación, se analizan los trabajos relacionados y luego se detallan el desarrollo del estudio y la metodología adoptada. Enseguida, se discuten los resultados y, finalmente, se presentan las consideraciones finales y las sugerencias para trabajos futuros.

2 REVISIÓN TEÓRICA

2.1 Ciencia abierta

La ciencia abierta promueve cambios en la producción, la organización, el intercambio y la reutilización del conocimiento científico (Costa; Shintaku, 2024). Con eso, además de fomentar publicaciones científicas, como artículos académicos, también prevé el acceso a datos generados por investigadores o científicos durante el proceso de investigación científica. Esto incluye el acceso a las metodologías, a los softwares y a los resultados generados. Así, la ciencia abierta pretende garantizar la reproducibilidad de la ciencia y el ahorro de recursos de forma colaborativa (Sales; Costa; Shintaku, 2020).

Henning *et al*. (2019) presentan las ventajas de los datos abiertos en el ámbito de los datos científicos mediante una comparación de dichas ventajas tanto para la ciencia como para la sociedad, lo que sirve de motivación para este estudio. Las ventajas para la ciencia incluyen la reutilización de los datos para nuevas investigaciones, lo que reduce costos visto que elimina la necesidad de recopilar estos datos otra vez, dado que, una vez recopilados y analizados, se pueden reutilizar en nuevas investigaciones desde perspectivas diferentes.

Henning *et al*. (2019) señalan que todos los beneficios que proporcionan ventajas para la sociedad están relacionados con la reutilización de los datos, destacándose dos ventajas principales: una centrada en la reutilización en pro de la innovación y la otra relacionada con el aumento de la competitividad. En otras palabras, abrir los datos puede ayudar a generar nuevos productos, servicios y, consiguientemente, empleos, mientras que la reutilización permite apoyar la toma de decisiones, lo que garantiza que formuladores de políticas se basen en evidencias proporcionadas por el análisis de dichos datos.

Sin embargo, se observa la necesidad de iniciativas para mejorar las investigaciones relacionadas con la disponibilidad de conjuntos de datos sensibles, sobre todo con respecto a la ciberdefensa. Para ello, considerar una posible estandarización de las técnicas de desidentificación, como la anonimización y la pseudoanonimización, puede permitir que se publiquen bases de datos sin el riesgo de hacer vulnerable a la organización que originó los datos (Machado; Duarte Neto; Bento Filho, 2019).

2.2 Seguridad de la información

La seguridad de la información tiene el objetivo de garantizar la confidencialidad, la integridad y la disponibilidad de la información (Hintzbergen *et al.*, 2018). Para protegerla, es fundamental aplicar controles de seguridad, teniendo en cuenta las posibles amenazas para el negocio. La norma ABNT NBR ISO/IEC 27001:2013 (ABNT, 2013) define estos controles con el objetivo de garantizar la continuidad de los negocios, actuando en las vulnerabilidades para reducir al mínimo los impactos de posibles incidentes. Esto es posible al elegir e implementar controles adecuados, que incluyen políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información.

En el ámbito del ciberespacio, la Estrategia Nacional de Ciberseguridad (Brasil, 2025) define la ciberdefensa como un conjunto de acciones centradas en la ciberseguridad de los activos estratégicos del país, lo que promueve la cooperación entre organizaciones y entidades públicas y privadas con el objetivo de hacer viable el intercambio de información para prevenir y responder a ciberincidentes. A su vez, la ciberseguridad se define como un conjunto de medidas capaces de proteger el ciberespacio, como herramientas, mejores prácticas, gestión de riesgos, entre otros.

Al mismo tiempo, con el crecimiento exponencial de la internet, los sistemas informáticos, la propia evolución de la tecnología de comunicación hacia el 5G y futuras tecnologías, es posible reflexionar sobre el aumento de vulnerabilidades y ciberamenazas como consecuencia del aumento del flujo de datos en las redes debido al intercambio de información (Oliveira, 2021).

