Artificial Intelligence Report

Ref. 2025/2026

1. ARTIFICIAL INTELLIGENCE:

Cemig recognizes Artificial Intelligence (AI) as a strategic technology for driving innovation, improving operational efficiency, enhancing competitiveness, and increasing service quality. The adoption of AI aims to ensure positive and sustainable impacts for both the Company and society, while adhering to ethical principles and sound governance practices.

Cemig has an Artificial Intelligence Policy that includes principles and guidelines related to the use and governance of AI. The policy can be accessed on the Company's website at: ARTIFICIAL INTELLIGENCE POLICY (AI)

2. GOVERNANCE:

The governance of AI solutions is the responsibility of the Information Technology Vice Presidency (VPI), which is tasked with classifying and managing these solutions according to their criticality and organizational objectives.

Cemig adopts specific processes to ensure the governance and security of AI solutions under its management, maintaining appropriate levels of protection and compliance:

- **Governed AI Solutions Management:** The Information Technology area is responsible for the classification and management of governed AI solutions.

- **Governed AI Risk Management:** AI risk management is conducted based on the corporate risk map maintained by the Compliance area, enabling the identification, assessment, and mitigation of potential vulnerabilities.

- **Governed AI Solutions Performance Management:** Responsibility for monitoring the performance and outcomes of governed AI solutions lies with the business area to which the solution is assigned, ensuring its effectiveness and strategic alignment. Whenever adjustments or corrective actions are required, the Information Technology area must be formally engaged to assess the situation and implement the necessary measures.

- **Awareness and Training:** The People Management area, in collaboration with the Information Technology and Innovation areas, is responsible for implementing awareness and training programs that foster a culture of development and promote the responsible and ethical use of AI throughout the Company.

3. PROGRAMS:

The Company has a Responsible Artificial Intelligence Program, with emphasis on the following initiatives:

3.1 Limiting Access to Sensitive AI Capabilities

Access to sensitive AI capabilities including, but not limited to, facial recognition, biometric identification, surveillance, automated monitoring, and behavioral analysis is restricted, controlled, and authorized only when there is a legitimate purpose, demonstrated need, and alignment with organizational objectives.

AI solutions are developed, classified, and managed according to their level of criticality, in compliance with information security, data protection, confidentiality, and privacy standards.

For example, the AI solution specialized for the electric power sector developed through the ANEEL R&D Program was designed to enable the inclusion of Cemig's sensitive information while maintaining strict security controls. To ensure data security, the system supports multiple user-classification levels. These classifications range from role-based assignments to document sensitivity levels and access-group permissions.

Figures 1, 2, and 3 below illustrate some of the controls implemented by Cemig to limit access to sensitive AI capabilities.

- **Figure 1** presents the user-creation interface available to system administrators, including the option to assign administrative privileges or standard-user permissions.

- **Figure 2** highlights the user-group management interface, which determines the data groups to which each user is granted access.

- **Figure 3** shows the controls for document expiration dates and sensitivity levels. These controls help maintain restricted access to specific documents, even for users belonging to an authorized group, limiting access to designated key users when necessary.

