

ISA resumme 2025

INTEGRATED MANAGEMENT REPORT 2025

In 2025, we consolidated value creation for our shareholders and strengthened market confidence, reflected in an outstanding stock performance, with a valuation increase of nearly 50% and a total return of 55%, driven by the highest dividend in our history.

This performance, together with the record highs reached at the beginning of 2026, confirms the strength of our strategy and our ability to deliver sustainable results over time.

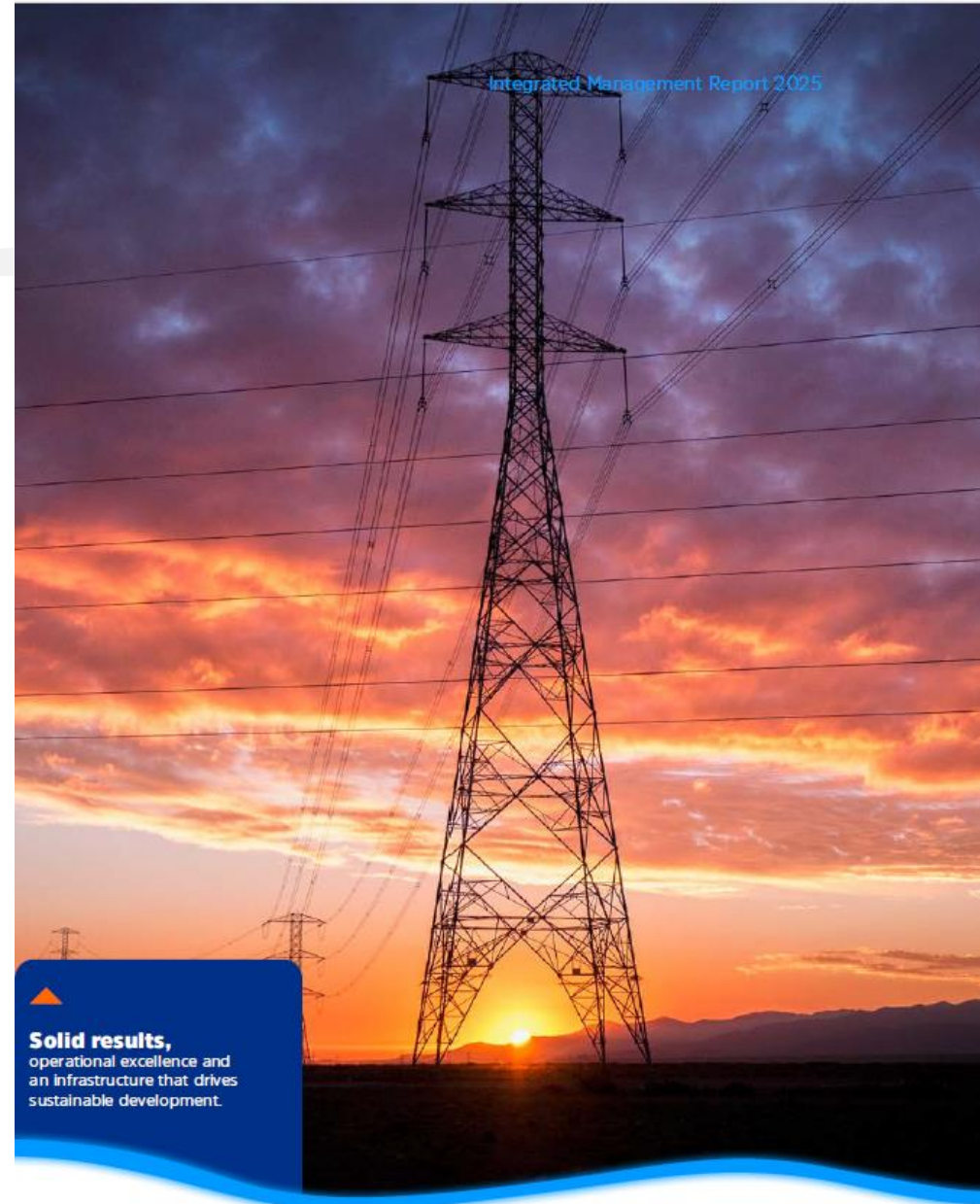
We reaffirmed our financial strength and excellence in execution by maintaining indicators aligned with international standards and accelerating our investment pace, achieving growth of more than 30% compared to recent years.

This disciplined approach enabled us to consistently advance in project execution, promote innovation as a source of value, and generate operational efficiencies, consolidating a management model focused on profitability, efficiency, and sustainable growth.

At the same time, we strengthened our position as a key enabler of the energy transition by developing strategic infrastructure, expanding our capacity and reliability across the region, with a network exceeding 50,000 km of circuits.

This progress is complemented by the implementation of the ISA2040 strategy, which provides a clear roadmap to diversify our portfolio, develop new energy businesses, and strengthen digital capabilities to create value at a regional scale.

Finally, we made decisive progress in sustainability, innovation, and social impact, with relevant investments, advances in decarbonization, and international recognitions that validate our practices. Despite a challenging environment, we demonstrated resilience and maintain a long-term growth vision, positioning ourselves as a key player in the energy transition, committed to creating sustainable value for all our stakeholders.



Solid results,
operational excellence and
an infrastructure that drives
sustainable development.

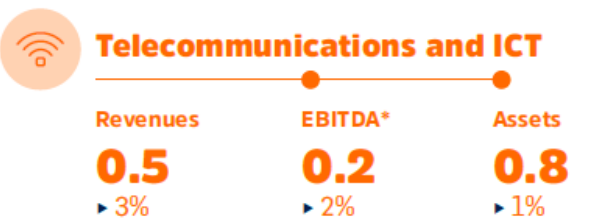
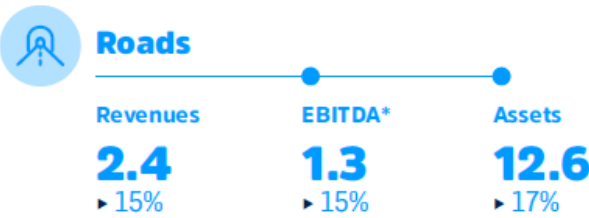
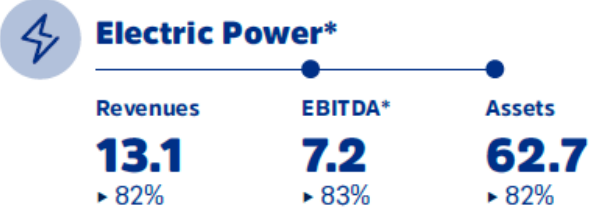
Dear shareholders

Financial figures

The financial figures contained in this report are expressed in COP trillion, unless another currency is specified.

By business unit

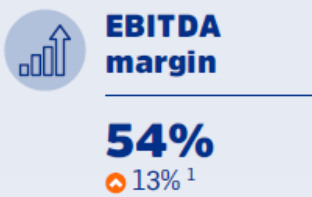
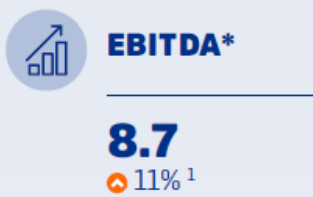
► Stake %



* The Electric Power business unit includes XM.
¹ Excluding the non-recurring effects in 2025 (regulatory adjustment of the Basic Network of the Existing System, RBSE, in Brazil and provisioning of the Air-e portfolio due to payment defaults) and the recognition of the Periodic Tariff Review (RTP) at ISA ENERGIA in Brazil in 2024, the results would have shown positive growth.
² This decrease is primarily due to the impact of currency translation.

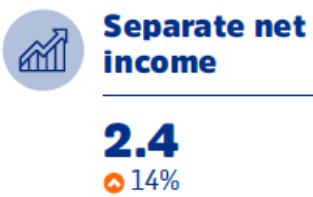
Consolidated

● Variation 2025 vs. 2024



Separate

● Variation 2025 vs. 2024



Included in the S&P yearbook



Quality seal of the Colombian Stock Exchange, for its transparency, corporate governance and commitment to the securities market.



Recognition: ALAS20 in Colombia, first place in the category "leading company in investor relations."

Presence of ISA and its companies

[GRI 2-6 III]



ISA
50+

subordinates

**Shareholding
in other 18 companies**

- Electric Power
- Roads
- Telecommunications and ICT
- Other businesses
- Investment vehicle

Operations in

6

**countries in South
and Central America**

* ATP headquartered in the U.S.; operates in Colombia, Peru, and Chile.

** Reinsurer for property damage and all risks construction and vehicle policies to access the reinsurance market.

ESG Data

[GRI 102-29]

Environmental

[GRI 305-5] [GRI 304-3]

Environmental investment
COP 143,010
million
▲ 23%

Tons of CO₂e offset*
24,192
equivalent to 100%
of emissions from
operations and
maintenance
▼ -2%

Protected habitats
5,309 h
▲ 84%

Hectares of
conservation or
restoration associated
to the Conexión Jaguar
program
321,000

ISA ENERGÍA in
Latam, ISA VÍAS in Chile and
Colombia, and InterNexa
Colombia **carbon neutral**
operations (scope 1 and 2)
12 companies
○ without variation

Non-monetary
fines or penalties
0
○ No variation

Monetary
penalties or fines
(in excess of USD
10,000)
6
▲ 200%

Social

Investment in communities
COP 28,000
million
▼ -23%

Local purchases
84.6%
○ No variation

Suppliers in
strengthening
47
▲ 97%

Shareholder
inquiries addressed
100%
○ No variation

Governance

[GRI 2-9-c I- II- III]

Board of Directors
78%
Independent members
○ No variation

Women on the
Board of Directors
22%
○ No variation

Average seniority
on the Board of
Directors
3.1 years
▲ 32%

Complaints addressed
by the Ethics Line
100%
○ No variation

Human Rights
violation cases
0
○ No variation

* Tons of CO₂ equivalent is the unit of
measurement of the gases that cause
global warming.

Economic dimension

Corporate governance



For ISA and its companies, governance and integrity mean counting on governing bodies that guarantee the transparency and independence of the company and ensure the creation of sustainable value.

Board of Directors

23

Meetings held during the year

Ordinary meetings

12

Extraordinary meetings

9

Remuneration
(165 UVT):

COP 8,216,835
per attended meeting

Remuneration of the
Chairman of the Board
of Directors (198 UVT):

COP 9,860,202
per attended meeting

Non-independent
members
22%

Independent
members
78%

Minimum
attendance
goal
80%

Attendance
99%

INSPIRING BOARDS is a unique platform that brings together independent and executive board members of ISA and its companies, with the aim of building trust, aligning strategic vision, and standardizing knowledge on ESG (environmental, social, and governance) issues.

Since its inception, INSPIRING BOARDS has evolved through three editions that reflect its commitment to corporate governance and sustainability. In its third edition, "*Resonamos con Energía*," (Resonating with Energy) held in June 2025, INSPIRING BOARDS reaffirmed its role as a leading event on best practices in corporate governance and sustainability. More than 100 executives, managers, and general secretaries participated, along with 6 speakers and panelists from more than 8 countries, and the event received an outstanding rating of 4.9 out of 5 from attendees.

Board Accountability

Board members election or re –election

Although ISA's Bylaws establish a two-year statutory term for the Board of Directors (Article 27), the General Shareholders' Meeting effectively submits the election of the Board of Directors to a vote at each annual ordinary meeting. As a result, all Board members are subject, year after year, to the shareholders' scrutiny and decision, thereby fulfilling the substantive purpose of the criterion: the annual accountability of the management body before the Shareholders' Meeting.

This practice is grounded in the shareholders' legal power to appoint and remove Board members at any time, set forth in Articles 198 and 199 of the Colombian Commercial Code and expressly incorporated into Article 27 of the Bylaws, under which members "may be re-elected or removed at any time by the General Shareholders' Meeting." The two-year statutory term operates as a maximum tenure ceiling, not as a barrier to annual election; the Meeting retains, and exercises, the authority to constitute the Board at each ordinary meeting.

ARTICLE 198. <DETERMINATIONS OF TERMS AND ELECTION OF ADMINISTRATORS>.

Should the functions indicate in article 196 not be applicable, according to the law, to a certain class of partners, the persons in charge of these functions shall be elected by the General Shareholders' Meeting or by the Partners' Meeting, subject to the provisions of the law and the corporate charter. The election may be delegated, by express provision of the bylaws, to boards of directors elected by the General Shareholders' Meeting.

Elections shall be for the terms established in the bylaws, notwithstanding the fact that appointments may be freely revoked at any time. Any clauses in the contract that cause to establish the irremovability of the administrators elected by the General Shareholders' Meeting, the Partners' Meeting or the Board of Directors, or that require special majorities other than the common ones for removal, shall be deemed not to be written.

ARTICLE 199. <TERM AND REMOVAL OF OTHER OFFICERS ELECTED BY A MEETING>.

Provisions of subsections two and three of article 198 shall be applicable to the members of the board of directors, statutory auditors, and other officers elected by the General Shareholders' Meeting or by the Partners' Meeting.

The effective application of this practice is supported by:

- Historical record of General Shareholders' Meetings published on the corporate website (<https://isa.co/nosotros/asamblea-general-de-accionistas/>), evidencing uninterrupted annual ordinary meetings, each with its corresponding minutes, whose agenda recurrently includes the election of the Board of Directors.
- Agenda of the two most recent Ordinary General Shareholders' Meetings.
- Minutes of the election of the Board members.

Agenda of the two most recent Ordinary General Shareholders' Meetings.

Ordinary General Shareholders' Meeting 2025

Notice of Ordinary General Shareholders' Meeting 2025

The CEO of INTERCONEXIÓN ELÉCTRICA S.A. E.S.P. summons to the ORDINARY GENERAL SHAREHOLDERS' MEETING to be held on Wednesday, March 26, 2025, at 9:00 a.m. at the Poblado office of the Medellín Chamber of Commerce for Antioquia, located at Carrera 43A #16 sur-245, in Medellín, Colombia

At the ORDINARY GENERAL SHAREHOLDERS' MEETING the following agenda will be submitted for consideration:

Quorum verification

Approval of the agenda:

1. Verification of quorum.
2. Approval of the agenda.
3. Election of the Chairman of the Meeting.
4. Secretary's report on the approval of Minutes 119 of March 21, 2024.
5. Election of the commission for the approval and signature of the minutes and scrutinies.
6. Greetings from the Chairman of the Board of Directors, Board of Directors' performance report and corporate governance report.
7. Presentation and approval of the Integrated Management Report for 2024.
8. Presentation of ISA's individual and consolidated financial statements as of December 31, 2024.
9. Statutory auditor's opinion.
10. Approval of ISA's Individual and Consolidated Financial Statements as of December 31, 2024.
11. Approval of the partial modification of the allocation of reserves for equity strengthening and their distribution as an ordinary dividend, approval of the project for the distribution of profits for fiscal year 2024 and the creation of an occasional reserve for equity strengthening.
12. Election of the Statutory Auditor and allocation of fees.
13. Election of the Board of Directors for the remaining statutory period April 2025 – March 2026.
14. Approval of the Remuneration Policy for the Board of Directors.
15. Miscellaneous or proposals from shareholders.

As of March 4, 2025, information on the topics of the Shareholders' Meeting and the proposals to be submitted for consideration will be available on the corporate website www.isa.co, for consultation by the shareholders.

Asamblea General Ordinaria de Accionistas Presencial 2026

Convocatoria Asamblea General Ordinaria de Accionistas Presencial 2026

El presidente de INTERCONEXIÓN ELÉCTRICA S.A. E.S.P. convoca a la ASAMBLEA GENERAL ORDINARIA DE ACCIONISTAS que se realizará el jueves 26 de marzo de 2026 a las 9:00 a.m. en la sede Poblado de la Cámara de Comercio de Medellín para Antioquia, ubicada en la Carrera 43 A # 16 sur-245, en Medellín, Colombia.

En la Asamblea General Ordinaria se pondrá a consideración el siguiente orden del día:

Aprobación del orden del día

1. Verificación del quórum.
2. Lectura y aprobación del orden del día.
3. Elección del presidente de la Asamblea.
4. Informe del secretario sobre la aprobación del acta 120 del 26 de marzo de 2025.
5. Elección de la comisión para escrutinios, aprobación y firma del acta.
6. Saludo del presidente de la Junta Directiva y presentación del informe anual de gobierno corporativo y de funcionamiento de la Junta Directiva
7. Presentación y aprobación del Reporte Integrado de Gestión del año 2025.
8. Presentación de los estados financieros individuales y consolidados de ISA a 31 de diciembre de 2025.
9. Presentación dictamen del revisor fiscal.
10. Aprobación de los estados financieros individuales y consolidados de ISA a 31 de diciembre de 2025.
11. Aprobación del proyecto de distribución de utilidades del ejercicio 2025 y la constitución de una reserva para fortalecimiento patrimonial.
12. Elección del revisor fiscal y asignación de honorarios para el periodo estatutario abril 2026 – marzo 2028.
13. Elección de la Junta Directiva para el periodo estatutario abril 2026 – marzo 2028.
14. Aprobación de honorarios de la Junta Directiva para el periodo estatutario abril 2026 – marzo 2028.
15. Varios o proposiciones de los accionistas.

A partir del 4 de marzo de 2026 estará disponible en el sitio web corporativo <https://isa-as-prod-sitioweb002.azurewebsites.net>, para consulta la información sobre los temas de la Asamblea de Accionistas y las proposiciones que se someterán a consideración.

DERECHO DE INSPECCIÓN

Para los accionistas interesados en ejercer el derecho de inspección, se informa que los documentos que ordena la Ley, correspondientes al último ejercicio social, estarán a su disposición a partir del 4 de marzo de 2026, en la sede principal de ISA en Medellín, Antioquia, ubicada en la Calle 12 Sur

Minutes of the election of the Board

members: documenting the effective vote and the shareholders' appointment of the members through the electoral quotient system, evidencing that the Board's composition was decided by the shareholders at the respective annual meeting.

The evidence demonstrates that, regardless of the nominal two-year statutory term, ISA's Board of Directors is submitted to election by the General Shareholders' Meeting at each annual ordinary meeting, in exercise of the power under Articles 198 and 199 of the Commercial Code. Accordingly, every Board member is subject to annual election by the shareholders, satisfying the assessed criterion both in its purpose —the annual accountability of the management body— and in its practical, verifiable application.



ASAMBLEA GENERAL ORDINARIA DE ACCIONISTAS

PUNTO 13 DEL ORDEN DEL DÍA

ELECCIÓN DE LA JUNTA DIRECTIVA PARA EL PERÍODO ESTATUTARIO ABRIL DE 2026 – MARZO DE 2028

Principales	Calidad
Ricardo Roa Barragán	No independiente - nominado por Ecopetrol S.A.
David Alfredo Riaño Alarcón	No independiente - nominado por Ecopetrol S.A.
Álvaro Torres Macías	No independiente - nominado por Ecopetrol S.A.
Mónica de Greiff Lindo	No independiente - nominado por Ecopetrol S.A.
Fabiola Leal Castro *	Independiente - nominado por Ecopetrol S.A.
Germán Arce Zapata *	Independiente – nominado por Fondos de Pensiones
Astrid Martínez Ortíz*	Independiente – nominado por Fondos de Pensiones
Juan Pablo Zárate Perdomo *	Independiente – nominado por Fondos de Pensiones
Juan Emilio Posada Echeverri *	Independiente - nominado por Empresas Públicas de Medellín

* Postulados como miembros independientes, conforme a lo dispuesto en la Ley 964 de 2005 y los Estatutos Sociales de ISA.

Board Accountability

CEO succession plan

Succession planning and management is key to the sustainability of ISA and its companies. It enables us to meet current talent needs, anticipate future leadership and technical expertise requirements, ensure continuity in the implementation of strategic plans, and support development and retention strategies for top talent.

The succession process at ISA and its companies follows a standardized methodology and is reviewed and updated annually

Article 37 of ISA's Bylaws provides that ISA's CEO is elected by the Board of Directors with the assistance of the Organizational Talent Committee (a board Committee). One of the main responsibilities of this Committee is to plan and manage the succession process of ISA's CEO, the Senior Management, and other relevant executives of ISA's companies (see Agreement 125, second article).

1

Successor eligibility criteria:

- Employees of ISA and its affiliated companies with at least one year in their current role.
- Consistently high performance over time (ratings of 2.3 – 3.2 or 3.3 on the 9-box performance matrix).
- Fulfillment of the required experience and academic qualifications for the target position.
- Positive potential assessment.
- Favorable results in the area's climate survey and leadership index in the current role

2

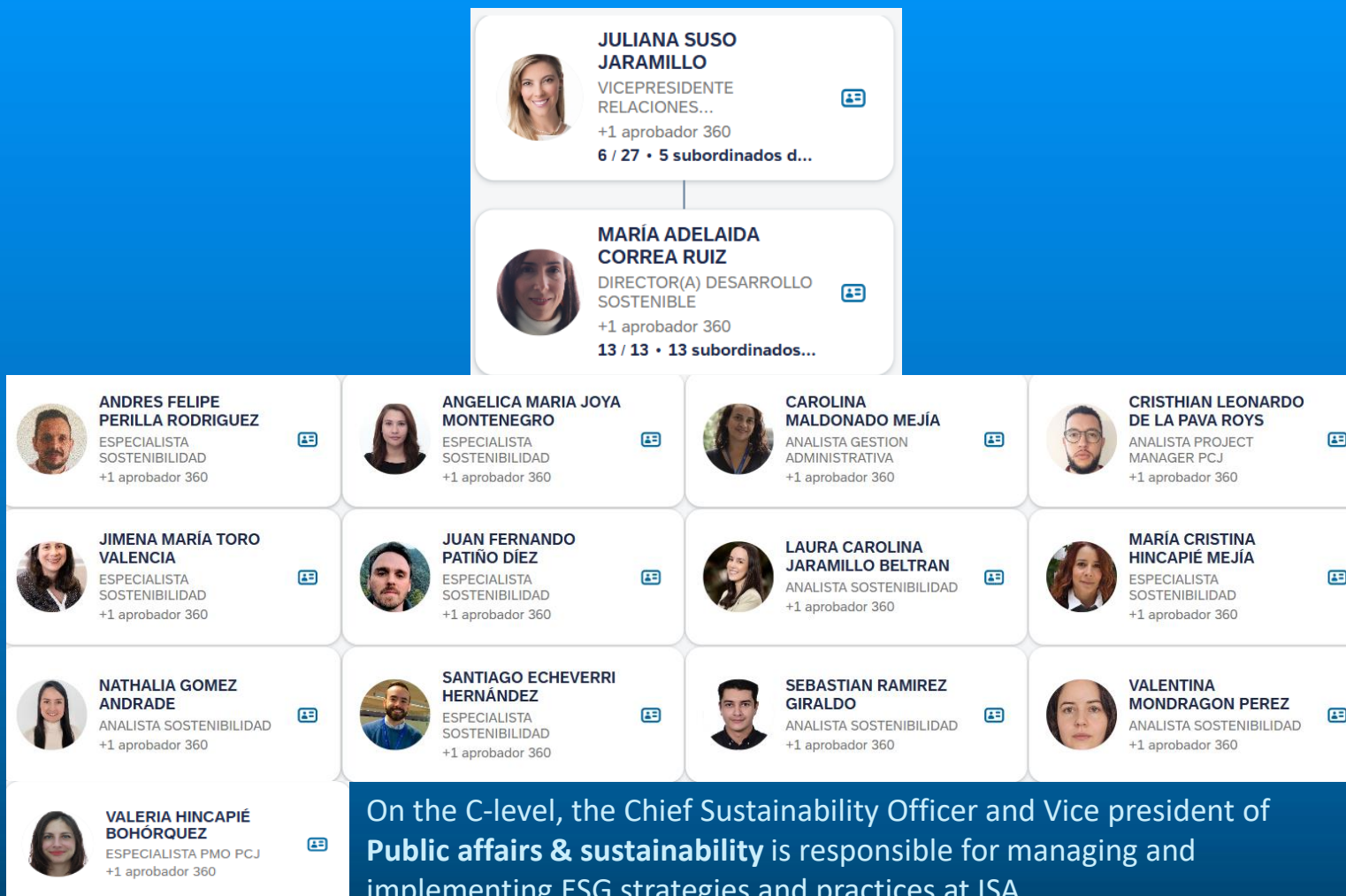
Once the eligibility criteria have been applied, the current and future challenges of the position to be succeeded are reviewed in order to determine the readiness level of each successor candidate. Successors are categorized as

- Competent (no gaps identified)
- Eligible (one development gap)
- Future (two development gaps)

3

The succession plan is defined by the current CEO in collaboration with the Organizational Talent Committee and is validated by the company's Board of Directors. According to Board Agreement No. 125, which governs the Organizational Talent Committee, Article 2, Clause 2 establishes the Committee's responsibility to: "Plan and manage the succession process for the Company's President, Senior Management, and other key executives within the business group (Executive Succession Policy)."

ESG Governance Oversight



ESG Governance Oversight

Board Oversight

ISA's Board of Directors is responsible for ensuring sustainability (Bylaws, article 34 # 38). To fulfill this responsibility the Board has established a Corporate Governance, Sustainability, Technology and Innovation Committee. This Committee is composed of 5 members of the Board of Directors, most of them independent. This Committee has several specific functions on sustainability matters listed on Agreement 129 (article 3, #21 to #33). In the Annual Corporate Governance Report can be seen this Committee performed its duties (see page 23).

Executive Oversight

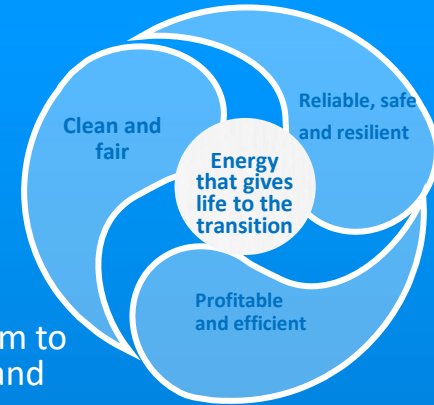
Sustainability projects and investments are overseen by the Sustainability Center of Excellence (CoE), a corporate body with the participation of the Corporate Audit VP, the Public affairs & sustainability VP, the Risk and Compliance VP, the CFO, and six other senior level directors in charge of assessing specific sustainability issues and advising decision-makers on ESG related investments and projects. The CoE meets as needed to assist the evaluation and implementation of sustainability initiatives throughout the Company's geographical locations. Its recommendations, though not binding, provide invaluable insights and guidance to adequately implement sustainability actions in line with the Company's strategy

Executive designated role to oversee ESG/sustainability issues

On the C-level, the Chief Sustainability Officer and Vice president of Public affairs & sustainability is responsible for managing and implementing ESG strategies and practices at ISA

ESG Governance Oversight

ESG strategies and practices at ISA



The Board Committee reviews and approves matters related to the company's sustainability efforts. The defined actions aim to achieve the company's corporate goals (Energía que da vida a la transición) across three key areas: environmental, social, and governance.

Key Elements Monitored

Climate change

- **% Net Zero Pathway Compliance**
- Positive nature outcomes: restored/conserved strategic ecosystems (hectares)
- Projects enabled through strategic social and environmental management
- Value of avoided/offset emissions (PCJ carbon credits)
- % reduction in SF₆ leaks
- Savings from energy efficiency and circularity initiatives

Social

- Critical municipalities with active social programs
- Number of people benefiting from social programs
- Enablement of conflict-prone maintenance activities
- Reduction of costs associated with work stoppages and blockades
- **SROI (Social Return on Investment)**

Governance

- Access to capital with ESG attributes
- Maturity level and recognition by key stakeholders
- **Valuation of societal impacts**

Sustainable Financing

- Assets with mitigated environmental and social risks
- % of critical assets and investment in climate adaptation plans
- **Financial impacts of climate change due to physical risks**

CEO & executives Compensation metrics

At ISA Group, compensation is a strategic tool that drives business success and organizational performance. It aligns with both Corporate and Talent Strategies, focusing on innovation, leadership, and connecting people to business objectives. The compensation system is dynamic, evolving to meet current and future business needs, respond to internal and external changes, and support employees throughout their careers

1

Long-Term Incentives for Employees

2

Full variable compensation vector for managers and non-managers

3

Senior management's remuneration

Long-Term Incentives for Employees



Goals



Initiatives



KPIs



Variable compensation system

Align and focus the individual contribution of each employee with the organizational results required by the strategy

For its calculation are selected

Comprehensive management chart indicators

Milestones of corporate and local initiatives

Results of individual employee performance

Additional bonus to salary

The management instruments governing variable compensation and the milestones associated with long-term incentives are approved by the Board of Directors.
Meeting minutes No. 930 (2025)

ACTA 930 JUNTA DIRECTIVA			
Acta número:	930	Fecha:	19 de febrero de 2025
Tema:	Junta Directiva sesión ordinaria		
Lugar/Modalidad:	Oficina ISA, Bogotá - Presencial		
Hora de inicio:	8:00 a. m.	Hora fin:	4:25 p. m.

N.º	Tema	Naturaleza	Hora	Duración
1	Instrucciones de seguridad	Informativa	8:00-8:05	5 min.
2	Inicio reunión • Verificación del quórum • Aprobación del orden del día • Declaración de conflictos de interés	Decisorio	8:05-8:15	10 min.
3	Actas para aprobación: • 924 del 22 de noviembre de 2024 • 925 del 20 de diciembre de 2024 • 927 del 20 de diciembre 2024	Decisorio	8:15-8:30	15 min.
4	Temas del presidente de la Junta Directiva y de sus miembros	Seguimiento	8:30-9:00	30 min.
5	Informe del presidente de la sociedad Presenta Jorge Andrés Carrillo.	Seguimiento	9:00-10:00	60 min.
6	Informes comités de la Junta Directiva Presentan presidentes de los comités • Informe del Comité de GSTI • Informe del Comité de Talento Organizacional • Informe del Comité de Negocios • Informe del Comité de Auditoría	Seguimiento	10:00-10:45	45 min.
7	Asamblea General Ordinaria de accionistas n.º 125 Presentes Sonia Abuchar, Jaime Fajardo, Juliana Bazo y Nicolás Geronzi. • Orden del día • Informe anual de gobierno corporativo y de funcionamiento de la Junta Directiva • Reporte integrado de gestión 2024 • Consideración estados financieros de ISA y consolidados al 31 de diciembre de 2024 • Proposiciones: ✓ Aprobación y distribución de utilidades del ejercicio 2024 y constitución de una reserva patrimonial. ✓ Elección del revisor fiscal y asignación de honorarios. ✓ Política de Remuneración de la Junta Directiva.	Decisorio	10:45-12:15	90 min.
8	Resultados autoevaluación Junta Directiva Presenta Sonia Abuchar.	Decisorio	12:15-12:35	20 min.
9	Resultados TBG 2024 y objetivos estratégicos metas volantes 2025 Presenta Olga Patricia Castaño.	Decisorio	12:35-1:35	60 min.
10	Informe del Impulso de Transición de energía Presenta Gabriel Melguizo.	Seguimiento	1:35-2:10	35 min.

9. RESULTADOS TBG 2024 Y OBJETIVOS ESTRATÉGICOS METAS VOLANTES 2025

Presentó Olga Patricia Castaño.

La administración expuso los resultados del trimestre IV y anual 2024 del Tablero Balanceado de Gestión (TBG) que fueron presentados previamente en el Comité de Talento Organizacional.

Informó que todos los indicadores cumplieron con la meta, excepto el capex de proyectos y el avance físico de proyectos que quedaron entre el límite inferior y el superior. Adicionalmente, en todos los objetivos estratégicos se cumplieron los hitos propuestos.

25

Acta 930 - 19 de febrero de 2025

También recordó las normalizaciones presentadas que recomendó aprobar el Comité de Talento Organizacional; indicó que ninguna de estas normalizaciones afecta la compensación variable de ISA, pero puede generar un cambio en algunas de las filiales. La primera normalización solicitada por ISA Intercolombia e ISA Transelca está relacionada con Air-e, ya que hicieron una provisión, pero el resultante materializado fue mayor a la provisión que se hizo. Otra normalización es el abito de ISA Transelca, con un tema de Bolivia, con la tasa de cambio oficial de mercado, que genera para ellos un cambio que no tiene afectación; la recomendación de ISA es aprobar. La siguiente normalización es en el proyecto PACE, en ISA Interchile. Ese proyecto lo trabajaron durante todo el 2024, se presentó la oferta en diciembre del 2024 y la oficialización de esa adjudicación fue en enero 2025.

La Junta Directiva consideró que está de acuerdo con las normalizaciones; sin embargo, esa discrecionalidad deberá ser también aplicada dinámicamente para buscar consistencia. Asimismo, solicitó no perder de vista el mensaje que se le está dando a las empresas.

Decisión de la Junta Directiva: la Junta Directiva aprobó los resultados del TBG, el pago de la compensación variable del cuarto trimestre y del componente anual del TBG 2024 de ISA, así como las normalizaciones.

Siendo las 4:25 p. m., se dio por terminada la sesión.

PRESIDENTE

CAMILO ZEÁ GÓMEZ

SECRETARIA

SONIA ABUCHAR ALEMÁN

Full variable compensation vector for managers and non-managers

Result ≥ Target
Result ≥ Minimum Threshold
Result < Minimum Threshold

Indicator Name	Managers and non-managers			
	Annual result	Absolute Achievement	Weight	Weighted Achievement
EBITDA % Achievement Achieve AOM compliance < 98%	118,2%	100%	20,00%	20,00%
Annual Base Project CAPEX % Achievement	100,69%	86,2%	15,00%	12,93%
Annual Base Project Physical Progress ¹ % Achievement	101,08%	100%	15,00%	15,00%
TRIF (Total Recordable Injury Frequency)				
Net Zero Pathway Compliance 2025 %	110%	100%	8,33%	8,33%
New Energy Storage Infrastructure and New Energy Solutions (Awarded/Won) 100 a 200 MW	0	0%	16,67%	0,00%
Strategic Milestones #	6,74	84,2%	25,00%	21,05%
Achievement				77,32%
Impact Due to Fatalities ¹	5			-30%
Total Achievement Excluding Impact Due to Fatalities				47,32%

(1) Durante 2025 se registraron 5 fatalidades relacionadas con el trabajo: 2 en ISA E Perú, 2 en ISA E Brasil y 1 en ISA Energía.

Full variable compensation vector for managers and non-managers

Managers and non-managers						
KPI	Quarterly Component				Annual component	Total bonus ¹
	Result Q1	Result Q2	Result Q3	Result Q4	Result	
EBITDA % Achievement Achieve AOM compliance < 98%	32,00%	16,00%	16,00%	16,00%	20,00%	20,00%
Annual Base Project CAPEX % Achievement	22,94%	11,18%	10,58%	10,34%	12,93%	13,26%
Annual Base Project Physical Progress ¹ % Achievement	24,00%	12,00%	10,91%	12,00%	15,00%	14,89%
TRIF #	20,00%	10,00%	9,30%	8,00%		4,73%
Net Zero Pathway Compliance 2025 %					8,33%	5,00%
New Energy Storage Infrastructure and New Energy Solutions (Awarded/Won) 100 a 200 MW					0,00%	0,00%
Strategic Milestones #		25,00%	50,00%	47,81%	21,05%	24,91%
Total	98,94%	74,18%	96,80%	94,16%	77,32%	82,80%
Total Achievement Excluding Impact Due to Fatalities	0	1	3	1	47,32%	64,80%

(1) Each quarter carries a weight of 10%, and the annual component accounts for 60% of the total bonus.

(2) Impact: A 10% reduction in the annual component result of the variable compensation bonus for each fatality (up to a maximum of 30%), applicable to all ISA areas regardless of the area or company where the fatality occurred



Senior management's remuneration

In ISA, employees' remuneration, including those that are part of Senior Management, is established within the 2030 Business Strategy "Sustainable Value".

Remuneration is a dynamic system that needs to leverage current businesses and facilitate future ones. It also needs to respond to external market and country conditions, as well as to specific internal conditions of the organization, and support employees' work life. Total remuneration consists of three components: fixed, variable, and benefits.

The components of total remuneration for Senior Management integrate to ensure talent attraction, motivation, and retention.

1. Fixed component

It recognizes the effective execution of the position's responsibility, based on

- Position's valuation.
- The position within the salary administration band, applying internal equality and external competitiveness principles.

This component represents the annual guaranteed cash remuneration, which includes legal and extralegal fixed payments granted by the organization to its employees.

2. Variable component

It recognized the added value achieved by employees and the Organization. This is not a guaranteed component, but rather granted according to the results of the area, ISA as a company and the results of the Group achieved in the short, medium, and long term. This component consists of the Short-term Variable Remuneration and the Long-term Variable Remuneration.

a. Short-term variable

Management tool, used to send a clear message to employees regarding what the goals are and what is valued in the short-term (one year). This way, the individual and his performance is linked to the company's performance and final success.

It is an annual variable amount equivalent to a number of salaries determined for each position and it is recognized through a scheme that seeks to achieve and exceed annual goals that are defined in line with ISA2030 Strategy as corporate, team, and individual metrics.

This model represents approximately 22.% of the total remuneration for directors.