Entre las soluciones de seguridad existentes, las más destacadas son las tecnologías de Sistemas de Detección de Intrusiones (Intrusion Detection Systems [IDS]), que permiten mitigar dichas vulnerabilidades mediante el monitoreo y el análisis de los flujos de datos en las redes, lo que posibilita detectar posibles ataques (Ceolin Junior *et al.,* 2023). Asimismo, técnicas de aprendizaje automático permiten detectar dichos ataques de una manera aún más robusta (Cortez; Cação, 2017), mientras que se sugiere que los algoritmos de detección de intrusiones se refinen a través de datos reales (Oliveira; Cavalcanti; Salles, 2017). Sin embargo, surge la preocupación por preservar la privacidad de las personas y organizaciones involucradas.

2.3 Protección de datos

Además de los controles técnicos y administrativos establecidos en la norma ABNT NBR ISO/IEC 27001:2013 (ABNT, 2013), que comprende la seguridad de la información, y en la guía de orientación sobre seguridad de la información de la Agencia Nacional de Protección de Datos (ANPD, 2021), Brito y Machado (2017) presentan estrategias para el problema de preservar la privacidad, que incluyen técnicas de anonimización de datos sensibles como una solución, lo que permite, consecuentemente, poner estos datos a disposición.

Junto a ello, la Ley nº 13.709, del 14 de agosto de 2018 (Ley General de Protección de Datos Personales [LGPD]) (Brasil, 2018), establece un marco legal para la protección de datos personales en Brasil, centrándose en la protección de la privacidad. Sin embargo, la LGPD también fomenta el tratamiento de estos datos para investigaciones, siempre que se garantice la

anonimización o la pseudoanonimización. En este contexto, la anonimización se convierte en la técnica que permite el uso de estos datos en estudios científicos, lo que minimiza los riesgos de exposición de personas u organizaciones.

Así, combinar los controles de seguridad con la adopción de técnicas de desidentificación contribuyen a equilibrar el avance de la ciencia abierta con la protección de datos.

3 TRABAJOS RELACIONADOS

Los trabajos relacionados están categorizados en dos aspectos: (i) trabajos que apoyan el intercambio de datos sensibles; y (ii) trabajos que recopilan opiniones utilizando la escala de Likert (1932), comúnmente aplicada a este tipo de estudio (Feijó; Vicente; Petri, 2020).

3.1 Intercambio de datos sensibles

En cuanto al intercambio de datos sensibles, se resaltan algunas iniciativas gubernamentales, como el Servicio de Acceso a Datos Protegidos (Sedap) (Serviço [...], 2022), del Instituto Nacional de Estudios e Investigaciones Educativas Anísio Teixeira (Inep), y el programa Information Marketplace for Policy and Analysis of Cyber-risk and Trust (IMPACT) (What we do, 2019), del Departamento de Seguridad Nacional de los Estados Unidos (U.S. Department of Homeland Security [DHS]).

El Sedap pone a disposición de los investigadores el acceso a los datos protegidos, producidos por el Inep, y tiene un alcance centrado en el desarrollo de investigaciones educativas. Para ello, define los requisitos mínimos de acceso, desde las etapas de solicitud hasta la ejecución del servicio, que se realiza en una sala segura en las instalaciones del servicio.

El programa IMPACT proporciona a los investigadores acceso a los datos a través de un repositorio, con un alcance centrado en evaluar riesgos cibernéticos, prevenir, detectar y mitigar ciberamenazas. Sin embargo, solamente los investigadores ubicados en Estados Unidos y otros lugares aprobados por el DHS –Australia, Canadá, Israel, Japón, Holanda, Singapur y Reino Unido– pueden solicitar una cuenta para acceder al IMPACT.

Sin embargo, en estos dos casos, se constató la falta de un mapeo de los procesos y de su arquitectura. Esto podría servir como referencia de buenas prácticas y posibilitar la transparencia y difusión de la metodología adoptada, lo que permitiría a otras instituciones adoptar el mismo método, como lo demuestra la iniciativa europea International Data Spaces Association (IDSA)[1].

