NO.78 – Artificial Intelligence Governance

Directory: Information Technology
Area: IT Governance and Architecture

Creation: 13/03/2025
Last update: 13/03/2025

1. OBJECTIVE

Establish rules and mechanisms to ensure the development and use of Artificial Intelligence (AI) solutions in an ethical, transparent, responsible, and sustainable manner at Dexco, in accordance with the General Personal Data Protection Law (LGPD) and other applicable legislation. In addition to promoting legal compliance and respect for privacy, this document reinforces the integration of Responsible AI principles into the areas of Architecture, IT Infrastructure, Information Security, Legal, and Business Partners (BPs), aligning AI solutions with corporate goals and ESG (Environmental, Social, and Governance) pillars.

2. COVERAGE

This document applies to all areas of the Company, its managers and employees, as well as to third parties who may be hired by Dexco and who represent it in the referred activities.

3. REFERENCES

- NO.72 – Data Governance – Personal Data Treatment (LGPD)
- NO.74 – Software Inventory Update Process
- General Personal Data Protection Law (LGPD) – Law nº 13.709/2018
- PO.19 – Information Security
- PGI – Information Security Incident Management Plan
- PO.23 – Data Governance and Privacy
- NO.15 – Document Archiving
- NO.40 – Contracts
- NO.41 – Hiring Service Providers and Suppliers
- NO.44 – Application of Disciplinary Measures

- NO.52 – Supply Chain
- NO.56 – IT Access Management
- NO.57 – Use of Microcomputer Resources
- NO.58 – Information Classification
- NO.63 – Backup and Restore Management
- Dow Jones Sustainability Indices (DJSI) – Reference Guide for Sustainable Artificial Intelligence

4. DEFINITIONS

- **Algorithm**: A set of well-defined instructions or rules for solving a problem or performing a specific task. In the context of AI, it refers to the computational method that processes data to generate predictions or make decisions.
- **Machine Learning**: A subset of AI consisting of algorithms capable of learning from data and making predictions or decisions without being explicitly programmed for each situation.
- **Deep Learning**: A subcategory of Machine Learning that uses deep neural networks. It allows the learning of data representations at different levels of abstraction and is highly effective in complex tasks such as natural language processing and computer vision.
- **Generative Model**: A type of AI model that learns to probabilistically distribute input data and can generate new samples that resemble the original information. Examples include Generative Adversarial Networks (GANs) and Large Language Models (LLMs).
- **Artificial Neural Network:** A structure inspired by the human brain, composed of interconnected artificial neurons capable of processing information and learning complex patterns from input data.
- **Natural Language Processing, NLP**: A field of AI focused on the interaction between computers and human language (spoken or written), enabling text analysis, speech comprehension, machine translation, among others.
- **Large Language Models – LLMs**: AI models trained on extensive text databases, capable of understanding and generating natural language in a coherent manner. They are applied in various solutions for conversation, sentiment analysis, content generation, and much more.
- **Personal Data**: Any information related to an identified or identifiable natural person, as defined by the LGPD (Law No. 13,709/2018). This includes data such as name, email address, social security number, address, as well as sensitive data (racial or ethnic origin, religious beliefs, political opinions, etc.).
- **Privacidade by Design**: A principle that emphasizes data protection and privacy as essential requirements in all stages of the design, development, and implementation of an AI solution or project.
- **Information Security**: A set of controls and practices designed to protect confidentiality, integrity, and availability of data and systems, ensuring protection against threats, unauthorized access, and leaks.
- **AI Life Cycle**: Covers the phases of design, risk assessment, development, implementation, validation, continuous monitoring, and, if applicable, decommissioning or change of purpose. Each stage involves specific requirements for security, privacy, and alignment with internal standards and applicable laws.
- **AI Impact Analysis**: An assessment process that identifies legal, ethical, and privacy risks in the use of AI, including potential biases and impacts on ESG. It involves the application of the AI Impact Assessment Form (Annex III) provided for in the Standard.
- **AI Bias**: The tendency of an algorithm or model to make biased or unfair decisions due to imbalances in training data or processing logic. This can result in discrimination or unequal treatment of specific groups.
- **Explainability**: The ability of an AI model to provide an understandable justification for its predictions, recommendations, or actions. Transparency is essential to ensure trust and compliance with the LGPD and other rights protection standards.