KPIs associated with this short-term variable include

- **EBITDA**
- **Annual Base Project CAPEX | % Achievement**
- **Annual Base Project Physical Progress¹ | % Achievement**
- **TRIF (Total Recordable Injury Frequency)**
- **Net Zero Pathway Compliance 2022–2025 | %**
- **New Energy Storage Infrastructure and New Energy Solutions (Awarded/Won) | MW**
- **Strategic Milestones | #**



b. Long-term variable

Long-term variable remuneration is a management tool, which seeks to reinforce the long-term business strategy thinking and the creation of value in the decision-making process, and to align the interests of directors and shareholders and to retain directors of high impact for ISA.

- The plan will be administered through a Pension and Severance Funds Administrator. ISA and its Companies will deliver the capital corresponding to the sum of the defined benefit for each eligible employee, which will be invested by the Fund in a portfolio of shares that includes ISA shares.
- The recognition of the plan for eligible executives in foreign companies will be made in the company's own accounting.
- ISA assigns benefits to each eligible Employee.
- The pension and severance fund acquires a portfolio of 100% ISA shares out of the total allocated.
- The contributions are not the participant's assets; they are held by the autonomous assets of the Pension Fund.
- The contribution varies according to the Fund's profitability (share price and dividends).
- If the goals are met, the assigned benefit passes to the eligible Employee

This model represents approximately 11% of the total remuneration for directors.



3. Benefits component

It reflects ISA's interest to contribute to the quality of life and well-being of employees and their family group. It may include monetary mechanisms that favor cash flow and promote the employee's equity building, reinforce ISA's employer brand and they must recognize the diversity of its workforce.

The components of total remuneration and the proportion of each component are approved by the Organizational Talent Committee, based on the market practices and the particular conditions of the company.

CEO & executives Compensation metrics

CEO Compensation - Success Metrics

Short-term variable compensation is a management tool designed to clearly communicate to employees what the organization aims to achieve and values in the short term (one year). It links individual performance to the overall performance and success of the organization. This incentive consists of an annual variable amount, up to a maximum number of monthly salaries defined for each role. It is awarded based on the achievement and surpassing of annual goals, which are aligned with the ISA 2030 strategy and measured through corporate and team metrics.

Long-term variable compensation is intended to reinforce strategic thinking and long-term value creation in decision-making. It aligns the interests of executives with those of shareholders and supports the retention of high-impact leaders within ISA. This incentive consists of a variable amount over a three-year period, also up to a maximum number of monthly salaries defined per role. It is granted based on the fulfillment of objectives tied to the ISA 2030 strategy.

The CEO's compensation is as follows:

- Fixed compensation : 50%
- Long-term variable compensation: 22%
- Short-term variable compensation: 22%
- Benefits: 6%

The CEO's variable compensation at ISA is structured to reinforce both short- and long-term value creation for the company:

1. Financial Return Metrics:

- **30% is based on Return on Average Equity (ROAE)** for ISA and its consolidated companies. This metric assesses the company's ability to generate profit from shareholders' equity, aligning compensation with capital efficiency and value creation.
- **15% is linked to committed investments in strategic energy infrastructure, including storage, Distributed Energy Systems (SED),** and grid connection technologies. These investments are aligned with the ISA 2030 strategy and are evaluated based on capital allocation effectiveness and return potential.
- **30% is tied to the execution of capital expenditure (CAPEX)** projects in the transmission and road infrastructure businesses. While CAPEX execution is not a traditional return metric, it is assessed based on adherence to budget, timelines, and expected returns—providing an indirect link to financial value creation.

CEO & executives Compensation metrics

CEO Compensation - Success Metrics

2. Non-Financial Performance Metrics:

- **25% of the CEO's variable compensation is based on the Total Recordable Injury Frequency (TRIF)**, a key health and safety indicator tracked at the consolidated level. Although not a financial metric, TRIF is a critical operational KPI within ISA's ESG agenda. TRIF supports the company's purpose of protecting life, raising awareness of self-care, and fostering responsibility for the well-being of others.
- The Total Recordable Injury Frequency (TRIF) directly supports the company's purpose of protecting lives, while fostering a strong culture of self-care awareness and shared responsibility for the well-being of others. As a core non-financial metric, TRIF reinforces the link between operational excellence and sustainable value creation. Eligibility for participation in the long-term variable compensation is contingent upon individual performance outcomes.

3. Relative financial metrics:

ISA also incorporates relative performance metrics in its evaluation framework. The CEO's compensation is influenced by shareholder return indicators, including **stock performance (variation in share price and dividend yield) and comparison to industry benchmarks such as the MSCI Colcap index and other regional energy infrastructure peers)**. These are considered by the Board in evaluating total performance and CEO impact over the fiscal year.

Eligibility for Long-Term Variable Compensation

Participation in the long-term incentive plan (three-year cycle) is subject to individual performance. To be eligible, the CEO must achieve a performance rating of 2.2 or higher on the 9-box matrix.

Executives must achieve a minimum rating of 2.2 on the nine-box matrix to qualify for inclusion in each three-year long-term incentive plan. This approach ensures that consistent high performance and leadership behaviors underpin participation in long-term rewards, aligning individual accountability with the organization's broader objectives of sustainable and responsible value creation.

CEO & executives Compensation metrics

CEO Compensation - Long-Term Performance Alignment

ISA has implemented a structured variable compensation system that fully integrates best practices in executive remuneration, including deferral of bonuses, performance-based periods, and time vesting. The system applies to the CEO and other senior executives, and it is designed to align compensation with long-term value creation.

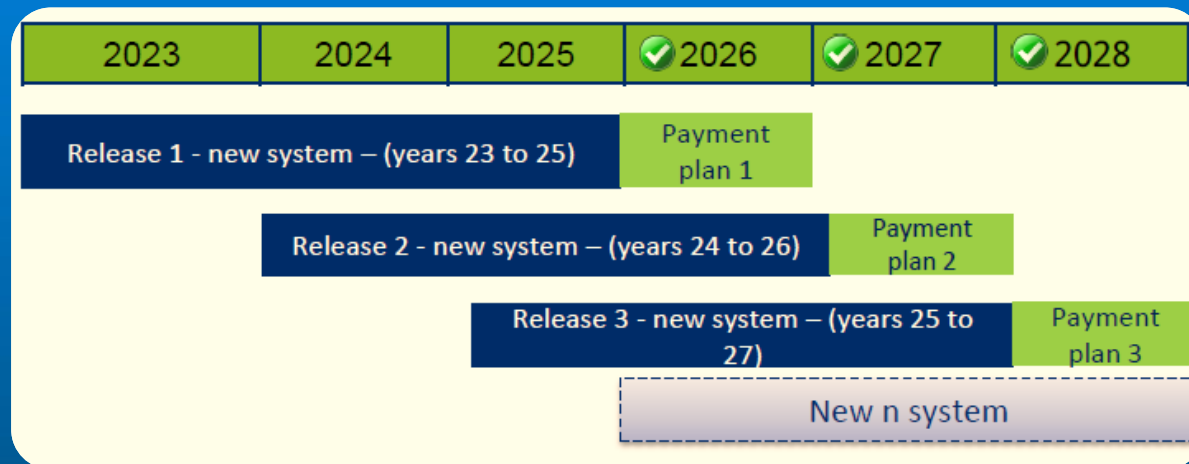
ISA's CEO compensation structure includes both short-term and long-term incentive components. **25% of the CEO's short-term bonus is deferred and paid in the form of ISA shares after a three-year vesting period, subject to continued performance and employment conditions.**

ISA's incentive system operates with defined performance windows:

- **Short-term incentive:** Assessed over a one-year fiscal cycle.
- **Long-term incentive:** Based on a three-year performance period, as illustrated in the following lifecycle:

Each year a new edition of the incentive will be launched with 3-year objectives.

Each launch may have different objectives and participants according to the strategic needs of ISA and its Companies.



CEO & executives Compensation metrics

CEO Compensation - Long-Term Performance Alignment

Both deferred STI and LTI compensation components are subject to a three-year vesting period, during which:

1. The compensation is allocated into a pension fund invested 100% in ISA shares.
2. The fund is only settled after the three-year period and subject to performance indicators being met, including:
 - EBITDA (25%)
 - ROE (25%)
 - Investment in infrastructure & technology (25%)
 - TRIF – Safety Indicator (25%)

Launch (year 1)

1. Each year a three-year plan is launched, with eligible managers who have obtained a 9-box evaluation (equal to or greater than 2.2).
2. The definition of the indicators with which the performance of the following three years will be evaluated (business plan goals) is carried out.

KPI	Weighing
EBITDA	25%
Annual Base Project CAPEX % Achievement	25%
New Energy Storage Infrastructure and New Energy Solutions (Awarded/Won) 100 a 200 MW	25%
TRIF	25%

3. Allocation of the target bond invested in a pension fund in the ISA stock portfolio. (Ownership requeriments/share ownership of times the annual base salary)

Level	# of salaries
CEO	6
VP ISA – General Managers of ISA companies	3
Managers / Directors of ISA companies	2

Settlement (year 3):

4. Evaluation of the results of the indicators, with compliance with EBITDA being a precondition for the liquidation of the system.
5. Participation in settlement subject to 9-box evaluation (equal to or greater than 2.2).
6. Settlement of the percentage of the fund assigned to the collaborator according to the result obtained.

Additionally, vesting and payout are subject to a minimum 9-box performance evaluation (≥ 2.2).

CEO & executives Compensation metrics

CEO Compensation - Long-Term Performance Alignment

Plan administration

In Colombia, the plan is administered through a Pension and Severance Fund Administrator (Administradora de Fondos de Pensiones y Cesantías). ISA and its affiliated companies in Colombia contribute the capital equivalent to the defined benefit for each eligible employee. This amount is then invested by the fund in a stock portfolio that includes ISA shares.

For eligible executives in international subsidiaries, the plan is recognized directly in the accounting records of each respective company.

ISA and its Companies will deliver the capital corresponding to the sum of the defined benefit for each eligible employee, which will be invested by the Fund in a portfolio of shares that includes ISA shares.

Unvested Contributions

100% Investment in ISA Shares

Each employee holds shares in a personal account under their own name

Vested Contributions



ISA assigns benefits to each eligible employee



The recognition of the plan for eligible executives in foreign companies will be made in the company's own accounting. The pension and severance fund acquires a **portfolio of 100% ISA shares** out of the total allocated which are held by the autonomous assets of the Pension Fund. The contribution varies according to the Fund's profitability (share price and dividends)



Requirement

If the goals are met, the assigned benefit passes to the eligible Employee

CEO & executives Compensation metrics

Management ownership and requirements

ISA establishes minimum shareholding requirements for its senior executives, expressed as multiples of their annual base salary and invested in a pension fund composed entirely of ISA shares. Specifically, the CEO must maintain a holding equivalent to six times their annual base salary; VPs, three times; and Directors, two times. These requirements are part of the long-term variable compensation structure and are publicly disclosed in the company's Integrated Management Report 2023. The Vice Presidents to whom the three-times base salary requirement applies are publicly identified in the 2025 Sustainability Report (<https://isa.co/wp-content/uploads/2026/06/integrated-management-report-2025-may-1.pdf>) , page 34.

Furthermore, the CEO's salary and compensation details are considered sensitive personal data under Colombian data protection law, particularly Law 1266 of 2008 and Article 15 of the Political Constitution of Colombia. According to this legal framework, salary information is classified as private data and its processing is subject to principles of confidentiality, purpose limitation, and prior authorization from the data subject. Therefore, such information can only be disclosed with the explicit consent of the individual or under a legal mandate.

In compliance with these legal provisions and in respect of the fundamental right to habeas data, ISA refrains from publicly disclosing personal salary data that could infringe upon the rights of the individuals concerned. This approach ensures legal compliance while maintaining transparency through shareholding disclosures expressed as multiples of base salary.

Beneficial owner	# of salaries	Calculation	# Shares
CEO	6	6	Not available
Chief Energy Transmission Officer	3	3	10,014
Chief Strategy Officer	3	3	10,014
Chief Growth and Business Development & Road Officer	3	3	10,014
Chief Institutional Relations Officer	3	3	10,014
Chief Risk and Compliance Officer	3	3	10,014
Chief Organizational Talent Officer	3	3	10,014
Chief Legal Officer	3	3	10,014
Chief Corporate Finance Officer	3	3	10,014
Chief Information Technology Officer	3	3	10,014
Chief Corporate Audit Officer	3	3	10,014
ISA Directors – ISA's companies Managers/Directors	2	2	10,014

Vice Presidency	
Base salary	78.974.200
Bonus target	3
Target bond amount	236.922.600
Share price	23.660
# shares held	10.014



CONEXIONES QUE INSPIRAN

Long-Term Incentives for Employees



1) the type of long-term incentive program	1. Cash incentives.
2) the type of employees below the senior management level the program applies to:	2. It applies to all non-executive employees of level 3 (analysts, specialists, and support staff) in the company, who participate in collective agreements
Our long-term incentives for employees below the senior management level are on average paid out after	Our long-term incentives for employees below the senior management level are on average paid out after
Percentage of your workforce below senior management level (max. two levels from the CEO) that this program applies to	12%
Do the long-term incentives include targets associated with sustainability performance	Every 5 years, people linked to the company receive a monetary incentive associated with the fulfillment of individual and corporate targets related to sustainable strategic goals: -Comply with project deadlines and expected quality levels. -Net zero pathway, the achievement of an individual employee performance rating above 90%, and meeting the target -Reach over 90 % individual performance by employees. -Total Recordable Injury Frequency Rate (TRIFF) for both employees and contractors



Human talent
that drives results and growth
of ISA and its companies.

Business Ethics

ISA and its companies understand that commitment to life, respect, transparency, honesty and responsibility are drivers of integrity, induce continuous improvement and represent a permanent invitation to live them in every decision, action and interaction with the various stakeholders

Anti-Bribery & Anti-Corruption Policy

Training for anti-bribery and anti-corruption

During 2025, ISA implemented a comprehensive ethics and compliance training and culture agenda under its cultural principle of “Always Ethical.” A total of 97% of employees, including both management and non-management personnel, received training on the updated Code of Ethics and Conduct. The training covered key compliance topics, including anti-corruption and anti-bribery practices, fraud prevention, anti-money laundering measures, and information confidentiality.

In addition, ISA conducted an Ethics Week, addressing topics such as anti-money laundering prevention, ethical business practices, and other compliance-related matters, further strengthening the organization’s culture of integrity and ethical decision-making.

Ethics and Compliance Training: Update to the Code of Ethics and Conduct course, with an emphasis on preventing corruption, bribery, fraud, AML/CFT/PWMD, and other risks. 97% of employees completed the training and signed the integrity pledge. In addition, specific training was provided to leaders.

Key milestones for 2025



Ethics and compliance training: Update to the Code of Ethics and Conduct course, with an emphasis on preventing corruption, bribery, fraud, AML/CFT/PWMD, and other risks. 97% of employees completed the training and signed the integrity pledge. In addition, specific training was provided to leaders.



The ethical culture was assessed.



Semana de la Integridad (Integrity Week): a regional initiative that brought together six countries, featuring over 5,000 hours of training, reaching 8,000 views, and involving employees, leaders, the Ethics Committee, and more than 4,000 suppliers.



The assessment of organizational climate (Great Place To Work) incorporated variables related to ethical behavior with particular emphasis on the perception of honest work and fair and impartial treatment.



Senior management: ethics forums with management teams to strengthen principled leadership.



100% of employees received communications about *Éticos Siempre* (always ethics), helping to Establish this cultural principle as one of the top three most viewed internal content topics, with over 44,000 views.

Training for anti-bribery and anti-corruption

[GRI 205-2] [GRI 205-2-a] [GRI 205-2-b] [GRI 205-2-c] [GRI 205-2-d] [GRI 205-2-e] Communication and Training on Anti-Corruption Policies and Procedures											
	ISA	ISA INTERCOLOMBIA	ISA TRANSELCA	ISA BOLIVIA	ISA REP/ISAP	ISA INTERCHILE	ISA CTEEP	XM	INTERNEXA	INTERVIAL	RUTA COSTERA
Number of members of the governance body	19	13	6	N. D.	11	10	10	22	7	9	5
Number of governance body members to whom the organization's anti-corruption policies and procedures have been communicated	19	13	6	N. D.	11	10	10	22	7	9	5
Percentage of governance body members to whom the organization's anti-corruption policies and procedures have been communicated	100%	100%	100%	N. D.	100%	100%	100%	100%	100%	100%	100%
Total number of employees	311	821	192	28	480	121	1626	404	351	315	265
Number of employees to whom the organization's anti-corruption policies and procedures have been communicated	294	811	192	28	480	119	1572	404	351	315	265
Percentage of employees to whom the organization's anti-corruption policies and procedures have been communicated	95%	99%	100%	N. D.	100%	98%	97%	100%	100%	100%	100%
Number of governance body members who have received anti-corruption training	19	13	6	N. D.	11	10	0	22	N.D	9	5
Percentage of governance body members who have received anti-corruption training	100%	100%	100%	N. D.	100%	100%	0%	100%	N.D	100%	0
Number of employees who have received anti-corruption training	294	811	192	N. D.	475	117	1572	404	N. D.	315	265
Percentage of employees who have received anti-corruption training	95%	99%	100%	N. D.	99%	97%	97%	100%	N. D.	100%	0

Ethics line

Established procedures for handling breaches

Purpose

To have a communication channel through which stakeholders of ISA and its companies can consult or report breaches of our Code of Ethics and Conduct.



Management

An external call center (independent third party) serves the ethics line. Once the cases have been received, recorded and classified (details of the reports received are kept confidential), these are managed by the Ethics Committee.

Information processing

The information received through the ethics line is classified and managed as confidential. Personal data are processed appropriately and for authorized purposes. The identity of the person is protected (reporters may submit their reports anonymously).



All reports submitted through the Ethics Hotline are captured in a secure case management system with strict, role-based access limited to authorized Compliance personnel. The Company provides multiple accessible reporting channels to ensure safe and confidential disclosure. Cases are handled with the **Ethical Matters Management Protocol**, which outlines investigation stages, defined roles and responsibilities, escalation pathways, & confidentiality standards, while ensuring strong protection against retaliation for whistleblowers & reporters.

Ethical Matters Management

The Company applies a formal protocol to manage ethical concerns, defining criteria, roles, and processes for assessment, investigation, and response under the Ethics and Compliance Program. Annual disclosures on Ethics Hotline activity—covering report volumes, case categories, investigation status, and actions taken—support transparency, accountability, and continuous improvement.



Anti-Bribery & Anti-Corruption Policy

Corrective or disciplinary actions when there is a breach of the policy

Aware of the importance of monitoring compliance with the provisions of the Corporate Ethics and Compliance Program, we have implemented a series of indicators, some of them with online information, which allow us to identify progress in management or alert situations that can be managed to avoid the materialization of any risk. This initiative is advanced as part of the development of the organizational capacity for digital transformation, seeking to provide the company with early signals through data analytics. Some of the issues being monitored to date are: payments made to PEP (politically exposed persons), reporting and management of conflicts of interest and disqualifications and incompatibilities, management of the Ethics Line, training, payments made to third parties in high-risk jurisdictions, payments for social management, donations, sponsorships and works for taxes. The results of management are reported for follow-up and evaluation to the required bodies, including: the Ethics Committee, the Audit and Risk Committee and/or the Board of Directors or whoever is acting in their stead in each of the companies.

Monitoring and Oversight

One hundred percent (100%) of the monitoring plan defined in the Compliance Plan was executed, focusing on risks related to bribery, corruption, fraud, money laundering, terrorist financing, proliferation financing, and violations of the Code of Ethics and Conduct. The results were reported to the corresponding governance bodies.

Ethics Hotlines

ISA and its companies have ethics hotlines operated by independent third parties in Latin America and Brazil, ensuring confidentiality, anonymity, and data protection. Their use is actively encouraged, and a zero-retaliation policy is maintained.

During 2025, 225 cases were received, 66% of which were related to ethical matters. Twenty-two cases were substantiated and managed through preventive and improvement actions. No cases of corruption, bribery, money laundering, terrorist financing, proliferation financing, or human rights violations were substantiated.

Anti-Bribery & Anti-Corruption Policy

Established procedures for handling breaches

ISA and its companies operate ethics hotlines managed by independent third parties across Latin America and Brazil, which guarantee confidentiality, anonymity, and data protection. Their use is actively encouraged, and a zero-retaliation policy protects anyone who reports in good faith. These channels are the entry point to a structured breach-handling procedure that governs how each report is assessed, investigated, and resolved once a potential violation — including bribery and corruption — has been identified.

The Company has established a formal protocol that defines the criteria, responsibilities, and end-to-end process for assessing, investigating, documenting, reporting, and responding to breaches of the Code of Ethics and Conduct and of the Business Ethics and Compliance Program, including incidents of bribery and corruption. The protocol governs the actions triggered once a potential breach has been reported or otherwise identified and operates under whistleblower safeguards and confidentiality protections at every stage.



Anti-Bribery & Anti-Corruption Policy

Established procedures for handling breaches

Once a report is received, the Ethics Line Channel Operator receives, registers, classifies, routes, and follows up on the case. The Compliance Department then analyzes and investigates the matter and documents its findings. Where warranted, the Ethics Committee reviews the case, requests or authorizes formal investigations, recommends the actions required to handle the report, and follows up on their implementation and on the overall management of the ethics line. This escalation path ensures that every identified breach is subject to structured analysis, independent investigation, and governance-level oversight.

When an allegation is substantiated, the Company applies corrective and disciplinary measures designed both to contain the impact and to remediate the underlying process weaknesses. The principal measures include:

- Termination of employee and contractor contracts;
- Disciplinary actions in accordance with internal regulations;
- Ethical reinforcement and targeted interventions in the areas where the conduct was identified;
- Initiation of legal or judicial proceedings where applicable.

Beyond case-specific sanctions, the Company implements process adjustments to prevent recurrence, addressing the root causes identified during the investigation. The operation of these procedures — including the number of reports received, case categorization, investigation status, and actions taken in response to substantiated cases — is documented and disclosed in the Company's annual management report, supporting audit, review, transparency, and continuous improvement of the ethics and compliance framework.

During 2025, the Company further reinforced these procedures through awareness and training sessions on the appropriate use of the reporting channels and conducted a perception survey of more than **3,800 employees to assess the awareness, accessibility, trust, and effectiveness of the mechanism.**

Whistleblowing Mechanism

Provision of training on the use of the Ethics Line

ISA provides ongoing training to its personnel on the purpose and use of the Ethics Line as the channel for reporting breaches of the Code of Ethics and Conduct. **During 2025, 97% of employees completed virtual training**, which covered the scope, appropriate use, and **reporting process of the Ethics Line**.

This training is delivered through a formal, **company-wide Code of Ethics and Conduct course**, available online and free of charge to all personnel, which reinforces how and when to raise concerns or report potential misconduct. The training makes clear that the Ethics Line guarantees confidentiality, protects the reporter's identity, and ensures that no retaliation will result from raising a concern or reporting a potential breach — reinforcing employees' trust in the mechanism and promoting transparency and accountability across the organization.



Curso código de ética y conducta

Información del curso

Tipo: En línea

Duración: 1.25 horas

Gratuito



Línea ética





La Línea Ética está diseñada para brindarte un medio a través del cual puedes resolver tus inquietudes, aclarar dudas o reportar cualquier incumplimiento al Código de Ética y Conducta de ISA y sus empresas.

Haz clic en el siguiente botón y conoce los datos de contacto de cada empresa.

Datos de contacto ←

Importante: La Línea Ética garantiza total confidencialidad, protege tu identidad y asegura que no habrá ningún tipo de represalia por consultar o reportar una situación de incumplimiento.

Information security

Information Security Governance

Information security and cybersecurity governance at ISA is composed of several elements, including the **Integrated Risk Management Model**, which adheres to international standards such as **ISO 31000**, **ISO 27001**, and the **NIST framework**. Oversight is provided by the **Board of Directors** and the **Executive Committee**, both of which are actively involved in risk management, including cyber risks.



ISA's [Board of Directors](#) includes a member with strong expertise in information security: **Camilo Zea**.

Camilo Zea has over 15 years of experience in IT systems implementation and more than 10 years of experience in information security, cybersecurity, and operational IT responsibility as a senior executive. He is the CEO of **PRONUS**, a company specializing in outsourced risk management for clients lacking in-house expertise or the organizational and technological capacity to manage risk internally.

Two key committees, defined under **Board Agreements 128, 129, and 136**, work in a complementary manner to ensure comprehensive cybersecurity governance at ISA, covering strategy, execution, and control:

- **Corporate Governance, Sustainability, Technology, and Innovation Committee**, which focuses on high-level oversight, strategy, and policies related to cybersecurity and IT (pp4). This role is established in [Board Agreement 129 of 2022](#)
- **Audit and Risk Committee**, responsible for the implementation, assessment, and operational control of risks, including cyber risks (pp 4-5). Its responsibilities are outlined in [Board Agreements 128 of 2022](#) and [136 of 2025](#)



Information Security Governance

- The executive-level oversight of information security matters is led by the Vice President of Information Technology (Chief Information Officer – CIO), who is responsible for supervising the company’s cybersecurity strategy and operations.
- At ISA, the CIO holds a strategic and cross-functional role within the business group. Their mission is to lead the management of information technology and telecommunications through an aligned, integrated, proactive, and innovative approach aimed at building business capabilities that drive the growth and sustainability of ISA and its companies.



Key Cybersecurity Responsibilities of the CIO:

- Design ICT security and contingency strategies to mitigate risks and ensure business continuity.
- Identify and define action plans to reduce risks associated with information assets.
- Review the legal framework applicable to ICT, including intellectual property, industrial rights, and third-party data protection.
- Participate in audits aimed at identifying and mitigating risks in the management and application of ICT.
- Establish the ICT management and service model, including monitoring service levels and conducting cost-benefit analyses.
- Provide technical support in technology-related negotiations.



Information Security Governance

- It's essential to mention also that, at the business group level, ISA has a Cybersecurity Coordinator who performs the duties of a Chief Information Security Officer (CISO). This individual leads the group-wide cybersecurity strategy and oversees the Cybersecurity Center of Excellence (CoE) for ISA and its affiliated companies.
- This role is responsible for defining and executing ISA's corporate and regional cybersecurity strategy, reporting directly to the Vice President of Information Technology. This role leads a robust organizational structure that includes functional liaisons, IT/OT specialists, and regional nodes, ensuring comprehensive coverage across all organizational levels.
- Additionally, the coordinator heads the Cybersecurity Center of Excellence, a key platform for standardization, innovation, and alignment with ISA Group's strategic objectives.

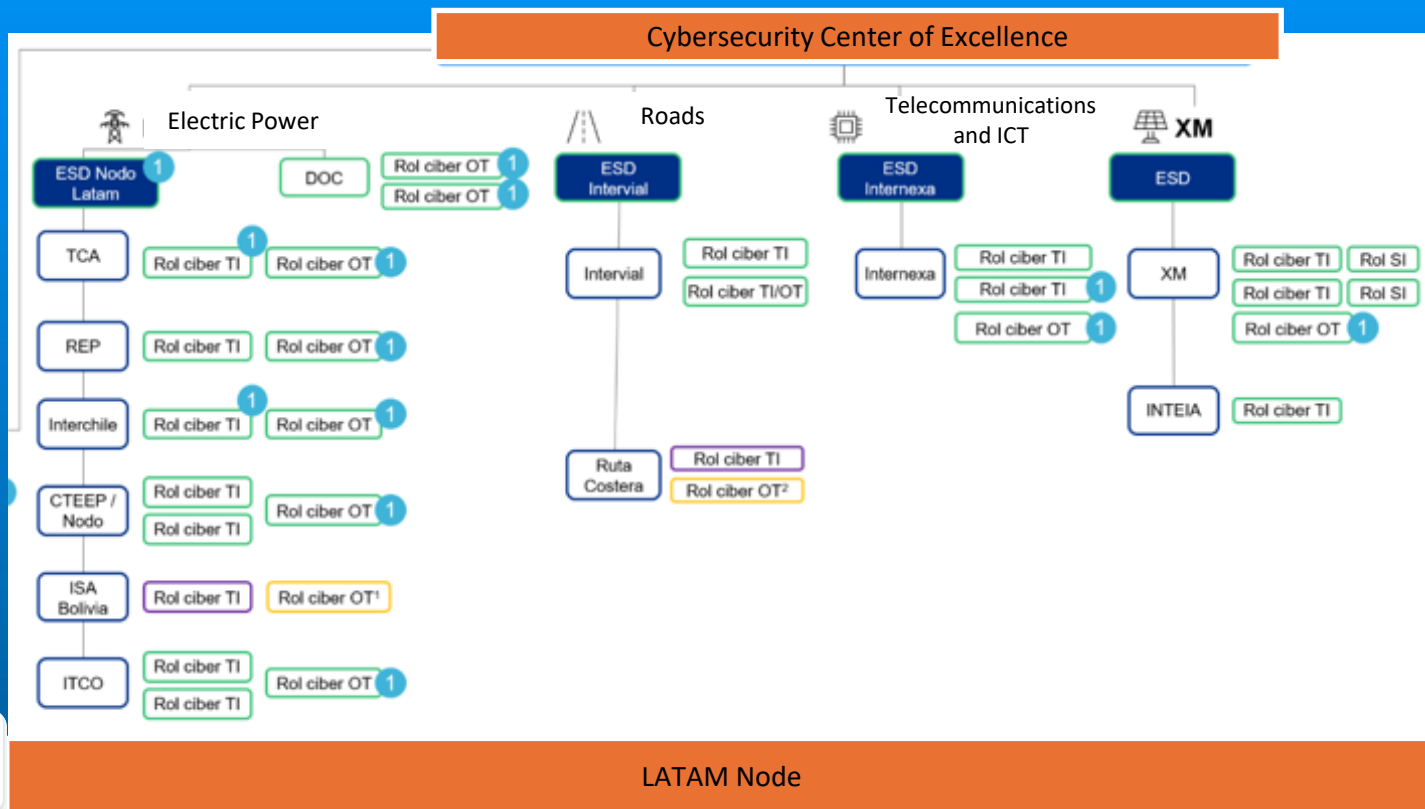
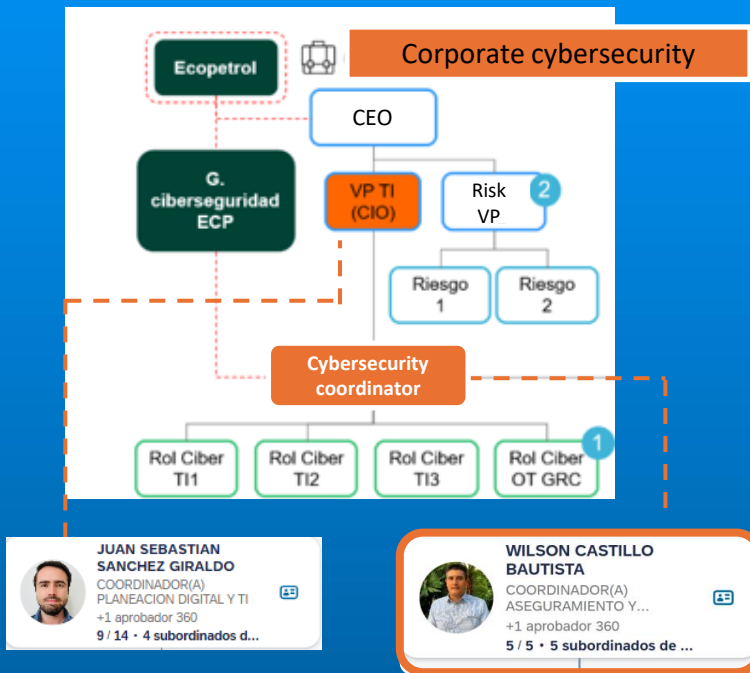


Key Responsibilities of the Cybersecurity Coordinator/CISO:

- Design and lead the Cybersecurity Roadmap, driving initiatives to mitigate third-party risks, strengthen architectures, and build cybersecurity capabilities and culture.
- Coordinate the Cybersecurity Center of Excellence, promoting best practices, reference frameworks, and innovative solutions aligned with the corporate vision.
- Define cybersecurity maturity goals for subsidiaries, ensuring consistency and continuous improvement in protection levels.
- Activate and participate in the Crisis Committee, leading cyber crisis simulations and strengthening the organization's response to high-impact incidents.
- Manage the cybersecurity budget and resource allocation, optimizing investments and capabilities across the organization.
- Oversee cyber incident management, coordinating internal and external teams to ensure **timely, effective responses in compliance with regulatory frameworks**

Information Security Governance

Cybersecurity organizational structure



The CoE will respond to IT activities by communicating with the OT workgroup through the ESDs and the Corporate OT Cybersecurity role, sharing responsibilities

Policy commitments

Continuously improving information security systems

ISA has integrated management systems across its subsidiaries, including the implementation of the ISO/IEC 27001 standard as a key framework for information security management. Several ISA companies have certified Information Security Management Systems (ISMS), ensuring structured risk management, compliance, and operational resilience.

Integrated management systems

Company	ISO9001	ISO14001 ¹	ISO27001	ISO45001	ISO55001	ISO39001	Gender equity ¹	EFR ²	Carbon neutral
ISA	✓			✓			✓		✓
ISA INTERCOLOMBIA	✓	✓	✓	✓	✓		✓		✓
ISA REP	✓	✓		✓	✓				✓
ISA ENERGÍA IN BRAZIL		✓		✓	✓		✓		✓
ISA ENERGÍA IN CHILE				✓					✓
ISA TRANSELCA	✓	✓		✓	✓		✓		✓
ISA BOLIVIA	✓	✓		✓	✓				✓
ISA VÍAS IN CHILE	✓	✓		✓		✓	✓		✓
RUTA COSTERA				✓					✓
INTERNEXA	✓		✓	✓				✓	✓
XM			✓				✓		✓
INTEIA	✓		✓	✓					✓

- We recognize that information security risks are dynamic and evolving. Therefore, ISA is committed to the continuous improvement of its ISMS, proactively addressing emerging threats and vulnerabilities. Our cybersecurity processes are regularly reviewed and updated to adapt to new technologies, regulatory changes, and evolving risk landscapes.

- In line with our commitment to operational excellence, we also adopt international standards such as **ISO 9001, ISO 14001, ISO 45001, ISO 55001, and ISO 39001** across various subsidiaries, reinforcing our culture of quality, environmental stewardship, workplace safety, and infrastructure reliability.

Policy commitments

Assurance

ICONTREC Certifica que el Sistema de Gestión de la organización:
ICONTREC certifies that the Organization's Management System of:

XM COMPAÑIA DE EXPERTOS EN MERCADOS S.A. E.S.P. XM S.A.
E.S.P.

Calle 12 sur No 18 - 168 bloque 2, Medellín, Antioquia, Colombia

ha sido auditado y aprobado con respecto a los requisitos especificados en:
has been audited and approved based on the specified requirements of:

ISO/IEC 27001:2022

Este Certificado es aplicable al siguiente alcance:
This certificate is applicable to the following scope:

Seguridad de la información para prestar servicios de operación en Sistemas Eléctricos Interconectados y administración de mercados energéticos, incluidos los servicios de información y capacitación. Declaración de Aplicabilidad 0602DSG4 Versión 7.0 de 2024-05-22

Information security for: Provide services related to the operation of interconnected power systems and energy markets, including information and training services. Statement of Applicability 0602DSG4 Version 7.0 dated 2024-05-22

Esta aprobación está sujeta a que el sistema de gestión se mantenga de acuerdo con los requisitos especificados, lo cual será verificado por ICONTREC.
This approval is subject to the maintenance of the management system according to the specified requirements, which will be verified by ICONTREC.

Certificado: SI-CER273919-1

Fecha de Otorgamiento: 2024-10-16
Fecha de Vencimiento del Ciclo Previo: 2024-10-16
Fecha de Inicio del ciclo actual de certificación: 2024-10-16
Fecha de Vencimiento ciclo actual: 2024-10-16
Fecha de Auditoria de Recertificación: 2024-10-16
Fecha de Revisión: 2024-10-16

Roberto Enrique Montoya Villa
Director Ejecutivo - CEO

ISO/IEC 27001:2022

ICONTREC

OONAC

IAF

Este certificado es propiedad de ICONTREC, ubicado en la Calle 12 Sur No. 18, Carrera Doccia, Torre 4 piso 10 y 11, Bogotá D.C., Colombia.

F 35-003 Versión 01

ICONTREC Certifica que el Sistema de Gestión de la organización:
ICONTREC certifies that the Organization's Management System of:

XM COMPAÑIA DE EXPERTOS EN MERCADOS S.A. E.S.P. XM S.A.
E.S.P.

Calle 12 sur No 18 - 168 bloque 2, Medellín, Antioquia, Colombia

ha sido auditado y aprobado con respecto a los requisitos especificados en:
has been audited and approved based on the specified requirements of:

ISO/IEC 27001:2022

Este Certificado es aplicable al siguiente alcance:
This certificate is applicable to the following scope:

Seguridad de la información para Recibir y validar el reporte de las mediciones de energía eléctrica enviadas por los representantes de las fronteras comerciales al Administrador del Sistema de Intercambios Comerciales (ASIC). Declaración de Aplicabilidad 0602DSG4 Versión 7.0 de 2024-05-22

Information security for: Receive and validate the report of measurements of electrical energy sent by the representatives of trade borders to the ASIC (Administrator of Commercial System Interchange). Statement of Applicability 0602DSG4 Version 7.0 dated 2024-05-22

Esta aprobación está sujeta a que el sistema de gestión se mantenga de acuerdo con los requisitos especificados, lo cual será verificado por ICONTREC.
This approval is subject to the maintenance of the management system according to the specified requirements, which will be verified by ICONTREC.