La IDSA propone un enfoque descentralizado para el intercambio de datos a través de espacios de datos, lo que asegura que cada empresa participante pueda intercambiar información de forma segura y confiable (Maranatha, 2023), y pone a disposición el modelo de arquitectura para desarrollar Data Spaces compatibles. Aún así, los papeles establecidos en la legislación no están representados, una vez que la responsabilidad del cumplimiento del Reglamento General de Protección de Datos europeo (General Data Protection Regulation [GDPR]) (União Europeia, 2016) recae en la propia organización (Steinbuss *et al.*, 2019).

1 Disponible en: https://internationaldataspaces.org. Acceso el: 23 sep. 2025.

3.2 Técnica de medición para recopilar opiniones

Para estructurar el cuestionario utilizado para recopilar opiniones, se realizó un estudio para identificar las técnicas de medición más utilizadas en este contexto. Se constató el uso predominante de la escala de Likert como método de medición, según Feijó, Vicente y Petri (2020). En el artículo, los autores relatan que "las escalas de actitud como la de Likert son ampliamente utilizadas, sobre todo en cuestiones de preferencias, gustos y percepciones. Conocida como una escala sencilla y fácil de entender [...]" (Feijó; Vicente; Petri, 2020, p. 28).

La escala de Likert permite definir una clasificación que refleja diferentes grados de acuerdo o desacuerdo para una cuestión. Suele aparecer representada en cinco puntos y es capaz de generar datos cualitativos. Para los fines de este estudio, se adoptaron las siguientes opciones: "totalmente en desacuerdo", "parcialmente en desacuerdo", "ni de acuerdo ni en desacuerdo", "parcialmente de acuerdo" y "totalmente de acuerdo". Dicho esto, este enfoque demostró ser compatible con la necesidad de evaluación esperada.

Diversos trabajos utilizan la escala de Likert para evaluar los grados de acuerdo o desacuerdo en diferentes contextos de investigación (Campos, 2020; Maranatha, 2023; Moreira *et al.*, 2024; Souza *et al.*, 2020), lo que demuestra su eficacia para captar opiniones.

Campos (2020) aborda el cumplimiento de las buenas prácticas en seguridad de la información, como el cumplimento de las normas de seguridad, por ejemplo la norma ABNT NBR ISO/IEC 27002:2013, y su impacto en la productividad de un organismo público. El autor analiza el grado de cumplimiento de la Base Administrativa del Comando Militar de la Amazonia, del Ejército Brasileño, utilizando la escala de Likert. El estudio revela un nivel satisfactorio de cumplimiento, además de identificar áreas que necesitan mejorar, lo que refuerza la importancia de la gestión de seguridad de la información para mitigar impactos adversos.

Souza *et al.* (2020) investigan la aplicación de metodologías activas y ludificación en la enseñanza de la contabilidad. Los resultados obtenidos a través de la escala de Likert demuestran que estos enfoques aumentan el compromiso y la motivación de los alumnos, haciendo evidente la eficacia de prácticas pedagógicas interactivas para promover un aprendizaje significativo.

Maranatha (2023) utiliza la escala de Likert para validar el modelo Clearing House, propuesto para intercambiar datos auditables en International Data Spaces en el sector logístico, alineado con los objetivos y motivaciones del estudio. Como resultado, la mayoría de los expertos considera el Clearing House una solución prometedora, tanto desde el punto de vista económico como desde el punto de vista técnico.

Moreira *et al.* (2024) analizan la utilización de juegos educativos digitales para capacitar a los estudiantes en la identificación de noticias falsas a través de la herramienta JEDi. Los resultados en estudios de caso con alumnos de la enseñanza secundaria, de grado y de posgrado demuestran la eficacia del JEDi como un instrumento para detectar noticias falsas en noticias en portugués. Para ello, se utilizó la escala de Likert para evaluar el grado de acuerdo o desacuerdo de los estudiantes.

En el Cuadro 1 se presentan los dominios y la escala de Likert utilizada en estos trabajos, resaltando su aplicación en diversos dominios para evaluar el grado de acuerdo o desacuerdo.

