

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 1 de 16

I. OBJECTIVE

This GeoPark Artificial Intelligence (AI) Governance Framework 2025-2028 establishes the structure, principles, and guidelines that steer the responsible, ethical, and secure use of AI across the organization. Its purpose is to ensure that all AI initiatives, tools, and use cases generate business value, protect information, people, and the company's reputation, and are developed with transparency, human oversight, and strategic alignment.

The document seeks to strengthen institutional trust in AI by promoting responsible innovation without compromising security or regulatory compliance.

II. SCOPE

The framework applies to all GeoPark areas, levels, and functions, and covers:

- The use of generative and analytical AI tools.
- The design, integration, or implementation of proprietary or third-party AI solutions.
- Decisions supported or assisted by AI.
- Training, culture, and change-management processes associated with AI adoption.

Its implementation is organized through an evolutionary approach made up of four waves developed between 2025 and 2028, progressively increasing the level of formality, maturity, and control.

III. GENERAL

DEFINITIONS

- **Artificial Intelligence (AI):** A set of technologies and computational capabilities that allow systems to perform tasks that normally require human intelligence, including content generation, information analysis, pattern recognition, decision-making support, and process automation.
- **Artificial Intelligence Governance:** A set of practices, structures, principles, processes, and mechanisms that enable the management, supervision, and control of the use of Artificial Intelligence in an ethical, secure, transparent manner aligned with business objectives.
- **AI Initiative:** A project, solution, tool, use case, or implementation that incorporates Artificial Intelligence capabilities to support, automate, or improve organizational processes, decisions, or activities.
- **AI User:** An employee, contractor, or authorized third party who uses company-approved Artificial Intelligence tools, platforms, or solutions to support activities, processes, or decisions related to their duties.
- **Approved AI Tool:** An Artificial Intelligence application, platform, or service that has been evaluated and authorized by the company's relevant instances, meeting established security, compliance, privacy, and risk-management requirements.
- **Human Oversight:** The participation of a responsible person in reviewing, validating, interpreting, or approving results generated by Artificial Intelligence systems, ensuring that final decisions remain under human control.

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 2 de 16

- **AI Risk:** The possibility that the use, implementation, or result of an Artificial Intelligence solution may generate adverse impacts on people, information, processes, regulatory compliance, reputation, or the organization's objectives.
- **AI Risk Assessment:** A structured process to identify, analyze, assess, and manage risks associated with an Artificial Intelligence initiative, considering its potential impact on people, data, processes, and the organization.
- **Personal Data:** Any information associated with, or that can be directly or indirectly related to, an identified or identifiable natural person.
- **Confidential Information:** Non-public information whose disclosure, modification, loss, or unauthorized access could generate operational, financial, legal, regulatory, or reputational impacts for the organization.
- **Transparency:** A principle under which the use, purpose, operation, and results of Artificial Intelligence can be clearly communicated, understood, and explained to stakeholders.
- **Traceability:** The ability to reconstruct and verify the origin, use, decisions, actions, and results associated with an Artificial Intelligence initiative or tool.
- **AI Hallucination:** A result generated by an Artificial Intelligence tool that presents incorrect, inaccurate, or unsupported information, even when it appears certain or truthful.
- **Algorithmic Bias:** A systematic distortion in the results produced by an Artificial Intelligence system that may generate unfair, discriminatory, or inconsistent decisions, recommendations, or outcomes.
- **Responsible Use of AI:** The application of Artificial Intelligence in accordance with the principles of ethics, security, transparency, human oversight, regulatory compliance, and sustainable value generation defined by the organization.

DOCUMENT STRUCTURE

The framework is organized into the following sections:

- Conceptual framework for AI governance
- Organizational model
- Framework architecture
- Development by waves (1-4)
- Global success metrics
- Governance and continuous improvement

GeoPark's Artificial Intelligence Governance Framework establishes how the company manages, controls, and leverages AI in a secure, ethical manner aligned with its strategy.