Certificado: SI-CER273919-2

Fecha de Otorgamiento: 2024-10-16
Fecha de Vencimiento del Ciclo Previo: 2024-10-16
Fecha de Inicio del ciclo actual de certificación: 2024-10-16
Fecha de Vencimiento ciclo actual: 2024-10-16
Fecha de Auditoria de Recertificación: 2024-10-16
Fecha de Revisión: 2024-10-16

Roberto Enrique Montoya Villa
Director Ejecutivo - CEO

ISO/IEC 27001:2022

ICONTREC

OONAC

IAF

Este certificado es propiedad de ICONTREC, ubicado en la Calle 12 Sur No. 18, Carrera Doccia, Torre 4 piso 10 y 11, Bogotá D.C., Colombia.

F 35-003 Versión 01

ICONTREC Certifica que el Sistema de Gestión de la organización:
ICONTREC certifies that the Organization's Management System of:

XM COMPAÑIA DE EXPERTOS EN MERCADOS S.A. E.S.P. XM S.A.
E.S.P.

Calle 12 sur No 18 - 168 bloque 2, Medellín, Antioquia, Colombia

ha sido auditado y aprobado con respecto a los requisitos especificados en:
has been audited and approved based on the specified requirements of:

ISO/IEC 27001:2022

Este Certificado es aplicable al siguiente alcance:
This certificate is applicable to the following scope:

Seguridad de la información para el diseño, implementación, administración, operación y mantenimiento del sistema centralizado de información de convocatorias públicas SICEP, que incluye la gestión de la información sobre las convocatorias públicas para la celebración de contratos de compras de energía del mercado regulado. Declaración de Aplicabilidad 0602DSG4 Versión 7.0 de 2024-05-22

Information security for the design, implementation, administration, operation and maintenance of the centralized information system for public calls SICEP, including the information management on public calls for the performance of energy purchase contracts in the regulated market. Statement of Applicability Version 7.0 dated 2024-05-22

Esta aprobación está sujeta a que el sistema de gestión se mantenga de acuerdo con los requisitos especificados, lo cual será verificado por ICONTREC.
This approval is subject to the maintenance of the management system according to the specified requirements, which will be verified by ICONTREC.

Certificado: SI-CER273919-3

Fecha de Otorgamiento: 2024-10-16
Fecha de Vencimiento del Ciclo Previo: 2024-10-16
Fecha de Inicio del ciclo actual de certificación: 2024-10-16
Fecha de Vencimiento ciclo actual: 2024-10-16
Fecha de Auditoria de Recertificación: 2024-10-16
Fecha de Revisión: 2024-10-16

Roberto Enrique Montoya Villa
Director Ejecutivo - CEO

ISO/IEC 27001:2022

ICONTREC

OONAC

IAF

Este certificado es propiedad de ICONTREC, ubicado en la Calle 12 Sur No. 18, Carrera Doccia, Torre 4 piso 10 y 11, Bogotá D.C., Colombia.

F 35-003 Versión 01

ICONTREC Certifica que el Sistema de Gestión de la organización:
ICONTREC certifies that the Organization's Management System of:

ISA INTERCOLOMBIA S.A. E.S.P.

Calle 12 Sur No. 18 - 168. Medellín, Antioquia, Colombia

ha sido auditado y aprobado con respecto a los requisitos especificados en:
has been audited and approved based on the specified requirements of:

ISO/IEC 27001:2013

Este Certificado es aplicable al siguiente alcance:
This certificate is applicable to the following scope:

Sistema de Gestión de Seguridad de la información para el mantenimiento de infraestructura eléctrica del Sistema de Transmisión de Energía. Declaración de Aplicabilidad SGI V8 - 2023/09

Information security management system for the maintenance of electrical infrastructure of energy transmission system. Statement of Applicability SGI V8 - 2023/09

Esta aprobación está sujeta a que el sistema de gestión se mantenga de acuerdo con los requisitos especificados, lo cual será verificado por ICONTREC.
This approval is subject to the maintenance of the management system according to the specified requirements, which will be verified by ICONTREC.

Certificado: SI - CER28012013

Fecha de Otorgamiento: 2023-11-14
Fecha de Vencimiento del Ciclo Previo: 2023-11-14
Fecha de Inicio del ciclo actual de certificación: 2023-11-14
Fecha de Vencimiento ciclo actual: 2023-11-14
Fecha de Auditoria de Recertificación: 2023-11-14
Fecha de Revisión: 2023-11-14

Roberto Enrique Montoya Villa
Director Ejecutivo - CEO

ISO/IEC 27001:2013

ICONTREC

OONAC

IAF

Este certificado es propiedad de ICONTREC, ubicado en la Calle 12 Sur No. 18, Carrera Doccia, Torre 4 piso 10 y 11, Bogotá D.C., Colombia.

F 35-003 Versión 01

Policy commitments

Assurance

ICONTEC ES MIEMBRO DE

IQNET

icontec
ISO / IEC
27001

ICONTEC Certifica que el Sistema de Gestión de la organización:
ICONTEC certifies that the Organization's Management System of:

INTERNEXA S.A.

Calle 12 Sur No. 16-166, Bloque - 5 Piso 2, Medellín, Antioquia, Colombia

Víase las actividades cubiertas por el sistema de gestión para cada una de las sedes permanentes diferentes a la sede principal en el anexo

ha sido auditado y aprobado con respecto a los requisitos especificados en:
has been audited and approved based on the specified requirements of:

ISO/IEC 27001:2022

Este Certificado es aplicable al siguiente alcance:
This certificate is applicable to the following scope:

Diseño, suministro, montaje, operación y mantenimiento de infraestructura para la prestación del servicio de transporte de información o los relacionados con las tecnologías de información y las comunicaciones. Declaración de Aplicabilidad Mp4.2.005 Versión 03 de 2025-02-10.

Design, supply, assembly, operation, and maintenance of infrastructure for the provision of the information transport service or those related to information and communication technologies. Statement of Applicability Mp4.2.005 Versión 03 dated 2025-02-10.

Esta aprobación está sujeta a que el sistema de gestión se mantenga de acuerdo con los requisitos especificados, lo cual será verificado por ICONTEC.
This approval is subject to the maintenance of the management system according to the specified requirements, which will be verified by ICONTEC.

Certificado: SI-CER/18021

Fecha de Otorgamiento: 2025-09-21
Fecha de Vencimiento del Ciclo Previo: 2025-07-29
Fecha de Inicio del ciclo actual de certificación: 2025-07-29
Fecha de Vencimiento ciclo actual: 2026-07-29
Fecha de Auditoría de Recertificación: 2026-09-02
Fecha de Renovación: 2026-07-02

Roberto Enrique Montoya Villa
Director Ejecutivo - CEO

icontec

OONAC
ACREDITADO

IAF
MEMBER OF ASSOCIATION
INTERNATIONAL ASSOCIATION

Este centro es en propiedad de ICONTEC, ubicado en la calle 1001 Sur 16.
Código: Documento: Item 4 plan y 10 Diagrama D.C., Colombia

F-PS-001 Versión 01

ICONTEC ES MIEMBRO DE

IQNET

icontec
ISO / IEC
27001

ICONTEC Certifica que el Sistema de Gestión de la organización:
ICONTEC certifies that the Organization's Management System of:

INTERNEXA S.A.

Calle 12 Sur No. 16-166, Bloque - 5 Piso 2, Medellín, Antioquia, Colombia

Víase las actividades cubiertas por el sistema de gestión para cada una de las sedes permanentes diferentes a la sede principal en el anexo

ha sido auditado y aprobado con respecto a los requisitos especificados en:
has been audited and approved based on the specified requirements of:

ISO/IEC 27001:2022

Este Certificado es aplicable al siguiente alcance:
This certificate is applicable to the following scope:

Diseño, suministro, montaje, operación y mantenimiento de infraestructura para la prestación del servicio de transporte de información o los relacionados con las tecnologías de información y las comunicaciones. Declaración de Aplicabilidad Mp4.2.005 Versión 03 de 2025-02-10.

Design, supply, assembly, operation, and maintenance of infrastructure for the provision of the information transport service or those related to information and communication technologies. Statement of Applicability Mp4.2.005 Versión 03 dated 2025-02-10.

Esta aprobación está sujeta a que el sistema de gestión se mantenga de acuerdo con los requisitos especificados, lo cual será verificado por ICONTEC.
This approval is subject to the maintenance of the management system according to the specified requirements, which will be verified by ICONTEC.

Certificado: SI-CER/18021

Fecha de Otorgamiento: 2025-09-21
Fecha de Vencimiento del Ciclo Previo: 2025-07-29
Fecha de Inicio del ciclo actual de certificación: 2025-07-29
Fecha de Vencimiento ciclo actual: 2026-07-29
Fecha de Auditoría de Recertificación: 2026-09-02
Fecha de Renovación: 2026-07-02

Roberto Enrique Montoya Villa
Director Ejecutivo - CEO

icontec

OONAC
ACREDITADO

IAF
MEMBER OF ASSOCIATION
INTERNATIONAL ASSOCIATION

Este centro es en propiedad de ICONTEC, ubicado en la calle 1001 Sur 16.
Código: Documento: Item 4 plan y 10 Diagrama D.C., Colombia

F-PS-001 Versión 01

Policy commitments

Establishing individual responsibilities for information security for the entire workforce

ISA and its companies have in place an articulated regulatory framework that assigns individual information security responsibilities to the entirety of their workforce. This framework is composed of the Information, Knowledge and Artificial Intelligence Policy, the Code of Ethics and Conduct, and Corporate Guide No. 62 on the use, development, and implementation of artificial intelligence and information security.

The Information, Knowledge and Artificial Intelligence Policy defines the general principles for information management and protection applicable across the organization. Building on this foundation, the Corporate Guide for the Use and Management of Information and Communications Technology develops the operational security guidelines governing the use of information systems by all users of ISA and its companies. The Code of Ethics and Conduct, in turn, reinforces the general duty of care and proper use of information assets that applies to every member of the workforce.

Corporate Guide No. 62 particularizes and reinforces this principle within the domain of artificial intelligence solutions. Section 5.3.4 — Individual Responsibility and the Indispensability of the Human Component — establishes that all persons working for or on behalf of ISA and its companies are individually responsible for protecting the confidentiality, integrity, and availability of the information they access, use, or manage. This responsibility translates into concrete, enforceable actions: acting diligently to prevent misuse, loss, unauthorized disclosure, or alteration of information, in compliance with the policies, standards, and guidelines established by the organization.

In this way, **individual responsibility for information security is not confined to a particular use case**, but constitutes a cross-cutting principle covering the entire workforce — including employees, contractors, and third parties acting on behalf of ISA and its companies — in any interaction with the organization's information systems and assets, regardless of whether that interaction involves artificial intelligence solutions.

Establishing individual responsibilities for information security for the entire workforce

Design Envelope ID: 4E02C1B7-7DEB-8BA3-80A0-91EEAFC0EE49

isa	GUÍA CORPORATIVA		N° 62
	GUÍA PARA USO, DESARROLLO E IMPLEMENTACIÓN DE LA INTELIGENCIA ARTIFICIAL		Versión: 2
	VICEPRESIDENCIA DE TECNOLOGÍA DE LA INFORMACIÓN		Fecha: 01-JUN-2026

1. INTRODUCCIÓN

La inteligencia artificial (IA) está transformando industrias como la transmisión de energía y las concesiones viales, al fortalecer la seguridad, la confiabilidad, la productividad y la eficiencia, y al habilitar nuevas capacidades digitales en los procesos de negocio. En particular, la inteligencia artificial generativa (GenAI) está ampliando las posibilidades de automatización, análisis y creación de contenido en múltiples funciones empresariales. No obstante, su adopción también implica riesgos relevantes en materia de ciberseguridad, privacidad, propiedad intelectual, sesgos, gobierno, calidad y disponibilidad de datos, escalabilidad y desarrollo de capacidades organizacionales y del talento.

2. OBJETIVO

ISA y sus empresas reconocen el valor estratégico de la tecnología de la información y de los datos para el logro de sus objetivos. En ese contexto, la IA tiene el potencial de transformar las industrias en las que opera la organización, al mejorar la eficiencia de los procesos, fortalecer la toma de decisiones y habilitar nuevas capacidades para responder a los retos presentes y futuros.

Esta guía establece los lineamientos para el uso, desarrollo e implementación responsable, seguro y eficaz de soluciones de inteligencia artificial y tecnologías relacionadas. Su propósito es orientar la adopción de estas capacidades bajo criterios de cumplimiento normativo, ética, gestión de riesgos, protección de la información y creación de valor para ISA y sus empresas.

3. ALCANCE

Esta guía establece los lineamientos que ISA y sus empresas deben seguir para el uso, desarrollo e implementación de inteligencia artificial. Aplica a todas las áreas de ISA y sus empresas, así como al personal interno, proveedores y terceros que intervengan o tengan incidencia en soluciones de IA. Cada empresa podrá definir lineamientos, procesos o procedimientos complementarios cuando así lo requiera, siempre que se mantengan alineados con lo dispuesto en este documento. Los desarrollos específicos derivados de requerimientos internos, normativa local u otras condiciones particulares de cada empresa serán responsabilidad de la respectiva organización.

Design Envelope ID: 4E02C1B7-7DEB-8BA3-80A0-91EEAFC0EE49

Guía Corporativa

5

mismo, debe propender por no exacerbar brechas digitales y, bajo el sentido de proporcionalidad, velar porque sea accesible y beneficiosa para todos, incluyendo a diversos agentes y promoviendo la igualdad de acceso, la igualdad de género y la diversidad cultural, evitando al mismo tiempo los efectos discriminatorios y los sesgos prohibidos por el ordenamiento jurídico.

ISA no implementará, promoverá ni tolerará el uso de sistemas de IA destinados al puntaje o clasificación social de personas, a la manipulación encubierta del comportamiento humano, a la explotación de vulnerabilidades de personas o grupos, ni a la vigilancia biométrica masiva no autorizada, en línea con la regulación aplicable y con referentes internacionales como el EU AI Act.

Los sistemas de IA deberán someterse a evaluaciones periódicas de sesgos mediante metodologías, herramientas o criterios definidos por la organización, con el fin de identificar, documentar, mitigar y monitorear impactos discriminatorios o resultados inequitativos durante su ciclo de vida.

Además de las prohibiciones ya definidas en esta guía, no podrán promoverse, desarrollarse, adquirirse, desplegarse ni utilizarse soluciones de IA cuyo propósito o efecto sea eludir controles corporativos, generar engaño material, vulnerar derechos fundamentales, facilitar conductas ilícitas o realizar tratamiento no autorizado de datos, perfiles o inferencias sobre personas.

Cualquier caso de uso que presente duda razonable sobre su licitud, proporcionalidad, legitimidad o aceptabilidad ética deberá escalarse para revisión previa por las instancias competentes antes de continuar su desarrollo o implementación.

5.3.2. Primero la vida

Las soluciones de IA deberán garantizar que priorizarán la vida y la integridad de las personas por encima de todo.

5.3.3. IA centrada en las personas

Los sistemas de IA se desarrollarán y utilizarán como una herramienta al servicio de las personas, que respete la dignidad humana, el conocimiento, la experiencia, y la autonomía personal, y que funcione de manera que pueda ser controlada y vigilada adecuadamente por seres humanos.

5.3.4. Responsabilidad individual e indispensabilidad del componente humano

En todos los casos, las soluciones de IA deberán operar bajo supervisión humana efectiva. La responsabilidad por las decisiones, recomendaciones o acciones apoyadas o ejecutadas mediante estas soluciones recae en el dueño del proceso y en las personas responsables designadas, con independencia del nivel de automatización. En consecuencia, la IA debe entenderse como una herramienta de apoyo y ampliación de capacidades, y no como un reemplazo integral del juicio, la responsabilidad ni la rendición de cuentas humanas. Toda solución deberá garantizar, de manera proporcional a su nivel de riesgo, mecanismos de intervención, ajuste, suspensión o corrección de su comportamiento, así como esquemas claros de supervisión y escalamiento cuando sea necesario.

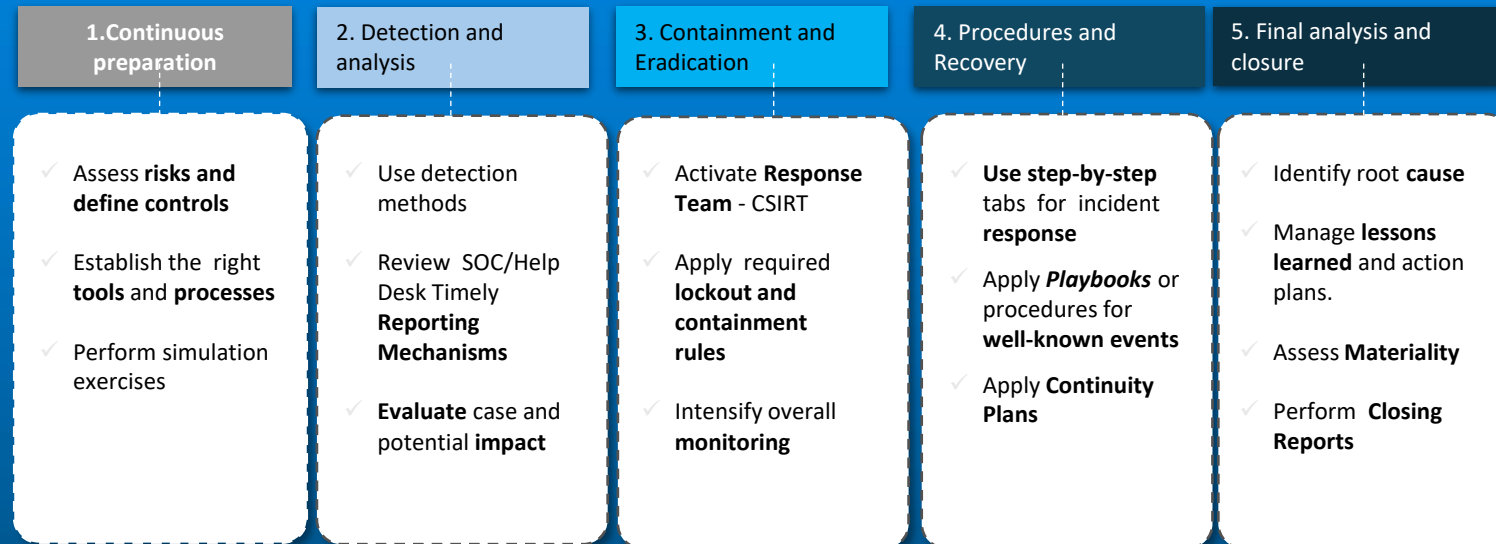
Asimismo, el uso de soluciones de IA no exime a las personas de las responsabilidades inherentes a la protección de la información. En este sentido, todas las personas que trabajen

Policy commitments

Monitoring and responding to information security threats

ISA operates a Cybersecurity Operations Center (SOC) that provides 24/7 monitoring of security events and threats across the organization. This is complemented by cyber threat intelligence and vulnerability management services, which enable proactive identification and prioritization of risks.

Our incident response methodology follows a structured five-phase model: continuous preparation, detection and analysis, containment and eradication, recovery procedures, and final closure. This process ensures rapid response, effective containment, and thorough analysis of root causes.



Policy commitments

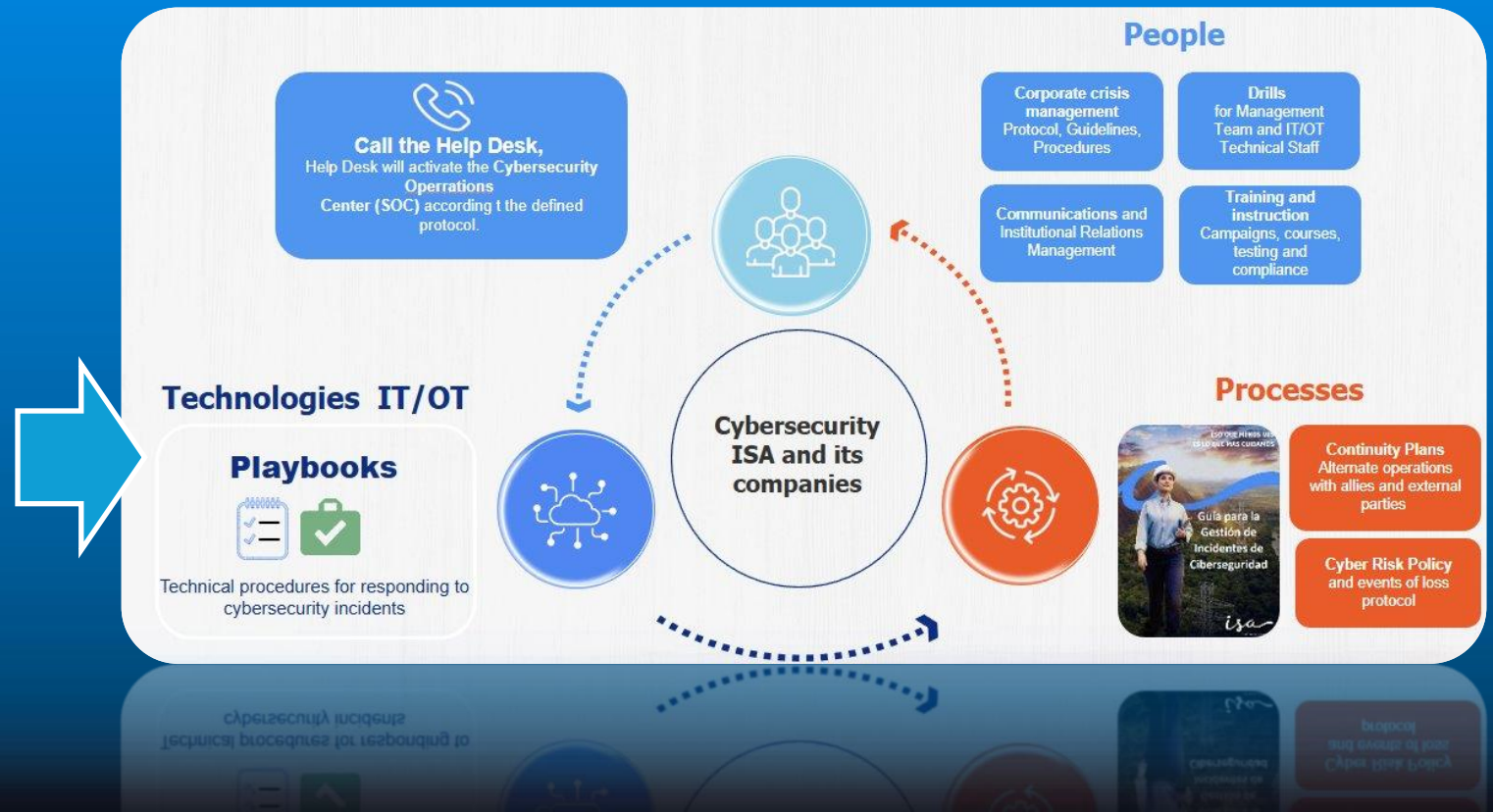
Monitoring and responding to information security threats

Key response activities include:

- Activation of the CSIRT (Computer Security Incident Response Team)
- Use of lockout and containment protocols
- Application of playbooks and continuity plans
- Final assessments, including lessons learned and materiality analysis

Real-time monitoring data (e.g., log volume, correlation rules, escalation metrics) are regularly analyzed to identify trends and optimize defense strategies. For instance, in 2025, ISA handled over 100,000 correlated alarms, 9287 managed cases, and 3708 escalated cybersecurity events.

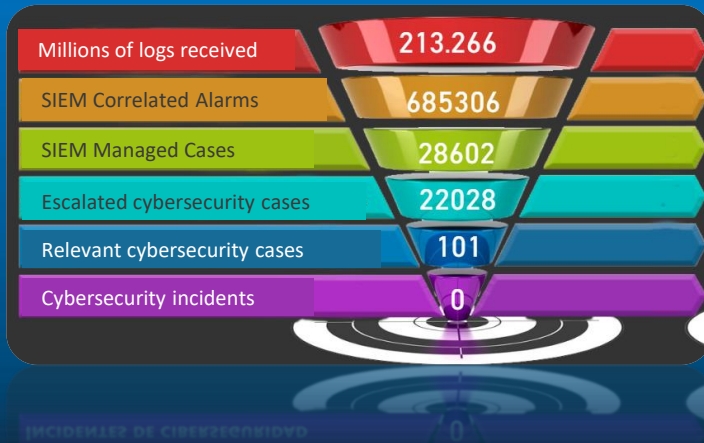
In addition, ISA has a comprehensive crisis framework. The following visual summarizes ISA's integrated approach to cybersecurity preparedness, combining continuous monitoring with clear crisis response protocols, cross-functional training, and alignment of people, processes, and technology:



Cibersecurity roadmap

ISA is also committed to transparency with stakeholders. In the event of incidents with potential impact, we ensure communication of relevant actions taken, mitigation measures, and future prevention plans in accordance with our internal protocols and regulatory frameworks.

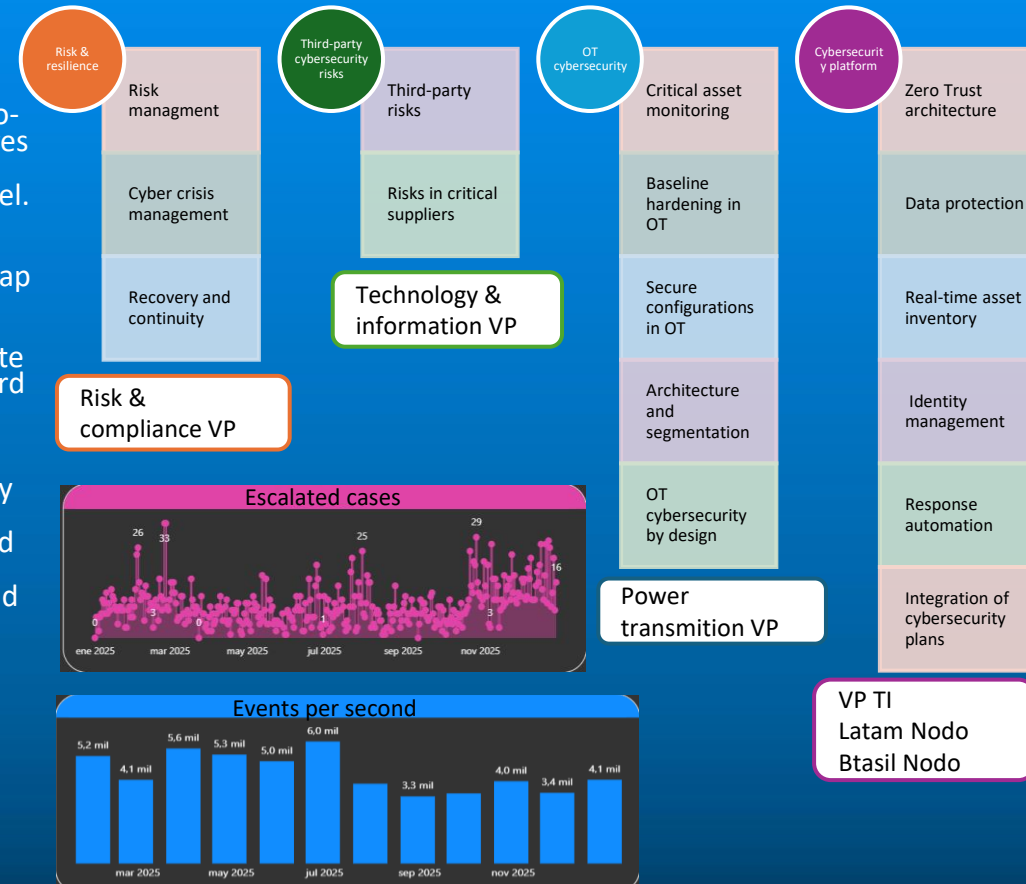
Throughout 2025, security events were continuously monitored, and it was identified that **none of them escalated into major, critical, or high-impact cybersecurity incidents.**



Establishing information security requirements for third parties

ISA has developed a structured and up-to-date Cybersecurity Roadmap, which serves as a strategic guide to strengthen information security at the corporate level. In addition to aligning with corporate governance, regulatory compliance, and secure digital transformation, the roadmap establishes specific functions for risk management across the supply chain, including guidelines to assess and mitigate cybersecurity threats associated with third parties.

In line with this approach, ISA is implementing a Third-Party Cybersecurity Risk Management Program, aimed at ensuring that suppliers meet the required security standards and at reducing risks associated with external relationships and shared infrastructures.



Information security requirements for third parties

This commitment is formalized through the internal document [Anexo Cláusulas Contratos Ciberseguridad.pdf](#), which contains specific contractual clauses that third parties must accept. The most relevant include:

Clause 108: Requires contractors to hold valid information security certifications (e.g., ISO 27001) or, alternatively, to adopt equivalent measures. It also includes provisions for audits, secure data destruction processes, and change management requirements.

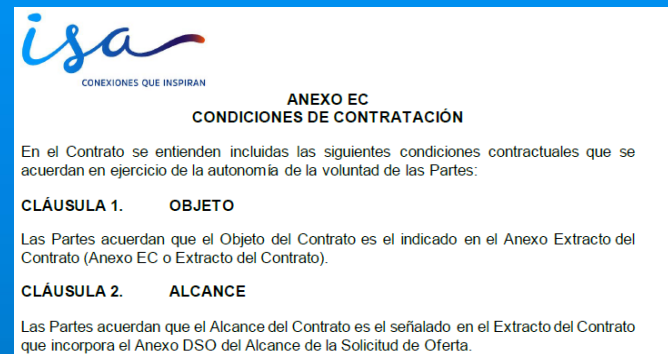
Clause 109: Regulates subcontracting security, requiring traceability of subcontractors, validation of certifications, and assurance of technological components.

Clause 107: Defines controls for subcontracted human resources, including background checks, access management, training, and compliance with policies, particularly in contexts such as remote work.

Clause 111: Establishes the obligation to report cybersecurity incidents within a maximum of 24 hours and to cooperate with the company in their analysis and resolution.

Clause 110: In case of contract termination, obligates third parties to return assets, destroy backups (including those stored in the cloud), and sign closure reports to ensure the secure conclusion of the relationship.

These clauses ensure that external parties operate under a clear and stringent information security framework, consistent with data lifecycle principles, respect for ISA's technological assets, and protection against shared risks.



Tipo	Cláusula	Descripción
AJUSTE	CLAUSULA 35. REQUISITOS BÁSICOS DE GESTIÓN AMBIENTAL PARA LA EJECUCIÓN DE ACTIVIDADES	Se incluyen ítems para la adopción de medidas preventivas para la protección de la infraestructura operativa, evitar daños a la infraestructura por malas prácticas y reportar los riesgos e incidencias a nivel ambiental que afecta la infraestructura operativa.
AJUSTE	CLAUSULA 39. CONFIDENCIALIDAD UNILATERAL	Se incluye obligación de la confidencialidad y reserva de la parte receptora.
AJUSTE	CLAUSULA 40. CONFIDENCIALIDAD BILATERAL	Se incluye exclusividad para suministrar información confidencial y aseguramiento de reintegro de la información y aseguramiento de borrado seguro.
AJUSTE	CLAUSULA 44. USO DE LICENCIAS COMERCIALES	Se incluye la obligación del licenciamiento, originalidad y actualización de versionamiento sobre la última declarada por los fabricantes, informar a la empresa de cualquier vulnerabilidad de seguridad identificada.
AJUSTE	CLAUSULA 45. USO LICENCIAS CÓDIGO ABIERTO	Se incluye la evaluación de los riesgos de ciberseguridad, identificación de posibles conflictos de licencias y el cumplimiento de los requisitos de atribución y divulgación, actualización de versionamiento sobre la última declarada por la comunidad de desarrollo y/o fabricante e información a la empresa de cualquier vulnerabilidad de seguridad identificada.
NUEVA	CLAUSULA 106. PROTECCIÓN DE DATOS PERSONALES.	Se incluye autorización a la Empresa, para efectuar el tratamiento de los datos personales respecto de la información suministrada como los análisis de desempeño, generación de informes, controles de ingreso a instalaciones físicas o plataformas virtuales, medidas HSE entre otros, también las obligaciones del contratista con respecto a la captura, manejo y administración, asegurar el cumplimiento de la ley vigente 1581 de 2012 y devolución de los datos en el momento de la terminación contractual, se relaciona documento anexo de transmisión de datos cuando aplique según el servicio que se esté contratando.
NUEVA	CLAUSULA 106. INFORMACIÓN CLASIFICADA Y RESERVADA.	Se incluye el aseguramiento de la conservación de la información clasificada o reservada como los reglamentos de las bolsas de valores o por orden gubernamental o judicial, decreto, reglamento o regla gubernamental, entre otros y la no destrucción de dicha información con fines legales.
NUEVA	CLAUSULA 107. SEGURIDAD DE LA INFORMACIÓN EN RECURSOS HUMANOS	Se incluye verificación de antecedentes de los contratistas, aseguramiento de la cláusula de confidencialidad, uso aceptable de los activos de información, capacitación sobre el tratamiento de la información, riesgos por uso indebido de la misma y sus consecuencias, aseguramiento de medidas de control sobre el teletrabajo y su auditoría, notificación de ausentismos o finalizaciones de contratos de sus empleados 15 días antes sobre los accesos, entrega de plan de continuidad y finalización, entrega de definición, matriz de roles y plan de comunicaciones en el servicio y actualización de cambios.

Information Security Management Programs

At ISA and its subsidiaries, business continuity planning and cybersecurity are deeply interconnected as strategic pillars to ensure operational resilience, the protection of critical assets, and the long-term sustainability of the business. Cybersecurity is considered the structural foundation of all digital transformation initiatives. Its purpose is to safeguard critical infrastructure, protect strategic information, and ensure the continuity of business operations.

ISA has a comprehensive business continuity plan, which includes:

- **Business Impact Analysis (BIA)**
- **Incident Response Plan**
- **Disaster Recovery Plan (DRP)**

- These plans are led by the **Vice President of Risk and Compliance** and are regularly tested to verify their effectiveness. In addition, cybersecurity incident management is aligned with standards such as **NIST SP 800-61**, allowing for a coordinated and scalable response to events that may compromise continuity.

- ISA also uses a **continuity “toolkit”** that includes:

- Continuity strategies
- Recovery plans
- Continuity testing
- Maturity assessments in continuity and crisis management

- These tools are aligned with cybersecurity frameworks and are updated as the organization’s maturity evolves.

- All of these elements strengthen ISA’s response and recovery capabilities, which are key to business continuity. The associated procedures are outlined in the **Organizational Resilience Guide**.

Envelope ID: BF555BF9-B8AA-4EB4-9590-ED0D218FA96A

Guía Corporativa 43. Gestión Resiliencia Organizacional

isa	GUÍA CORPORATIVA	Nº 43
	GESTIÓN RESILIENCIA ORGANIZACIONAL	Versión: 4
	VICEPRESIDENCIA RIESGOS Y CUMPLIMIENTO	Fecha: 22-ENE-2025

1. INTRODUCCIÓN

Como parte del cumplimiento a la Política de Gestión Integral de Riesgos, aprobada en Junta Directiva de ISA del 29 de mayo de 2020, y cuyo objetivo es “Declarar las decisiones corporativas orientadoras de la Gestión Integral de Riesgos, a través de la cual se busca generar y proteger el valor de ISA y sus empresas, la integridad de los recursos empresariales, la continuidad y sostenibilidad de los negocios”; se publica esta guía, para fortalecer el nivel de madurez en las prácticas de resiliencia organizacional en ISA y empresas, dinamizando su aplicación.

2. OBJETIVO

Facilitar lineamientos y herramientas necesarios que permitan una gestión homologada en ISA y sus empresas para la implementación, desarrollo y mantenimiento de la resiliencia organizacional, mediante el fortalecimiento de capacidades de respuesta y recuperación, para la atención de incidentes que comprometan la integridad de las finanzas empresariales, su reputación o la continuidad de los negocios.

Information security-related business continuity plans Guide

- **Guide abstract**

- Objective

- Facilitate necessary guidelines and tools that allow approved management for the implementation, development and maintenance of business continuity, by strengthening response and recovery capabilities to deal with incidents that compromise the integrity of business resources, its reputation and the business continuity

- **Business continuity strategies** frame the organization's actions and solutions to materialize the necessary response and recovery capacity in the face of the different interruption scenarios to which it may be exposed.

- a) Identify the company's current response capabilities to identify disruption scenarios, their risks and impacts.

- b) Identify requirements and solutions to improve response capacity.

- c) Identify implementation costs of the solutions and mechanisms that support the identified strategies.