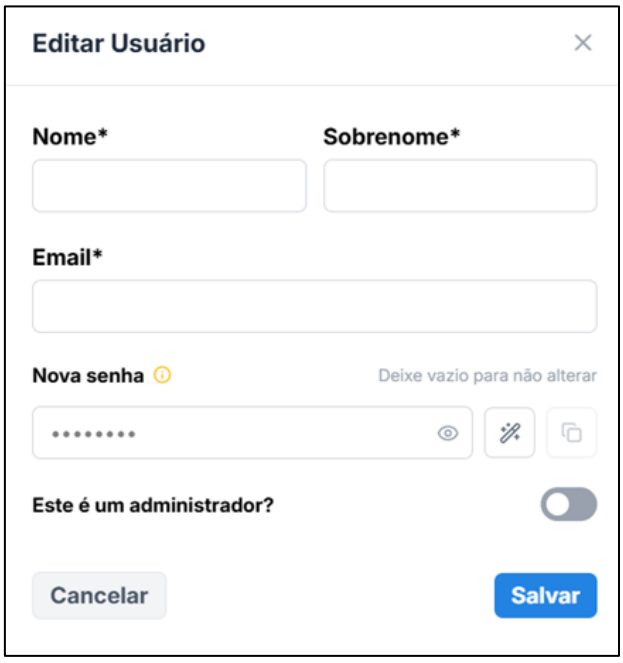

Figure 1 – User Assignment and Password Reset Control.

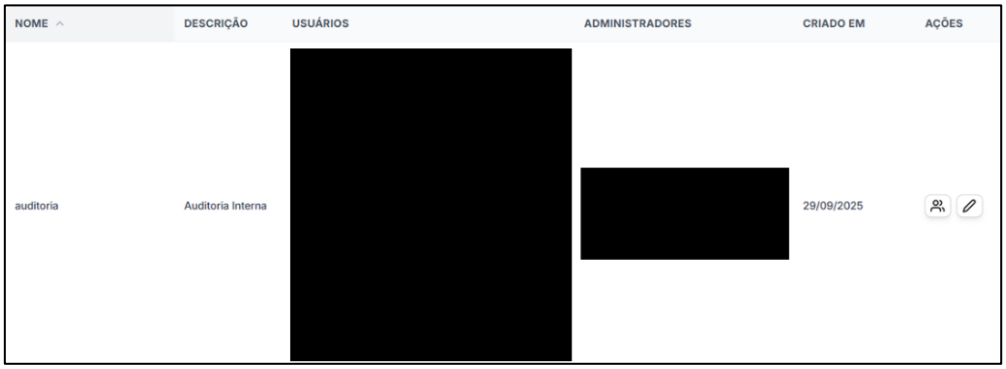

Figure 2 – User Grouping Control. The black bars were added to conceal the names of actual users and system administrators.

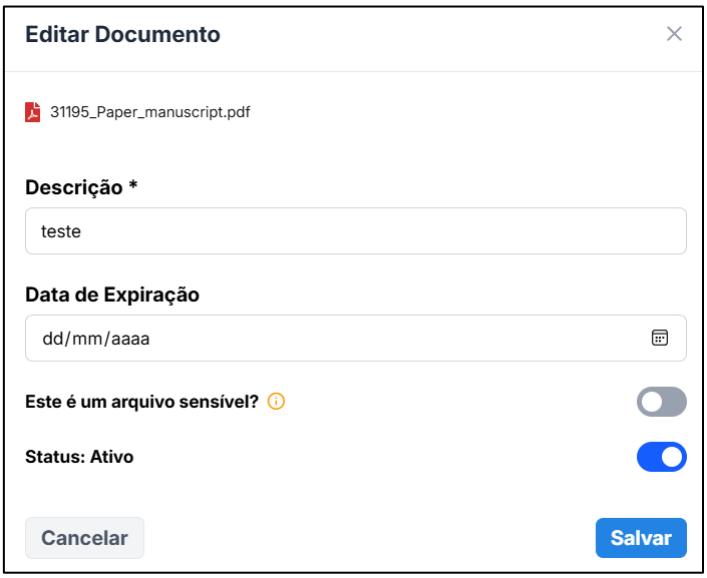

Figure 3 – Access Control for Documents Stored in the Database.

In corporate and operational environments, only properly governed, approved, and monitored AI solutions may be used, whether they are deployed on proprietary servers or on systems with continuous access to corporate data.

The assessments are carried out by various Cemig teams, including IT, data privacy, regulatory affairs, and any other area deemed relevant. In addition, at the time of contracting, suppliers are required to sign an agreement acknowledging the confidentiality of the data and committing to provide all necessary guarantees.