Cuadro 1 – Utilización de la escala de Likert en diversos dominios

Trabajo	Dominio	Utilización de la escala de Likert
Campos (2020)	Gestión de seguridad de la información en organismo público	Escala de 5 puntos
Souza *et al.* (2020)	Educación, enseñanza de contabilidad con metodologías activas	Escala de 5 puntos
Maranatha (2023)	Auditoría para el intercambio de datos en International Data Spaces	Escala de 5 puntos
Moreira *et al*. (2024)	Educación, utilización de herramienta para identificar noticias falsas	Escala de 5 puntos
Este artículo	Ciencia abierta y ciberdefensa	Escala de 5 puntos

Fuente: Elaborado por los autores (2024).

4 METODOLOGÍA DE DESARROLLO

Se realizó un estudio exploratorio en busca de soluciones que abordan la gestión de datos para la ciberdefensa en el contexto de la ciencia abierta y de conformidad con las legislaciones de protección de datos.

Dada la necesidad de acceder a datos sensibles relacionados con ciberataques para desarrollar investigaciones académicas, primero se realizó un estudio preliminar sobre la motivación de las organizaciones para ceder datos concretos con el fin de promover la ciencia abierta. También se abordó cómo se debe gestionar estos datos, sobre todo respecto a la necesidad de recuperar parte de ellos, una vez anonimizados, a través de datos de procedencia, con el fin de profundizar la investigación.

Puesto que promover la ciencia abierta en el contexto de la ciberdefensa depende no solo de técnicas de anonimización eficaces, sino también del compromiso entre las partes involucradas, el estudio buscó la opinión de expertos sobre la viabilidad de un servicio de gestión de datos sensibles, con el objetivo de intercambiar estos datos de forma segura.

La metodología aplicada en este trabajo fue precedida por una investigación bibliográfica, realizada principalmente en la base de datos Google Académico, debido a su amplio alcance. El estudio se centró en los siguientes temas: (i) ciberdefensa; (ii) ciencia abierta; (iii) protección de datos sensibles; y (iv) gestión de datos de investigación.

Así, se analizaron los principales puntos para desarrollar un proceso, los cuales se han listado y formateado como preguntas en un formulario. Las preguntas incluyen: ¿Cree que sería oportuno que exista un PGDS? ¿Qué documentos, políticas y procedimientos serían necesarios para garantizar la seguridad de la información y hacer viable el PGDS? ¿Qué factor motiva el intercambio de datos?

Al mismo tiempo, se evaluaron las siguientes cuestiones: ¿A quién y cómo se dirigirá el formulario? ¿Quiénes serían los expertos? ¿Qué preguntas (y cuántas) se deben listar? Estas ponderaciones tuvieron como objetivo recopilar opiniones de expertos acerca de las etapas necesarias para el posterior mapeo de un proceso de gestión de datos sensibles.

Dicho esto, se propuso a los expertos establecer un Programa de Gestión de Datos Sensibles, para el cual se realizó una investigación cualitativa que consideró organizaciones que monitorean el tráfico de sus respectivas redes de datos. La investigación se basó en el recopilado de opiniones de expertos, civiles y militares, que actúan en el área de ciberseguridad y/o de gestión de datos.

Para dicha investigación, se elaboraron dos formularios en la plataforma Google Forms, uno dirigido al público civil (elaborado en portugués y en inglés) y el otro dirigido al público militar. La divulgación al público civil se realizó mediante contacto directo, mientras que al público militar se realizó a través del canal institucional, mediante un documento interno del Ejército.

Finalmente, para evaluar el grado de acuerdo o desacuerdo acerca de los principales puntos que propuso el PGDS, se utilizó la escala de Likert (1932) con el objetivo de demostrar la relevancia del programa y las principales etapas de su proceso.

5 RESULTADOS

Tras divulgar los formularios para recopilar las opiniones de expertos, se obtuvieron 59 respuestas, de las cuales 40 provinieron de integrantes de organizaciones militares, pertenecientes al sector de Defensa, y 19 de civiles, provenientes del segmento académico, de la administración pública federal, de la industria y de servicios, según la Tabla 1.