It proposes an evolution across four waves that combines responsible experimentation, progressive formalization, institutionalization of control, and sustainable maturity. The ultimate objective is to integrate AI with trust, transparency, and value, consolidating responsible and secure use that strengthens GeoPark's business performance and culture.

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 3 de 16

AI GOVERNANCE PRINCIPLES AT GEOPARK

The principles below guide all decisions, actions, and controls related to the adoption, use, and oversight of Artificial Intelligence at GeoPark. These principles reflect the corporate values, the Code of Ethics, and the company's commitment to responsible, secure, and sustainable use of technology.

- **Principle 1 — Ethics, accountability, and compliance:** GeoPark acts with integrity in every Artificial Intelligence initiative. Every AI solution or project must comply with applicable laws, regulations, and internal policies, reflect corporate values, and have clear owners for its use and outcomes. Each initiative must include a risk analysis proportional to its scope and impact.
- **Principle 2 — Security, privacy, and information protection:** The protection of personal and corporate information is a priority. AI is used only in secure environments and under Cybersecurity guidelines, ensuring the confidentiality, integrity, and availability of data and technology resources.
- **Principle 3 — Human oversight and technological reliability:** Artificial Intelligence is an enabler, not a replacement for human judgment. Every AI-assisted decision requires appropriate human oversight, contextual checks, and controls that ensure reliability, traceability, and continuous improvement.
- **Principle 4 — Transparency, fairness, and inclusion:** The use of AI at GeoPark must be explainable, auditable, and clearly communicable. Solutions must avoid bias, promote fair and inclusive decisions, and allow their results to be understood by all relevant stakeholder groups.
- **Principle 5 — Value, sustainability, and responsible innovation:** AI is adopted to generate tangible value, optimize processes, and strengthen GeoPark's competitiveness. Its use must promote a positive impact on people, communities, and the environment, driving responsible innovation and integrating continuous learning and sustainability into its implementation.
- **Purpose of the principles:** These principles serve as the normative and cultural basis of the governance framework. Together, they make it possible to:
 - Guide the development and use of AI solutions in the organization.
 - Align technology with GeoPark's values.
 - Strengthen trust, internally and with third parties.
 - Provide clear criteria for decision-making, risk assessment, and oversight.

CONCEPTUAL FRAMEWORK FOR AI GOVERNANCE AT GEOPARK

Artificial Intelligence Governance at GeoPark is understood as the set of practices, structures, and mechanisms that ensure AI is used ethically, securely, under supervision, and aligned with business objectives. Its purpose is to enable AI to deliver real value while protecting people, information, and the company's reputation.

- **GeoPark approach: "Experiment responsibly, govern with agility"**

GeoPark adopts an approach that combines agility and innovation with responsibility and control.

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 4 de 16

This approach does not imply the absence of controls in early stages. From the first pilot, each initiative operates under minimum conditions for security, human oversight, and regulatory compliance:

- **Move fast:** enable pilots and safe experimentation to identify real value opportunities.
- **Then govern:** once the use, impact, and risks are understood, the necessary guidelines, controls, and oversight are formalized.
- **Always responsibly:** each initiative includes risk analysis, cybersecurity measures, human oversight, and regulatory compliance.
- **Continuous improvement:** governance evolves as digital maturity advances and AI capabilities and risks change.

This approach enables progress at speed without compromising security or corporate values. GeoPark adopts an AI risk-management approach in which each initiative is assessed proportionally to its impact, complexity, and level of exposure.

o Foundations that inspire the model

GeoPark's conceptual framework is inspired by the main international AI governance references, adapted to the company's operational and cultural reality:

- **Gartner AI Governance Framework (2025):** Basis of the three-pillar model: operating model, policies and controls, and oversight systems.
- **NIST AI Risk Management Framework (2023):** Introduces risk-based management: identify, assess, mitigate, and monitor risks proportionally to impact.
- **ISO/IEC 42001 (2023):** Provides a systematic approach to leadership, controls, oversight, and continuous improvement for responsible AI use.
- **AI Act (European Union):** Proposes differentiated governance according to risk level and requires transparency and human oversight.