- **Anonymization**: Process of removing or modifying information in a data set so that the individual cannot be identified, either directly or indirectly. It is one of the practices that help protect personal data in AI solutions.
- **Pseudonymization**: Technique of replacing data that directly identifies the data subject (such as name or social security number) with artificial identifiers (pseudonyms), reducing the risk of linking the data to a specific person, but still allowing re-identification under certain conditions.
- **Data Lake**: Centralized repository of raw data in various formats and sources, used for advanced analytics, including AI applications. Its architecture seeks flexibility and scalability for storing large volumes of data.
- **Scalability**: The ability of a system (infrastructure, data architecture, etc.) to adapt to growth in demand or data volume while maintaining adequate performance without compromising security and reliability.

5. ROLES AND RESPONSIBILITIES

5.1 AI Governance Group

- **Mission:** Define the Company's AI strategy, ensuring alignment with the principles of Responsible AI, privacy and data protection guidelines, and other applicable guidelines.

- **Responsibilities:**
    - Evaluate and approve high-impact AI projects;
    - Ensure adherence to this Standard by reviewing processes and providing guidance to the areas involved;
    - Conduct periodic reviews of AI maturity and governance, proposing continuous improvements;

5.2. Information Technology Business Partner (IT BP)

- Act as a link between the business area and technical areas (Architecture, IT Infrastructure, Information Security, Legal, Privacy, among others);
- Promote communication and engagement among all stakeholders in AI projects;
- Assist in defining business requirements.

5.3. Architecture

- Align strategic direction based on business capabilities with implementations at the operational level;
- Support technology inventory management by documenting applications, tools, LLMs, and other technological components;
- Define and monitor the base architecture of AI solutions, ensuring efficiency, scalability, and technical compliance;
- Evaluate performance and resilience aspects, preventing slowness, instability, and vulnerabilities;
- Cooperate with technical areas to integrate robust and secure solutions.

5.4. IT Infrastructure

- Align strategic direction based on business capabilities with implementations at the operational level;
- Support technology inventory management by documenting applications, tools, LLMs, and other technological components;
- Define and monitor the base architecture of AI solutions, ensuring efficiency, scalability, and technical compliance;
- Evaluate performance and resilience aspects, preventing slowness, instability, and vulnerabilities;
- Cooperate with technical areas to integrate robust and secure solutions.

5.5. Information Security

- Define and validate security controls (access, encryption, etc.), monitoring threats;
- Protect user data and privacy, ensuring the integrity of AI systems;
- Manage AI risks and incidents that impact the confidentiality, integrity, and/or availability of information, in accordance with the PGI-SI - Information Security Incident Management Plan, attached to PO.19 Information Security and other related standards;
- Activate the Data Privacy team in the event of AI incidents involving personal data and/or violations of data subjects' rights;
- Cooperate with technical areas to integrate robust and secure solutions;
- Promote ongoing information security training, education, and awareness programs for all employees who use AI resources in their daily activities;
- Define and validate secure authentication mechanisms for critical operations and access to AI systems with or without human interaction;
- Ensure robust security measures to protect AI infrastructure against cyber threats, including firewalls, access control, network monitoring, and intrusion detection.

5.6. Legal

- Ensure the legal compliance of AI solutions (LGPD, sectoral laws, contracts, etc.);
- Mitigate legal risks through contractual clauses and civil liability verification;
- Protect and manage intellectual property rights and copyrights related to AI projects;
- Provide guidance on national and international laws and regulations applicable to AI;
- Cooperate with technical areas to integrate robust and secure solutions.

5.7. General Employees

- Comply with the guidelines of this standard;
- Contact the IT BP responsible for your area, as well as technical areas when necessary, to ensure alignment with the principles of Responsible AI, privacy and data protection guidelines, and other applicable guidelines;
- Respect the recommendations provided by the technical areas and report non-compliance;
- Participate in training on AI, privacy and data protection, information security, and other applicable topics;
- Report suspected or confirmed incidents, in accordance with the guidelines of PO.19 Information Security and NO.72 Data Governance – Personal Data Processing.

5.8. Data & Analytics

- Support the construction and/or validation of specific data for AI;
- Verify that the databases used are from reliable and validated sources;
- Mitigate risks of problems with information within internal data processes;
- Validate and, when necessary, internalize acquired information by making it available to the requesting area or project;
- Support the Privacy Area with adjustments related to the use of personal data and/or sensitive personal data, when necessary;
- Cooperate with technical areas to integrate robust and secure solutions.

5.9 Data Privacy and *DPO – Data Protection Officer*

- Develop rules and provide guidelines for evaluating projects and processes involving the use of personal data and/or sensitive personal data, in which AI is used, in accordance with the LGPD and applicable regulations;
- Support the responsible and technical areas in adopting Privacy by Design measures during the life cycle of AI projects;
- Provide, in the process of fulfilling the rights of data subjects, information related to data processing in AI solutions;
- Ensure the recording of processing operations related to processes involving AI in the corporate Data Inventory (RoPA - Record of Processing Activities), with the preparation of complementary documents, such as Legitimate Interests Assessment (LIA) and Data Protection Impact Report (RIPD), when applicable;
- Report to the Privacy and Data Protection Committee on projects and processes involving AI, when applicable;
- Cooperate with technical areas to integrate robust and secure solutions.