3.2 Distinct Labeling of AI-Generated Content and AI-Based Decision Outcomes

As established in the AI Policy, regarding explainability and transparency, transparency, identification, and clear communication practices must be adopted to enable users, data subjects, and other stakeholders to recognize, whenever applicable, when content has been generated, modified, or supported by AI, as well as when a decision, recommendation, or outcome resulted from automated processing or an AI-based solution.

Furthermore, regarding traceability and auditing, it is established that activities related to the development, deployment, and use of AI solutions must be properly documented. This documentation must enable the auditing and traceability of automated decisions.

3.3 Mechanisms for Detecting and Correcting AI Model Drift or Degradation Over Time

Governed AI solutions must undergo periodic testing and technical and functional reviews to identify any misalignment with the principles established in the Artificial Intelligence Policy.

For models developed by Cemig and its partners, adjustments are continuously made based on updates to the underlying datasets and feedback from internal users. When necessary, new specialized assistants may also be made available to address emerging demands resulting from regulatory changes.

Figures 4 and 5 present examples of the management of the files that comprise the dataset used by the model, as well as the additional feedback interface, through which users can provide written comments to explain positive and/or negative aspects of an AI-generated response.

Figure 4 – Example of Data Repository Control.

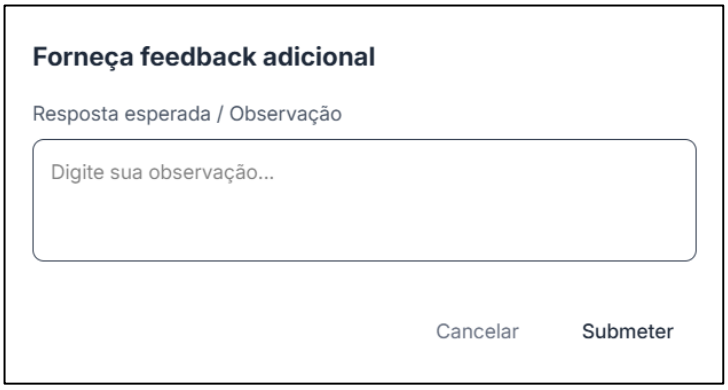

Figure 5 – Additional Feedback Screen Displayed After a Positive or Negative Evaluation of an AI-Generated Response.

The management of the results generated by governed AI solutions is the responsibility of the business area to which the application is linked. This area is responsible for monitoring the outputs produced, ensuring efficiency and strategic alignment. Whenever the need for adjustments or corrections is identified, a technical assessment and the definition of the necessary corrective actions may be formally requested.

For Cemig's proprietary systems, efforts are being made to implement tools aimed at monitoring the quality of AI models. The following image (Figure 6) presents an example of a monitoring dashboard, including performance indicators by activity and usage metrics.