These frameworks provide rigor and clarity, but GeoPark applies only what is relevant and practical for its context, always prioritizing cybersecurity, ethics, and business value.

o Purpose of the conceptual framework

The conceptual framework fulfills four essential functions:

- **Align AI with corporate strategy:** ensure AI is used where it generates value and strengthens GeoPark's competitiveness.
- **Protect the organization:** ensure secure, supervised use that complies with regulations and internal policies.

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date	12/06/2026	Effective Date	12/07/2027	Prepared by	Approved by
				Edgardo Arrieta - Cybersecurity and Compliance Manager	Cinthya Sánchez (Ithink Director)
					N° Versión
					01
					Página
					5 de 16

- **Guide responsible decisions:** provide common criteria to assess initiatives, mitigate risks, and escalate findings.
- **Consolidate digital culture:** promote conscious, ethical, and sustainable AI adoption among all areas and employees.

o Core components of the framework

The conceptual framework translates into three components that structure the entire governance system:

- **Operating model:** Defines roles, responsibilities, decision processes, and coordination flows across the organization.
- **Policies and controls:** Establish rules, limits, security measures, compliance, and risk-assessment requirements.
- **Oversight systems:** Enable monitoring of AI use, traceability, incident identification, risk escalation, and continuous improvement.

These components are applied progressively and proportionally during the four implementation waves.

o How this framework is integrated into GeoPark

The conceptual framework:

- Is based on the existing corporate structure, without creating unnecessary layers.
- Is applied proportionally to the risk and complexity of each initiative.
- Ensures that each area is responsible for its AI projects, while using a common framework that provides coherence and control.
- Reinforces the importance of human oversight, cybersecurity, transparency, and sustainability in every use of AI.

MODELO ORGANIZACIONAL DE LA GOBERNANZA DE IA

AI governance at GeoPark is supported by the company's existing leadership structure, combining distributed accountability with centralized oversight. This allows the organization to move with agility, maintain control, and ensure coherence across all AI initiatives, without creating unnecessary parallel structures. Each Artificial Intelligence initiative has a defined owner for its use, results, and associated risks.

o Roles and responsibilities

AI governance is a cross-functional effort led by the CEO, Vamos, and IThink, who oversee, approve, and are accountable for the use of AI in their respective areas. Responsibilities are distributed as follows:

Role / Area	Main AI Responsibilities
-------------	--------------------------

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 6 de 16

Chief Executive Officer (CEO)	Defines the strategic vision for AI use in the company. Oversees overall progress and relevant risks, ensuring coherence with corporate values and priorities.
Chief Information Officer (CIO)	Leads implementation of the AI governance framework. Coordinates adoption, manages licenses, monitors use, and consolidates institutional information on AI.
Chief Information Security Officer (CISO)	Assesses cyber risks associated with AI and defines the required technical and security controls. Ensures data protection and platform integrity.
Chief Exploration Officer (CXO)	Oversees AI projects in exploration and development, ensuring technical consistency and compliance with established policies.
Chief Financial Officer (CFO)	Assesses the financial impact of AI solutions and ensures that projects comply with control and audit policies.
Chief Operation Officer (COO)	Directs the safe and efficient implementation of AI in operational and production processes. Ensures compliance, efficiency, and reliability.
Chief People Officer (CPO)	In addition to overseeing AI projects in the area, leads the human perspective of AI adoption: digital skills, impact on people, and organizational culture.
Legal and Compliance	Analyzes legal, regulatory, contractual, and privacy implications to ensure legal compliance and ethics in AI use.
IThink	Supports the identification of opportunities, technological exploration, and development of innovative use cases in coordination with business areas.