Tabla 1 – Perfil de los expertos

Segmento	Académico	Administración Pública Federal	Defensa	Industria	Servicios
Total de expertos	2	2	40	2	13

Fuente: Elaborado por los autores (2024).

Debido a la significativa representatividad del sector de Defensa en las respuestas recopiladas, en este artículo solamente se analizaron las opiniones de los expertos de dicho sector. El análisis de estas opiniones puede ayudar en el desarrollo de mejores prácticas y en la colaboración interagencial para mitigar riesgos a las infraestructuras en el contexto de gestión e intercambio de datos sensibles.

Como resultado, se constató que el 92,5% de los encuestados (el 55% totalmente y el 37,5% parcialmente) estuvo de acuerdo con la existencia de una institución responsable del PGDS que realice el tratamiento, el control y el intercambio de datos sensibles anonimizados provenientes del tráfico de las redes. Esto representaría una oportunidad para investigar y desarrollar tecnologías centradas en detectar vulnerabilidades en las redes.

En este sentido, el 100% de los encuestados estuvo de acuerdo en que, para que las organizaciones se sientan seguras para compartir sus datos a través del PGDS, la institución que los atiende debe adoptar políticas como una política de seguridad de la información, política de privacidad y política de gestión de datos sensibles y de investigación, con el fin de representar el compromiso de la institución en proteger los datos, según se demuestra en la Tabla 2.

Tabla 2 – Adopción de políticas

Políticas	Totalmente de acuerdo	Parcialmente de acuerdo	Ni de acuerdo ni en desacuerdo	Parcialmente en desacuerdo	Totalmente en desacuerdo
Seguridad de la información	85%	15%	0%	0%	0%
Privacidad	87,5%	12,5%	0%	0%	0%
Gestión de datos	95%	5%	0%	0%	0%

Fuente: Elaborado por los autores (2024).

En la Tabla 3 se observa que la mayoría de los encuestados considera esencial la firma de un instrumento de colaboración para el intercambio de datos. Para ejemplificar, se citaron la celebración de un convenio y de un acuerdo de confidencialidad entre la organización y la institución, que detallan todo el tratamiento que se debe realizar con el dato, de conformidad con las normas, reglamentos y legislaciones vigentes, como la ley que promueve la protección de datos.

Tabla 3 – Necesidad de firmar un convenio y un acuerdo de confidencialidad

Totalmente de acuerdo	Parcialmente de acuerdo	Ni de acuerdo ni en desacuerdo	Parcialmente en desacuerdo	Totalmente en desacuerdo
85%	7,5%	2,5%	5%	0%

Fuente: Elaborado por los autores (2024).

Para permitir al investigador acceder a una instancia del conjunto de datos sensibles, garantizando al mismo tiempo la seguridad de la información, se sugirió que se entregaran tres conjuntos de documentos: comprobante oficial de vínculo con una institución académica, proyecto de investigación y currículo Lattes, ORCID o equivalente. La Tabla 4 muestra el grado de acuerdo o desacuerdo de los encuestados acerca de la afirmación de que presentar dichos documentos favorecería la seguridad de la información.

Tabla 4 – Documentos comprobatorios del investigador

Documento	Totalmente de acuerdo	Parcialmente de acuerdo	Ni de acuerdo ni en desacuerdo	Parcialmente en desacuerdo	Totalmente en desacuerdo
Vínculo	95%	2,5%	0%	2,5%	0%
Proyecto	82,5%	12,5%	5%	0%	0%
Currículo	55%	27,5%	17,5%	0%	0%

Fuente: Elaborado por los autores (2024).

Una vez recibidos los documentos, se sugirió analizar la relevancia de la investigación para la comunidad científica, considerando como criterios el riesgo de acceso a los datos y el cumplimiento de las políticas de seguridad de la información, de privacidad y de gestión de datos sensibles y de investigación. La Tabla 5 muestra el grado de acuerdo o desacuerdo de los encuestados acerca de la afirmación de que se deben realizar dichos análisis en el proceso.