- d) Select the strategies that offer the greatest benefits considering the recovery variables, and implement selected business continuity and disaster recovery strategies and solutions

Thumbnail Envelope ID: BF555BF9-B6AA-4EB4-9690-ED00218FA96A

Guía Corporativa 43. Gestión Resiliencia Organizacional

isa	GUÍA CORPORATIVA	Nº 43
	GESTIÓN RESILIENCIA ORGANIZACIONAL	Versión: 4
	VICEPRESIDENCIA RIESGOS Y CUMPLIMIENTO	Fecha: 22-ENE-2025

1. INTRODUCCIÓN

Como parte del cumplimiento a la Política de Gestión Integral de Riesgos, aprobada en Junta Directiva de ISA del 29 de mayo de 2020, y cuyo objetivo es "Declarar las decisiones corporativas orientadoras de la Gestión Integral de Riesgos, a través de la cual se busca generar y proteger el valor de ISA y sus empresas, la integridad de los recursos empresariales, la continuidad y sostenibilidad de los negocios"; se publica esta guía, para fortalecer el nivel de madurez en las prácticas de resiliencia organizacional en ISA y empresas, dinamizando su aplicación.

2. OBJETIVO

Facilitar lineamientos y herramientas necesarios que permitan una gestión homologada en ISA y sus empresas para la implementación, desarrollo y mantenimiento de la resiliencia organizacional, mediante el fortalecimiento de capacidades de respuesta y recuperación, para la atención de incidentes que comprometan la integridad de las finanzas empresariales, su reputación o la continuidad de los negocios.

3. ALCANCE

La presente guía y sus anexos deberán ser aplicadas por todas las empresas de ISA, para el desarrollo de la gestión homologada de continuidad del negocio, gestión de crisis y respuesta a incidentes, de acuerdo con su contexto y operación (tamaño, negocio, necesidades y expectativas de las partes interesadas).

isa

VICEPRESIDENCIA DE RIESGOS Y CUMPLIMIENTO GUÍA GESTIÓN RESILIENCIA ORGANIZACIONAL ANEXO No. 1 PROCESO CONTINUIDAD DEL NEGOCIO

1. PROPÓSITO

Proporcionar lineamientos y herramientas para la implementación y actualización del modelo de continuidad del negocio a través de la adopción de buenas prácticas internacionales

2. DESARROLLO DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Guía de Herramientas (Toolbox)

Complementario a la presente guía se ha estructurado una caja de herramientas, la cual incluye formatos y plantillas con instructivos para la aplicación de los conceptos metodológicos expuestos en los siguientes capítulos. Esta caja de herramienta se encuentra publicada en el micrositio web de [Resiliencia Organizacional de ISA](#) y en la misma se irán actualizando y sumando nuevos elementos de acuerdo con la madurez de ISA y sus empresas.

Elementos que comprende la caja de herramientas:

- BIA: Estratégico, táctico y operativo
- Estrategias de continuidad
- Plan de continuidad del negocio
- Plan de recuperación de desastres DRP

1.1. Planificación de la continuidad del negocio

Antes de iniciar el ciclo de continuidad, se debe realizar una planificación del esquema de actualización y mejoramiento de la gestión de continuidad del negocio, esa planificación se divide en los siguientes dos alcances:

- **Planificación del ciclo de continuidad del negocio**
Consta de la actualización y mejora del ciclo de continuidad del negocio (BIA, Riesgos, Estrategias, Documentación, Formación y Pruebas). Dentro de este alcance se establece el periodo donde se va a realizar las actividades y el responsable.
- **Planificación del fortalecimiento de la gestión de la continuidad del negocio**
Consta de las actividades para el cierre de brechas identificadas en las autoevaluaciones de madurez, auditorías internas o externas y en los resultados de las pruebas de continuidad. Se debe designar la fecha de cumplimiento de la actividad y el responsable de su ejecución. Antes de formalizar esta actividad se debe validar que se cuentan con los recursos necesarios para ejecutarlas.

Information security-related business continuity plans

1. BIA Estratégico		
1.1. Priorización de productos y servicios		
A continuación, se deberá determinar cuáles son los productos o servicios que se deben priorizar ante una situación de interrupción de las operaciones en el corto o mediana plazo.		
Instrucciones Generales	Para el diligenciamiento de esta herramienta que apoya el desarrollo del Análisis de Impacto al Negocio en un nivel estratégico se debe de tener en cuenta lo siguiente:	
	1. Identificación de productos y servicios de la organización que hacen parte de la propuesta de valor. Se identifica el negocio al cual están asociados.	
	2. Identificación de información que permita entender la prioridad de dicho negocio / producto / servicio para la organización	
	3. Determine el comportamiento de los impactos de interrupción en el tiempo para el negocio / producto / servicio.	
	4. Con base en la información analizada determine la priorización del Negocio / Producto / Servicio. Califique con un SI o un NO.	
5. Defina la estrategia de continuidad del negocio, ya sea de que exista o de que considere una alternativa que pueda ser la dirección a considerar cuando se estén definiendo formalmente las estrategias de continuidad del negocio.		
Fecha del taller	Entrevistador	
Asistentes	Nombre	Cargo / Rol
1.2. Priorización de macroprocesos críticos		
Determinar cuales son los procesos de negocio que deben ser recuperados ante una situación de interrupción de las operaciones en el corto o mediana plazo, teniendo en cuenta los productos / servicios priorizados por la organización		
Fecha del taller	Entrevistador	
Asistentes	Nombre	Cargo / Rol
2. BIA Táctico		

REGISTRO DE PRUEBAS DE CONTINGENCIA DE TI			
Proceso/Servicio	PRUEBAS DE CONTINUIDAD DE SERVICIOS CRITICOS ISA INTERCOLOMBIA	Notificación de Evento	Enviada
Duración Estimada	08:05:00	Fecha Programada	03/04/2025
Duración Real	06:25:00	Fecha Ejecución	03/04/2025
Lugar de Ejecución	Centro de Cómputo Alterno (CCA)	Tipo de Prueba	Interrupción Total
Metodología y Alcance	Alcance: - DA completo con Catalogo global - Aplicaciones completas (catalogo revisado y actualizado por proveedor) - File server de ISA1 e ITCO1 - SharePoint - INTERNEXA confirmó participación y se unirá para la prueba del File server INTERNEXA (Julio Lopera)	Responsables	CAUSERVIDORES - Juan Molina, Gustavo Restrepo, Johan Sebastian Arango, Giovanni Alzate CAUSEGURIDAD - John Fonseca CAUBD - Adriana Obando CAUESTACIONES - Jorge Delgado CAUREDES - Juan David Suarez CAUAPLICACIONES - Martha Trujillo, Isabel Cristina Villegas, Yurley Yammir Viveros, Elizabeth Blanco (SAGES), Juan Ignacio Gandara (SAGES), Jonathan Ortiz (APPRIL LABS), Sergio Guatama (APPRIL LABS), Alvaro Carvajal CONTINUIDAD ISA - Jonathan Soto, Lina Oquendo CONTINUIDAD INTERNEXA: Martín Octavio Tapias CONTINUIDAD UNISYS - Juan Mauricio Vélez
	Cambios entre la última prueba y esta: Garantizar que al romper canales se tengan en cuenta: Backups, Corporativo (red de datos normal) y Cluster No se tienen CMS y/o IMAC adicionales que hayan obligado a cambio de los procedimientos de recuperación de cada grupo. Por lo cual se ejecutan igual, sin afectación en actividades y tiempos.		
	Por fuera del alcance de esta prueba: - SAP ERP (debido a que se encuentra en proceso de migración a la nube)		
	RTO pactado: - Subir plataformas: 3:00 horas - Pruebas técnicas: 4:00 horas		

Besides, Continuity plans are tested regularly to verify their effectiveness and ensure compliance with the RPOs (Recovery Point Objective) and RTOs (Recovery Time Objective) required by the business.



CONEXIONES QUE INSPIRAN

DocuSign Envelope ID: SAF56108-928B-403A-B8D3-298CA3C34D8D



CONTRATO DE PRESTACIÓN DE SERVICIOS 4600005621

Hoja 2

ALCANCE.

1. El contrato se ejecutará por órdenes de entrega las cuales serán acordadas previamente con el proveedor con un enfoque específico, objetivo y alcance.
2. Las evaluaciones y/o consultorías serán ejecutadas para ISA y sus Empresas desde las instalaciones del proveedor.
3. Las evaluaciones en ciberseguridad podrán abarcar diferentes plataformas en tecnologías de la Información o tecnologías operativas del Negocio.

Las ordenes de entrega se pactan con el contratista indicando:

- a. Las definiciones particulares del objeto y alcance
- b. La cantidad de horas requeridas o el valor global por entregable
- c. Los entregables
- d. Plazo de entrega

5. El valor de la Orden de Entrega estará definido por el número de horas requeridas para la realización del trabajo y el valor de la hora acordado con el Contratista, o por el valor global acordado por el entregable.

6. El Contratista deberá realizar las actividades de validación de los informes con el personal involucrado en los procesos e incluir sus comentarios en el informe final.

7. El contratista deberá contar con las herramientas tecnológicas necesarias que faciliten la ejecución de las actividades a realizar.

8. Algunos de los servicios que se pueden solicitar durante la ejecución del presente Contrato son:

- **Pentesting:** El experto en, ciberseguridad realizará un ejercicio de Pentesting (caja negra) para las siguientes empresas de ISA: ISA-INTERCOLOMBIA, XM, ITX, TRAN, CTEEP, REP, INTERVIAL, INTERCHILE, Costera e ISA Bolivia. Producto del ejercicio se genera un informe con el resultado donde se identifiquen las vulnerabilidades a las que está expuesta la red de datos, una conclusión sobre la seguridad de la red y las recomendaciones necesarias para mitigar el riesgo.
- **Evaluación de monitoreo de la Red:** Una vez finalice el pentesting y se presente el informe a las áreas de tecnología, el experto en ciberseguridad tomando como insumo los resultados el pentesting realizará un análisis sobre el nivel de detección y contención que tienen los SOC – Centro de operaciones de Seguridad de ISA y sus empresas, para la realización de esta actividad se realizarán las interacciones necesarias con el personal del SOC e inspección de los log. Como resultado emitirá un informe concluyendo sobre

Interconexión Eléctrica S.A. E.S.P.
NIT: 860.016.010-3

Calle 12 Sur 1B - 168 / Bloque 1,
Rios 4 / Medellín, Colombia
Tel + 57 4 325 22 70

Línea ética: 01 8000 94 1341
lineaetica@isa.com.co

www.isa.co

Internal and external audits

ISA regularly conducts cybersecurity audits—both internal and external—with a fundamental strategic and technical purpose: to assess the security posture, identify vulnerabilities, and strengthen resilience against threats in both IT and OT environments. In addition, the company carries out vulnerability assessments, ethical hacking, and Red Team exercises.

ISA holds the ISO/IEC 27001 certification, which validates its Information Security Management System (ISMS). This certification has been issued by ICONTEC and is currently valid for the maintenance of electrical infrastructure within the Energy Transmission System



Incident Escalation

ISA has a comprehensive cybersecurity incident response framework in place

Technical and Cybersecurity Response

This includes the Cybersecurity Operations Center (SOC), Information Technology and Operations teams, and service partners

Design Envelope ID: 24F2971E-7191-4A6C-9274-9230D719F95

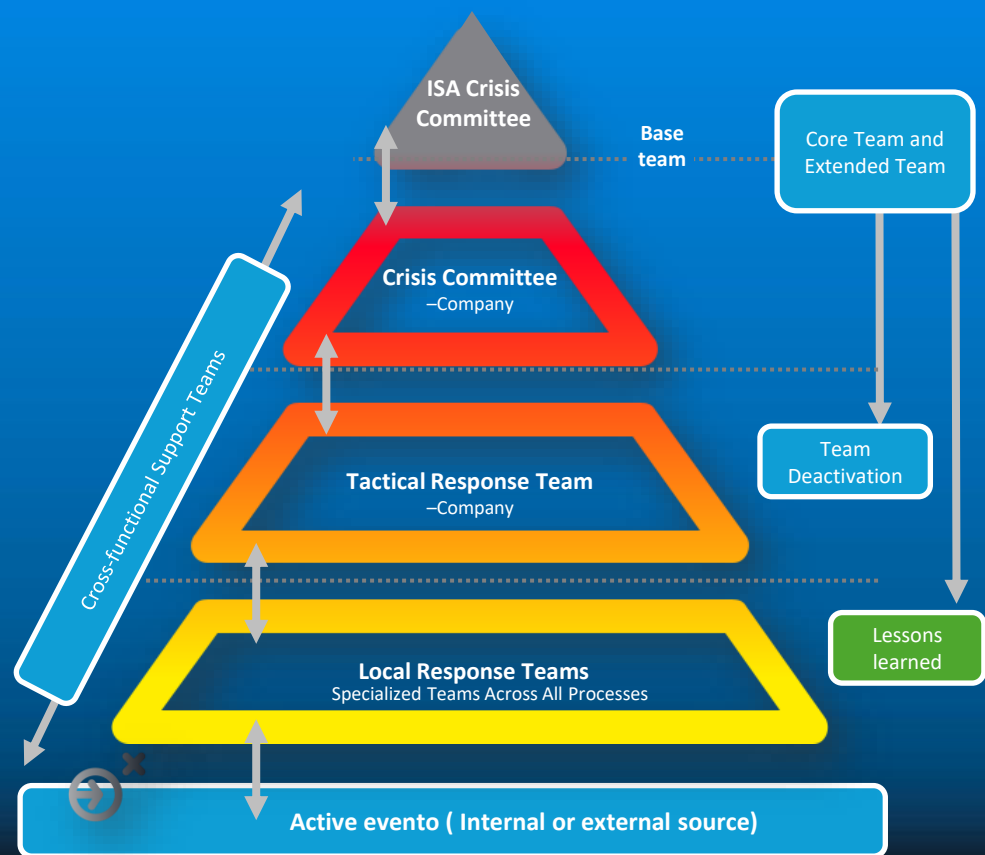
Guía Corporativa gestión de incidentes de ciberseguridad en ISA y sus empresas

GUÍA CORPORATIVA		N° 59
GUÍA CORPORATIVA DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD		Versión: 2
VICEPRESIDENCIA DE TECNOLOGÍA DE INFORMACIÓN		Fecha: 14-JUL-2025
1	INTRODUCCIÓN	2
2	OBJETIVO	2
3	ALCANCE	2
4	DEFINICIONES	3
5	ROLES Y RESPONSABILIDADES	3
6	DESARROLLO	7
6.1	PREPARACIÓN	8
6.1.1	Tipología de incidentes	8
6.1.2	Recursos y herramientas	11
6.1.3	Ejercicios de simulación	11
6.1.4	Sensibilización y capacitación a colaboradores	11
6.2	DETECCIÓN Y ANÁLISIS	11
6.2.1	Detección de incidentes	11
6.2.2	Evaluación del impacto y materialidad	11
	Flujo específico de incidentes de ciberseguridad	20
6.2.3	Reporte de incidentes a Terceros	21
6.2.4	Conservación de pruebas	21
6.2.5	Análisis del incidente	21
6.2.6	Documentación del incidente	21
6.2.7	Tiempos de respuesta inicial y frecuencia de actualización	21
6.3	CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN	22
6.3.1	Contención	22
6.3.2	Erradicación	22
6.3.3	Recuperación	23
6.4	ACTIVIDADES POST INCIDENTE	23
6.4.1	Análisis Ex post (Análisis de causa raíz y lecciones aprendidas)	23
6.4.2	Mejoras y ajustes	23
6.4.3	Informes y comunicación	24
7	GESTIÓN DE INCIDENTES DE TERCEROS	24
8	PASOS DEL PROTOCOLO DE GESTIÓN DE INCIDENTES CON AGENTES DEL MERCADO	24

Página 1 de 26

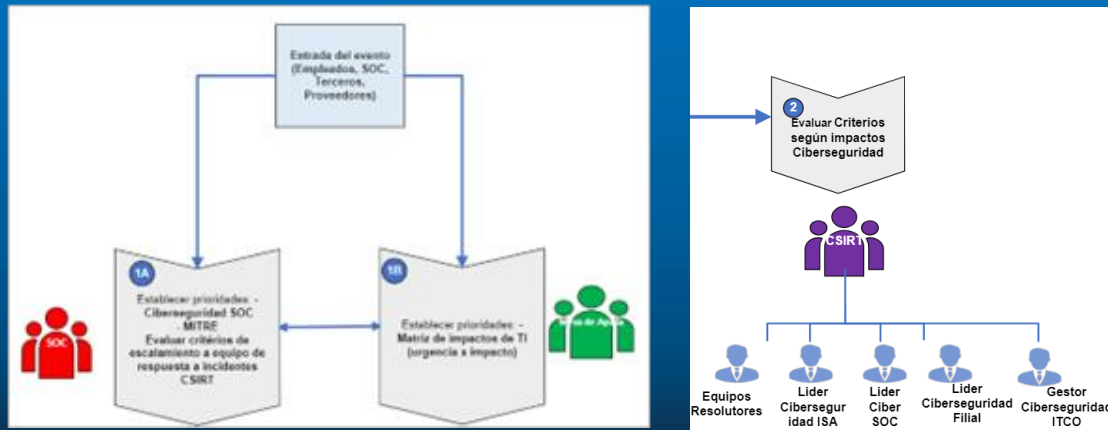
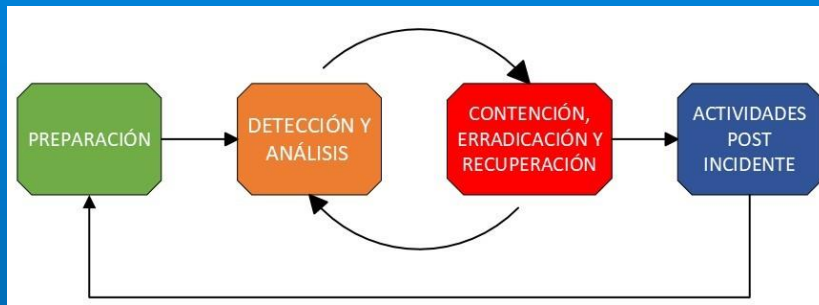
Organizational and Strategic Response

This involves crisis management, executive leadership, business units, legal, risk and compliance, and communications (Investor Relations).



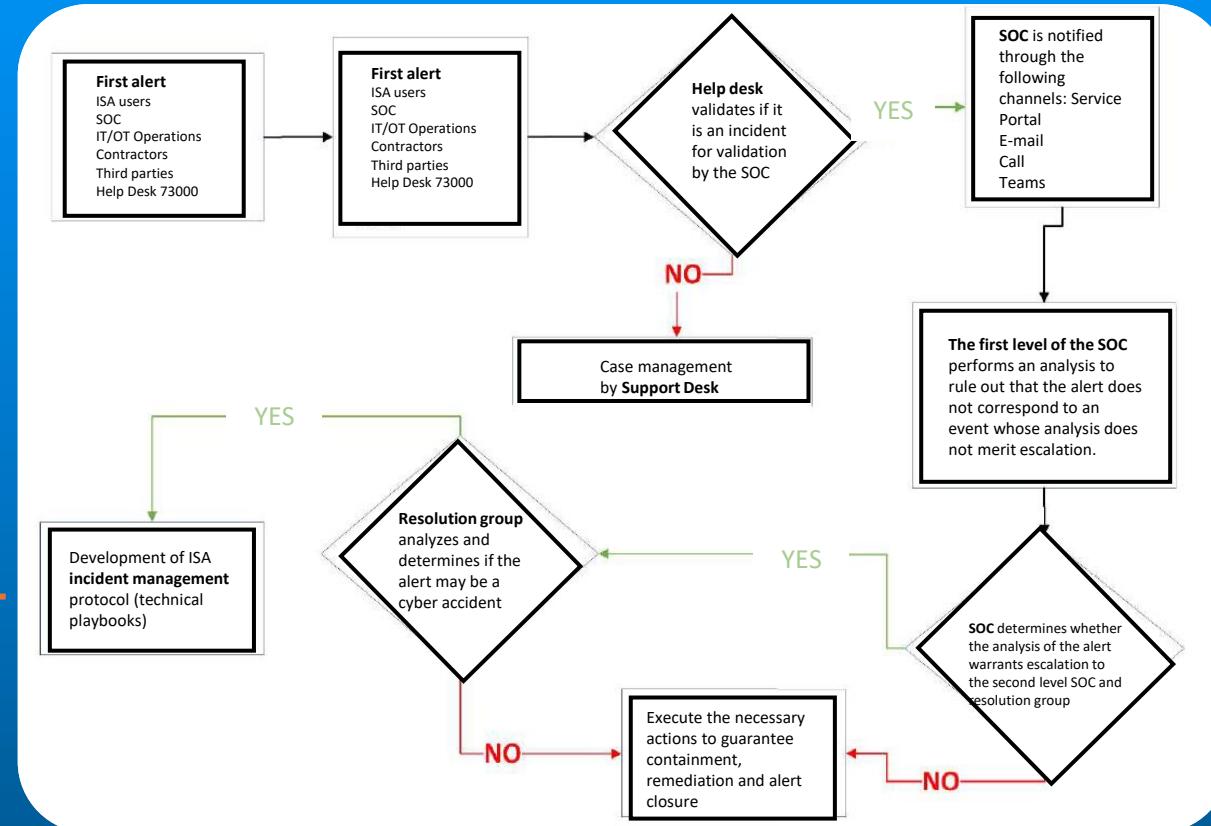
Escalation process for employees to report incidents, vulnerabilities or suspicious activities

ISA outlines the criteria and escalation procedures for incident response and the activation of the internal CSIRT in its Cybersecurity Incident Management Guide. Cybersecurity incident management at ISA S.A. and its subsidiaries is based on the international standard NIST SP 800-61 Revision 2 and the UK's National Cyber Security Centre (NCSC) Incident Management Guide, both of which include the following actions:



It also has a clear process for incident escalation based on their criticality and impact.

Incident Escalation



Incident Escalation Flow

The incident response process highlights the involvement of business, legal, institutional relations, risk, finance, and technology areas, representing an organizational response to the crisis.

Information security awareness training

Information security awareness training

ISA fosters a cybersecurity-driven organizational culture through awareness campaigns, training sessions, and simulations designed to empower employees in identifying and responding to digital threats. These initiatives include role-specific training sessions, the distribution of communication toolkits, and cyberattack simulations that incorporate real-world techniques such as social engineering. ISA also promotes safe behaviors, including the use of strong passwords, information protection, and, most importantly, the timely reporting of incidents

Empowerment of workers

The culture program empowers individuals to identify and respond to the most common cybersecurity threats.

Cybersecurity Awareness Month



99%: A total of 4,636 employees across ISA and its subsidiaries successfully completed the mandatory cybersecurity training.



88%: Energy transmission business locations and operations were reached through cybersecurity awareness initiatives, including more than 200 of 300 substations.



100%: Executive administrative assistants supporting the Presidency and Vice Presidencies received specialized training on the most common cyber threats relevant to their roles, as well as threats targeting senior executives.



Information security awareness training

Employees are considered the first line of defense in cybersecurity, as they interact daily with critical systems and data. ISA provides continuous training to help them detect suspicious behavior and report cybersecurity events effectively. This strategy aligns with international standards such as ISO 27001 and NIST, aiming not only to reduce human risk but also to increase organizational resilience against threats like ransomware and phishing, thereby strengthening the company's overall security posture.

The numbers that activated our digital culture

Total weekly connections

2.331

Conexiones

Employees who participated in the on-site experience

205

Participants

Content engagement

8.405

Engagement

Reactions and interactions

230

Reactions

Cybersecurity culture plan implemented in 2025

Digital Transformation Capability Cybersecure Culture



Awareness

- Communication and Awareness**
- Constant deployment of communications
 - Commemoration of key dates in cybersecurity and 15' I Am Digital
 - Microsite I Am Cybersecure for learning and reinforcement

- Workshops**
- Workshop on cyber risk for the Board of Directors and Presidency Committee
 - Workshop practical with Administrative Assistants at the ISA companies
 - Workshops on cybersecurity at TE and Roads Business locations

- Recognition and Analysis**
- Scheme of recognitions for people with cyber-secure habits
 - Analysis of Behavior through solutions of artificial intelligence



Education

- General Training**
- Cybersecurity course for all employees
 - Training kit for administrative assistants
- Practices**
- Practical workshops with leaders by Vice-presidencies
 - Exercises and simulations for the Presidency Committee and Board of Directors
- Drills and Crisis Management**
- Drills of cyber crisis management
 - Drills of fake emails / Phishing
- Conferences and Demonstrations**



Training

- Information Management and Prevention**
- Classification and labeling of corporate information – Data leak prevention
- Risk Assessment and Management**
- Evaluation of risk in Third Parties and critical suppliers
- Digital Transformation**
- Promote the safe use of new technologies
- Zero Trust**
- Strengthen the concept of the benefits, for the organization, of zero trust security – ZeroTrust

“La tecnología por sí sola no garantiza la seguridad. Las personas informadas y capacitadas son un control de seguridad crítico.”



Estándar NIST SP 800-50 Rev. 1: Programa de Aprendizaje en Ciberseguridad y Privacidad.
NIST: Instituto Nacional de Estándares y Tecnología USA

EDUCACIÓN

Aprendo para fortalecer la seguridad con mis decisiones y acciones.

La educación fomenta conocimientos (saber) y una actitud de contribución a la ciberseguridad (ser), a mediano y largo plazo.

- ✓ Fundamentos y desarrollo de hábitos
- ✓ Liderazgo

ENTRENAMIENTO

Desarrollar hábitos ciberseguros en el trabajo cotidiano

Habilidades prácticas necesarias para proteger la información desde mi rol.

- ✓ Enfocada en el “cómo”
- ✓ Verificada mediante pruebas o evaluaciones

CONCIENCIACIÓN / SENSIBILIZACIÓN

Reconocer el riesgo y actuar de forma segura

Para crear conocimiento básico y percepción del riesgo, no habilidades técnicas.

- ✓ Riesgo y consecuencias
- ✓ Identificación
- ✓ Comportamiento seguro o esperado

Information security awareness training

Safe Cyberculture Plan

ISA continues to strengthen its cybersecurity culture by promoting safe behaviors, mitigating cyber risks, and reducing the impact of security incidents

Development

Objective 2

Increase the **Board of Directors'** awareness, knowledge, and understanding of ISA's cybersecurity landscape to enable informed strategic decision-making.

Learning Opportunities

- Periodic Board learning sessions on cybersecurity and digital transformation.
- Asynchronous awareness and knowledge-building interventions.
- Continuous tailored development program delivered with an expert external partner.
- Reverse mentoring program for Board members.
- Participation in the Digital Transformation Fair through a dedicated immersive experience focused on strategic digital and cybersecurity challenges.

Risk-Based Decision Making

- Prioritize decisions based on risk, not technology.
- Use real-world insights to develop short learning capsules that showcase both successes and risks.
- Connect learning to specialty-specific use cases.

Innovative Learning Methods

- Use real-life scenario videos, simulations, and engaging micro-learning content to strengthen awareness and accountability.
- Simulations
- Share lessons learned and cybersecurity incidents, including relevant ISA cases, to make risks tangible, reinforce key behaviors, and drive lasting engagement.

Active Leadership Engagement

- Position Board members as cybersecurity advocates by integrating cybersecurity messages into Board meetings and leveraging experienced directors to promote awareness and peer learning.

Strategic Business Impact

- Emphasize that emerging technologies are key drivers of competitive advantage.
- Clearly articulate how AI and cybersecurity contribute to business growth, operational resilience, sustainability objectives, and long-term value creation.





Awareness

Communication and Awareness

- Constant deployment of **communications**
- Commemoration of **key dates** in cybersecurity and **15' I Am Digital**
- Microsite **I Am Cybersecure** for learning and reinforcement

Workshops

- **Workshop** on cyber risk for the **Board of Directors** and **Presidency Committee**
- **Workshop** practical with **Administrative Assistants** at the **ISA companies**
- **Workshops** on cybersecurity at **TE** and **Roads Business locations**

Recognition and Analysis

- Scheme of **recognitions** for people with **cyber-secure habits**
- **Analysis of Behavior** through solutions of **artificial intelligence**



Education

General Training

- **Cybersecurity course** for all employees
- **Training kit** for administrative assistants

Practices

- **Practical workshops** with leaders by **Vice-presidencies**
- **Exercises and simulations** for the **Presidency Committee** and **Board of Directors**

Drills and Crisis Management

- **Drills** of **cyber crisis** management
- **Drills** of fake emails / **Phishing**

Conferences and Demonstrations



Training

Information Management and Prevention

- **Classification and labeling** of corporate information – **Data leak prevention**

Risk Assessment and Management

- Evaluation of **risk in Third Parties** and critical suppliers

Digital Transformation

- **Promote the safe use** of new technologies

Zero Trust

- Strengthen the concept of the benefits, for the organization, of **zero trust security** – **ZeroTrust**

Artificial Intelligence



isa

CONEXIONES QUE INSPIRAN

Responsible Artificial Intelligence Policy

In accordance with our Information, Knowledge, and **Artificial Intelligence Policy and Corporate Guideline No. 62** – Use, Development, and Implementation of Artificial Intelligence (Version 2, June 1, 2026), which has been formally approved by ISA's Executive Team, under the leadership of the Information Technology Vice Presidency, ISA and each of its subsidiaries are committed to the responsible use of Artificial Intelligence.

esign Envelope ID: 4E02C1B7-7DEB-8BA3-80A0-91EEAFC6EE49

	GUÍA CORPORATIVA	N° 62
	GUÍA PARA USO, DESARROLLO E IMPLEMENTACIÓN DE LA INTELIGENCIA ARTIFICIAL	Versión: 2
	VICEPRESIDENCIA DE TECNOLOGÍA DE LA INFORMACIÓN	Fecha: 01-JUN-2026

1. INTRODUCCIÓN

La inteligencia artificial (IA) está transformando industrias como la transmisión de energía y las concesiones viales, al fortalecer la seguridad, la confiabilidad, la productividad y la eficiencia, y al habilitar nuevas capacidades digitales en los procesos de negocio. En particular, la inteligencia artificial generativa (GenAI) está ampliando las posibilidades de automatización, análisis y creación de contenido en múltiples funciones empresariales. No obstante, su adopción también implica riesgos relevantes en materia de ciberseguridad, privacidad, propiedad intelectual, sesgos, gobierno, calidad y disponibilidad de datos, escalabilidad y desarrollo de capacidades organizacionales y del talento.

2. OBJETIVO

ISA y sus empresas reconocen el valor estratégico de la tecnología de la información y de los datos para el logro de sus objetivos. En ese contexto, la IA tiene el potencial de transformar las industrias en las que opera la organización, al mejorar la eficiencia de los procesos, fortalecer la toma de decisiones y habilitar nuevas capacidades para responder a los retos presentes y futuros.

Esta guía establece los lineamientos para el uso, desarrollo e implementación responsable, seguro y eficaz de soluciones de inteligencia artificial y tecnologías relacionadas. Su propósito es orientar la adopción de estas capacidades bajo criterios de cumplimiento normativo, ética, gestión de riesgos, protección de la información y creación de valor para ISA y sus empresas.

3. ALCANCE

Esta guía establece los lineamientos que ISA y sus empresas deben seguir para el uso, desarrollo e implementación de inteligencia artificial. Aplica a todas las áreas de ISA y sus empresas, así como al personal interno, proveedores y terceros que intervengan o tengan incidencia en soluciones de IA.

Cada empresa podrá definir lineamientos, procesos o procedimientos complementarios cuando así lo requiera, siempre que se mantengan alineados con lo dispuesto en este documento. Los

Cada empresa podrá definir lineamientos, procesos o procedimientos complementarios cuando así lo requiera, siempre que se mantengan alineados con lo dispuesto en este documento. Los

Cada empresa podrá definir lineamientos, procesos o procedimientos complementarios cuando así lo requiera, siempre que se mantengan alineados con lo dispuesto en este documento. Los

Data Privacy in the Use and/or Development of AI

- **The Corporate AI Guideline** addresses this element comprehensively in **Section 5.3.8 (Privacy)**, establishing that AI solutions must protect individuals' right to privacy and the personal data of data subjects, ensuring that such data are used only for authorized purposes and in accordance with the applicable legal and regulatory requirements of each jurisdiction.
- As minimum operational requirements, the Guideline requires that users be informed about the nature of the data being processed and the purpose of such processing. It incorporates the principles of **Privacy by Design** and **Privacy by Default**, together with data minimization, purpose limitation, data accuracy, security, traceability, and limited retention.
- The Guideline also requires an **Enhanced Privacy Impact Assessment (PIA)** for AI solutions involving sensitive personal data, decisions with significant effects on individuals, or systematic monitoring activities.
- This element is further reinforced by **Section 5.3.9 (Confidentiality)**, which establishes that prompts, instructions, interaction histories, and AI-generated outputs are considered **Corporate Information** and, therefore, may not be processed using unlicensed or unauthorized AI tools.
- In addition, **Section 5.4.8.2** establishes **Data Assessment as a Mandatory Deployment Gate** prior to production, requiring the evaluation of data sources, data quality, information classification, access permissions, retention requirements, and applicable restrictions on data use before any AI solution is deployed.
- **Implementation, Monitoring, and Oversight:** The **Information Technology Vice Presidency** is responsible for the implementation, ongoing monitoring, and evaluation of the Corporate AI Guideline and its related controls. Governance oversight is further strengthened through regular review by the **Board of Directors**, acting through the **Corporate Governance, Information Technology & Cybersecurity, Sustainability, and Innovation Committee**, which monitors progress, compliance, risk management, and the effective implementation of AI governance across the organization.

5.3.8. Privacidad

Las soluciones de IA deben proteger el derecho a la intimidad y a los datos personales de sus titulares, y utilizarse únicamente conforme a los fines autorizados y a la normativa aplicable en cada jurisdicción. En desarrollo de este principio, ISA y sus empresas deberán asegurar que el tratamiento de datos personales asociado a soluciones de IA se rija por criterios de legalidad, necesidad, proporcionalidad, transparencia y protección efectiva, de acuerdo con el nivel de riesgo del caso de uso.

Como criterios operativos mínimos, los usuarios y responsables del proceso deberán ser informados, cuando aplique, sobre la naturaleza de los datos utilizados, la finalidad del tratamiento y las condiciones aplicables, de conformidad con la Guía Corporativa de Protección de Datos Personales de ISA y con la normativa vigente.

Asimismo, en el uso y desarrollo de soluciones de IA se deberán aplicar, cuando corresponda, principios de privacidad desde el diseño y por defecto, minimización de datos, limitación de finalidad, exactitud, seguridad, trazabilidad, retención limitada y acceso basado en necesidad de conocer.

Solo podrán tratarse los datos personales estrictamente necesarios para la finalidad autorizada del caso de uso, y su conservación deberá limitarse al tiempo requiriendo conforme a la normativa aplicable, la finalidad definida y las tablas de retención o lineamientos corporativos correspondientes.

Requerirán evaluación reforzada de impacto en privacidad y protección de datos, antes de su despliegue y durante su operación cuando corresponda, las soluciones de IA que impliquen tratamiento de datos personales sensibles, decisiones con impacto significativo sobre personas, uso intensivo de datos, monitoreo sistemático o transferencia a terceros.

En estos casos, los responsables del proceso y el Área de TI deberán asegurar que los titulares, cuando aplique, sean informados de forma clara sobre la intervención de sistemas de IA, la finalidad del tratamiento, las categorías de datos utilizadas, las medidas de protección adoptadas y los canales disponibles para ejercer sus derechos.

5.3.9. Confidencialidad

Para desarrollar, implementar y usar la IA, se deberán asegurar protocolos de protección para la información confidencial y tomar medidas requeridas para que esta no entre en el dominio público ni se divulgue a terceros no autorizados.

Para efectos de esta guía, los prompts, instrucciones, historiales de interacción, archivos cargados y resultados generados por soluciones de Inteligencia Artificial se consideran información corporativa y deberán gestionarse conforme a la clasificación de la información definida por ISA y sus empresas (pública, uso interno, confidencial o restringida).

5.4.8.2 Pasos mínimos (gates) y evidencias requeridas

- **Registro e ideación:** el Área interna contacta al equipo del COE Digital para registrar el caso de uso, objetivo, alcance, datos involucrados y nivel de riesgo preliminar.
 - **Evaluación de datos:** se documentan fuentes, calidad, clasificación, permisos, retención y restricciones de uso, se define si hay datos personales o confidenciales.
 - **Evaluación de riesgos:** se realiza análisis de riesgos (ético, sesgos, seguridad, privacidad, operación, legal) y plan de tratamiento; debe quedar documentado y aprobado. Los sistemas de IA deben diseñarse para operar de forma resiliente, fallar de manera segura y no comprometer la continuidad operativa de los servicios críticos, incorporando mecanismos de respaldo y fallback.
- La evaluación de riesgos deberá incluir de forma expresa y documentada:
- i. riesgos de privacidad y protección de datos;
 - ii. riesgos de ciberseguridad específicos de IA;
 - iii. riesgos éticos y de sesgo;
 - iv. riesgos de opacidad o insuficiente explicabilidad;
 - v. riesgos por dependencia de terceros o cambios de proveedor/modelo;
 - vi. riesgos operativos y de continuidad;
 - vii. riesgos por uso fuera del alcance autorizado; y
 - viii. riesgos ambientales cuando el caso de uso implique consumo computacional relevante o dependencia de infraestructura intensiva.