- o **Integration with the corporate governance structure:** AI governance is fully integrated into existing corporate governance processes. This avoids duplication and ensures traceability in decision-making.
 - **Institutional reporting and monitoring mechanisms:**
 - **Quarterly Digital Agenda meeting:** Reports on AI adoption, risks, and progress are presented to Vamos (C-level team).
 - **Annual Audit Committee session:** Updates are presented on technology, technology risks, and, where applicable, AI governance matters.
 - **Risk-based escalation:** Relevant incidents or risks are escalated to Internal Control, the Audit Committee, CIO/CISO, or CEO, depending on their nature.

This scheme provides executive visibility, strategic alignment, and institutional control without creating new approval layers.

- o **Coordination flows:** AI governance at GeoPark operates under a centralized-federated hybrid model, combining area-level autonomy with central control over security and technology adoption.
 - **Distributed accountability:**
 - Define AI needs and opportunities.
 - Formulate initiatives and justify their impact.

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 7 de 16

- Oversee project execution and results.
- **Centralized monitoring and control (IThink):**
 - Management of AI tool licenses and users.
 - Monitoring usage statistics and search for efficiencies.
 - Promotion of safe adoption and good practices.
 - Consolidation of the institutional inventory of AI initiatives.
 - Technical and cybersecurity review of new initiatives.
- **Institutional decision flows**
 - **Digital Agenda:** reviews, assesses, prioritizes, and monitors formal projects for the year.
 - **Vamos (C-level):** approves additional initiatives specific to each area.
 - **IThink:** supports conceptualization and design of initiatives when new capabilities or innovation approaches are required.

This model ensures effective coordination, responsible use, and agile progress without unnecessary friction or bureaucracy.

- **AI risk typology:** GeoPark recognizes that the use of Artificial Intelligence introduces different types of risks that must be managed comprehensively. These risks include, among others:
 - **Behavioral risks:** errors, bias, misuse, or outdated information.
 - **Security and data risks:** exposure of sensitive information, unauthorized access, or misuse of data.
 - **Legal and regulatory risks:** regulatory non-compliance, improper use of content, or legal liabilities.
 - **Transparency risks:** lack of explainability or non-disclosure of AI use.
 - **Organizational risks:** impact on people, technological dependency, or process changes.

GeoPark's AI governance framework is designed to identify, assess, and manage these risks proportionally, integrating them into policies, controls, and oversight mechanisms.

Level	Criterion	Escalation instance
High	Exposure of sensitive data, regulatory non-compliance, reputational impact	CEO / Audit Committee
Medium	Failure in an AI-assisted process, unauthorized use of a tool	CIO / CISO / Internal Control
Low	Minor deviation from guidelines, incident with no operational impact	IThink / Responsible area

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 8 de 16

AI GOVERNANCE FRAMEWORK ARCHITECTURE

The architecture of GeoPark's Artificial Intelligence Governance Framework is organized into three complementary pillars, which integrate innovation, control, security, ethics, and sustainability throughout the organization. These pillars evolve progressively across implementation waves and work in coordination to ensure responsible and strategic AI use.

GeoPark's AI governance model is aligned with the main reference components in AI governance, including:

- AI risk management
- Responsible Artificial Intelligence
- Definition of roles, teams, and decision rights
- Organizational culture and capability development
- Monitoring, compliance, and reporting
- Data governance, validation, and lifecycle oversight

These elements are integrated practically into the three pillars of the model, ensuring comprehensive governance without unnecessary complexity

o **Pillar 1 — Operating Model:** The operating model defines how AI initiatives at GeoPark are managed, assessed, prioritized, and supervised. It is based on combining distributed accountability by area with centralized oversight from Technology, ensuring coherence, security, and agility. The components of the operating model are detailed below:

- **Distributed accountability:** Each area owns its AI initiatives and the associated results.
- **Centralized oversight:** IThink consolidates institutional information, manages licenses, monitors use, oversees cybersecurity, and ensures technical compliance.
- **Approval through existing structures:**
 - **Digital Agenda:** assesses, prioritizes, and monitors formal projects for the year.
 - **Vamos (C-level):** approves additional initiatives that respond to specific strategic needs.
 - **Control instances:** in the event of risks, escalation occurs to Internal Control, Audit, CIO/CISO, or CEO, as applicable.
- **Common governance criteria:** Every AI initiative must include:
 - Risk analysis proportional to impact.
 - Mandatory human oversight.
 - Regulatory compliance and data protection.
 - Traceability and basic documentation.
- **AI initiative approval process**
 - **Formulation:** the area or IThink defines the use case, objective, and expected impact.

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 9 de 16

- **Risk assessment:** AI Management and Cybersecurity Management review the proposed tool or solution.
- **Approval:** depending on scope, the initiative is included in the Digital Agenda for approval by Vamos.
- **Supervised implementation:** the area executes with human oversight and documents results.
- **Follow-up:** IThink consolidates the initiative in the institutional inventory and monitors its evolution.
- **Institutional evaluation criteria for initiatives:** GeoPark uses uniform Impact and Effort criteria to assess and prioritize projects, including AI projects. This ensures decisions are consistent with corporate strategy.
- **Impact criteria:**
 - **Alignment with the Scorecard:** contribution to strategic pillars.
 - **Speed of capitalization:** speed at which the benefit materializes.
 - **Risk mitigation:** reduction of operational, technological, or corporate risks.
 - **Future enablement:** creation of capabilities or subsequent projects.
- **Effort criteria**
 - **Implementation time:** estimated duration.
 - **Process and people complexity:** number of processes or stakeholders involved.
 - **Technology and data complexity:** maturity of the technology and required data governance.

This framework makes it possible to select AI initiatives that generate the greatest impact with reasonable effort, ensuring optimal use of resources.

- **Risk escalation:** Relevant risks must be escalated to the appropriate instance according to their nature:
 - Internal Control
 - Audit Committee
 - CIO / CISO
 - CEO

This mechanism ensures a timely and coherent institutional response.

- **Pillar 2 — Policies and Controls:** The second pillar establishes the rules, limits, and protection measures that all AI initiatives at GeoPark must follow. These policies ensure safe, ethical, responsible, and consistent use across the organization.
 - **Main elements**
 - Institutional principles that guide any decision related to AI.
 - **Technical and usage requirements, including:**
 - Secure tool configurations.

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 10 de 16

- Criteria for data use.
 - Restrictions on sensitive information.
- **Regulatory compliance:** personal-data protection, copyright, and applicable legislation.
 - **Risk criteria:** every initiative must document potential risks and mitigation measures.
 - **Progressive updating:** policies that evolve as GeoPark's maturity and technology advance.
- **Restricted or prohibited AI uses:** To protect information, reputation, and compliance, the following AI uses are considered restricted or prohibited:
 - Use of confidential information or sensitive data in tools not approved by the company.
 - Automation of critical decisions without appropriate human oversight.
 - Generation of external content without prior validation and review.
 - Any use that violates information-security policies, the Code of Ethics, or applicable regulations.
- **AI vendor management:** GeoPark recognizes that a significant portion of AI tools used comes from third parties. Therefore, every external AI tool or service must:
 - Be evaluated by AI Management and Cybersecurity Management before adoption.
 - Have contractual terms that protect the confidentiality and ownership of GeoPark data.
 - Be included in the institutional inventory of approved tools.
 - Be monitored and periodically reviewed to verify its validity, security, and alignment with internal policies.
- **Pillar 3 — Oversight Systems:** Oversight systems make it possible to monitor, measure, and improve the use of AI in the organization, ensuring reliability, security, and continuous learning.
 - **Oversight components**
 - **Centralized tool monitoring:** Technology manages licenses, analyzes usage statistics, and detects efficiency opportunities.
 - **Institutional inventory of initiatives:** Single record of AI tools, projects, and use cases.
 - **Mandatory human oversight:** No AI solution operates without human intervention or verification.
 - **Risk management:** Timely identification, assessment, and escalation of technical, ethical, or operational risks.
 - **Continuous improvement:** Periodic evaluation of performance, incidents, lessons learned, and adjustment needs.
 - **Executive visibility:** Quarterly reports to Vamos and annual updates to the Audit Committee.