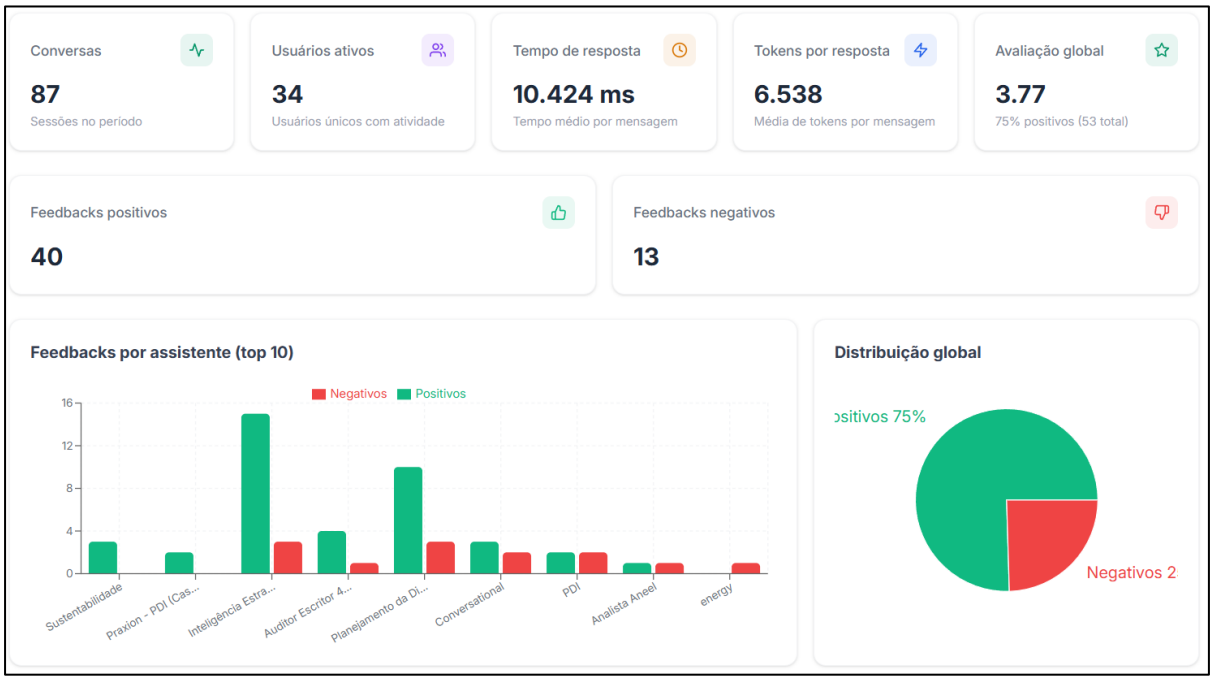

Figure 6 – Dashboard for Monitoring Response Quality and System Performance.

3.4 Regular Evaluations of Deployed AI Models for Fairness and Bias

As established in the principle of “Ethics, Fairness, and Inclusion” described in the AI Policy, AI solutions must be developed and applied in an ethical, responsible, and inclusive manner, ensuring that they are fair, inclusive, and free from discrimination and bias, while respecting human rights and promoting diversity.

Governed AI solutions must undergo periodic testing, validation, and reviews to verify their compliance with the principles established in the Artificial Intelligence Policy.

To ensure that the development of new initiatives — such as products, services, projects, or systems involving the processing of personal data — complies with the requirements of Brazil’s General Data Protection Law (Law No. 13,709/2018 – LGPD), Cemig adopts the Privacy by Design (PbD) methodology.

This assessment also considers the potential use of Artificial Intelligence tools and the implementation of mechanisms designed to mitigate risks, including possible cases of algorithmic discrimination against data subjects, as illustrated in Figures 7 and 8 below.