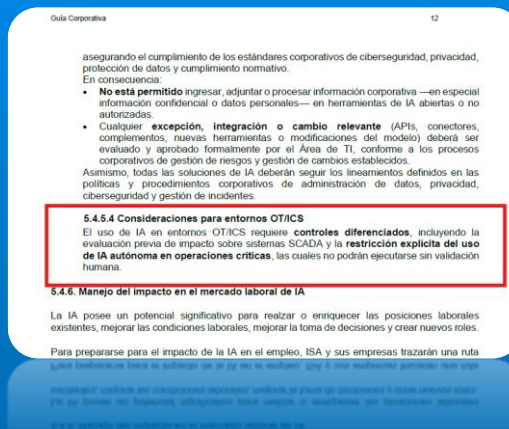
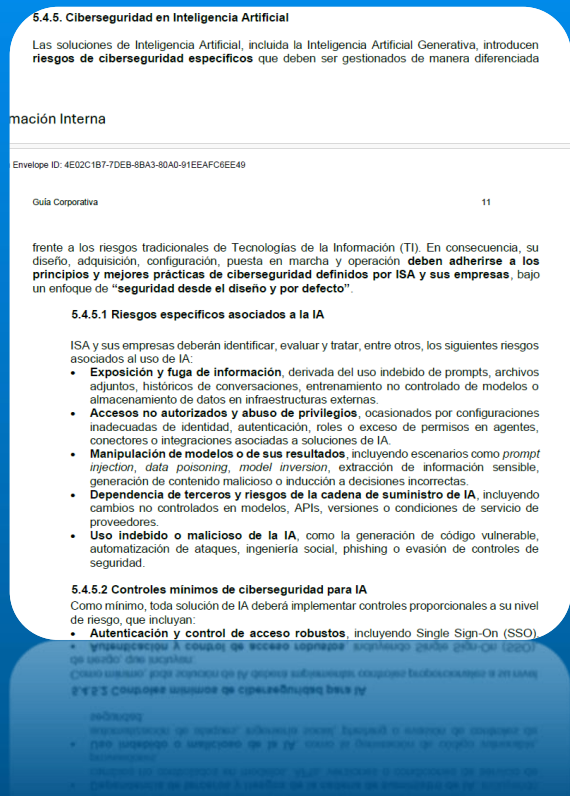
Nota: Las soluciones de IA clasificadas como de riesgo medio y alto deberán

Protecting the cybersecurity of systems in the use and/or development of AI

Section 5.4.5 (Artificial Intelligence Cybersecurity) is entirely dedicated to this element. It establishes that AI solutions introduce **distinct cybersecurity risks** that must be managed through a **security-by-design and security-by-default** approach. The **Information Technology Vice Presidency** is responsible for the implementation, ongoing monitoring, and evaluation of the Corporate AI Guideline and its related controls.

The Guideline identifies AI-specific cybersecurity risks, including:

- Information exposure and data leakage;
- Unauthorized access and abuse of privileged access;
- Model manipulation, including **prompt injection**, **data poisoning**, and **model inversion** attacks;
- Third-party and supply chain risks; and
- Malicious or unauthorized use of AI systems.



To address these risks, the Guideline establishes the following **minimum security controls**:

- Robust authentication through **Single Sign-On (SSO)** and **Multi-Factor Authentication (MFA)**;
- Segregation of duties and application of the **principle of least privilege**;
- Encryption of data **in transit and at rest**;
- Traceability and continuous monitoring of AI interactions and prompts to detect anomalous behavior;
- Periodic security testing, including **static, dynamic, and adversarial testing**; and
- Vulnerability and incident management integrated with ISA's **Corporate Computer Security Incident Response Team (CSIRT)**.

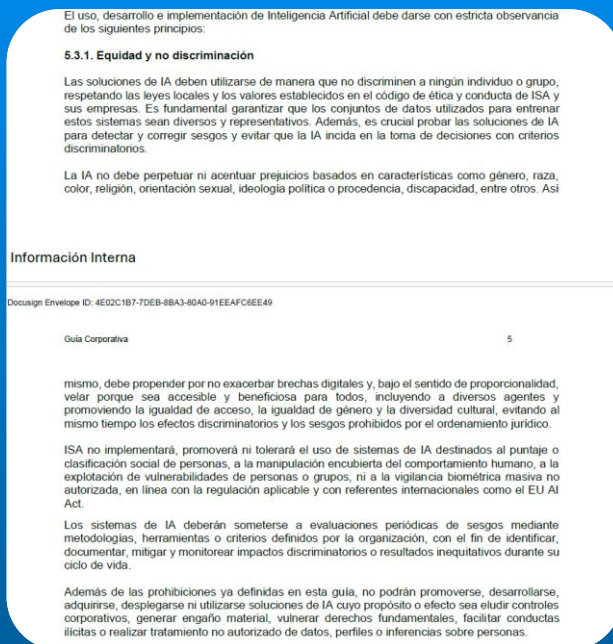
In addition, **Section 5.4.5.4** establishes **enhanced cybersecurity controls for Operational Technology (OT) and Industrial Control Systems (ICS)** environments. These include mandatory impact assessments prior to deploying AI solutions that could affect **SCADA** systems, as well as the explicit prohibition of autonomous AI operation in critical operational environments.

Preventing potential bias in the use and/or development of AI

This element is addressed through two complementary sections of the Corporate AI Guideline.

Section 5.3.1 (Fairness and Non-Discrimination) establishes that AI solutions must not discriminate against any individual or group. It expressly prohibits the use of AI for **social scoring or classification of individuals, covert manipulation of human behavior, exploitation of vulnerable persons or groups, and unauthorized large-scale biometric surveillance.**

The Guideline further requires that AI systems undergo **periodic fairness and bias assessments** using methodologies and evaluation criteria defined by the organization to identify, document, mitigate, and continuously monitor discriminatory impacts throughout the AI solution's lifecycle.



Section 5.4.3 (Management of Algorithmic Bias in AI) provides the operational framework for this requirement by establishing that every AI solution must identify, assess, and minimize bias arising from:

- Training datasets;
- Design and configuration decisions; and
- Inherent limitations of the underlying algorithms.

It also requires organizations to **test, measure, and remediate bias in a timely manner** whenever it is identified.

Las soluciones de IA en operación deberán contar con mecanismos de monitoreo orientados a detectar deriva, degradación de desempeño, cambios en patrones de uso, variaciones en la calidad de los datos de entrada y desviaciones relevantes en los resultados. Dicho monitoreo deberá definir, como mínimo: métricas aplicables, frecuencia de revisión, umbrales de alerta, responsables del seguimiento y protocolo de actuación ante hallazgos, incluyendo evaluación, contención, ajuste, reentrenamiento, suspensión o retiro de la solución cuando corresponda.

La identificación, evaluación, tratamiento y monitoreo de los riesgos asociados a la Inteligencia Artificial deberán alinearse con el AI Risk Management Framework (AI RMF) del NIST, asegurando un enfoque integral que fortalezca el gobierno, diseño, operación, medición y mejora continua de las soluciones de IA.

Además de los controles anteriores, la gestión del riesgo debe contemplar riesgos no técnicos que impactan directamente la calidad de los resultados, como los sesgos algorítmicos y la representatividad de los datos, los cuales se abordan en la siguiente sección.

5.4.3. Manejo de sesgos algorítmicos en IA

El desarrollo e implementación de soluciones de IA debe abordar y minimizar los sesgos asociados a los conjuntos de datos usados para entrenar los algoritmos, a decisiones de diseño y a limitaciones inherentes de los propios algoritmos. Es crucial probar y validar los sistemas de IA para detectar, medir y corregir sesgos de forma oportuna.

5.4.4. Proceso de apelación de decisiones de IA

ISA cuenta con la **Línea Ética** como mecanismo institucional para que empleados, clientes, proveedores u otros terceros potencialmente afectados soliciten la revisión de decisiones o resultados materialmente relevantes generados o soportados por sistemas de IA. Este mecanismo ya existe y contiene, como mínimo: i) un canal de recepción accesible; ii) plazos de respuesta; iii) la asignación de un responsable de revisión humana, de acuerdo con las instancias competentes definidas por la organización; iv) la evaluación del caso con base en la información disponible; y v) la documentación del resultado y de las medidas correctivas que correspondan.

Cuando corresponda, la Línea Ética se articula con otros canales institucionales ya existentes de atención corporativa, asegurando trazabilidad, revisión humana efectiva y respuesta oportuna conforme a los responsables definidos por ISA y sus empresas.

5.4.5. Ciberseguridad en Inteligencia Artificial

Las soluciones de Inteligencia Artificial, incluida la Inteligencia Artificial Generativa, introducen **riesgos de ciberseguridad específicos** que deben ser gestionados de manera diferenciada



CONEXIONES QUE INSPIRAN

In addition, **Section 5.4.8.2** establishes **bias validation** as a **mandatory deployment gate** before any AI solution can be placed into production. **Section 5.4.8** further requires that **medium- and high-risk AI solutions** undergo **periodic fairness and bias assessments in production**, with a **minimum review frequency of every six months** to ensure that potential discriminatory impacts are identified and addressed throughout the operational lifecycle of the solution.

licenciada, manejo de información según clasificación, revisión humana y registro básico del caso de uso.

- **Medio:** chatbot o agente que consulta repositorios corporativos o recomienda acciones, con impacto limitado y con confirmación humana previa a la ejecución. Requiere, además: evaluación de riesgos, pruebas de sesgos/precisión, controles de acceso y trazabilidad.
- **Alto:** agentes de proceso con jerarquía organizacional, soluciones que ejecutan acciones en sistemas, soportan decisiones críticas (seguridad, operación, cumplimiento) o tratan datos sensibles a escala. Requiere, además: aprobación formal del dueño del proceso y TI, evaluación de ciberseguridad y privacidad reforzada, monitoreo continuo, auditoría, plan de continuidad y gestión del cambio organizacional. La clasificación del nivel de riesgo deberá considerar expresamente, además del caso de uso y de los datos tratados, los siguientes factores:
 - i. grado de autonomía de la solución;
 - ii. posibilidad de ejecutar acciones en sistemas internos o externos;
 - iii. impacto potencial sobre derechos, seguridad, continuidad operativa o cumplimiento;
 - iv. uso de datos personales o sensibles;
 - v. alcance sobre clientes, empleados, proveedores u otros terceros; y
 - vi. posibilidad de afectar materialmente decisiones individuales o colectivas.

Toda solución que soporte, recomiende o influya de manera relevante en decisiones sobre personas, cumplimiento, seguridad, operación crítica, asuntos legales o financieros deberá ser clasificada, como mínimo, como de riesgo medio o alto, según su nivel de autonomía e impacto potencial.

5.4.8.2 Pasos mínimos (gates) y evidencias requeridas

- **Registro e ideación:** el Área interna contacta al equipo del COE Digital para registrar el caso de uso, objetivo, alcance, datos involucrados y nivel de riesgo preliminar.
 - **Evaluación de datos:** se documentan fuentes, calidad, clasificación, permisos, retención y restricciones de uso; se define si hay datos personales o confidenciales.
 - **Evaluación de riesgos:** se realiza análisis de riesgos (ético, sesgos, seguridad, privacidad, operación, legal) y plan de tratamiento; debe quedar documentado y aprobado. Los sistemas de IA deben diseñarse para operar de forma resiliente, fallar de manera segura y no comprometer la continuidad operativa de los servicios críticos, incorporando mecanismos de respaldo y fallback.
- La evaluación de riesgos deberá incluir de forma expresa y documentada:
- i. riesgos de privacidad y protección de datos;
 - ii. riesgos de ciberseguridad específicos de IA;
 - iii. riesgos éticos y de sesgo;
 - iv. riesgos de opacidad o insuficiente explicabilidad;
 - v. riesgos por dependencia de terceros o cambios de proveedor/modelo;
 - vi. riesgos operativos y de continuidad;
 - vii. riesgos por uso fuera del alcance autorizado; y
 - viii. riesgos ambientales cuando el caso de uso implique consumo computacional relevante o dependencia de infraestructura intensiva.

Nota: Las soluciones de IA clasificadas como de riesgo medio y alto deberán

Human-in-the-Loop for Critical Decisions and Human Oversight

The Corporate AI Guideline establishes that **all AI solutions must operate under meaningful human oversight**. Responsibility for decisions always remains with the **process owner**, regardless of the level of automation, and every AI solution must incorporate mechanisms for **human intervention, adjustment, suspension, or correction** that are proportionate to its risk level.

The Guideline classifies AI solutions into **three levels of autonomy**, each with corresponding oversight, escalation, and intervention requirements:

- **Decision-support systems;**
- **Supervised automation;** and
- **High-autonomy automation.**

Each category is subject to governance controls that ensure an appropriate degree of human supervision based on the potential risks associated with the solution.

In addition, **Section 5.4.7** establishes that **no AI solution may fully replace human judgment** in critical decisions involving legal, financial, employment, disciplinary, operational, security, compliance, or human rights-related matters.

For **Operational Technology (OT)** and **Industrial Control Systems (ICS)** environments, **Section 5.4.5.4** further strengthens this safeguard by **explicitly prohibiting the use of autonomous AI in critical operations without prior human validation**. This ensures that AI supports, rather than replaces, human decision-making in high-impact operational contexts.

Human-in-the-Loop for Critical Decisions and Human Oversight

de continuar su desarrollo e implementación.

5.3.2. Primero la vida

Las soluciones de IA deberán garantizar que priorizarán la vida y la integridad de las personas por encima de todo.

5.3.3. IA centrada en las personas

Los sistemas de IA se desarrollarán y utilizarán como una herramienta al servicio de las personas, que respete la dignidad humana, el conocimiento, la experiencia, y la autonomía personal, y que funcione de manera que pueda ser controlada y vigilada adecuadamente por seres humanos.

5.3.4. Responsabilidad individual e indispensabilidad del componente humano

En todos los casos, las soluciones de IA deberán operar bajo supervisión humana efectiva. La responsabilidad por las decisiones, recomendaciones o acciones apoyadas o ejecutadas mediante estas soluciones recae en el dueño del proceso y en las personas responsables designadas, con independencia del nivel de automatización. En consecuencia, la IA debe entenderse como una herramienta de apoyo y ampliación de capacidades, y no como un reemplazo integral del juicio, la responsabilidad ni la rendición de cuentas humanas. Toda solución deberá garantizar, de manera proporcional a su nivel de riesgo, mecanismos de intervención, ajuste, suspensión o corrección de su comportamiento, así como esquemas claros de supervisión y escalamiento cuando sea necesario.

Asimismo, el uso de soluciones de IA no exime a las personas de las responsabilidades inherentes a la protección de la información. En este sentido, todas las personas que trabajen

Información Interna

Design Envelope ID: 4E02C1B7-7DEB-8BA3-80A0-91EEAFC6EE49

Guía Corporativa

6

para o en nombre de ISA y sus empresas son responsables de manera individual, de proteger la confidencialidad, integridad y disponibilidad de la información a la que acceden, utilizan o gestionan, y deben actuar de forma diligente para prevenir su uso indebido, pérdida, divulgación no autorizada o alteración, en cumplimiento de las políticas, estándares y lineamientos establecidos por la organización. La adopción de capacidades de IA deberá fortalecer, y en

adecuado de la información, riesgos asociados y buenas prácticas de seguridad. La organización deberá definir el formato mínimo, los mecanismos de certificación o constancia de cumplimiento y la conservación de evidencia para fines de seguimiento y auditoría.

5.4.7. Lineamientos sobre el uso e implementación de soluciones de inteligencia artificial

Toda iniciativa de IA, incluyendo GenIA, asistentes conversacionales, agentes personales y agentes de proceso, debe gestionarse mediante un proceso formal que articule las exigencias ya desarrolladas en esta guía sobre clasificación por riesgo, evaluación de privacidad y ciberseguridad, validación humana, trazabilidad, operación, monitoreo y aprobación previa al

Información Interna

Design Envelope ID: 4E02C1B7-7DEB-8BA3-80A0-91EEAFC6EE49

Guía Corporativa

13

despliegue. En consecuencia, esta sección consolida las condiciones mínimas para integrar dichos requisitos dentro del ciclo de implementación de cada solución.

Todo contenido, documento, informe, comunicación o resultado generado total o parcialmente con asistencia de IA y que sea utilizado en procesos de negocio, comunicaciones formales o soporte a la toma de decisiones deberá identificarse de conformidad con los lineamientos de transparencia y revisión humana definidos en esta guía, especialmente en la sección 5.3.5. Cuando aplique, deberá conservarse evidencia de la revisión realizada por la persona responsable.

Como condición mínima para su paso a producción, toda solución de IA deberá contar con evidencia documentada del cumplimiento de los requisitos aplicables definidos en esta guía, incluidos: definición del caso de uso y del objetivo; identificación de responsables; evaluación de datos; evaluación de riesgos, privacidad y ciberseguridad; pruebas y validación; esquema de operación y soporte; plan de monitoreo y revisión; gestión de cambios; y análisis de valor para la organización. El detalle de estos requisitos se desarrolla en las secciones 5.4.2, 5.4.5, 5.4.8 y concordantes.

Gestión de cambios: toda implementación o cambio relevante del modelo, prompts base, conectores, datos, reglas de decisión, fuentes de información, versiones o integraciones deberá gestionarse conforme al proceso corporativo de gestión de cambios, considerando su impacto en riesgos, seguridad, resultados y operación. Los cambios que alteren el comportamiento, el alcance o el nivel de riesgo de la solución exigirán reevaluación y aprobación del dueño del proceso y del Área de TI, de conformidad con lo previsto en las secciones 5.4.2 y 5.4.8.

Transparency and Explainability of AI Systems

Section 5.3.5 (Transparency and Explainability) directly addresses this element.

The Corporate AI Guideline establishes that AI solutions must be designed with appropriate levels of **traceability and explainability**, enabling individuals to identify when they are interacting with an AI system, understand how AI-generated outputs are produced, and recognize the system's capabilities and limitations.

The Guideline also prohibits the use of AI as the **sole source of truth** or as an **autonomous decision-making mechanism** for matters involving critical impact. It requires that all AI-generated outputs be **reviewed, validated, and contextualized by a responsible individual** before they are used in business processes or decision-making.

Furthermore, the Guideline requires each AI solution to **define and document, prior to deployment, the level of explainability required** based on its intended purpose, criticality, and potential impact.

This element is further reinforced by **Section 5.4.7**, which requires that any AI-generated content used in business processes or formal communications include a **clear and visible indication of its AI origin**, together with evidence that the content has undergone **human review**.

In addition, the responsibilities assigned to the organization's **AI Champions** under **Section 5.5** explicitly include promoting the proper identification and labeling of AI-generated content, thereby strengthening transparency and fostering responsible AI use across the organization.

gestionan, y deben actuar de forma diligente para prevenir su uso indebido, pérdida, divulgación no autorizada o alteración, en cumplimiento de las políticas, estándares y lineamientos establecidos por la organización. La adopción de capacidades de IA deberá fortalecer, y en ningún caso sustituir, el compromiso individual con la seguridad de la información, la gestión responsable de los datos y el cumplimiento de las disposiciones corporativas aplicables.

Para efectos de gestión de riesgos y definición de controles, las soluciones de IA deberán clasificarse según su nivel de autonomía, distinguiendo al menos entre: i) soporte a decisiones, ii) automatización supervisada y iii) automatización de alta autonomía. Cada nivel deberá contar con criterios de supervisión humana, escalamiento e intervención proporcional al riesgo.

5.3.5. Transparencia y explicabilidad

Las soluciones de IA deberán diseñarse y operar con niveles adecuados de trazabilidad y explicabilidad. Esto permitirá que las personas identifiquen cuándo interactúan con un sistema de IA, comprendan de forma razonable cómo se generan sus resultados y conozcan sus capacidades y limitaciones.

Las soluciones de IA, en especial las basadas en modelos generativos pueden producir resultados incorrectos, incompletos, desactualizados o no verificables. En consecuencia, la IA no deberá utilizarse como fuente única de verdad ni como mecanismo autónomo de decisión en asuntos operativos, legales, financieros, de seguridad, cumplimiento o impacto crítico.

Todo resultado generado por IA deberá ser revisado, validado y contextualizado por una persona responsable antes de ser utilizado en procesos de negocio o toma de decisiones.

Toda solución de IA deberá definir y documentar, de forma previa a su despliegue, el nivel de explicabilidad requerido según su finalidad, criticidad, impacto potencial y perfil de riesgo, así como los mecanismos dispuestos para comunicar dicha explicabilidad a usuarios, responsables del proceso y demás partes interesadas.

5.3.6. Colaboración y participación

En ISA y sus empresas se debe fomentar la colaboración entre las áreas involucradas en el desarrollo, implementación y uso de soluciones de IA, promoviendo el intercambio de conocimientos, capacidades y mejores prácticas, de acuerdo con las responsabilidades y competencias de cada una.

5.3.7. Integridad y ética profesional

El talento humano que desarrolla, implementa, gestiona y usa soluciones de IA debe actuar y adherirse a altos estándares de integridad y ética profesional, asegurando siempre que todas las prácticas estén en concordancia con los lineamientos contenidos en el Código de Ética y

5.4.7. Lineamientos sobre el uso e implementación de soluciones de inteligencia artificial

Toda iniciativa de IA, incluyendo GenAI, asistentes conversacionales, agentes personales y agentes de proceso, debe gestionarse mediante un proceso formal que articule las exigencias ya desarrolladas en esta guía sobre clasificación por riesgo, evaluación de privacidad y ciberseguridad, validación humana, trazabilidad, operación, monitoreo y aprobación previa al

Información Interna

Document Envelope ID: 4E02C1B7-7DEB-8BA3-80AD-91EEAFC6EE49

Guía Corporativa

13

despliegue. En consecuencia, esta sección consolida las condiciones mínimas para integrar dichos requisitos dentro del ciclo de implementación de cada solución.

Todo contenido, documento, informe, comunicación o resultado generado total o parcialmente con asistencia de IA y que sea utilizado en procesos de negocio, comunicaciones formales o soporte a la toma de decisiones deberá identificarse de conformidad con los lineamientos de transparencia y revisión humana definidos en esta guía, especialmente en la sección 5.3.5. Cuando aplique, deberá conservarse evidencia de la revisión realizada por la persona responsable.

Como condición mínima para su paso a producción, toda solución de IA deberá contar con evidencia documentada del cumplimiento de los requisitos aplicables definidos en esta guía, incluidos: definición del caso de uso y del objetivo; identificación de responsables, evaluación de datos; evaluación de riesgos, privacidad y ciberseguridad; pruebas y validación; esquema de operación y soporte; plan de monitoreo y revisión; gestión de cambios; y análisis de valor para la organización. El detalle de estos requisitos se desarrolla en las secciones 5.4.2, 5.4.5, 5.4.8 y concordantes.

Gestión de cambios: toda implementación o cambio relevante del modelo, prompts base, conectores, datos, reglas de decisión, fuentes de información, versiones o integraciones deberá gestionarse conforme al proceso corporativo de gestión de cambios, considerando su impacto en riesgos, seguridad, resultados y operación. Los cambios que alteren el comportamiento, el alcance o el nivel de riesgo de la solución exigirán reevaluación y aprobación del dueño del proceso y del Área de TI, de conformidad con lo previsto en las secciones 5.4.2 y 5.4.8.

Entrenamiento: antes del despliegue se debe capacitar a los usuarios en alcance

cumplido integralmente el proceso de evaluación, aprobación y gestión de riesgos previsto en esta guía.

Con estas condiciones, el uso corporativo de herramientas de IA debe entenderse siempre como una extensión de los controles definidos para toda la solución, y no como una excepción a los requisitos de evaluación, aprobación, monitoreo o rendición de cuentas previstos en esta guía.

5.5 ROLES Y RESPONSABILIDADES

Rol	Responsabilidades
Comité de Gobierno Corporativo, Sostenibilidad, Tecnología e Innovación de la Junta Directiva	- Orientar, en el marco de sus competencias, la visión corporativa sobre tecnología, innovación y sostenibilidad aplicable al uso estratégico de la IA. - Conocer y dar seguimiento, en el marco de sus competencias, a los lineamientos corporativos y a los asuntos estratégicos asociados a la adopción de IA.
Comité de Auditoría y Riesgos Corporativos de la Junta Directiva	- Supervisar, en el marco de sus competencias, la gestión de los riesgos asociados al uso, desarrollo e implementación de soluciones de IA. - Conocer y dar seguimiento, en el marco de sus competencias, a los asuntos de riesgo y control relevantes derivados de la adopción de IA.
Comité de ética	- Gestionar, en el marco de sus competencias, las investigaciones relacionadas con conductas contrarias a la ética o a la integridad derivadas del uso de IA. - Promover, en el marco de sus competencias, la observancia de los principios éticos aplicables al uso, desarrollo e implementación de la IA.
Área de Tecnología de la Información de ISA	- Definir, administrar y actualizar el marco corporativo para el uso, desarrollo e implementación de la IA. - Gestionar esta guía y los lineamientos corporativos asociados a la adopción de IA. - Evaluar y aprobar, cuando corresponda, aplicaciones, herramientas, integraciones o usos excepcionales de IA. - Implementar y verificar controles para asegurar el

Clear Accountability for the Outcomes Produced by AI Models and Tools

Section 5.3.11 (Accountability and Responsibility) provides a comprehensive framework for this element.

The Corporate AI Guideline establishes that every AI solution must operate under a **dedicated governance model** that is proportionate to its level of risk and includes clearly assigned responsibilities, decision traceability, and meaningful human oversight.

Before deployment, each AI solution must have a formally documented allocation of roles and responsibilities, identifying at a minimum:

- The process owner;
- The technical owner;
- The business/functional owner;
- The cybersecurity owner;
- The privacy owner;
- The approving authority; and
- The individuals responsible for monitoring, periodic review, and retirement of the solution.

The Guideline further establishes that the involvement of third-party providers, external AI models, or APIs does not relieve ISA of responsibility for the use, outputs, or impacts of the AI solution. ISA remains accountable for the outcomes generated through the deployment and use of AI within its business processes.

This governance framework is complemented by Section 5.5 (Roles and Responsibilities), which provides a comprehensive allocation of responsibilities across the organization—from Board-level committees to operational personnel—covering every stage of the AI lifecycle.

In addition, Section 5.4.4 (AI Appeals Process) establishes a formal mechanism for the investigation, review, and remediation of errors or adverse impacts arising from AI-supported decisions. Appeals are managed through the Ethics Hotline, ensuring that concerns related to AI use are subject to structured investigation, human review, and, where appropriate, corrective action.

5.3.10. Fuentes de información

Debe garantizarse claridad sobre las fuentes de información utilizadas por las soluciones de IA y, cuando aplique, sobre las fuentes citadas o referenciadas en los resultados generados. Las personas responsables de la toma de decisiones deben conocer la procedencia, el método de obtención y las limitaciones de la información utilizada, así como abstenerse de atribuir autoría humana o incurrir en plagio respecto de contenidos generados por IA.

5.3.11. Rendición de cuentas y responsabilidad

Las soluciones de IA deberán asegurar que quienes intervienen en su ciclo de vida sostengan una responsabilidad profesional sobre el impacto de los usos de esta tecnología, facilitando así un proceso efectivo y transparente de rendición de cuentas.

Las soluciones de IA desarrolladas, adquiridas u operadas por ISA y sus empresas, en entornos IT, OT, ICS y/o servicios digitales, deben contar con un modelo de gobierno específico por solución, proporcional a su nivel de riesgo, que asegure la asignación clara de responsabilidades, la trazabilidad de decisiones, la supervisión humana y la integración con los modelos corporativos de gobierno de TI, riesgos y seguridad de la información, durante todo su ciclo de vida.

Toda solución de IA deberá contar, de manera previa a su análisis, desarrollo, adquisición o despliegue, con una asignación formal y documentada de roles y responsabilidades, que identifique como mínimo: i) dueño del proceso; ii) responsable técnico; iii) responsable funcional o de negocio; iv) responsable de ciberseguridad, cuando aplique; v) responsable de privacidad o protección de datos, cuando aplique; vi) instancia de aprobación; y vii) responsables del monitoreo, revisión, retiro y gestión de incidentes.

Esta asignación deberá mantenerse actualizada durante todo el ciclo de vida de la solución y reflejarse en los registros corporativos, matrices de responsabilidad, evidencias de aprobación y mecanismos de seguimiento aplicables.

En ningún caso la participación de terceros proveedores, modelos externos, APIs, integradores o herramientas de IA generativa eximirá a ISA y sus empresas de la responsabilidad sobre el uso, los resultados y los impactos de la solución en sus procesos, usuarios, clientes, trabajadores o terceros.

5.3.12. Sostenibilidad ambiental de la IA

ISA y sus empresas deberán incorporar criterios de sostenibilidad ambiental en la evaluación, selección, contratación, renovación y operación de soluciones de IA, de forma proporcional al nivel de riesgo, escala, criticidad y consumo computacional de cada caso de uso.

En los procesos de adquisición o renovación de soluciones de IA propias o de terceros, se deberán considerar y documentar, como mínimo cuando aplique:

- i. compromisos verificables del proveedor en materia de energía renovable, reducción de

- monitorear el comportamiento de la analítica e IA, teniendo en cuenta por ejemplo palabras clave, usabilidad, etc.
- Identificar e investigar interacciones sospechosas (alertas).
- Cumplir con los controles de acceso y autorización
- Otros que sean apropiados para esta finalidad.

Las soluciones de IA en operación deberán contar con mecanismos de monitoreo orientados a detectar deriva, degradación de desempeño, cambios en patrones de uso, variaciones en la calidad de los datos de entrada y desviaciones relevantes en los resultados. Dicho monitoreo deberá definir, como mínimo: métricas aplicables, frecuencia de revisión, umbrales de alerta, responsables del seguimiento y protocolo de actuación ante hallazgos, incluyendo evaluación, contención, ajuste, reentrenamiento, suspensión o retiro de la solución cuando corresponda.

La identificación, evaluación, tratamiento y monitoreo de los riesgos asociados a la Inteligencia Artificial deberán alinearse con el AI Risk Management Framework (AI RMF) del NIST, asegurando un enfoque integral que fortalezca el gobierno, diseño, operación, medición y mejora continua de las soluciones de IA.

Además de los controles anteriores, la gestión del riesgo debe contemplar riesgos no técnicos que impactan directamente la calidad de los resultados, como los sesgos algorítmicos y la representatividad de los datos, los cuales se abordan en la siguiente sección.

5.4.3. Manejo de sesgos algorítmicos en IA

El desarrollo e implementación de soluciones de IA debe abordar y minimizar los sesgos asociados a los conjuntos de datos usados para entrenar los algoritmos, a decisiones de diseño y a limitaciones inherentes de los propios algoritmos. Es crucial probar y validar los sistemas de

5.4.4. Proceso de apelación de decisiones de IA

ISA cuenta con la **Línea Ética** como mecanismo institucional para que empleados, clientes, proveedores u otros terceros potencialmente afectados soliciten la revisión de decisiones o resultados materialmente relevantes generados o soportados por sistemas de IA. Este mecanismo ya existe y contiene, como mínimo: i) un canal de recepción accesible; ii) plazos de respuesta; iii) la asignación de un responsable de revisión humana, de acuerdo con las instancias competentes definidas por la organización; iv) la evaluación del caso con base en la información disponible; y v) la documentación del resultado y de las medidas correctivas que correspondan.

Cuando corresponda, la Línea Ética se articula con otros canales institucionales ya existentes de atención corporativa, asegurando trazabilidad, revisión humana efectiva y respuesta oportuna conforme a los responsables definidos por ISA y sus empresas.

5.4.5. Ciberseguridad en Inteligencia Artificial

Las soluciones de Inteligencia Artificial, incluida la Inteligencia Artificial Generativa, introducen **riesgos de ciberseguridad específicos** que deben ser gestionados de manera diferenciada

Clear limits on what AI can and cannot do

The Corporate AI Guideline establishes clear governance mechanisms that define the **permitted scope, operational boundaries, and prohibited uses** of AI solutions throughout their lifecycle.

Section 5.4.8.1 introduces a **formal risk-based classification** of AI use cases into **low-, medium-, and high-risk** categories. Each category is subject to differentiated governance requirements based on factors such as the level of autonomy, the ability to execute actions within information systems, the potential impact on individual rights, and the capacity to influence individual or collective decisions.

In addition, **Section 5.4.7** requires every AI solution to have a **documented definition of its scope, intended purpose, capabilities, limitations, operating conditions, usage restrictions, and underlying assumptions** before it may be deployed. This ensures that the intended use and operational boundaries of every AI solution are clearly established and understood.

The **Corporate AI Inventory**, described in **Section 5.4.8.3**, further reinforces these limits by classifying AI tools as **approved, restricted, or prohibited**, with the inventory subject to review at least annually to ensure continued alignment with organizational requirements and evolving regulatory expectations.

The Guideline also establishes **absolute prohibitions**. Under **Section 5.3.1**, ISA will **not implement, promote, or permit** the use of AI for:

- Social scoring or social classification of individuals;
- Covert manipulation of human behavior;
- Exploitation of vulnerable persons or groups; or
- Unauthorized large-scale biometric surveillance.

Finally, **Section 5.4.8.3** requires every AI solution to **explicitly declare whether it incorporates sensitive capabilities**. The deployment of any such capability is subject to **enhanced approval** by the **Legal, Privacy**, and the **competent business authority**, ensuring that high-impact AI functionalities cannot be enabled without appropriate governance, oversight, and authorization.

5.4.8.1 Clasificación del caso de uso por nivel de riesgo

- **Bajo:** apoyo a productividad (p. ej., redacción, resumen, análisis) sin decisión automatizada ni ejecución en sistemas productivos. Requiere: uso de herramienta licenciada, manejo de información según clasificación, revisión humana y registro básico del caso de uso.
- **Medio:** chatbot o agente que consulta repositorios corporativos o recomienda acciones, con impacto limitado y con confirmación humana previa a la ejecución. Requiere, además: evaluación de riesgos, pruebas de sesgos/precisión, controles de acceso y trazabilidad.
- **Alto:** agentes de proceso con jerarquía organizacional, soluciones que ejecutan acciones en sistemas, soportan decisiones críticas (seguridad, operación, cumplimiento) o tratan datos sensibles a escala. Requiere, además: aprobación formal del dueño del proceso y TI, evaluación de ciberseguridad y privacidad reforzada, monitoreo continuo, auditoría, plan de continuidad y gestión del cambio organizacional. La clasificación del nivel de riesgo deberá considerar expresamente, además del caso de uso y de los datos tratados, los siguientes factores:
 - i. grado de autonomía de la solución;
 - ii. posibilidad de ejecutar acciones en sistemas internos o externos;
 - iii. impacto potencial sobre derechos, seguridad, continuidad operativa o cumplimiento;
 - iv. uso de datos personales o sensibles;
 - v. alcance sobre clientes, empleados, proveedores u otros terceros; y
 - vi. posibilidad de afectar materialmente decisiones individuales o colectivas.

Toda solución que soporte, recomiende o influya de manera relevante en decisiones sobre personas, cumplimiento, seguridad, operación crítica, asuntos legales o financieros deberá ser clasificada, como mínimo, como de riesgo medio o alto, según su nivel de autonomía e impacto potencial.

5.4.8.2 Pasos mínimos (gates) y evidencias requeridas

- **Registro e ideación:** el Área interna contacta al equipo del COE Digital para registrar el caso de uso, objetivo, alcance, datos involucrados y nivel de riesgo preliminar.
- **Evaluación de datos:** se documentan fuentes, calidad, clasificación, permisos, retención y restricciones de uso; se define si hay datos personales o confidenciales.
- **Evaluación de riesgos:** se realiza análisis de riesgos (ético, sesgos, seguridad, privacidad, operación, legal) y plan de tratamiento; debe quedar documentado y aprobado. Los sistemas de IA deben diseñarse para operar de forma resiliente, fallar de manera segura y no comprometer la continuidad operativa de los servicios críticos, incorporando mecanismos de respaldo y fallback.

La evaluación de riesgos deberá incluir de forma expresa y documentada:

- i. riesgos de privacidad y protección de datos;
- ii. riesgos de ciberseguridad específicos de IA;
- iii. riesgos éticos y de sesgo;
- iv. riesgos de opacidad o insuficiente explicabilidad;
- v. riesgos por dependencia de terceros o cambios de proveedor/modelo;
- vi. riesgos operativos y de continuidad;
- vii. riesgos por uso fuera del alcance autorizado;
- viii. riesgos operativos y de continuidad;
- ix. riesgos por dependencia de terceros o cambios de proveedor/modelo;
- x. riesgos de opacidad o insuficiente explicabilidad;
- xi. riesgos éticos y de sesgo;

5.4.7. Lineamientos sobre el uso e implementación de soluciones de inteligencia artificial

Toda iniciativa de IA, incluyendo GenIA, asistentes conversacionales, agentes personales y agentes de proceso, debe gestionarse mediante un proceso formal que articule las exigencias ya desarrolladas en esta guía sobre clasificación por riesgo, evaluación de privacidad y ciberseguridad, validación humana, trazabilidad, operación, monitoreo y aprobación previa al

Formación Interna

Design Envelope ID: 4E02C1B7-7DEB-8BA3-80A0-91EEAFC6EE49

Guía Corporativa

13

despliegue. En consecuencia, esta sección consolida las condiciones mínimas para integrar dichos requisitos dentro del ciclo de implementación de cada solución.