This pillar ensures that GeoPark advances with confidence, combining innovation with institutional control. This system not only makes it possible to monitor AI use, but also to detect and manage the different types of risk associated with its use, including behavioral, security, compliance, and transparency risks.

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 11 de 16

- **Integration of the three pillars:** The three pillars form an integrated governance system in which:
 - The operating model defines roles and processes.
 - Policies and controls establish clear and consistent rules.
 - Oversight systems provide visibility, traceability, and continuous improvement.

Thanks to this structure, GeoPark can innovate with agility, maintain control and ethics, and ensure an AI use that is sustainable, secure, and aligned with its corporate strategy.

EVOLUTIONARY DEVELOPMENT BY WAVES

The implementation of AI Governance at GeoPark is structured into four successive waves, making it possible to move from initial experimentation to mature, auditable, and sustainable governance. Each wave strengthens capabilities and increases the level of formality, control, and organizational culture, ensuring orderly and proportionate growth.

○ **Wave 1 — Responsible Experimentation (February 2025 - July 2025)**

Purpose: Establish the minimum security, ethical, and training conditions required to begin the responsible use of AI in the organization.

- **Main objectives**

- Evaluate and approve AI tools under cybersecurity and compliance criteria.
- Define initial responsible-use guidelines.
- Configure accounts, permissions, and adequate protections to prevent data exposure.
- Train 100% of the target population in ethical, secure, and responsible use.
- Introduce its use in productivity and personal assistants.

- **Deliverables**

- Approved and securely configured enterprise tools.
- Published responsible-use guidelines.
- Initial adoption statistics.
- Initial training completed.

- **Expected maturity**

- Basic awareness of risks and ethics.
- Ability to experiment without compromising security or compliance.
- Foundations to advance toward formalization.

○ **Wave 2 — Formalization of the Governance Framework (August 2025 - April 2026)**

- **Purpose:** Define principles, base policies, common evaluation criteria, and institutional mechanisms to regulate AI adoption.
- **Main objectives**
 - Publish AI governance principles.

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 12 de 16

- Issue initial responsible-use policies.
- Build the inventory of initiatives and usage statistics.
- Deepen training, moving toward assistive and autonomous AI.
- Perform risk analyses associated with use cases.

- **Deliverables**

- AI Governance Framework v1.0.
- Institutional base policies.
- Initial inventory of use cases.
- Documented risk assessments.
- Second wave of training and support.

- **Expected maturity**

- Initial processes and rules formalized.
- Evaluation of initiatives with uniform criteria.
- Clearer roles and responsibilities.

- **Wave 3 — Institutionalization and Control (May 2026 - December 2026)**

- **Purpose:** Consolidate governance as an institutional capability through thematic policies, specific controls, and continuous monitoring.

- **Main objectives**

- Develop thematic policies (security, ethics, privacy, data, vendors).
- Implement TRiSM-type oversight practices (manual or initial).
- Measure organizational maturity and detect gaps.
- Assess the value capture generated by AI already in operation.
- Continue the evolution toward agentic AI, under the principle of human oversight.

- **Deliverables**

- Specific policies formalized.
- First monitoring dashboard ("TRiSM-lite").
- Maturity assessment and value reports.
- Update of inventory and risk register.

- **Expected maturity**

- Active governance applied systematically.
- Risks managed visibly and under control.
- Discipline in documentation, monitoring, and continuous improvement.