Tabla 5 – Análisis de los documentos

Análisis	Totalmente de acuerdo	Parcialmente de acuerdo	Ni de acuerdo ni en desacuerdo	Parcialmente en desacuerdo	Totalmente en desacuerdo
Riesgo	57,5%	25%	12,5%	5%	0%
Cumplimiento	87,5%	5%	7,5%	0%	0%

Fuente: Elaborado por los autores (2024).

También se preguntó a los expertos sobre la necesidad de que la institución que gestiona los datos emita un dictamen técnico. Dicho dictamen, destinado a evaluar la organización que compartió

los datos con el PGDS, expondría la viabilidad técnica y el cumplimiento de los requisitos necesarios para el intercambio seguro. En este caso, se obtuvieron las respuestas que constan en la Tabla 6.

Tabla 6 – Necesidad de emitir un dictamen técnico

Totalmente de acuerdo	Parcialmente de acuerdo	Ni de acuerdo ni en desacuerdo	Parcialmente en desacuerdo	Totalmente en desacuerdo
72,5%	17,5%	10%	0%	0%

Fuente: Elaborado por los autores (2024).

Si la organización aprueba el acceso a los datos sensibles, se sugiere que se firmen dos acuerdos, para garantizar la protección de los datos: un nuevo acuerdo de confidencialidad entre el PGDS y la organización, y un acuerdo de confidencialidad entre el PGDS y el investigador. La Tabla 7 muestra el grado de acuerdo o desacuerdo de los encuestados respecto a la necesidad de firmar dichos acuerdos.

Tabla 7 – Necesidad de firmar acuerdos de confidencialidad

Acuerdo	Totalmente de acuerdo	Parcialmente de acuerdo	Ni de acuerdo ni en desacuerdo	Parcialmente en desacuerdo	Totalmente en desacuerdo
Entre el PGDS y la organización	77,5%	10%	7,5%	2,5%	2,5%
Entre el PGDS y el investigador	82,5%	12,5%	2,5%	0%	2,5%

Fuente: Elaborado por los autores (2024).

Una vez firmados los acuerdos, la institución asume la responsabilidad de garantizar el control adecuado de seguridad al compartir los datos sensibles directamente con el investigador solicitante. En este contexto, los controles evaluados por los expertos se refieren al acceso a los datos en un entorno seguro y durante un período determinado, y el 92,5% de los encuestados estuvo de acuerdo con esta afirmación (el 82,5% totalmente y el 10% parcialmente).

Finalmente, se buscó identificar motivaciones para que las organizaciones compartan sus datos sensibles, presentándose las siguientes sugerencias: notificación sobre datos sensibles anonimizados y publicados en el repositorio; recepción de informes estadísticos sobre el acceso al conjunto de datos compartido; y recepción de informes sobre las investigaciones realizadas con el acceso a sus datos sensibles. En la Tabla 8 se presenta la opinión de los encuestados acerca de dichas motivaciones.

Tabla 8 – Motivaciones para el intercambio de datos

Motivación	Totalmente de acuerdo	Parcialmente de acuerdo	Ni de acuerdo ni en desacuerdo	Parcialmente en desacuerdo	Totalmente en desacuerdo
Notificación de publicación	65%	27,5%	5%	2,5%	0%
Informes estadísticos	62,5%	25%	12,5%	0%	0%
Informes de investigaciones	75,0%	25%	0%	0%	0%

Fuente: Elaborado por los autores (2024).

Tras analizar los resultados presentados en todas las tablas, se pudo comprobar que la mayoría de los expertos consultados se muestra favorable a todas las propuestas presentadas en este trabajo respecto al PGDS. Esto indica que implementarlo puede ser una forma de garantizar el compromiso de la institución con la seguridad de la información y la protección de datos.