Todo contenido, documento, informe, comunicación o resultado generado total o parcialmente con asistencia de IA y que sea utilizado en procesos de negocio, comunicaciones formales o soporte a la toma de decisiones deberá identificarse de conformidad con los lineamientos de transparencia y revisión humana definidos en esta guía, especialmente en la sección 5.3.5. Cuando aplique, deberá conservarse evidencia de la revisión realizada por la persona responsable.

Como condición mínima para su paso a producción, toda solución de IA deberá contar con evidencia documentada del cumplimiento de los requisitos aplicables definidos en esta guía, incluidos: definición del caso de uso y del objetivo; identificación de responsables; evaluación de datos; evaluación de riesgos, privacidad y ciberseguridad; pruebas y validación; esquema de operación y soporte; plan de monitoreo y revisión; gestión de cambios; y análisis de valor para la organización. El detalle de estos requisitos se desarrolla en las secciones 5.4.2, 5.4.5, 5.4.8 y concordantes.

Gestión de cambios: toda implementación o cambio relevante del modelo, prompts base, conectores, datos, reglas de decisión, fuentes de información, versiones o integraciones deberá gestionarse conforme al proceso corporativo de gestión de cambios, considerando su impacto en riesgos, seguridad, resultados y operación. Los cambios que alteren el comportamiento, el alcance o el nivel de riesgo de la solución exigirán reevaluación y aprobación del dueño del proceso y del Área de TI, de conformidad con lo previsto en las secciones 5.4.2 y 5.4.8.

- o **Entrenamiento:** antes del despliegue se **debe** capacitar a los usuarios en alcance, limitaciones, verificación humana, riesgos, seguridad, manejo de la información, uso ético y uso aceptable de la solución.

- o **Entrenamiento:** antes del despliegue se **debe** capacitar a los usuarios en alcance,

consultado; I = Informado. Cuando la solución se implemente en una filial, el Área de Tecnología de la Información de ISA articulará la participación del Área de TI de la filial conforme al Modelo de Gobierno de TI y a las definiciones corporativas aplicables. En soluciones de riesgo alto podrán intervenir además otras instancias o actores de control, como Riesgos, Privacidad, Ciberseguridad o comités competentes, según corresponda.

5.4.8.3 Inventario y registro corporativo de IA

El Área de TI **debe** administrar un inventario corporativo de soluciones de IA, agentes y herramientas de IA generativa en un repositorio corporativo definido para tal fin, con control de versiones, trazabilidad de cambios y acceso restringido según el rol. Este inventario constituye la fuente oficial para el registro, seguimiento, control y evaluación de soluciones de IA en análisis, piloto, producción, suspensión, retiro o descarte, y **debe** utilizarse como insumo para auditorías, revisiones de riesgo, decisiones de continuidad y evaluación del valor generado.

La actualización del inventario **debe** realizarse, como mínimo, en los siguientes momentos: (i) al registrar una nueva iniciativa o herramienta para análisis; (ii) al aprobar su paso a piloto o producción; (iii) ante cambios relevantes de modelo, proveedor, conectores, datos, riesgos, costos, responsables o estado; (iv) en cada revisión periódica definida por el dueño del proceso y el Área de TI; y (v) al retiro, suspensión o descarte de la solución. Toda actualización **debe** dejar evidencia de la fecha, responsable del cambio y motivo de actualización.

Como mecanismo mínimo de gobierno, el inventario corporativo **debe** diferenciar al menos dos registros complementarios: **(a) inventario de agentes**, para agentes personales, asistentes conversacionales, agentes de proceso y sistemas multiagente.

mismo, debe propender por no exacerbar brechas digitales y, bajo el sentido de proporcionalidad, velar porque sea accesible y beneficiosa para todos, incluyendo a diversos agentes y promoviendo la igualdad de acceso, la igualdad de género y la diversidad cultural, evitando al mismo tiempo los efectos discriminatorios y los sesgos prohibidos por el ordenamiento jurídico.

ISA no implementará, promoverá ni tolerará el uso de sistemas de IA destinados al puntaje o clasificación social de personas, a la manipulación encubierta del comportamiento humano, a la explotación de vulnerabilidades de personas o grupos, ni a la vigilancia biométrica masiva no autorizada, en línea con la regulación aplicable y con referentes internacionales como el EU AI Act.

Los sistemas de IA deberán someterse a evaluaciones periódicas de sesgos mediante metodologías, herramientas o criterios definidos por la organización, con el fin de identificar, documentar, mitigar y monitorear impactos discriminatorios o resultados inequitativos durante su ciclo de vida.

Además de las prohibiciones ya definidas en esta guía, no podrán promoverse, desarrollarse, adquirirse, desplegarse ni utilizarse soluciones de IA cuyo propósito o efecto sea eludir controles corporativos, generar engaño material, vulnerar derechos fundamentales, facilitar conductas ilícitas o realizar tratamiento no autorizado de datos, perfiles o inferencias sobre personas.

Cualquier caso de uso que presente duda razonable sobre su licitud, proporcionalidad, legitimidad o aceptabilidad ética deberá escalararse para revisión previa por las instancias competentes antes de continuar su desarrollo o implementación.

Prohibition on the use of AI systems prohibited under the EU AI Act

Section 5.3.1 (Fairness and Non-Discrimination) explicitly establishes that ISA will **not implement, promote, or permit** the use of AI systems intended for:

- **Social scoring or social classification of individuals;**
- **Covert manipulation of human behavior;**
- **Exploitation of the vulnerabilities of individuals or groups; or**
- **Unauthorized large-scale biometric surveillance.**

These prohibitions are aligned with applicable legal and regulatory requirements, including internationally recognized frameworks such as the **EU AI Act**.

The Guideline further provides that AI solutions **may not be promoted, developed, acquired, deployed, or used** if their purpose or effect is to:

- Circumvent corporate controls or governance mechanisms;
- Materially deceive individuals or stakeholders;
- Infringe fundamental rights;
- Facilitate unlawful or illegal activities; or
- Perform unauthorized processing of personal data, profiling, or inferences about individuals.

Where there is **reasonable uncertainty** regarding the legality, proportionality, or ethical acceptability of a proposed AI use case, the matter must be **escalated for formal review prior to implementation**.

This principle is operationalized through **Section 5.4.8.3**, which requires the **Corporate AI Inventory** to identify and classify AI tools that incorporate **sensitive capabilities** and subjects such tools to an **enhanced approval process** before deployment. The same section also requires the organization's list of **prohibited AI tools and technologies** to be reviewed **at least annually**, ensuring that it remains aligned with evolving legal, regulatory, and ethical requirements

5.4.8.3 Inventario y registro corporativo de IA

El Área de TI debe administrar un inventario corporativo de soluciones de IA, agentes y herramientas de IA generativa en un repositorio corporativo definido para tal fin, con control de versiones, trazabilidad de cambios y acceso restringido según el rol. Este inventario constituye la fuente oficial para el registro, seguimiento, control y evaluación de soluciones de IA en análisis, piloto, producción, suspensión, retiro o descarte, y debe utilizarse como insumo para auditorías, revisiones de riesgo, decisiones de continuidad y evaluación del valor generado.

La actualización del inventario debe realizarse, como mínimo, en los siguientes momentos: (i) al registrar una nueva iniciativa o herramienta para análisis; (ii) al aprobar su paso a piloto o producción; (iii) ante cambios relevantes de modelo, proveedor, conectores, datos, riesgos, costos, responsables o estado; (iv) en cada revisión periódica definida por el dueño del proceso y el Área de TI; y (v) al retiro, suspensión o descarte de la solución. Toda actualización debe dejar evidencia de la fecha, responsable del cambio y motivo de actualización.

Como mecanismo mínimo de gobierno, el inventario corporativo debe diferenciar al menos dos registros complementarios: (a) inventario de agentes, para agentes personales, asistentes conversacionales, agentes de proceso y sistemas multiagente.

El uso, desarrollo e implementación de Inteligencia Artificial debe darse con estricta observancia de los siguientes principios:

5.3.1. Equidad y no discriminación

Las soluciones de IA deben utilizarse de manera que no discriminen a ningún individuo o grupo, respetando las leyes locales y los valores establecidos en el código de ética y conducta de ISA y sus empresas. Es fundamental garantizar que los conjuntos de datos utilizados para entrenar estos sistemas sean diversos y representativos. Además, es crucial probar las soluciones de IA para detectar y corregir sesgos y evitar que la IA incida en la toma de decisiones con criterios discriminatorios.

La IA no debe perpetuar ni acentuar prejuicios basados en características como género, raza, color, religión, orientación sexual, ideología política o procedencia, discapacidad, entre otros. Así

nación Interna

Envelope ID: 4E02C1B7-7DEB-8BA3-80A0-91EEAF08EE49

Guía Corporativa

5

mismo, debe propender por no exacerbar brechas digitales y, bajo el sentido de proporcionalidad, velar porque sea accesible y beneficiosa para todos, incluyendo a diversos agentes y promoviendo la igualdad de acceso, la igualdad de género y la diversidad cultural, evitando al mismo tiempo los efectos discriminatorios y los sesgos prohibidos por el ordenamiento jurídico.

ISA no implementará, promoverá ni tolerará el uso de sistemas de IA destinados al puntaje o clasificación social de personas, a la manipulación encubierta del comportamiento humano, a la explotación de vulnerabilidades de personas o grupos, ni a la vigilancia biométrica masiva no autorizada, en línea con la regulación aplicable y con referentes internacionales como el EU AI Act.

Los sistemas de IA deberán someterse a evaluaciones periódicas de sesgos mediante metodologías, herramientas o criterios definidos por la organización, con el fin de identificar, documentar, mitigar y monitorear impactos discriminatorios o resultados inequitativos durante su ciclo de vida.

Además de las prohibiciones ya definidas en esta guía, no podrán promoverse, desarrollarse, adquirirse, desplegarse ni utilizarse soluciones de IA cuyo propósito o efecto sea eludir controles corporativos, generar engaño material, vulnerar derechos fundamentales, facilitar conductas ilícitas o realizar tratamiento no autorizado de datos, perfiles o inferencias sobre personas.

Cualquier caso de uso que presente duda razonable sobre su licitud, proporcionalidad, legitimidad o aceptabilidad ética deberá escalarse para revisión previa por las instancias competentes antes de continuar su desarrollo o implementación.

5.3.2. Primero la vida

Las soluciones de IA deberán garantizar que priorizarán la vida y la integridad de las personas por encima de todo.

5.3.3. IA centrada en las personas

Los sistemas de IA se desarrollarán y utilizarán como una herramienta al servicio de las personas, que respete la dignidad humana, el conocimiento, la experiencia, y la autonomía personal, y que

Responsible Artificial Intelligence Program

5.4.5.2 Controles mínimos de ciberseguridad para IA

Como mínimo, toda solución de IA deberá implementar controles proporcionales a su nivel de riesgo, que incluyan:

- **Autenticación y control de acceso robustos**, incluyendo Single Sign-On (SSO), Multi-Factor Authentication (MFA), segregación de funciones y aplicación del principio de mínimo privilegio.
- **Restricciones explícitas de acceso a la información según su clasificación** (pública, uso interno, confidencial o restringida), evitando su uso en entrenamiento, procesamiento o almacenamiento no autorizado.
- **Protección de la información**, incluyendo cifrado en tránsito y en reposo cuando aplique, así como segmentación y segregación de ambientes.
- **Trazabilidad, registro y monitoreo continuo**, que permitan auditar interacciones, prompts, uso de datos, acciones ejecutadas por agentes y resultados generados, con el fin de detectar comportamientos anómalos, uso indebido o fugas de información.
- **Pruebas periódicas de seguridad**, que contemplen análisis estático, dinámico y pruebas específicas frente a amenazas propias de la IA.
- **Gestión de vulnerabilidades e incidentes**, incorporando escenarios propios de IA e integrándolos al modelo corporativo de respuesta a incidentes de ciberseguridad y al CSIRT.

Toda solución de IA deberá declarar de forma expresa si incorpora capacidades sensibles, entendidas como aquellas que puedan implicar riesgos elevados para los derechos fundamentales, la privacidad o la autonomía de las personas, incluyendo, entre otras, reconocimiento facial, vigilancia de personas, biometría de voz o identificación biométrica remota. La habilitación de estas capacidades requerirá una aprobación reforzada por parte de las áreas Jurídica, Privacidad y la Dirección competente, independientemente de su nivel de riesgo operativo.

Limiting access to sensitive AI capabilities (e.g. facial recognition, surveillance)

ISA and its subsidiaries have implemented a set of measures to ensure compliance with the requirement to restrict access to sensitive AI capabilities, in accordance with the Corporate Guidelines for the Use, Development, and Implementation of Artificial Intelligence (see attached image).

To achieve this, the following mechanisms have been established and implemented:

Risk-based access controls

All AI solutions implemented at ISA must include access controls proportionate to their level of risk. These controls include robust authentication through Single Sign-On (SSO) and Multi-Factor Authentication (MFA), segregation of duties, and application of the principle of least privilege. These measures ensure that only authorized personnel can access AI tools approved by the organization, including those incorporating higher-sensitivity capabilities.

Explicit declaration and enhanced approval for sensitive capabilities

The Corporate AI Guidelines require that every AI solution explicitly declare whether it incorporates sensitive capabilities, defined as capabilities that may pose significant risks to fundamental rights, privacy, or individual autonomy. This category includes, among others, facial recognition, surveillance of individuals, voice biometrics, and remote biometric identification.

The enablement of any of these capabilities requires enhanced approval from the Legal, Privacy, and the relevant Business/Functional Directorate, regardless of the solution's operational risk level. This mechanism ensures that no sensitive capability can be deployed without the explicit review and authorization of the organizational functions responsible for safeguarding fundamental rights.

Corporate AI Tools Inventory

ISA maintains a corporate inventory of AI solutions that classifies tools into three categories: approved, restricted, and prohibited. This inventory is reviewed at least annually by the IT Department, specifically under the leadership of the Data, Analytics, and AI Center of Excellence, and more frequently whenever regulatory, technological, cybersecurity, or risk-related changes warrant an update. These periodic reviews ensure that access controls remain aligned with the evolving AI landscape and the applicable regulatory environment.

Regardless of the enhanced approval process, ISA and its subsidiaries will neither implement nor permit the use of AI systems for the following purposes, which are considered strictly prohibited:

- Social scoring or classification of individuals based on their behavior or personal characteristics;
- Unauthorized large-scale biometric surveillance in publicly accessible spaces;
- Covert manipulation of human behavior in ways that circumvent individuals' awareness or autonomy; and
- Any use classified as a prohibited practice under the EU AI Act or other applicable regulations in the countries where ISA operates.

Traceability, Monitoring, and Oversight of AI Use

ISA has established traceability and continuous monitoring requirements for the use of all AI tools, including the logging of interactions, prompts, data usage, and actions performed by AI agents. These controls enable the detection of anomalous behavior, misuse, or unauthorized access and provide an ongoing oversight mechanism for the use of AI capabilities across the organization.

Exclusive Use of Licensed and Approved AI Tools

Consistent with its access control principles, the use of unlicensed or unapproved AI tools for processing corporate information is strictly prohibited. No AI solution—including those incorporating sensitive capabilities—may be deployed in a production environment unless it has successfully completed the evaluation, approval, and risk management process established in the Corporate AI Guidelines.

Distinct labeling of AI-generated content and outcomes of AI-driven decisions

ISA and its subsidiaries have implemented specific measures to comply with the AI-generated content labeling requirement under the ISA Group Corporate Artificial Intelligence Guidelines. The mechanisms currently in place to support this requirement are described below.

Mandatory Labeling of AI-Generated Outputs in Business Processes

The Corporate AI Guidelines establish that any content, document, report, communication, or output generated wholly or partially with the assistance of AI, when used in business processes, formal communications, or decision-making support, must include a visible indication that AI was used, together with confirmation that the content has undergone the appropriate human review.

During 2025 and 2026, ISA implemented a labeling application project in partnership with Unisys. This project was deployed across ISA and all of its subsidiaries:



Distinct labeling of AI-generated content and outcomes of AI-driven decisions

Coverage of Conversational Interfaces and External Interactions

The labeling requirement explicitly extends to conversational interfaces, virtual assistants, and chatbots used to interact with third parties or customers. This ensures that anyone engaging with an AI system operated by ISA is proactively informed that they are interacting with AI, in accordance with the principle of transparency toward external users.

Transparency and Explainability as a Foundational Principle

The Guidelines require every AI solution to define and document, prior to deployment, the level of explainability required based on its intended purpose, criticality, potential impact, and risk profile, as well as the mechanisms established to communicate that explainability to users, process owners, and other relevant stakeholders. This principle ensures that labeling is not an isolated requirement but rather an integral part of a transparency-by-design approach embedded in the development of every AI solution.

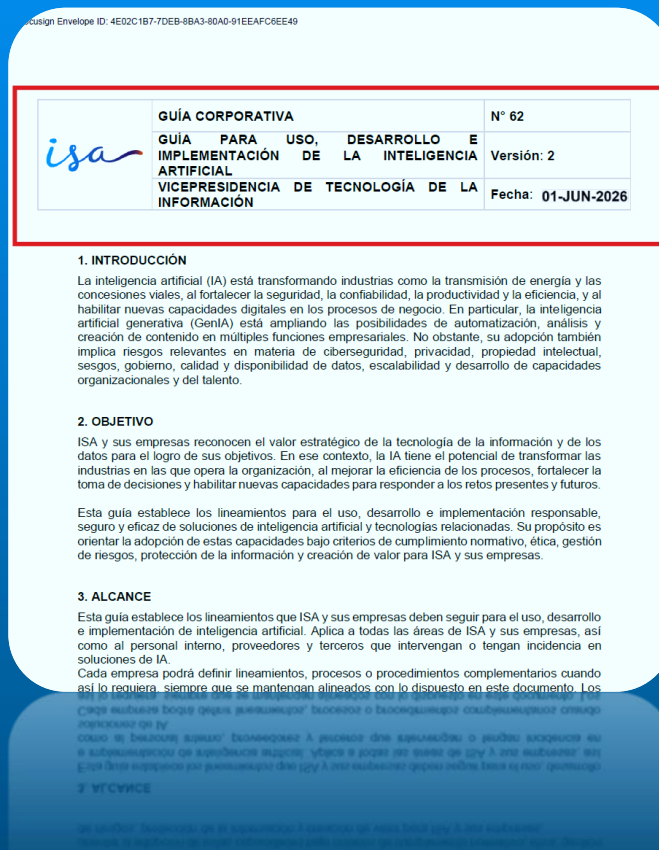


Distinct labeling of AI-generated content and outcomes of AI-driven decisions

Structured Lifecycle Management of AI Solutions

The Guidelines require that every AI initiative—including generative AI, chatbots, personal AI agents, and process automation agents—be managed through a defined governance process with designated owners, supporting evidence, and the necessary approvals prior to deployment. This framework ensures that compliance with the labeling requirement is assessed and verified before any AI solution is placed into operation.

To support this, we have defined a capability framework based on the different categories of AI agents, along with an assessment checklist that must be reviewed prior to creating or publishing an agent (see attached images):



Checklist de evaluación

Antes de construir o publicar un agente, validar:

	Pregunta	Sí / No
01	¿El objetivo del agente está claramente definido?	☐ Sí ☐ No
02	¿Existe un dueño funcional del proceso?	☐ Sí ☐ No
03	¿Las fuentes de conocimiento son confiables y están actualizadas?	☐ Sí ☐ No
04	¿Se definieron límites de lo que el agente puede y no puede hacer?	☐ Sí ☐ No
05	¿Se identificaron riesgos de seguridad, privacidad o permisos?	☐ Sí ☐ No
06	¿Se requiere consumo medido o licencia adicional?	☐ Sí ☐ No
07	¿Se probaron casos exitosos, errores y excepciones?	☐ Sí ☐ No
08	¿Existe un plan de monitoreo y mejora continua?	☐ Sí ☐ No
09	¿Está claro el proceso de publicación o requerimiento formal?	☐ Sí ☐ No
10	¿Se entregaron ejemplos reales de preguntas de usuario?	☐ Sí ☐ No
11	¿Está claro si el agente responde, guía o ejecuta acciones?	☐ Sí ☐ No
12	¿Las documentos fuente son legibles y están actualizados?	☐ Sí ☐ No
13	¿Las tablas, Excel o CSV fueron revisados técnicamente?	☐ Sí ☐ No
14	¿Se definió la frecuencia de actualización de las fuentes?	☐ Sí ☐ No
15	¿Se estableció el tono de voz del agente?	☐ Sí ☐ No
16	¿Se definió que el agente no debe inventar respuestas fuera de sus fuentes?	☐ Sí ☐ No



Aspectos clave

- Alcance y propósito
- Gobierno y seguridad
- Consumo y licenciamiento
- Pruebas, monitoreo y despliegue



Objetivo: validar **preparación, riesgos y condiciones de despliegue** antes de publicar el agente.

Responsible Information Protection to Enable Trustworthy Artificial Intelligence

ISA and its subsidiaries strengthen information protection as a key enabler for the safe and responsible use of digital technologies and Artificial Intelligence. Since 2025, the organization has implemented capabilities designed to prevent information leakage and ensure the protection of data throughout its lifecycle, including:

- Information classification and labeling, enabling the identification and management of different levels of sensitivity for corporate data.
- Monitoring, detection, and traceability, enhancing the identification, tracking, and management of risk events.
- Data Loss Prevention (DLP) through preventive controls and alerts to protect sensitive information across collaboration and productivity environments.

Key 2025 Milestones

- Implementation of the corporate information classification and labeling platform.
- Execution of a pilot program followed by a phased ring-based rollout.
- Delivery of technical training and change management initiatives to support user adoption.

Contribution to Responsible AI

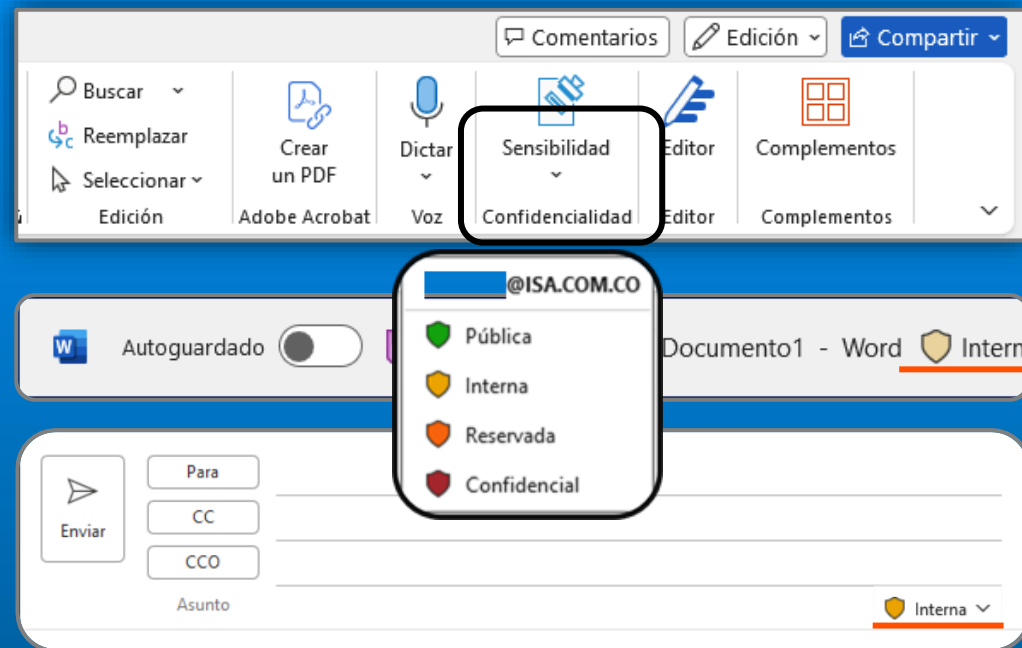
Information classification and labeling serve as a foundational control for reducing the risk of exposing or misusing sensitive information within digital tools and Artificial Intelligence solutions. By ensuring that data is appropriately identified and protected, these measures support the secure, transparent, and responsible deployment of AI across the organization

Number of Documents Currently Labeled (July 2026):

● Public: **207.296** ● Internal: **7.498.902** ● Restricted: **54.837** ● Confidential: **43.779**

Total labeled documents: 7.804.814

Labels are available in:
Word, Excel, PowerPoint y Outlook



Content labeling uses visual elements—such as footers, headers, and watermarks—to indicate the sensitivity of information and help users comply with the organization's information security policies.

Mechanisms to detect and correct drift or degradation of AI models over time

ISA and its subsidiaries have established structured mechanisms for the continuous monitoring of AI solutions in operation, designed to detect and promptly address any model drift or performance degradation that could compromise the reliability of AI-generated outcomes.

Continuous Operational Monitoring

All AI solutions in production are subject to systematic monitoring covering:

- Model drift;
- Performance degradation;
- Changes in usage patterns;
- Variations in input data quality; and
- Significant deviations in generated outputs.

This monitoring is conducted continuously throughout each solution's lifecycle, from deployment through retirement.

Components of the Monitoring Plan

Each AI solution in operation is supported by a monitoring plan that defines:

- The metrics applicable based on the nature and purpose of the solution;
- The frequency for reviewing those metrics;
- Alert thresholds that trigger a formal review;
- Clearly assigned roles and accountability for monitoring activities; and
- A response protocol for identified issues, including evaluation, containment, adjustment, retraining, suspension, or retirement of the solution, as appropriate.

This framework establishes monitoring as a managed, documented, and auditable process, with designated owners responsible for each AI solution.

	Productivity-Extending Agents	Autonomous Process Agents	Multiagent Systems
Description	Support users with queries, drafting, and summarization through conversational interfaces.	Integrated into APIs, drones, or industrial equipment; perform tasks equivalent to human tasks.	Specialized roles for coordination (Queens + executors). Operate multiple human tasks.
System Control	Cannot execute changes in production systems. 	Can register, route, update, and close tasks.	Governed by embedded rules, followed and supervised by the Process Owner.
Human Oversight	Direct user supervision.	Governed by embedded rules. Supervised by the user.	Strictly managed by IT and the Process Owner due to organizational impact.
IT Needs	Driven by the end user, enabled by IT.	Strictly driven by IT and the Process Owner.	



Diagnostic Matrix: Risk-Proportional Governance

	Low Risk	Medium Risk	High Risk
Autonomy Level	None (Productivity support)	Limited (Human confirmation prior to execution)	High / Autonomous (Process agents)
Use Case Examples	Drafting, summarization, text analysis.	Internal chatbots, agents that query corporate repositories.	Solutions that execute actions in production systems, support critical decisions (operations, security).
Deployment Requirements	Use of licensed tool, information handling per classification, human review.	Risk assessment, bias testing, access controls and traceability.	Formal approval from Process Owner + IT + Legal, continuous monitoring, strict auditing.

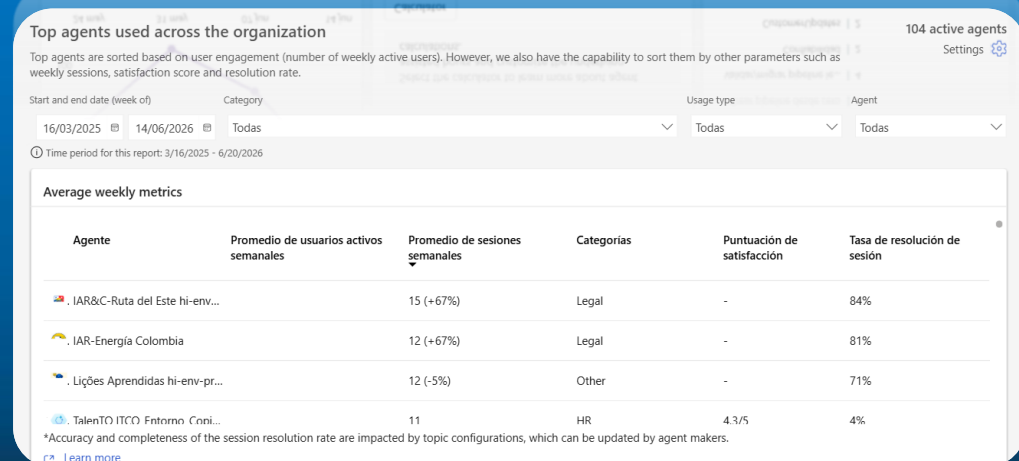
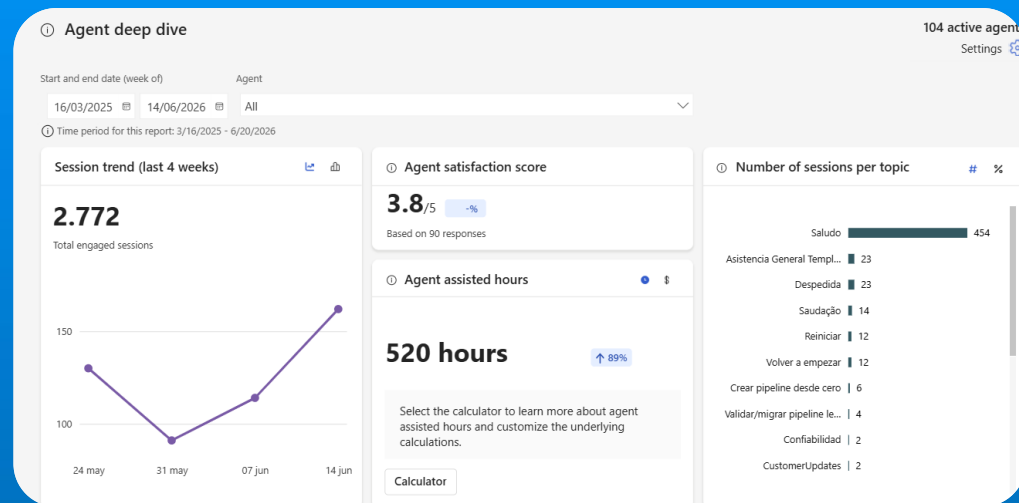
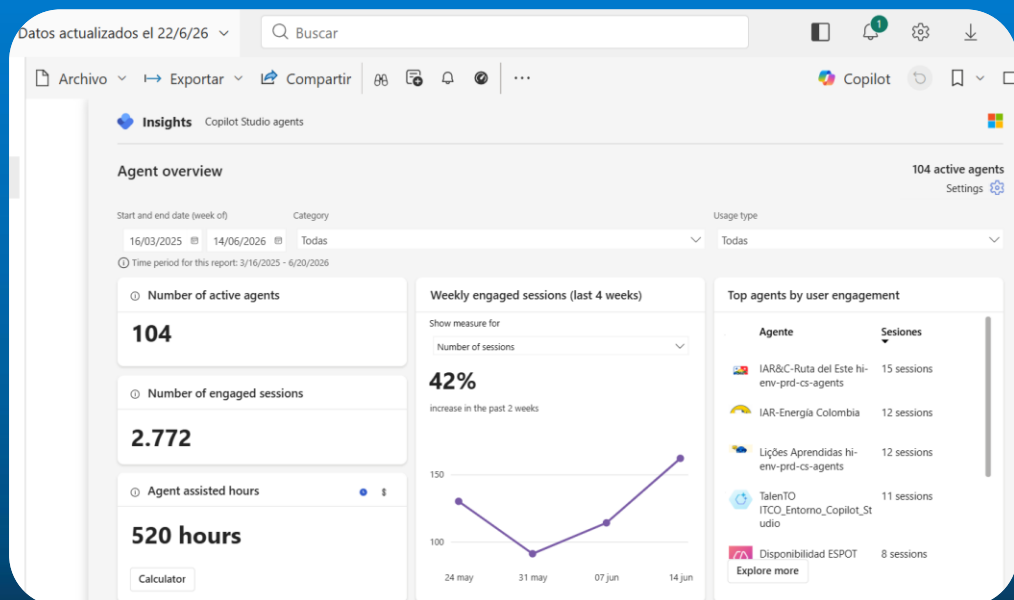
Mechanisms to detect and correct drift or degradation of AI models over time

Reference Framework: NIST AI Risk Management Framework (AI RMF)

The management of AI-related risks—including the detection and correction of model drift—is aligned with the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF). This ensures a comprehensive approach to the governance, design, operation, measurement, and continuous improvement of AI solutions throughout their lifecycle.

Management of Non-Technical Risks

The monitoring approach recognizes that model drift is not limited to technical phenomena. Algorithmic bias and insufficient data representativeness can also degrade the quality, fairness, and reliability of AI outcomes over time. Accordingly, these non-technical risks are managed in coordination with the organization's fairness and bias assessment process, as an integral component of the continuous monitoring of every AI solution.



Regular assessments of deployed AI models for fairness/bias

Provider Responsibility for the AI Model

ISA's primary generative AI tool is Microsoft Copilot, whose underlying model is developed and maintained by Microsoft. As the model provider, Microsoft is primarily responsible for conducting fairness and bias assessments related to the model architecture, training data, and overall model behavior.

Microsoft documents and publishes these assessments in its annual Responsible AI Transparency Report, which includes gender and age bias testing, multilingual fairness evaluations, pre-deployment red teaming exercises, and methodologies aligned with internationally recognized AI risk measurement standards. As part of its governance process, ISA verifies that its principal AI providers maintain these mechanisms as part of the criteria for the selection, approval, and ongoing authorization of AI tools used within the organization.

The Microsoft platform fully addresses this requirement (how often and how fairness and bias are evaluated in production AI models) through three complementary layers of native capabilities supported by Microsoft's governance framework:

- **Fairness and bias assessment by subgroup** using the **Responsible AI Dashboard** in **Azure Machine Learning**, which integrates **Fairlearn** and provides an exportable **Responsible AI (RAI) Scorecard**. This enables the evaluation of fairness metrics across different demographic groups and supports the identification of potential bias in model outputs.
- **Continuous monitoring in production** through **Azure Machine Learning Model Monitoring**, which tracks model drift, performance degradation, and data quality over time, together with **Microsoft Foundry's continuous evaluation capabilities** for generative AI models and AI agents. These mechanisms enable ongoing monitoring throughout the operational lifecycle of AI solutions.
- **Governance and review cadence** in accordance with the **Microsoft Responsible AI Standard v2**, which requires the **AI Impact Assessment** to be reviewed at least annually and whenever a significant event or material change occurs. A **semiannual review cycle** for medium- and high-risk AI solutions exceeds Microsoft's minimum governance requirements and provides an additional level of assurance regarding fairness, bias, and overall model performance.

Regular assessments of deployed AI models for fairness/bias

- **ISA's Responsibility for AI Outputs and Context of Use**

Notwithstanding the provider's responsibility for the underlying model, ISA assumes responsibility for the outputs generated by AI tools and the context in which they are used.

Accordingly, the fairness and bias assessments conducted by ISA focus on the observable outputs produced by AI tools within its specific business processes, with particular attention to processes involving decisions or recommendations that may affect individuals, such as recruitment, supplier evaluation, or the generation of institutional communications.

These assessments seek to identify whether AI-generated outputs create inequitable or discriminatory patterns within ISA's specific operating context, regardless of the model's general behavior. Where evidence of systematic bias is identified in a particular process, ISA's response may include formally reporting the issue to the provider, restricting the use of the AI tool for that process, and, where necessary, suspending its use until corrective actions have been verified.

- **Bias Management by Design**

For internally developed AI solutions or solutions configured with a higher degree of customization, ISA addresses and mitigates bias at three levels:

- Bias associated with the datasets used;
- Bias arising from design and configuration decisions; and
- Bias inherent to the limitations of the underlying algorithms.

This bias management approach extends throughout the operational lifecycle of each solution through periodic assessments integrated with the organization's continuous monitoring mechanisms.

- **Prohibition on the Full Replacement of Human Judgment in High-Impact Decisions**

As an additional safeguard against the risk of perpetuating bias in critical decisions, **no AI solution may fully replace human judgment** in legal, financial, employment, disciplinary, operational, security, compliance, or human rights-related matters, unless expressly authorized by applicable regulations and supported by enhanced controls and effective human oversight.

This requirement ensures that any potential bias identified in an AI system cannot result in a significant decision without prior human review.

At present, ISA classifies all of its AI solutions as **augmented productivity tools**. These solutions operate solely as decision-support tools for specific tasks and do not possess autonomous decision-making authority.

In anticipation of the future adoption of AI agents with higher levels of autonomy, ISA has established a **defined governance process** that assigns and limits each agent's level of responsibility through the formal creation of its digital identity. This approach ensures traceability, oversight, and accountability as the scope and capabilities of AI agents evolve over time.

Initiatives (own/with suppliers) to lower the ecological footprint of AI data centers/models

ISA and its subsidiaries integrate **environmental sustainability criteria** throughout the lifecycle of AI solutions—from evaluation and selection to procurement, renewal, and operation—in a manner proportionate to the **risk level, scale, criticality, and computational intensity** of each AI use case.

- **Environmental Criteria in the Procurement and Renewal of AI Solutions**

During the procurement or renewal of internally developed or third-party AI solutions, ISA evaluates and documents, where applicable, the following criteria:

- The provider's verifiable commitments to **renewable energy, greenhouse gas emissions reduction, or energy efficiency**;
- Available information regarding the solution's **computational resource consumption, model efficiency, or infrastructure optimization practices**;
- Measures implemented to prevent **model over-sizing** or unnecessary computational workloads; and
- Selection criteria that favor **technically suitable alternatives with a lower environmental footprint**, where equivalent options are available.