6. AI GOVERNANCE PROCESS

To ensure that AI initiatives at Dexco are beneficial and aligned with corporate and social values, the following fundamental principles are adopted:

1) Respect Privacy and Data Protection: comply with the LGPD and corporate privacy and data protection guidelines, seeking the appropriate treatment of personal and sensitive data used in AI models.

2) Ensure Transparency: Clearly specify when interactions or content are generated by AI. AI must be developed, trained, and used ethically, with clear documentation and availability of information about its operation, ensuring the protection of intellectual property rights.

3) Protect Cybersecurity: Meet the security requirements described in PO.19, mitigating vulnerabilities and risks associated with the use of AI algorithms and their processing environments, as well as enabling the repair of damage in the event of failures.

4) Avoid Bias and Discrimination: Develop and maintain AI models that are fair, inclusive, and free from discriminatory biases, ensuring that automated analyses and decisions do not negatively affect social groups or minorities.

5) Multidisciplinary Collaboration: Promote the integration of technical, legal, cybersecurity, business, and other areas when necessary to ensure that AI is applied safely, effectively, and in compliance with current laws and regulations.

6) Contribute to ESG Goals: Promote AI initiatives that support energy efficiency, reduction of environmental impacts, improvement of social relations, and strengthening of corporate governance, in line with Dexco's commitments to sustainability and innovation.

6.1. Design

- The IT BP and the Requesting Area define the scope, objectives, and expected benefits of the AI project.

6.2. Risk Evaluation

- The proposal is submitted to the technical areas, which assess risks and legal impacts, in addition to providing the necessary technical support before, during, and after the implementation of solutions involving AI.

6.3. Development and Implementation

- Apply the guidelines provided by the technical areas, performing tests and validations to minimize the identified risks.

procedures described in the applicable standards must be observed.

6.4. Validation and Continuous Monitoring

- Conduct tests to assess any deviations in the use of AI and possible negative impacts they may cause; environmental (use of computational resources, energy efficiency) and social outcomes;
- Implement monitoring metrics (KPIs) that measure effectiveness, ESG impact, and adherence to privacy and security requirements.

6.5. Use of AI for ESG Goal

- **Environmental:** AI solutions that optimize energy, reduce waste, or support sustainable logistics should be documented and monitored with specific indicators (e.g., X% reduction in energy consumption).
- **Social:** AI projects that promote inclusion and diversity, improve working conditions, or analyze employee and customer satisfaction should be transparent about the criteria and algorithms used.
- **Governance:** AI applied to compliance, fraud identification, and risk assessment in the supply chain must be in line with the guidelines of this standard, fostering a culture of corporate responsibility and ethics.

6.6. Deactivation or Change of Purpose

- Consult Data Privacy and Information Security Areas for the secure discontinuation of the data used (disposal, anonymization, pseudonymization, etc.), in accordance with corporate privacy and data protection guidelines;
- Inform Data Privacy Area about the discontinuation of the process or change of purpose involving personal data and/or sensitive personal data.

6.7. Third-Party Management and Maturity Assessment

- In cases where suppliers or partners are involved in the implementation or processing of AI solutions, the corporate

7. PUBLICITY AND TRANSPARENCY

Dexco will publish a summary of this AI Standard and its principles on its corporate website (or intranet, in a public area), demonstrating its commitment to privacy, security, and ESG values.

8. PENALTIES

Failure to comply with the guidelines of this document will be subject to the application of appropriate disciplinary measures.

9. VALIDITY

This document shall come into force on the date of its publication and shall be reviewed every two (2) years or whenever there is a relevant change in AI procedures, applicable laws, or best market practices.

10. APPROVAL

This document was developed by the Architecture department and approved by the Information Technology Board.

11. APPENDIX

1. Appendix I – AI Project Assessment Guide

Framework for BPs and employees to understand the minimum requirements necessary to structure an AI project effectively, observing privacy and security issues at each stage (design, development, implementation, and monitoring).

Assessment Guide

2. Appendix II – AI Impact Assessment Form

Tool that supports areas in defining the purpose of the project, specifying the types of data involved, adopting risk mitigation mechanisms, and complying with applicable legal obligations, in accordance with NO.72, when contracting suppliers that offer AI solutions.

Impact Assessment Form

DEXCO

Deca Portinari Hydra Duratex Castelatto Ceusa Durafloor