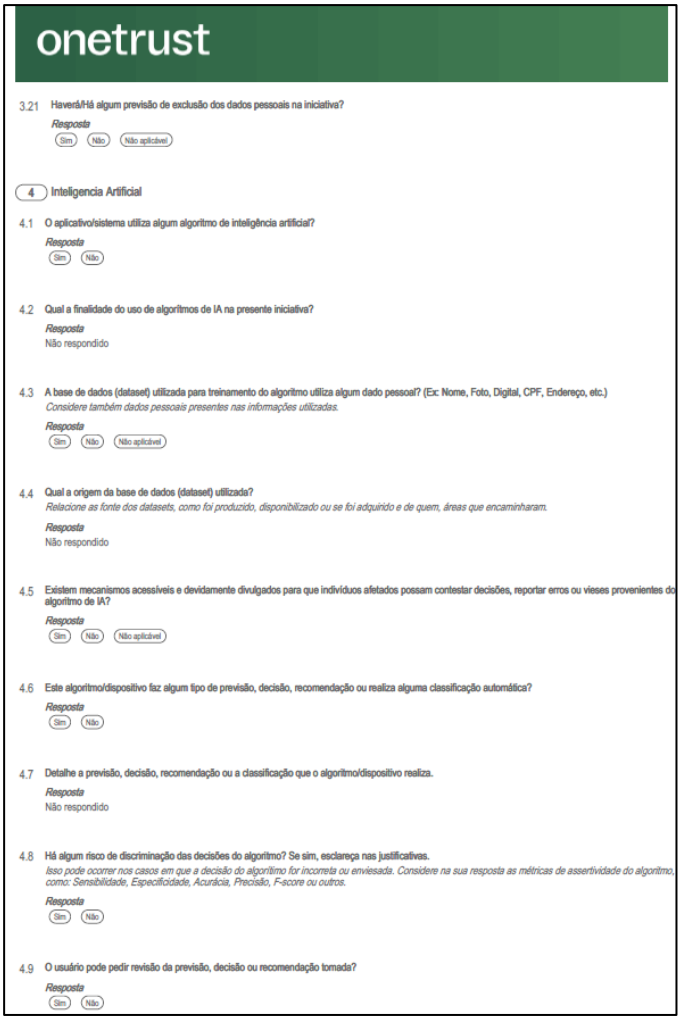

Figure 7 – Screen for the Regular Evaluation of Deployed AI Models.

Figure 8 – Screen for the Regular Assessment of Discrimination Risk in AI Models Prior to Deployment.

3.5 Initiatives (Internal and Vendor-Led) to Reduce the Environmental Footprint of Data Centers and AI Models

As established in the principle of **"Sustainability and Social Impact"** described in the AI Policy, the development and use of AI solutions must take into account their environmental and social impacts, particularly with regard to energy consumption, the use of computing resources, and the efficiency of the models employed.

Whenever applicable, the evaluation, procurement, and operation of AI solutions must consider sustainability criteria, energy efficiency, responsible scalability, resource reuse, reduction of computational waste, and suppliers' commitment to sound environmental practices. These measures should seek to balance innovation, performance, security, cost, environmental impact, and the creation of social value.

3.6 Appeals Process for Users/Third Parties Affected by an AI Decision or Outcome

Transparency and explainability practices must be adopted to enable users to understand, whenever possible and applicable, when a decision, recommendation, or outcome has been produced, influenced, or supported by an AI solution.

Activities related to the development and use of AI solutions must be properly documented, enabling audits and the traceability of automated decisions.

As established under "Application and Guidelines," Cemig adopts specific processes to ensure the governance and security of governed AI solutions, providing appropriate levels of protection and compliance. Under "Management of Results of Governed AI Solutions," it is stated that responsibility for monitoring the results of governed AI solutions lies with the business area to which the solution is assigned, ensuring its efficiency, compliance, and strategic alignment. If inconsistencies, undue impacts, failures, or the need for adjustments are identified, the VTI must be formally engaged to conduct a technical assessment and implement the necessary corrective actions.

3.7 Quantification of the Impact of AI Initiatives/Tools on Sustainability Outcomes

As mentioned previously, under the principle of "Sustainability and Social Impact" described in the AI Policy, the development and use of AI solutions must take environmental and social impacts into account, seeking solutions that reduce resource consumption and promote social well-being.

Currently, systems that use artificial intelligence to support sustainability-related activities are under development. One example is the identification of bottlenecks in the rural power grid, with the objective of enabling the electrification of processes that currently depend on diesel fuel. This initiative is the result of an open innovation challenge, presented in Figure 9 below, and is currently in the development phase.