- **Wave 4 — Maturity and Transparency (January 2027 - 2028)**

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 13 de 16

- **Purpose:** Reach a sustainable, auditable, and transparent level of governance that strengthens internal and external trust in AI use.
- **Main objectives**
 - Define and incorporate specialized roles (for example, AI model validator).
 - Establish integrated value, maturity, risk, and reliability metrics.
 - Publish a Responsible AI Report with progress, incidents, and lessons learned.
 - Maintain alignment with relevant international standards.
 - Prepare the organization for advanced AI ecosystems (including agentic AI).
- **Deliverables**
 - Specialized roles implemented.
 - Institutional AI metrics scheme.
 - GeoPark Responsible AI Report.
 - Update of the governance framework.
- **Expected maturity**
 - Stable, auditable, and dynamic governance.
 - Controlled residual risk.
 - Ability to innovate with trust, control, and transparency.

EXECUTIVE SUMMARY OF THE WAVES

WAVE	PURPOSE / FOCUS	DELIVERABLES	EXPECTED MATURITY
RESPONSIBLE EXPERIMENTATION (Feb-Jul 2025)	* Enable secure, ethical, and controlled use of AI. * Level knowledge and validate tools. * Prepare the organization for progressive adoption.	* Approved and secure AI tools. * Initial use guidelines. * 100% initial training. * Initial adoption statistics.	* Basic awareness of AI risks and ethics. * Foundations for governance and responsible use.
FORMALIZATION OF THE GOVERNANCE FRAMEWORK (Aug 2025-Apr 2026)	* Define principles, base policies, and common criteria. * Create institutional inventory and assess risks. * Deepen training and move toward assistive AI.	* AI Governance Framework v1.0. * Base policies published. * Inventory of use cases. * Risk assessments.	* Uniform evaluation of initiatives. * Initial standardized practices. * Clarity in roles and guidelines.
INSTITUTIONALIZATION AND CONTROL (May-Dec 2026)	* Implement thematic policies and controls. * Incorporate TRISM-type oversight practices. * Measure maturity and capture value.	* Specific policies formalized. * Monitoring dashboard (TRISM-lite). * Maturity and value reports. * Inventory and risk updates.	* Active and measurable governance. * Risk managed visibly. * Controls integrated into operations.
MATURITY AND TRANSPARENCY (Jan 2027-2028)	* Achieve sustainable and auditable governance. * Establish institutional AI metrics. * Publish Responsible AI Report.	* Advanced roles implemented. * Integrated value and risk metrics. * GeoPark Responsible AI Report. * Framework update.	* Stable and auditable governance. * Controlled residual risk. * Innovation with trust and transparency.

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 14 de 16

GLOBAL SUCCESS METRICS

Artificial Intelligence Governance at GeoPark is measured through a set of indicators that make it possible to evaluate effectiveness across four dimensions: value, risk, maturity, and trust.

GeoPark is currently in Wave 2 of its AI governance framework, focused on formalizing principles, base policies, and common management criteria.

These metrics are not intended to create unnecessary complexity, but to provide practical and actionable visibility into the framework's progress, facilitating decision-making and continuous monitoring.

- **Measurement principles:** AI governance metrics at GeoPark are based on the following criteria:
 - **Relevance:** focused on impact and risk management.
 - **Simplicity:** feasible to measure and maintain over time.
 - **Progressive evolution:** adjusted as AI adoption matures.
 - **Practical use:** oriented to decision-making, not only to reporting.
- **Dimension 1 - Value:** Measures the impact that AI generates in terms of productivity, efficiency, and innovation.
 - **Indicators:**
 - Active use cases with impact on key processes.
 - Identified improvements in productivity or efficiency (qualitative).
 - AI initiatives that enable new capabilities or decisions.
- **Dimension 2 - Risk:** Assesses the level of control over risks associated with AI use, including security, compliance, and reputation.
 - **Indicators:**
 - Number of initiatives with documented risk analysis.
 - Incidents or alerts related to AI use.
 - Compliance with responsible-use and security policies.
 - Level of exposure to critical risks (qualitative assessment).
- **Dimension 3 - Maturity:** Reflects the level of capability development to govern and use AI effectively.
 - **Indicators:**
 - Level of framework formalization (by wave).
 - Number of areas using AI in a structured manner.
 - Progress level in training and digital competencies.
 - Existence of defined processes for assessment, monitoring, and improvement.
- **Dimension 4 - Trust:** Measures the perception of security, transparency, and responsibility in AI use.

