árido software	AI Usage Policy	Code: PO-0
		Version: 0
		Date: 01-04-2026

Artificial Intelligence Usage Policy

Comentado [GC1]: aclarar reglas de como configurar las IA Tools para que no pushee codigo a nombre de la IA

1. Objective

The objective of this policy is to define the guidelines and controls for the responsible, secure, and ethical use of Artificial Intelligence (AI) tools within the organization, ensuring protection of company information, client data, and intellectual property.

2. Scope

This policy applies to:

- All employees, contractors, and third parties working with or on behalf of the organization.
- All AI tools and platforms, including but not limited to generative AI, machine learning services, and AI-assisted development tools.
- All environments where company or client data is accessed, processed, or generated using AI.

3. Definitions

- **Artificial Intelligence (AI):** Systems or tools capable of performing tasks that typically require human intelligence (e.g., content generation, data analysis, code assistance).
- **Generative AI:** AI systems that can create content such as text, images, code, or audio.
- **Sensitive Information:** Any confidential, proprietary, or regulated data, including client data, source code, credentials, or personal information.
- **Approved AI Tools:** AI tools that have been reviewed and authorized by the organization for use.

4. General Principles

- AI tools must be used responsibly, ethically, and in compliance with company policies.
- Employees remain accountable for all outputs generated using AI.
- Employees are fully responsible for any code, content, or artifacts they commit or deliver, regardless of whether they were created manually or generated with AI tools.
- AI must not replace critical human judgment in decision-making processes.
- All use of AI must comply with applicable legal, contractual, and regulatory requirements.
- The use of AI tools, agents, or automated systems does not transfer or mitigate employee accountability. Employees remain fully responsible for any actions triggered directly or indirectly through such tools, including unintended or harmful outcomes.
- All commits, deployments, and changes to company or clients systems must be performed by authorized human users. The use of AI tools, agents, bots, or automated systems to directly execute commits or changes is strictly prohibited.

5. Acceptable Use

Employees are allowed to use AI tools for:

- Improving productivity (e.g., drafting documents, summarizing content).
- Assisting in software development (e.g., code suggestions, debugging).
- Data analysis using non-sensitive or anonymized data.
- Learning and research purposes.
- Supporting tasks that do not involve autonomous execution of actions on production or critical systems.

All usage must comply with this policy and internal security guidelines.

6. Restricted Use

The following actions are strictly prohibited:

- Uploading or sharing **sensitive information** with AI tools that are not explicitly approved.
- Using AI tools to process client data without authorization.
- Relying solely on AI-generated outputs for critical business decisions without validation.
- Circumventing security controls using AI tools.
- Allowing AI tools, agents, bots, or automated systems to directly perform commits, deployments, or changes to company systems.

7. Data Protection and Confidentiality

- Sensitive or confidential information must **never** be entered into public or unapproved AI platforms.
- When possible, data must be anonymized before being used with AI tools.
- AI-generated content must be reviewed to ensure no unintended data leakage occurs.
- Employees must comply with all data protection policies and agreements with clients.

8. Approved Tools and Authorization

- Only AI tools approved by the organization may be used for work-related purposes involving company or client data.
- New AI tools must go through an evaluation and approval process before being adopted.
- IT/Security teams are responsible for maintaining a list of approved tools.

9. Output Validation

- All AI-generated outputs must be reviewed and validated by a qualified individual.
- Special attention must be given to:
  - Accuracy
  - Bias
  - Security implications
  - Compliance with business requirements

10. Intellectual Property

- Employees must ensure that AI-generated content does not violate intellectual property rights.
- Ownership of AI-generated outputs must be aligned with company policies and contractual obligations.
- AI must not be used to reproduce proprietary content from third parties without authorization.

11. Monitoring and Compliance

- The organization reserves the right to monitor the use of AI tools.
- Non-compliance with this policy may result in disciplinary actions.
- Periodic audits may be conducted to ensure adherence to this policy.

12. Training and Awareness

- Employees must be trained on:
  - Risks associated with AI usage
  - Secure handling of data
  - Proper use of approved AI tools
- Continuous awareness initiatives should be conducted.

13. Exceptions

- Any exception to this policy must be formally requested and approved by Management and/or the Security team.

14. Review and Updates

- This policy will be reviewed periodically and updated as needed to reflect technological, legal, and business changes.