6 CONSIDERACIONES FINALES

Los resultados demuestran que los expertos apoyan la implementación de un Programa de Gestión de Datos Sensibles. El alto grado de acuerdo, del 92,5%, respecto a la importancia de contar con una institución responsable del tratamiento, control e intercambio de datos sensibles anonimizados revela la necesidad de una mayor fundamentación en este proceso. Esta iniciativa facilitaría tanto la investigación como la innovación en el desarrollo de nuevas tecnologías para detectar vulnerabilidades en las redes.

Otro punto que destacar es la unanimidad (el 100%) respecto a la necesidad de adoptar políticas, como las de seguridad de la información, de privacidad y de gestión de datos sensibles, para garantizar la protección de la información y mitigar los riesgos asociados al tratamiento de datos sensibles. Este consenso entre los encuestados resalta el papel esencial que desempeñan estas políticas en la creación de una estructura confiable y transparente, que es necesaria para la cooperación entre las organizaciones y el PGDS.

Este enfoque está alineado con la Estrategia Nacional de Ciberseguridad, que subraya la importancia de establecer mecanismos de intercambio de información sobre ciberincidentes. Sin embargo, el análisis crítico de este punto sugiere que implementar estas políticas no solo debe ser un compromiso formal, sino que también debe incluir mecanismos de auditoría y revisión continua para garantizar los resultados esperados, así como la adopción de otras políticas o procedimientos de seguridad.

En cuanto a la exigencia de instrumentos de colaboración, los resultados indican que la mayoría de los expertos considera esta medida importante, lo que demuestra preocupación por la seguridad y el cumplimiento legal en el intercambio seguro de los datos. Sin embargo, se puede cuestionar la viabilidad a largo plazo de dicha exigencia, visto que puede aumentar la complejidad del proceso, siendo necesario equilibrar los procedimientos administrativos con la accesibilidad.

La presentación de documentos comprobatorios por parte de los investigadores fue ampliamente apoyada, visto que representa un factor de confianza en el proceso para conceder acceso a datos sensibles. Esto refleja la preocupación por controlar y proteger la información. Sin embargo, aunque estos documentos garantizan la legitimidad de las investigaciones, también plantean el desafío de equilibrar la seguridad con la agilidad deseada, sobre todo por parte de los investigadores. La necesidad de emitir un dictamen técnico y la responsabilidad de la institución de proporcionar un entorno seguro para el acceso a los datos también son aspectos fundamentales para garantizar la integridad del proceso.

Finalmente, las motivaciones presentadas por los expertos, como la notificación sobre datos anonimizados y la recepción de informes de investigación, demuestran que existe un interés en colaborar con la investigación científica, siempre que se respeten los requisitos de seguridad de la información y de privacidad. Así, implementar un PGDS puede no solo contribuir a la innovación

y al avance de la investigación tecnológica, sino también apoyar la creación de una cultura de intercambio seguro de datos. De hecho, los requisitos preliminares para su implementación pueden inferirse a partir de las cuestiones abordadas en el formulario.

Además, aunque los resultados son prometedores, hay que reconocer algunas limitaciones. Este artículo se centró en analizar únicamente las opiniones de los expertos del sector de Defensa, lo que puede no reflejar la diversidad de opiniones presentes en otros sectores que también tratan datos sensibles. El análisis cualitativo, basado únicamente en las opciones preestablecidas de la escala de Likert, podría profundizarse con métodos adicionales, con el objetivo de captar mejor las opiniones y sugerencias de los participantes.

La investigación tampoco aborda en profundidad las implicaciones prácticas de la implementación del PGDS, como la arquitectura que garantizará la seguridad tanto en el almacenamiento como en el acceso a los datos anonimizados, los desafíos del cumplimento de la LGPD y los aspectos éticos y administrativos del intercambio de datos sensibles a gran escala, que son temas que se pueden investigar en estudios futuros.

Los resultados demuestran que las medidas propuestas para el PGDS son ampliamente aceptadas por los expertos, mientras que la implementación de medidas técnicas y administrativas para la gestión de datos sensibles asegura la transparencia y la responsabilidad en el intercambio seguro, lo que promueve una cultura colaborativa en la ciencia abierta.

REFERENCIAS

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.