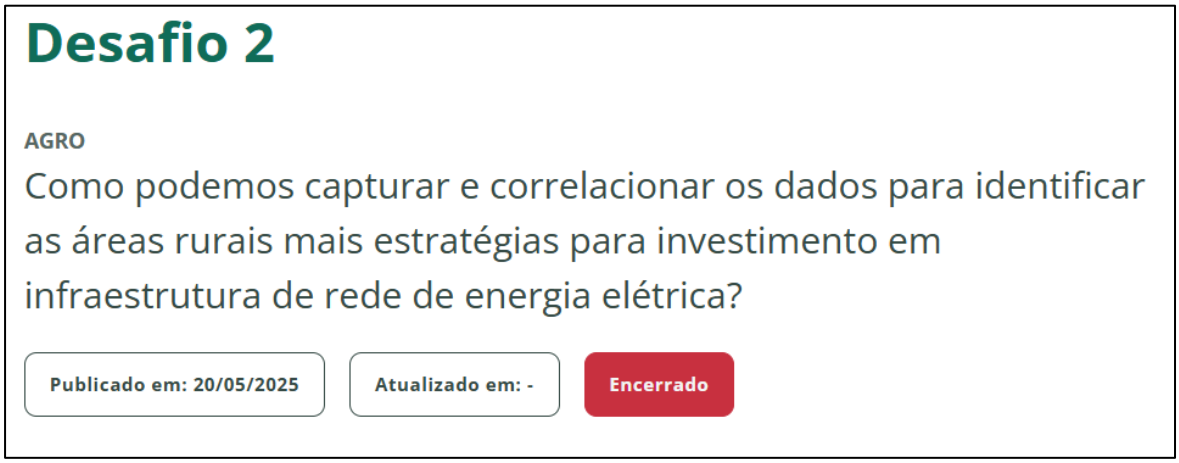

Figure 9 – Challenge Launched by Cemig Through Its Innovation Program Focused on Identifying the Decarbonization Potential of Rural Activities Using AI.

The project developed under this challenge deserves special attention for its use of artificial intelligence to identify customers with high diesel consumption for electricity generation due to limitations in the adequate supply of power through Cemig's distribution network. This situation may result in emissions of up to 800 gCO_2/kWh, whereas the use of electricity could reduce this level to approximately 140 gCO_2/kWh under favorable conditions.

Considering an estimated unmet demand of more than 500 MW in the agricultural sector of Minas Gerais, replacing diesel-powered generation with the electrification of these processes could lead to a reduction of up to 82.5% in emissions per kWh consumed, making it one of the initiatives currently showing the greatest potential for positive environmental impact.

3.8 Employee Training on the Ethical and Secure Use of AI

To promote ongoing awareness of the ethical, responsible, and secure use of artificial intelligence, the Company provides learning, training, and upskilling opportunities for its employees and other internal stakeholders involved in the development, deployment, operation, or use of AI solutions.

As established in the principle of "Operational Security and Cybersecurity" described in the AI Policy, AI solutions must be implemented with robust security measures to prevent vulnerabilities and ensure that they do not pose risks to the Company's operations, protecting against cyberattacks and unauthorized access. To this end, employees must be guided regarding the procedures, controls, and expected conduct for the secure use of these solutions.

Cemig also adopts specific processes to ensure governance and security, providing appropriate levels of protection and accountability, as described in the AI Policy under the principle of "Accountability," according to which the responsible use of AI solutions is the duty of every employee, contractor, supplier, consultant, and partner of the Company.

Furthermore, as established in the “Application and Guidelines” and “Awareness and Training” sections of the AI Policy, the Company must maintain processes focused on the governance and security of governed AI solutions, as well as implement awareness and training programs. These initiatives must be conducted by the People Management area in collaboration with the Information Technology and Innovation areas, with the objective of strengthening the culture of ethical AI development and use at Cemig.

To keep employees engaged in best practices for the use of artificial intelligence and to encourage skill development in the use of these tools, Cemig regularly promotes events and distributes educational materials on the subject.

Figure 10 presents one of the most recent events organized by the Company, during which applications of the AI platform developed for Cemig were demonstrated. The initiative reached more than 300 participants, including both employees and contractors.

Figure 10 – Announcement of a Workshop Through Cemig’s Internal Portal, Accessible to All Employees.