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 15 de 16

- **Indicators:**

- Level of employee trust in AI use (internal surveys).
- Degree of responsible adoption (use aligned with policies).
- Perception of AI's positive impact on daily work.

- **Use of metrics:** Metrics are used to:

- Provide executive visibility into framework progress.
- Support decision-making in the Digital Agenda and Vamos.
- Identify risks, gaps, and improvement opportunities.
- Support the framework's evolution throughout the waves.

Monitoring these metrics is progressive and adaptable, always prioritizing practical usefulness over complexity.

GOVERNANCE AND CONTINUOUS IMPROVEMENT

GeoPark's Artificial Intelligence Governance Framework is a dynamic and evolutionary system designed to adapt to technological progress, organizational maturity, and changes in the regulatory and business environment.

Its governance is based on a continuous-improvement approach, which allows practices to be adjusted, controls to be strengthened, and lessons learned to be captured progressively.

- **Continuous improvement principles**

The evolution of the framework is governed by the following principles:

- **Adaptability:** the framework is adjusted as business needs, technology, and AI-related risks change.
- **Proportionality:** controls and policies evolve according to the level of risk and complexity of initiatives.
- **Continuous learning:** experiences, incidents, and results feed the improvement of the framework.
- **Practicality:** applicable and sustainable solutions are prioritized over unnecessary complexity.

- **Monitoring and update mechanisms**

Framework governance relies on institutional mechanisms that allow monitoring and evolution:

- **Continuous monitoring from Technology (IThink):** monitoring of tool use, adoption, technical compliance, and relevant findings.
- **Digital Agenda review (quarterly):** analysis of progress, risks, opportunities, and framework adjustment needs in the context of current initiatives.
- **Updates in executive instances (Vamos):** alignment of framework evolution with the company's strategic priorities.
- **Reporting to the Audit Committee (as applicable):** inclusion of AI governance topics within annual technology updates or when relevant risks are identified.

Document	05 Otro (detallar en "nombre")	Name	Artificial Intelligence Governance Framework		
System	03 Finanzas	Sub-System	05 IT		
Code	03 -05 - 195				
Issue Date 12/06/2026	Effective Date 12/07/2027	Prepared by Edgardo Arrieta - Cybersecurity and Compliance Manager	Approved by Cinthya Sánchez (Ithink Director)	N° Versión 01	Página 16 de 16

o Management of lessons learned and incidents

Framework improvement is fed by real-world experience in AI use. To this end, GeoPark:

- Records and analyzes incidents, deviations, or risks associated with AI use.
- Identifies improvement opportunities in policies, controls, or processes.
- Adjusts guidelines and practices when necessary.
- Reinforces training and awareness based on findings.

This approach enables informed evolution and strengthens governance based on evidence.

o Framework evolution

The AI governance framework:

- Is not static or rigid.
- Is updated progressively and as needed, without depending on fixed cycles.
- Evolves as implementation waves advance and organizational maturity increases.

As GeoPark incorporates new capabilities (for example, more autonomous AI or new usage models), the framework will adapt to ensure innovation remains secure, responsible, and sustainable.



IV. REFERENCES

3-05-192 AI Governance Policy

V. VERSION CONTROL TABLE

Version	Date	Author	Description
1	12/06/2016	Cybersecurity and Compliance Manager	Document creation

Responsibility	Name	Position
Creation	Edgardo Arrieta	Cybersecurity and Compliance Manager
Approval	Cinthya Sánchez	IThink Director