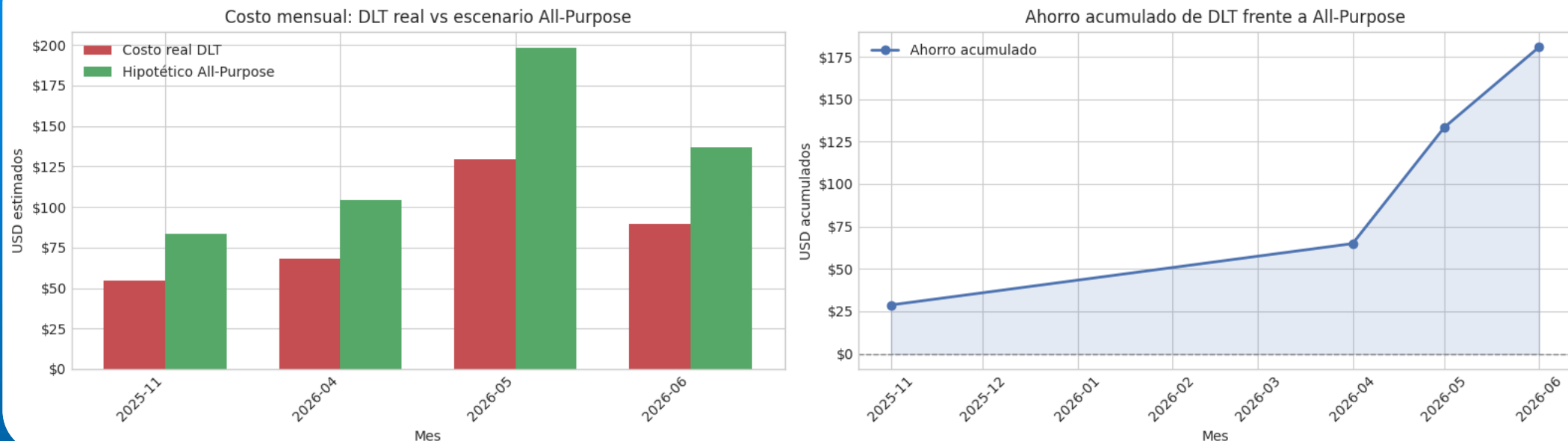
This approach ensures that environmental sustainability is an **explicit consideration in technology procurement decisions**, rather than a secondary or retrospective criterion.

- **Assessment of Computational Efficiency for Higher-Impact Use Cases**

For **medium- and high-risk AI use cases**, or those requiring significant computational resources, the solution assessment must include **documented evidence** of the evaluation of computational efficiency and environmental sustainability, together with the rationale for the selected approach. This requirement ensures that AI solutions with the greatest potential environmental impact are supported by a deliberate, transparent, and traceable assessment process.

Initiatives (own/with suppliers) to lower the ecological footprint of AI data centers/models

Impacto económico de DLT vs All-Purpose (precios referenciales Azure)



The Data, Analytics, and AI Center of Excellence (CoE) continuously reviews and improves its processes to drive ongoing optimization. As part of this approach, ISA has optimized the ingestion of information into its data lake to effectively reduce the environmental footprint associated with its operation.

The charts illustrate this reduction by comparing the actual operating cost of the Data Lake (DLT) with the estimated monthly cost that would have been incurred had the implemented remediation measures and optimization initiatives not been applied. These results demonstrate the effectiveness of ISA's continuous optimization efforts in reducing computational resource consumption and the associated environmental impact.

Initiatives (own/with suppliers) to lower the ecological footprint of AI data centers/models

- **Management of Limited Environmental Information from Providers**

Where sufficient information regarding a provider's environmental practices is not available, ISA formally documents this circumstance as part of the **risk assessment process** and considers it as a factor in procurement and renewal decisions. This approach ensures that a provider's lack of transparency does not go unnoticed and is explicitly incorporated into the AI solution's risk management process.

- **Primary AI Provider: Microsoft**

For **Microsoft Copilot**, ISA's primary generative AI solution, Microsoft has publicly disclosed and verifiable environmental sustainability commitments, including the use of **100% renewable energy** for its operations and its commitment to become **carbon negative by 2030**, as documented in its annual **Sustainability Report**.

These commitments are consistent with ISA's environmental evaluation criteria and support the continued use of Microsoft Copilot from an environmental sustainability perspective.

Appeals process for users/affected third parties to contest an AI decision or outcome

ISA and its subsidiaries have established a **formal mechanism** that enables employees, customers, suppliers, and other potentially affected stakeholders to request a review of materially significant decisions or outcomes generated or supported by AI systems.

- **Minimum Components of the Appeals Process**

The appeals mechanism includes the following elements:

- **Accessible reporting channel:** Any individual affected by a decision supported by AI may request a review through the **Ethics Hotline**.
- **Defined response timelines:** Each request is subject to established response deadlines to ensure the process is timely and effective.
- **Human review responsibility:** Every appeal is assigned to a representative from the **Compliance function**, working jointly with the individual responsible for the **AI Adoption Strategy**, to review and, where appropriate, reverse or modify the challenged decision. **Meaningful human review** is a mandatory and non-negotiable component of the process.
- **Case assessment:** Each review is conducted based on the available information regarding the challenged decision, the AI system that supported it, and the specific circumstances of the case.
- **Case governance and escalation:** All requests and reports submitted through the **Ethics Hotline** are reviewed and discussed by the appropriate committee as part of the organization's governance process. Following this review, each case is assigned to the competent business function for resolution. Where required by the nature of the matter, the case may also be referred to the relevant competent authorities in accordance with applicable legal and regulatory requirements.
- **Documentation of outcomes:** The outcome of each appeal, together with any corrective actions taken, is formally documented to ensure traceability and support organizational learning.

- **Alignment with Corporate Integrity Standards**

The appeals process is aligned with the principles of **integrity and professional ethics** established in the **ISA Code of Ethics and Conduct**. All personnel involved in the development, implementation, management, or use of AI solutions are responsible for reporting instances of non-compliance and acting in accordance with these standards, thereby reinforcing a culture of accountability for the responsible use of AI across the organization.

During **2025**, **no ethics reports related to AI** were submitted through the Ethics Hotline.

Quantification of the impact of AI initiatives/tools on sustainability outcomes

- **Value Assessment as a Pre-Deployment Requirement**

Before any AI solution is deployed into production, it must undergo a **value assessment** that quantifies the expected costs and operational efficiencies generated for the organization. This assessment forms part of the minimum approval requirements for every AI initiative, together with the definition of the use case, risk assessment, cybersecurity evaluation, and monitoring plan.

This approach ensures that the expected value and impact of each AI solution are documented at the approval stage, establishing a **baseline** against which actual operational performance can subsequently be measured.

- **Continuous Monitoring as the Primary Source of Impact Data**

The monitoring and periodic review plan required for every AI solution in operation systematically generates data on the solution's **performance, utilization, and operational efficiencies**. This information serves as the primary source for measuring the actual impact of AI initiatives on business processes and, consequently, on the organization's sustainability performance.

Data collected through the monitoring process are consolidated annually and incorporated into ISA's **sustainability information management system** for reporting purposes.

- **Sustainability Impact Indicators**

ISA measures the impact of its AI initiatives and tools through a set of **key performance indicators (KPIs)** organized across the organization's sustainability dimensions.

The **first year of measurement** establishes the baseline against which future performance will be assessed, while **performance targets are defined beginning in the second year** of measurement.

Quantification of the impact of AI initiatives/tools on sustainability outcomes

Social dimension

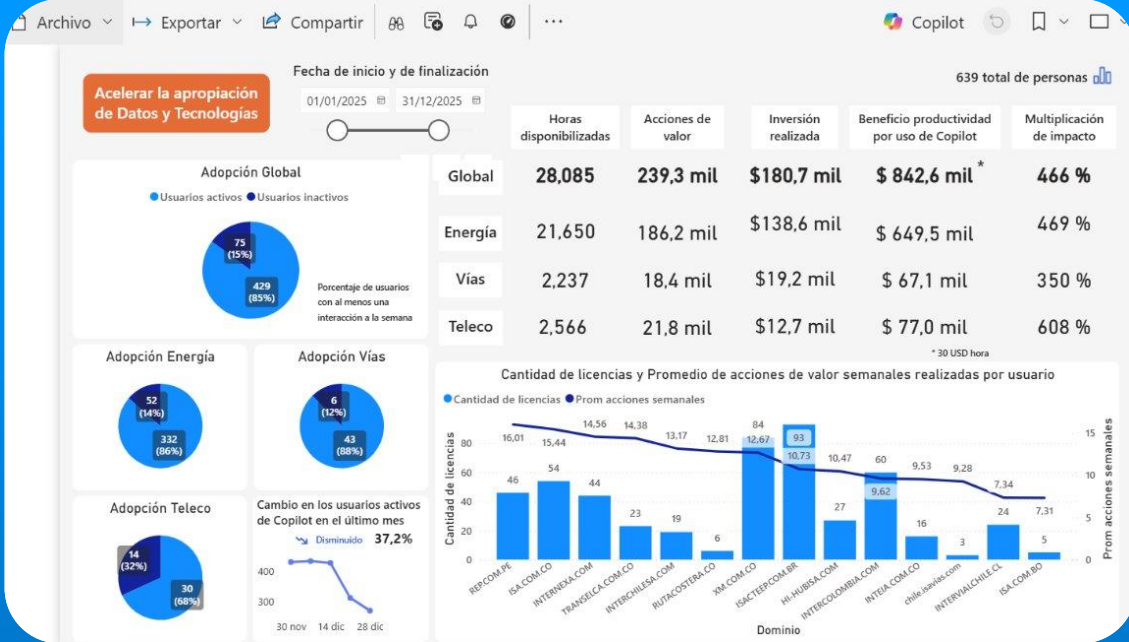
Indicator	Definition	Unidad	Source
Hours Enabled by AI	Number of working hours redirected from repetitive tasks to higher-value activities through the use of AI tools.	Hours/year 45,452	IT
Active AI Tool Users	Number of employees actively using at least one organization-approved AI tool.	People 1497	IT / Active licenses
Employees Trained in the Ethical and Safe Use of AI	Number and percentage of employees who completed the organization's mandatory AI training during the reporting year.	30 %	Human Resources

Environmental dimension

Indicator	Definition	Unidad	Source
AI Providers with Verifiable Environmental Commitments	Number of AI providers with publicly verifiable commitments related to the use of renewable energy, carbon neutrality, or equivalent environmental sustainability objectives.	6	IT

Governance dimension

Indicator	Definition	Unidad	Source
AI Tools with Active Documented Monitoring	Number of AI tools included in the corporate AI inventory that have a current and documented monitoring plan in place.	3	IT
Appeals of AI-Supported Decisions	Number of appeals received regarding AI-supported decisions, number resolved, and the average time required for resolution.	0	Risk and Compliance

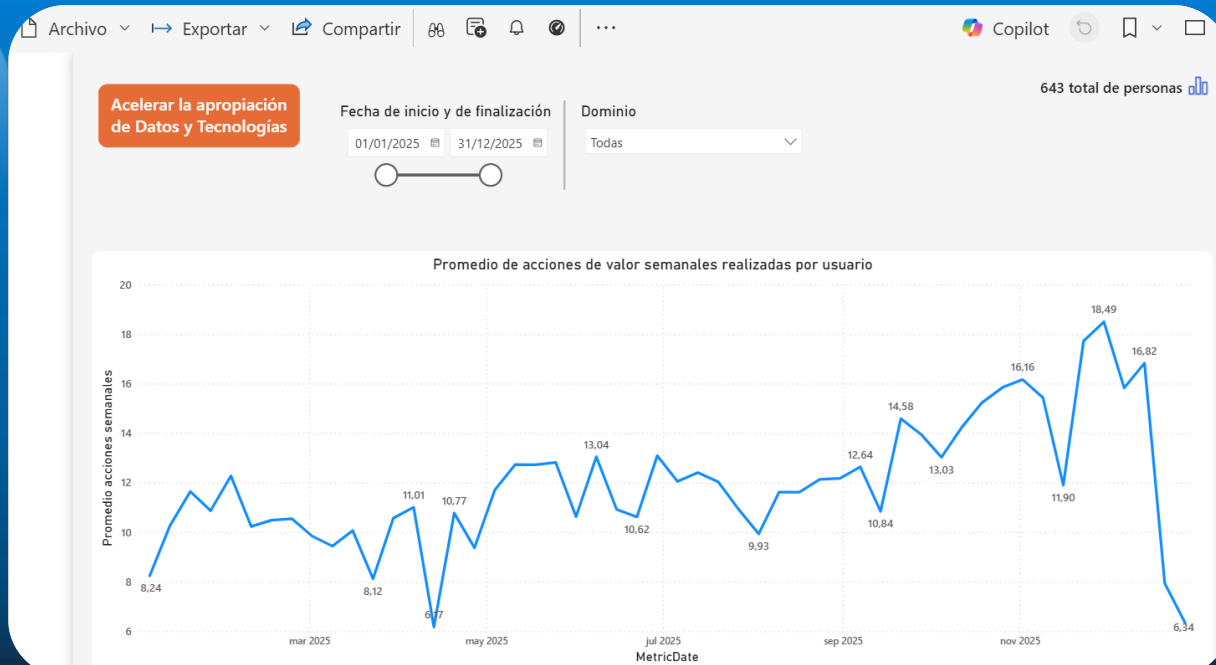


Overall Results

The implementation of AI tools has generated **28,085 hours** of work redirected from repetitive tasks, delivering an estimated **productivity benefit of USD 842.6 thousand** compared with an investment of **USD 180.7 thousand**, representing an overall **466% return on investment (impact multiplier)**.

Results by Business Unit

- Energy** generated the greatest absolute impact, with **21,650 hours** redirected and an estimated productivity benefit of **USD 649.5 thousand**, consistent with its higher adoption rate, representing **52% of active AI users**.
- Telecommunications** achieved the **highest relative return**, with an **impact multiplier of 608%**, despite having the **lowest adoption rate (14%)**. This indicates that, while adoption remains limited, employees who use AI tools are realizing substantial productivity gains.
- Road Infrastructure** recorded the **lowest impact multiplier (350%)**, with a moderate adoption rate of **32%**.



Training of employees on the ethical use and/or security of AI

Development program	Benefits for the business	Quantitative impacts	% of employees (FTE)
Cutting-edge skills: Building key capacities in line with the ISA2040 Strategy, focusing on infrastructure, digital literacy, adaptability, and O&M. Campus ISA: A central hub that links learning to strategic results, promoting self development through a flexible, accessible virtual environment. Performance and development: Integrating training, leadership support, and applied learning to the role, fostering shared responsibility in talent development.	- Digitization: AI and automation optimized processes, freeing up man-hours and generating efficiencies. - Performance: Data-driven decisions strengthened agility, accuracy, and operational excellence. - Culture and innovation: A regional leader in digital learning (LinkedIn Power User Award) with an 84% adoption rate at Campus ISA.	- Educational performance: High coverage (96%), over 425,000 hours of training. - Adoption and efficiency: Expansion of the offering (+23%), high usage of Campus ISA (84%), freeing up more than 33,000 man-hours using AI (≈ USD 1 M). - Strategy: Development of 28 key skills aligned with transformational projects and the ISA2040 Strategy. - Alignment with strategic projects: Training initiatives connected with key business projects. - Norte Project: Transformation of the transmission business in Colombia. - Hub Digital: Boosting efficiency and innovation through digital literacy and the use of AI. - Nova Project: Development of energy solutions in Colombia and Chile.	1,497 employees completed their training program in cutting-edge skills.

-  Programs in relation to other schools
-  Investment
-  Training hours
-  Training hour %
-  Level of satisfaction

Digital and Innovation School **32%**

Contribution to the development of digital and innovation skills, application of technologies, and digitization of processes.

 **USD 202,394**
6% investment in relation to the other schools.

 **45,452**
 **4.75/5**

 **11%**

Environmental Management and Policy

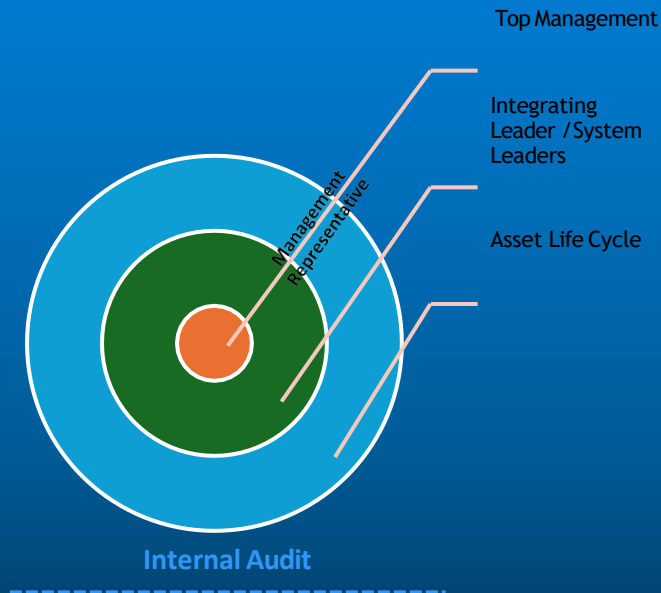
isa
CONEXIONES QUE INSPIRAN



Accountability for policy implementation

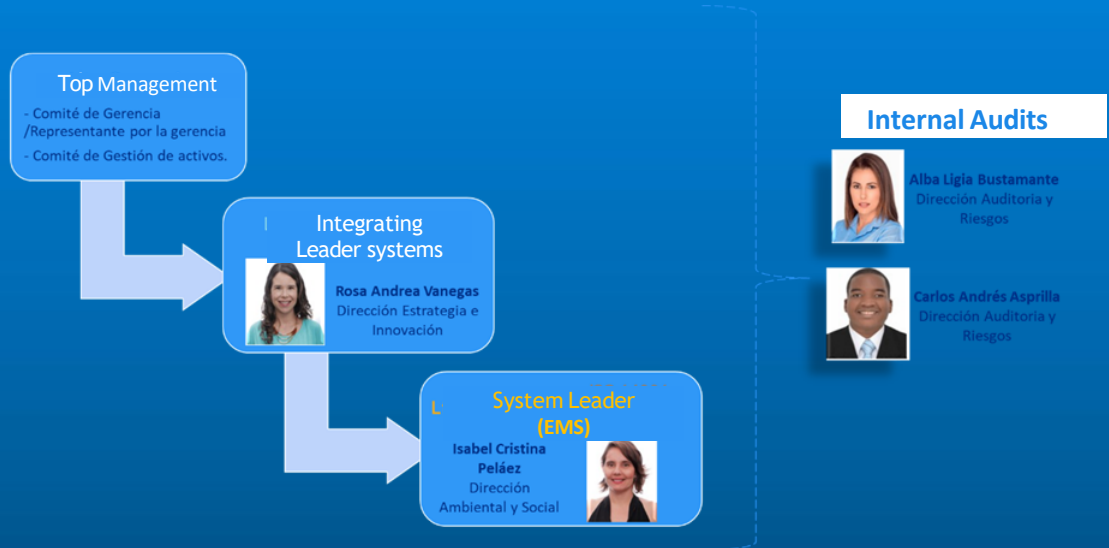
The Group's Environmental Policy establishes that specific responsibilities for applying the defined guidelines must be clearly outlined within each company's Environmental Management System (EMS). As an integral part of the EMS, the policy supports its effective implementation and compliance.

Roles within the Integrated Management System – Environmental Management System (EMS)



Accordingly, each company defines clear roles and responsibilities aimed at both implementing and continuously improving the EMS, while ensuring alignment with the principles of the Environmental Policy.

For example, ISA INTERCOLOMBIA defines these roles and responsibilities through its Integrated Management System, appointing an EMS Leader and detailing how each leader contributes to the system's operation, as illustrated below.



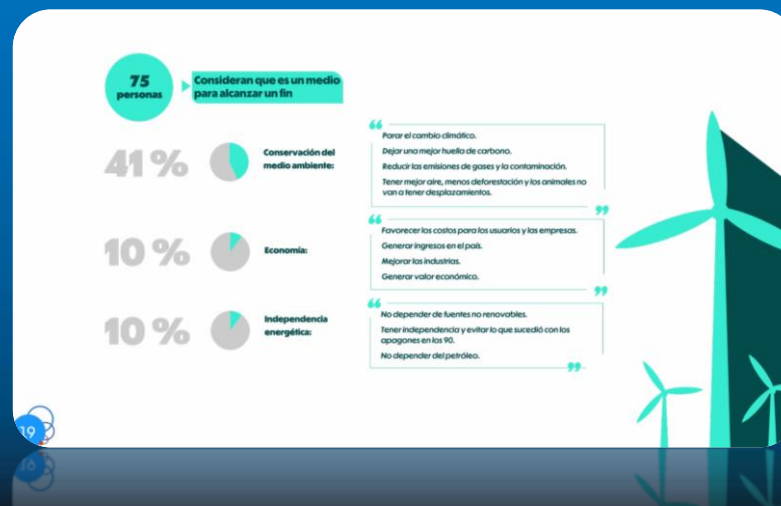
Consulting external stakeholders in the development or implementation of the environmental policy

The Dialogues are an invaluable space to share, build and project a common future. That is why at ISA we have used them as an opportunity to present how we take on the challenge of the energy transition, positioning ourselves as a company that drives transformative connections and works to mitigate the effects of climate change, aligning the expectations of our different stakeholder groups. Our strategic evolution recognizes the differentiated role we have as an agent of change in the sustainable development of the region.

These spaces have allowed us to gather the viewpoints of the stakeholder groups in order to integrate them into the commitments we have included in the Environmental Policy. Below we present some of the results of the spaces developed in 2023 that subsequently contributed to the construction of the environmental policy in 2023.

ISA research together with EAFIT University “We have to talk about energy transition”:

- 75 people considered that the energy transition is regarded as a means to achieve an end.
- Ends such as the conservation of the environment, the management of climate change, a better carbon footprint, reducing pollution, having less deforestation and displacement of animals.



To see more detailed information you can visit the following link:
Dialogues with stakeholders - ISA

Consulting external stakeholders in the development or implementation of the environmental policy

- Topics addressed in dialogue tables with stakeholder groups:
 - Stakeholder groups as drivers of the energy transition.
 - Multidimensional education for the transition.
 - Decarbonization of thinking.
 - Economic and productive transition.
 - Promotion of human roads in a sustainable manner.
 - Use of materials with lower environmental impacts and that use circular economy practices.
 - Strengthening alliances with strategic actors to promote knowledge and innovation.
 - Self-generation of energy on ISA's roads.
 - Empowerment of communities and suppliers.



Diálogos con grupos de interés

TRANSICIÓN ENERGÉTICA

RETO: ¿Cómo podríamos transformar juntos el negocio de vías de ISA en un referente global en la transición energética?

Descripción y propuesta de valor: Impulse vías humanas de manera sostenible, aumentando la eficiencia en su trazado y construcción, usando materiales que generan menores impactos ambientales y que usan prácticas de economía circular. Vías humanas que se articulan con el entorno para dinamizar su uso y apropiación social.

Población foco: Constructores Comunidad Proveedores de materiales de construcción Usuarios	Claves de éxito: Medición de la disminución de las emisiones Mayores incentivos Regulación favorable
Problema a resolver: Impactos ambientales (Contaminación y emisión de CO2) Inclusión social	Barreras / obstáculos: Regulación Falta de incentivos Falta de compromiso Desconocimiento de los grupos de interés



CONEXIONES QUE INSPIRAN



Diálogos con grupos de interés

TRANSICIÓN ENERGÉTICA

RETO: ¿Cómo podríamos lograr juntos que los grupos de interés se conviertan en movilizadores activos de la transición energética?

Descripción y propuesta de valor:
Educación multidimensional para la transición

Población foco: Grupos de interés Comunidades vulnerables Proveedores Trabajadores Infancia	Claves de éxito: Aprender de las diferentes cosmovisiones Suma de voluntades Diálogo multiactor Tener claro el para qué Mostrar el beneficio final
Problema a resolver: Descarbonizar el pensamiento Transición económica y productiva Diferencias en el conocimiento desde los territorios y de la cadena de la energía Aceptar las diferencias y necesidad de aprender	Barreras / obstáculos Diferencias culturales y sociales Acceso a tecnología Acceso a información amplia Necesidades básicas no satisfechas



CONEXIONES QUE INSPIRAN



Diálogos con grupos de interés

TRANSICIÓN ENERGÉTICA

RETO: ¿Cómo podríamos transformar juntos el negocio de vías de ISA en un referente global en la transición energética?

Descripción y propuesta de valor: "ISA referente en consumo eficiente vial"
Potencializar alianzas y co-crear con todos los actores estrategias que impulsen el conocimiento e innovación para promover el consumo eficiente de energía en la construcción, operación, mantenimiento y uso de las vías.

Población foco: Usuarios de las vías, proveedores, reguladores. (Grupos de Interés de ISA)	Claves de éxito: Paso libre, eficiente y seguro (cobro de peaje sin barrera) por las vías de ISA Resultados positivos en las mediciones de huella de carbono en las vías de ISA Uso eficiente de materiales para la construcción Autogeneración en las vías de ISA (paneles solares) Barreras / obstáculos ISA con capacidad de influencia en los actores regulatorios de los países en donde tiene presencia. Empoderar a los proveedores para optimizar los procesos.
Problema a resolver: Consumo eficiente de energía en las vías	



CONEXIONES QUE INSPIRAN

Consulting external stakeholders in the development or implementation of the environmental policy

Likewise, at ISA we have developed different initiatives so that our Stakeholders implement the commitments defined in our Environmental Policy. Below we present one of those examples called “Just Decarbonization in the supply chain” – Integrating sustainability, competitiveness and equity (Success case of ISA Energía Colombia)

A multi-level mandate for corporate climate action



Global sphere: multilateral agreements

The United Nations Framework Convention on Climate Change, Kyoto Protocol (1997) and Paris Agreement (2015). Binding 2 °C limit and ILO just transition guidelines.



National sphere: regulation and Country goals
Colombian carbon neutrality strategy (2020) and 2050 strategy. Transition toward a resilient economy.



Cross-cutting sphere: global frameworks and standards
Greenhouse Gas Protocol (GHG Protocol), SBTi, CDP, TCFD, IFRS S2, NET ZERO.

Strategy architecture: 4 axes of systemic intervention

Hybrid measurement

Adaptive application of the GHG Protocol according to the maturity of the supplier's data.

Maturity model

Evolutionary classification of suppliers to customize goals and requirements.

Green clauses

Innovation in procurement through contracts that incentivize footprint reduction.

Support ecosystem

Training, circular economy, strategic alliances to facilitate advancement.

Hybrid measurement matrix (GHG Protocol - Scope 3) success case ISA Energía Colombia

Progressive migration toward greater data precision.

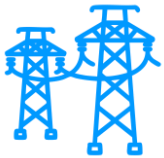
	Level 1 (Baseline estimation)	Level 2 (Supplier - Specific)	Level 3 (Service footprint)
 Mechanisms	Calculation by annual corporate spending.	Supplier's corporate GHG inventory adjusted to the contract value.	Direct and exclusive measurement of the carbon footprint of the service/product.
 Data	Sectoral emission factors (EPA, 2022).	Primary supplier data (accelerated through partnerships with CAIA and BONO).	Verified certifications and precise telemetry.
 Precision	Low / reference.	Medium / high.	Exact.

Strategic focus: criticality mapping in procurement

ISA Energía Colombia success case

The prioritization cross-referenced commercial volume, operational relevance, and emission factors (EPA), identifying the hotspots that concentrate the greatest climate impact.

Higher criticality



Construction of lines and substations.



Transport of heavy and oversized loads.



Maintenance of transmission lines.



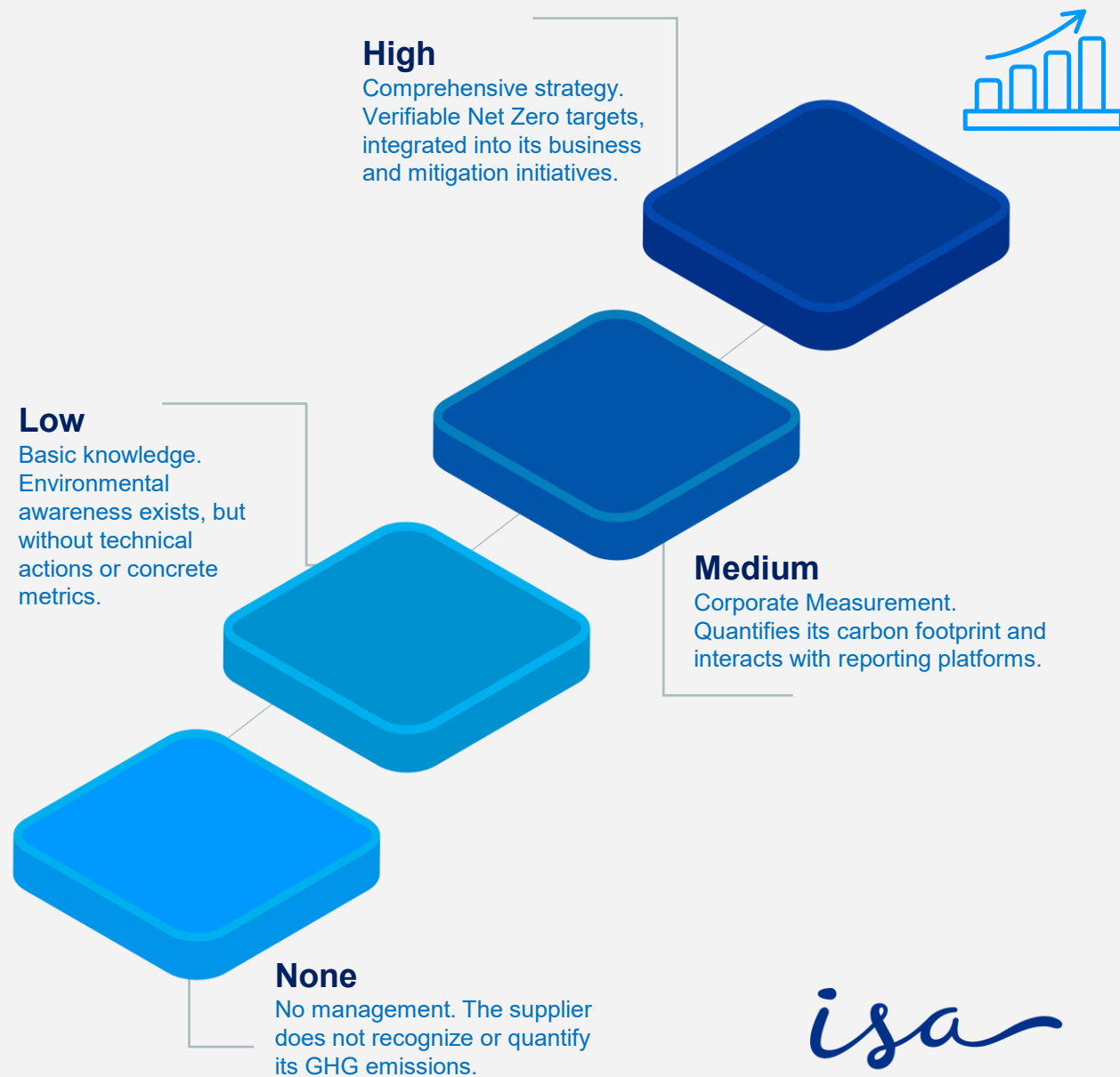
Acquisition of capital goods.

Lower criticality

The supplier's climate maturity ladder ISA Energía Colombia success story

Initial diagnosis

Most critical suppliers started at early levels, validating the need for a model based on proportionality and technical assistance rather than punishment.

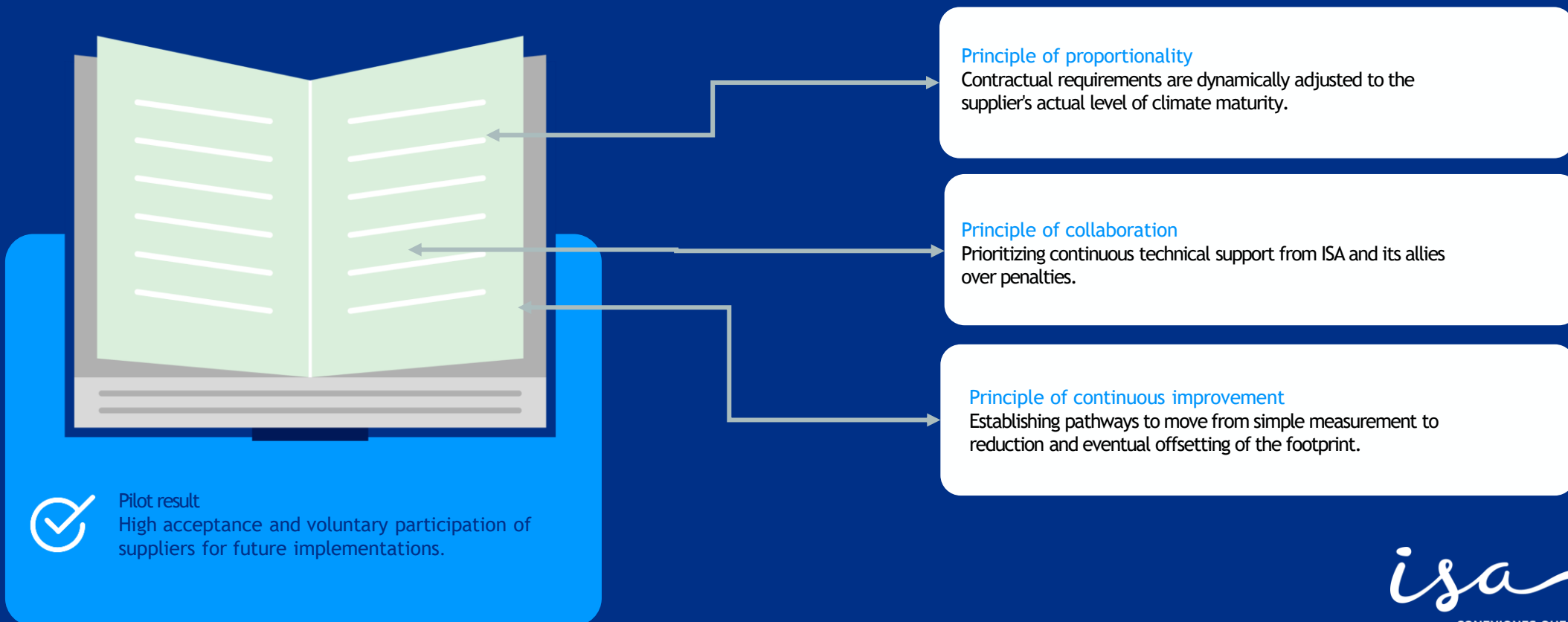




Innovation in procurement: the anatomy of green clauses

ISA Energía Colombia success case

Incorporation of GHG measurement, reporting and reduction obligations into contracting processes (pilots in dam and oversized cargo transport, and transmission line maintenance).





Knowledge transfer

Participatory workshops on methodologies.

Personalized advisory services integrating expert allies (CAIA and BONO) to facilitate the technological leap from level 1 to 2.

Learning communities and best-practice networking.

Circular economy in operations

Low-carbon design: nature-based solutions for substations.



Logistics optimization of heavy cargo transport.



Circular management on site: prioritizing reuse and recycling of materials.

ISA Energía Colombia success story



531

commercial contracts
analyzed.



162

purchasing
subcategories
evaluated.



45 %

of the Organization's
total annual spending.



51% of total emissions are concentrated in the top 4 categories: civil works, metal structures, line maintenance, and substation assembly.

isa

CONEXIONES QUE INSPIRAN

From diagnosis to mitigation: the direct impact ISA Energía Colombia success story

Phase 1 - Strategic ESG
assessment

**81 critical suppliers
comprehensively
assessed
(17% with
outstanding level
>80%).**

Phase 2 - Specific
measurement

**9 suppliers
measured directly
on the technology
platform.**

Phase 3 -
Decarbonization
roadmaps

**6 suppliers with
climate action plans
formulated
and roadmaps in
execution.**

19,391

tons of CO₂e
identified as direct
reduction potential
through these
roadmaps.



Inclusion of climate criteria in contracting processes

Pilot of "Green Clause" in three processes (transport and maintenance) to integrate climate commitments and strengthen co-responsibility. Feasibility was assessed and high supplier acceptance was achieved, better environmental traceability, and foundations for its progressive incorporation into future contracts, driving innovation and transparency.

Recognition of excellence: shared responsibility in action

ISA Energía Colombia success story



Energy efficiency
projects applied to
operational contracts



Circular
management of
materials

Category:
Supplier
connected with
the environment



Carbon footprint
measurement



Application of
nature-based
solutions

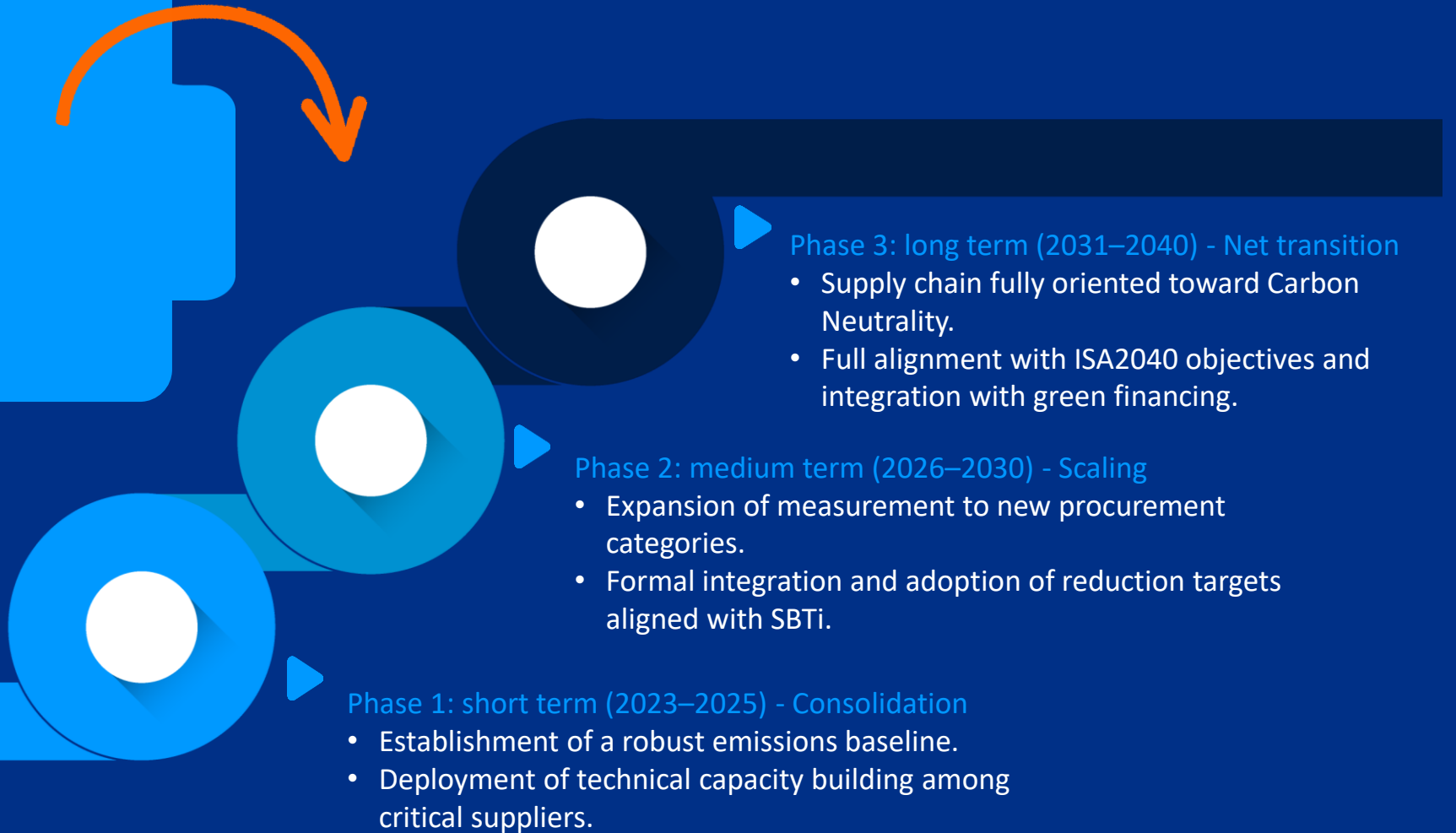


Recognition transforms climate efforts into a reputational and competitive asset
for SMEs within the electricity sector.

isa
CONEXIONES QUE INSPIRAN

The climate roadmap (2023 - 2040)

ISA Energía Colombia success case





CONEXIONES QUE INSPIRAN

Environmental Policy endorsement

Board of Directors Meeting No. 894 – May 2023

The Environmental Policy for ISA and its affiliates was presented for approval by the Board of Directors. The purpose of the presentation was to review and approve updates to the Environmental Policy, aiming to align it with ESG standards and stakeholder expectations.

The proposed changes were justified by the need to strengthen the organization's environmental governance framework, respond to evolving regulatory and market demands, and reinforce ISA's commitment to sustainable development. Updating the policy ensures consistency with international best practices and enhances the company's ability to manage environmental risks and opportunities across its operations

6. MODIFICACIÓN DE LA POLÍTICA AMBIENTAL

Presentó Juliana Suso.

La Administración expresó que los cambios propuestos a la Política Ambiental de ISA se requieren para diligenciar el índice de sostenibilidad de Dow Jones de Standard & Poor's. En la práctica, la compañía está cumpliendo con los estándares que se proponen incluir, pero hay que dejarlos explícitos en la política. En conclusión, se busca formalizar lo que se viene haciendo, incluyendo ajustes como la declaración del impacto neto positivo y hacer extensiva a los contratistas y demás aliados del negocio el cumplimiento de la política, incluyendo formación y entrenamiento.

Por lo anterior, se solicitó a la Junta Directiva, por recomendación del Comité de GSTI, aprobar las modificaciones a la Política Ambiental para cumplir con los nuevos lineamientos solicitados por los estándares de reportes internacionales.

9

Acta 894_24 de mayo de 2023

estratégicos de ISA y sus empresas, durante la última semana de junio y la primera de julio de 2023.

12. PENDIENTES JUNTA DIRECTIVA

Se presentaron los asuntos pendientes de la Junta Directiva.

13. RETROALIMENTACIÓN DE LA SESIÓN

No se presentaron comentarios en este punto.

Próxima Junta Directiva: Según la programación aprobada, la secretaria recordó que el 23 de junio de 2023 se realizará la siguiente sesión de Junta.

Siendo la 1:00 p. m. se dio por terminada la sesión.

PRESIDENTE

SANTIAGO MONTENEGRO T.

SECRETARIA

SÓNIA M. ABUCHAR A.

The Environmental Policy is available at: [Politica-Ambiental-ingles.docx.pdf](#)

Environmental Management Systems Verification

Company	% EMS certification	% Third party certification	% Internal certification
ISA	NA		
XM	100	0	0
ISA Intercolombia	100	0	0
ISA ENERGÍA in PERÚ	100	0	0
ISA ENERGÍA in BRAZIL	63	37	0
ISA ENERGÍA in Chile	0	100	0
ISA Transelca	100	0	0
ISA BOLIVIA	100	0	0
ISA VÍAS in Chile	100	0	0
Ruta Costera	0	0	100
Ruta del Este	100	0	0
INTERNEXA	0	0	0
INTEIA	100	0	0
TOTAL	82,53	16,87	0,60
TOTAL COVERAGE %	100,00		
Percentages associated with the number of operations covered in different audit or verification spaces			

Disclaimer: ISA are dedicated to administrative & management tasks & do not generate significant impacts, for this reason we were decided that they did not need ISO 14000 certification for their processes.

Environmental Violations

	2022	2023	2024	2025
Number of violations of legal obligations/ regulations	0	5	2	6
Amount of fines/ penalties related to the above. (COP)	0	784,090,556	309,868,826	1,032,794,992
Environmental liability accrued at year-end. (COP)	622,216,790	1,002,552,642*	1,376,788,384*	822,219,450
*The values reported as environmental liabilities correspond to internal estimates of ISA, as the environmental authorities have not yet ruled on the value of the possible violations				

Labor practices

Discrimination & Harassment

Code of Ethics and Conduct

Explicit statement prohibiting harassment:

ISA ensures a workplace free from violence, sexual and workplace harassment, and labor rights violations (p. 14). “We strongly reject these behaviors that undermine human rights, affecting people’s well-being, safety, dignity, and integrity.”

Commitment to human rights:

(pp. 16–17)

“At ISA and its companies, we are aware of, respect, and actively promote human rights.”

Defined escalation and reporting mechanisms for incidents:

(p. 22 – “You are part of the solution”) Employees are encouraged to speak up through established channels, including the Ethics Line:

Web: <https://www.isa.co/en/isa-group/ethics-line/>

Toll-free: 01 8000 94 13 41

Email: lineaetica@isa.com.co

See also: Ethical Management Procedure.

Link: <https://www.isa.co/en/code-of-ethics-and-conduct/>



Supplementary Information 2025

See the Excel file, section: Attractive and Desirable Employer, indicator: Cases of discrimination and corrective actions taken / Cases of workplace harassment and corrective actions taken.

Link: <https://isa.co/wp-content/uploads/2026/07/consolidated-attachments-gri.xlsx>

Workforce Breakdown: Gender

Diversity Indicator	Percentage (0 – 100 %)	Public Target
Share of women in total workforce (as % of total workforce)	29%	35% Target year: 2030
Share of women in all management positions, including junior, middle and top management (as % of total management positions)	36%	35% Target year: 2030
Share of women in junior management positions, i.e. first level of management (as % of total junior management positions)	31%	There is no defined target; however, the company has a gender parity policy in place for these positions

Workforce Breakdown: Gender

Diversity Indicator	Percentage (0 – 100 %)	Public Target
Share of women in top management positions, i.e. maximum two levels away from the CEO or comparable positions (as % of total top management positions)	42%	There is no defined target; however, the company has a gender parity policy in place for these positions
Share of women in management positions in revenue-generating functions (e.g. sales) as % of all such managers (i.e. excluding support functions such as HR, IT, Legal, etc.)	71%	
Share of women in STEM-related positions (as % of total STEM positions)	15%	25 % Target year: 2030

Definition of Positions – Share of Women in Management Roles in Revenue-Generating Functions

The definitions for positions included under the indicator “Share of women in management positions in revenue- generating functions” are based on the role itself, with the objective of selecting the most qualified professional for the position, regardless of gender. However, the organization actively seeks to promote gender balance at the executive level, in alignment with its diversity and inclusion policy.

Achievement of Target – Share of Women in All Management positions

The target associated with the share of women in all management positions, including junior, middle, and top management was achieved and exceeded during this reporting period. This outcome is the result of the company’s leadership development plan, which maps key management roles to be filled by internal talent. In several cases, these roles have been occupied by participants of the leadership and mentoring program led by women in executive positions. This initiative has contributed significantly to increasing the number of management positions held by women.

Workforce Breakdown: Gender



STEM Positions Indicator Adjustment

The number of positions in STEM roles shows a variation compared to previous years due to an adjustment in the measurement methodology to ensure greater accuracy. This indicator is now calculated using the total number of individuals occupying STEM positions as the denominator, rather than the total number of women, as was done in previous years. This figure was restated in the management report (Supplementary Information).

STEM by 2025	ISA	ISA INTERCOLOMBIA	ISA TRANSELCA	ISA BOLIVIA	ISA REP	RUTA COSTERA
Total STEM positions	123	278	129	1	329	0
Number of women in STEM careers	34	59	15	0	38	0
% of women in STEM careers (science, technology, engineering, and mathematics professionals)	28%	21%	12%	0%	12%	0%

Supplementary Information 2025

See the Excel file, section: Attractive and Desirable Employer, indicator: [GRI 2-7a] Size of the Organization

Link: <https://isa.co/wp-content/uploads/2026/07/consolidated-attachments-gri.xlsx>

STEM by 2025	ISA INTERCHILE	ISA CTEEP	XM	INTEIA	INTERNEXA	ISA INTERVIAL	RUTA D. ESTE	Total
Total STEM positions	38	1153	307	30	241	37	0	2666
Number of women in STEM careers	9	100	86	11	49	11	0	412
% of women in STEM careers (science, technology, engineering, and mathematics professionals)	24%	9%	28%	37%	20%	30%	0%	15%

Workforce Breakdown: Race/ Ethnicity & Nationality

In line with ISA's diversity and inclusion policy, the company and its affiliates employ individuals from a variety of national backgrounds, not limited to the countries where the companies are originally based. This commitment reflects our belief in the value of diverse perspectives and the importance of creating inclusive opportunities, including for migrant talent.

Supplementary Information 2025

See the Excel file, section: Attractive and Desirable Employer, indicator: Nationality

Link: <https://isa.co/wp-content/uploads/2026/07/consolidated-attachments-gri.xlsx>

Breakdown based on nationality	Share in total workforce (as % of total workforce)	Share in all management positions, including junior, middle and senior management (as % of total management workforce)
Colombians	47.7	5.81
Brazilian	31.8	2.97
Peruvians	10.1	5.02
Chileans	7.5	10.91
Bolivians	0.6	9.4
Others	2.3	3.7



Gender Pay Indicators

Employee Level	Average Women Salary	Average Men Salary
Executive level (base salary only)	44.994.000	52.405.000
Executive level (base salary + other cash incentives)	53.702.244	59.302.212
Management level (base salary only)	28.662.000	29.784.000
Management level (base salary + other cash incentives)	32.593.000	33.786.000
Non-management level (base salary only)	9.890.000	10.105.000

Currency: COP Colombian Peso

Trade union and collective bargaining coverage

21
Trade union
organizations
in ISA and its
companies

2
Collective
Pacts in ISA
and its
companies

Unionized
workers

1.370

26.2% of ISA and its
companies'
workforce

472

Workers affiliated to
Collective Pacts

9.0% of ISA and its
companies'
workforce

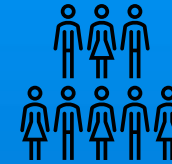
Workers benefited by extension of
Collective Bargaining Agreements

1.490

28.5% of ISA and its
companies'
workforce.

22

Collective Agreements in
ISA and its companies



5,2321
Total number of workers of ISA
and its companies



Country	Trade union organizations	Members	Beneficiaries by extension
Colombia	5	679 ²	218 ³
Peru	2	143	-
Chile	4	198	-
Brazil	11	350 ⁴	1.272

1. The total workforce includes apprentices and interns of ISA and its companies (152)
2. In Colombia, those affiliated to a union are those who have the union fee deducted, which corresponds to a monthly amount.
3. Beneficiaries by extension in Colombia are those who benefit from the collective agreement because when more than one third of a company's workers are affiliated to a union, the benefits of the agreement are extended to the other workers even if they are not affiliated. (Art. 471 of the Substantive Labor Code) (Applies to Transelca and Intercolombia)
4. In Brazil, although the majority of workers benefit from the collective agreements entered into with the regional unions, only 350 of them have an effective affiliation to the unions.

Human Capital Management



isa

CONEXIONES QUE INSPIRAN



Leadership development program



Cultural education program



Transition program for retiring



Digital transition program



Teams and networks



Contractors' trainings

Employee Development Programs

Mentorship

The Campus ISA Leadership School strengthens the pillars of the essence of the ISA leader: Connect with purpose, team development, and mobilizing strategy, through high-quality programs, built with leading national and international partners.

We complement the training with individual mentoring to accompany our leaders in real challenges, accelerate their development, and consolidate a leadership style that inspires, cares for people, and turns strategy into results.

Quantitative impact of our program:

- Leadership style: 81% positive opinion in the results of the Great Place to Work workplace environment index.
- ISA and companies leadership index: 77 points, equivalent to an outstanding result.



**100% Presidency
Committee**

**We impacted more than
20 top-level leaders**

Duration: 9 months

PAD programa de autodesarrollo

The PAD Self-Development Program provided employees with development opportunities through workshops, mentoring, and a virtual learning platform. The program focused on building critical soft skills and leadership capabilities in three key areas: Conversation as a Tool for Transformation, High-Impact Communication, and Collaboration and Teamwork. These initiatives supported continuous learning, employee development, and the strengthening of a collaborative organizational culture.



Leadership in action: Leadership development program aimed at strengthening capabilities to mobilize decisions and results aligned with the organizational strategy, through applied learning experiences.

Structured in three modules that refer to the 3 pillars of the Essence of the leader:

Develops the ability to build bonds of trust through empathy, integration and authentic communication, strengthening the connection between people and teams to give meaning and purpose to action.

Connect
with
Purpose

Develop
Potential

Boosts the development of capabilities, commitment and contribution through learning, performance and teaching, enabling leaders to strengthen talent and respond to changing environments.

Drive the
Strategy.

Focused on turning ideas into action through decision-making, inspiration and building the future, aligning teams with the strategy and generating sustainable results.

3 sessions (one for each pillar)

We impact more than 300 leaders

Methodology

The program is developed under an experiential and participatory approach, based on transformative conversations, peer learning, applied coaching and action commitments to ensure transfer to the role.

Cultural education program

Learning methods: Coaching or Mentorship

1. Corporate course (Virtual) on Human Wealth



More than 1,400 participants

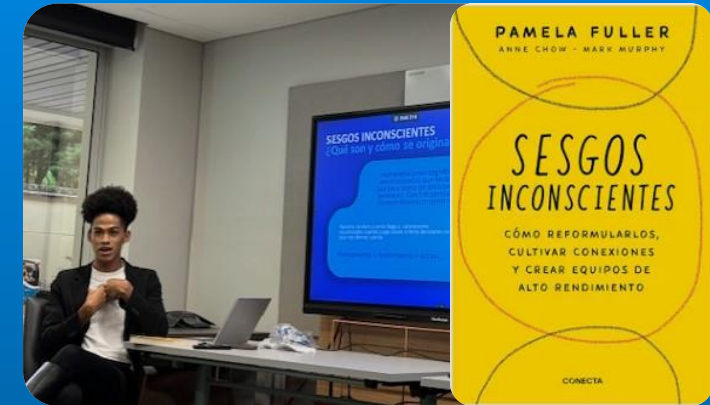
2. A training path with webinars and workshops (virtual and synchronous in-person) on topics such as:

- Basic concepts of Human Wealth
- Ethnic approach
- Reconciliation and inclusive social dialogue
- Life cycle and youth
- Co-responsible masculinities
- Female leadership
- Inclusive communication

More than 900 participations

3. Reading club

Book: Unconscious Biases



More than 25 participants –
Focus: Talent Vice Presidency

Impact: Adoption of inclusive organizational practices evidenced in the integration of diversity, equity, and inclusion criteria into communications, culture, and talent cycle processes. This approach has been recognized externally, highlighting ISA at the Construimos a la Par 2025 Awards in the Companies for Diversity and Inclusion category, for its Human Wealth initiative.

Digital transition program

Learning methods: Coaching or Mentorship

Strategic initiative aimed at strengthening digital capabilities in the organization, enabling the adoption of new technologies, the use of data, and process automation as support for the ISA 2040 strategy.

The program combines training, immersive experiences, and the development of digital products, promoting skills in analytics, artificial intelligence, cybersecurity, and digital tools applied to business.

Impact:

- Generative AI adoption: 580 users in 2025 vs 380 users in 2024
- + 1,000 digital assistants
- +33,000 man-hours freed up with AI (≈ USD 1 M).



Some initiatives that reflect the management of this program are:

1. Training path for the development of the Cutting-Edge Skill: Digital Literacy



1,259 (25% of employees)

Each employee selects a digital literacy pathway as part of their individual development plan

2. Technology and Innovation Week



Technology and Innovation Week

4,400 hours of learning
44 interactive offerings
22 immersive experiences.

Making the impossible possible: Technology and innovation as strategic enablers that drive us toward a shared purpose: our 2040 Strategy.

We anticipate challenges

Generative Artificial Intelligence as an **ally to automate, create, and support decision-making.**
Smart cybersecurity that **protects and enables the business.**
Advanced analytics that **transforms data into strategic decisions.**

Digital transition program

Learning methods: Coaching or Mentorship

3. 15 minutes I Am Digital

► 15 Soy Digital

Creamos un espacio para **inspirar a las personas a descubrir el poder de la tecnología**. Impulsamos la evolución hacia una cultura digital mediante sesiones cortas, prácticas y dinámicas que te conectan con **nuevas herramientas digitales** diseñadas para potenciar tu productividad y transformar la manera en que trabajas.



12 sesiones

GenIA, Ciber, Colaboración
Inteligente, Analítica.



300-600

conexiones por
sesión.



NPS* 94%

La experiencia logró
una alta recomendación
entre los participantes.

4. Cybersecurity Week

► Semana de la ciberseguridad

La ciberseguridad no es solo tecnología, **¡Es cultura, comportamiento y conciencia!**: 4 días de charlas, experiencias, juegos y aprendizajes con **expertos que nos ayudarán a identificar riesgos digitales y actuar con responsabilidad**.

Durante estos días reforzamos nuestro compromiso con la **protección de la información y la resiliencia digital**, compartiendo tendencias clave, buenas prácticas y herramientas **para enfrentar los retos actuales**.



+2.500

personas conectadas.



Calificación:

9,58 / 10

Transition program for retiring/terminated employees

Learning methods: Coaching or Mentorship

Jubilo Program: is an initiative aimed at supporting employees in the closing of their work cycle and their transition to the retirement stage, through a comprehensive approach that combines 3 components:

- support in the pension process,
- closing of the work cycle, and
- tools for the transition into retirement.

In this case, we will focus on the Tools for the transition to retirement component, whose objective is to make available to the employee a portfolio of mechanisms that enables them to face the transition to retirement naturally on a personal and financial level.



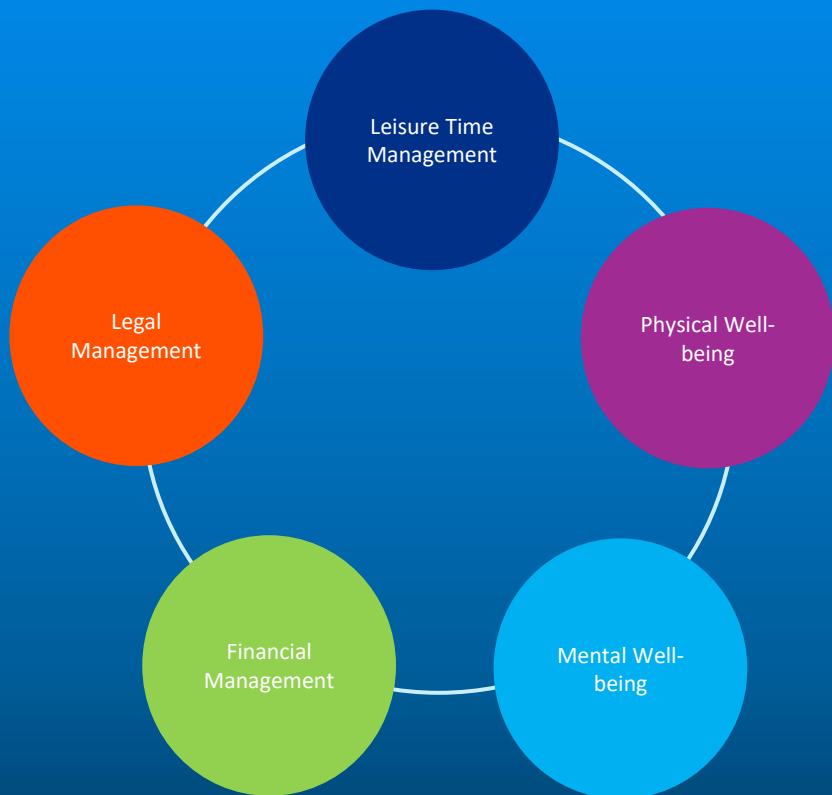
The Saberes de vida program, developed in partnership with Universidad EAFIT and the FEISA Employees' Fund, is a training space designed to promote the understanding of life beyond the workplace, facilitating processes of personal reinvention and the building of new life projects.

Impact: Enabling a more informed and sustainable transition to retirement, through the development of personal and financial capabilities that facilitate decision-making, the continuity of the life project, and the responsible management of the closing of the work cycle.

16 employees participated in the Saberes de vida program

Transition program for retiring/terminated employees

Saberes de Vida Program (Life Skills): Key Dimensions



Retirement Transition Program – Learning Modules

- The New Generation of Older Adults
- Life Roles and the Future Context
- Returning Home and Redefining Daily Life
- Rediscovering the Value of Simplicity
- Healthy Habits: Body, Mind, and Creativity
- Love, Relationships, and Intimacy
- Finding Purpose Through Life Experience
- Social Engagement and Community Participation
- Investment Portfolio Management
- Social Security and Retirement Readiness

Modality: Hybrid
Duration: 63 hours

Transition program for retiring/terminated employees

Legacy Program: is a knowledge management strategy that seeks to preserve and transfer the critical knowledge of employees nearing retirement or with highly specialized profiles. It is activated with a five-year projection before retirement and focuses on ensuring operational continuity and the achievement of the organization's strategic objectives.

The specific objective is to ensure the effective transfer of critical knowledge residing in key people of the organization, through structured development actions such as mentoring, training, technical documentation, and the creation of multimedia materials. This makes it possible to preserve essential organizational capabilities and facilitate an orderly transition toward new generations of talent.

Impact: Implementation of structured mechanisms for the transfer of critical knowledge, materialized in:

- 8 collective transfer spaces (talks, workshops, and specialized sessions)
- 6 personalized knowledge transfer support sessions (Shadowing)
- 5 formalized knowledge assets (manuals, guides, and procedures)

These mechanisms help ensure operational continuity, the effective transfer of key knowledge, and the reduction of the risk associated with the departure of critical talent.

Legacy Program Methodology

1

Identification of critical knowledge

- Annual review
- Retirement within 5 years
- Evaluation of critical knowledge.
- Prioritization

2

Program activation

- Design of the individualized plan
- Participation of leaders and HR

3

Definition of transfer mechanism

- Technical training and mentoring
- Process documentation
- Multimedia material
- Technical talks
- Book

4

Execution of transfer mechanism

- Identification of successors.
- Support for experts
- Training of successors
- Creation of material
- Production and publication of the book.
- Event logistics

5

Monitoring and closure

- Consolidation of results

Teams and Network

Book Club – Vice Presidency of Talent

An open and voluntary conversation space to bring us closer to reading, through bimonthly in-person meetings in which GetAbstract, as our ally, guides us in these valuable conversations, boosting our awareness by questioning ourselves about the challenges, hurdles, needs, and future of the area.

The books and abstracts covered in the 2025 sessions can be found on the Campus ISA Corporate University platform.

More than 25 participants

6 sessions: The readings were the following

1. Outliers
2. Flux
3. Grit
4. Leaders Eat Last
5. Humanocracy
6. Unconscious biases



Book Club – Vice Presidency of Talent

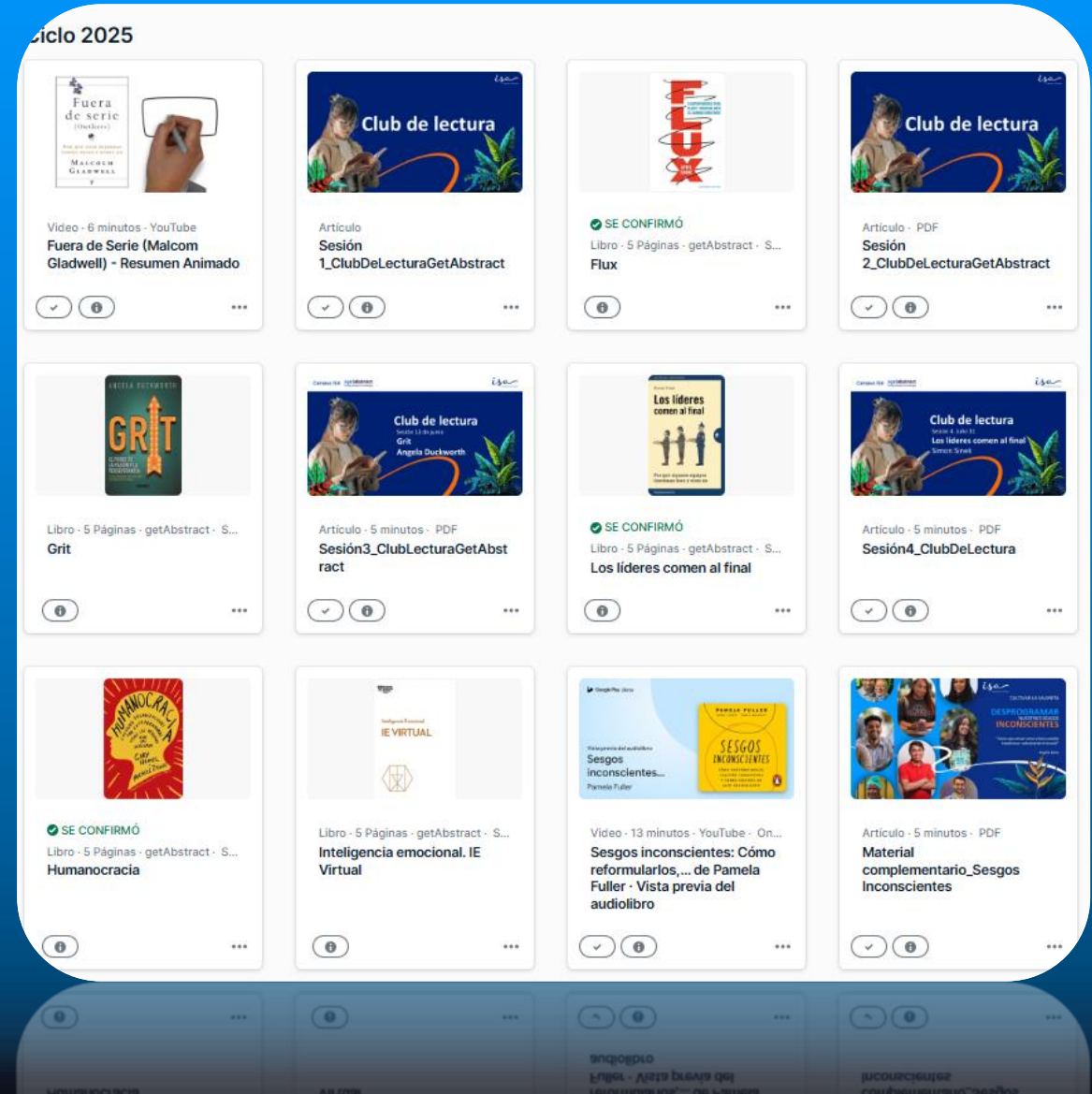
An open and voluntary conversation space to bring us closer to reading, through bimonthly in-person meetings in which GetAbstract, as our ally, guides us in these valuable conversations, boosting our awareness by questioning ourselves about the challenges, obstacles, needs, and future of the area.

The books and abstracts covered in the 2025 sessions can be found on the Corporate University Campus ISA platform.

More than 25 participants

6 sessions: The readings were the following

1. Outliers
2. Flux
3. Grit
4. Leaders Eat Last
5. Humanocracy
6. Unconscious Biases



Contractors' trainings

Contractor Training as a Strategic Pillar

ISA considers the training of its contractors a strategic pillar. It ensures the adoption of best practices in occupational health and safety, helping to prevent accidents and reduce operational and legal risks. By equipping contractors with specialized tools and knowledge, the company enhances project productivity and quality, aligning performance with operational excellence standards.

Occupational Health and Safety (OHS) training

The Company implements a structured strategy for employees and **contractors, integrating mandatory training, technical certifications, and specialized programs for critical risks**. These initiatives are delivered through digital platforms (ISA Campus) and power sector training schools across multiple countries, strengthening capabilities and promoting a consistent safety culture.

In 2025, training programs were deployed across Colombia, Peru, and Chile, with a focus on critical risk management and contractor capabilities, achieving broad operational coverage of high-risk personnel.

Technical Capacity Building

Technical training programs have been implemented to close skill gaps in specific areas essential for contractors to effectively perform their roles.

Digital Transformation

Training also includes learning pathways in areas such as Artificial Intelligence and cybersecurity, raising the level of maturity in digital transformation capabilities.

Quantitative business impact

1.

Competency Development

The Leadership School has enabled the development of key competencies among ISA's leaders, including self-leadership, team management, change management, and strategic management skills.

2.

Leadership Brand Ownership

Leaders have worked on connecting with their purpose, unlocking their potential, and driving the organization's strategy forward.

3.

Learning and Support Experiences

The school has provided valuable learning experiences, including mentoring and coaching programs, workshops, learning pathways, and hands-on experiences.

ISA's Leadership School has had a positive and significant impact on the organization, improving both quantitative and qualitative indicators. It has strengthened ISA's leadership brand, developed essential competencies in its leaders, and enhanced the work environment and operational efficiency.

Quantitative business impact

Quantitative Indicators

1,497 employees completed their training program in cutting-edge skills.

Training Hours

The Leadership School has delivered a total of **425,803 training hours**. On average, each employee has received **83 hours of training per year**.

Training Investment

The total investment in training amounts to **USD3,669,104**, with an average investment of **USD714** per person.

Vacancy Coverage

35,7% of vacancies have been filled with internal talent, reflecting a high level of employee readiness and development.

Satisfaction Levels

The average **satisfaction rating** for training events is **4.75 out of 5**.

Conclusion

The implementation of ISA's Leadership School has had a significant impact on both quantitative and qualitative indicators. Below are some of the key results achieved:

- **Strengthened internal talent pipeline**
- **Increased employee engagement and satisfaction**
- **Enhanced operational efficiency through targeted skill development**



CONEXIONES QUE INSPIRAN

Human Capital Return on Investment

Human Capital Return on Investment

	FY 2022	FY 2023	FY 2024	FY 2025
a) Total Revenue, as specified in the "Denominator" question. Currency: "COP - Colombian Peso"	13'357'506'000'000	14'168'266'000'000	15'828'605'000'000	16'033'736'929'177
b) Total Operating Expenses Currency: "COP - Colombian Peso"	6'540'253'721'442	6'858'380'778'937	8'080'093'000'000	9'212'432'000'000
c) Total employee-related expenses Currency: "COP - Colombian Peso"	1'042'985'320'281	1'218'351'529'280	1'253'182'000'000	1'159'219'000'000
Resulting HC ROI (a - (b- c)) / c	7.53629	6.99982	7.183069977	6.443187765
Total Employees, as specified in the "Denominator" question.	4'713	5'011	5'101	5' 085

Hiring



Hiring

	FY 2022	FV 2023	FY 2024	FY 2025
Total number of new employee hires	770	760	846	403
Percentage of open positions filled by internal candidates (internal hires)	20	14	12.4	35.7

The significant reduction in new hires compared to the previous year was primarily the result of organizational restructuring initiatives across Grupo Ecopetrol, combined with enhanced cost control measures. During the year, the company also placed greater emphasis on internal mobility and promotions, which increased the proportion of vacancies filled by existing employees and reduced the need for external hiring.



CONEXIONES QUE INSPIRAN

Employee Turnover Rate

Employee Turnover Rate

Turnover Rate Analysis

During 2025, the group recorded a total of 438 departures from an initial workforce of 3,685 employees, representing a consolidated turnover rate of 12.24% and a year-end headcount of 3,471 people. It is important to note that voluntary turnover remained at low levels, at 3.33%, while 51% of the separations corresponded to involuntary departures (223 cases), mainly associated with adjustment and organizational optimization processes in specific subsidiaries. This behavior reflects that the departure dynamics of the period responded to strategic decisions of the organization and not to a widespread loss of talent.

The behavior of the indicator was concentrated in a few subsidiaries. ISA Vías Chile recorded the highest volume of departures in the group (90 departures, with a turnover of 26.87%), mostly derived from an operational restructuring process. INTEIA presented the highest turnover rate (41.10%), including a voluntary turnover of 10.27%, in response to which the company has defined follow-up actions regarding retention and employee value proposition. Meanwhile, ISA Energía Colombia, the largest subsidiary, contributed the second highest absolute volume of departures (71), although with healthy indicators: a turnover of 8.29%, below the group average, and the lowest voluntary turnover of all companies (0.70%).

	FY 2022	FY 2023	FY 2024	FY 2025
Total employee turnover rate	10	10.98	11.88	12,24
Voluntary employee turnover rate	6	2.98	4.33	3,33
Data coverage (as % of all FTEs globally)	100	100	100	100

Turnover Rate Analysis

Taken together, these results show that the group's consolidated turnover was driven by focused organizational transformation processes, while most operations maintained moderate turnover levels, such as ISA parent company (8.61%) and ISA Energía Perú (5.88%). The low voluntary turnover at the consolidated level reaffirms the commitment and retention of talent in the organization. For 2026, the group will continue monitoring turnover indicators, with special attention to the subsidiaries that underwent adjustment processes, within the framework of its human talent management and workplace wellbeing strategy.



CONEXIONES QUE INSPIRAN

Type of Performance Appraisal

Performance management appraisals

Performance management is the fundamental mechanism for ensuring alignment and clarity in the **individual and team contributions** of employees toward achieving the strategy. Furthermore, it represents the natural and ideal setting for developing skills, aptitudes, and knowledge, through exposure to the challenges established in the objectives of the individual performance plan.

It is a **continuous process** that begins by defining **individual and team objectives** through the challenge sheet that the CEO shares with all leaders so that each leader can hold objective-agreement conversations with their teams. It is ensured to be continuous through the leader's support and the feedback and **agile conversations** that employees receive permanently.

When evaluating the performance result, each employee performs a self-assessment of their competencies and the results obtained on the agreed objectives, their leader evaluates them, and a **360° perspective** is ensured by including the **performance calibration methodology**, where the leader validates how the employee's performance was with peers, clients, and other leaders they worked with during the year. In the end, this result is reflected in the nine box matrix.





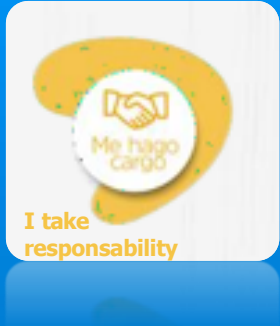
The performance process is systematic, in which each employee has clear and measurable objectives (results and development) that are agreed upon with their leader at the beginning of the year and which are continuously monitored throughout the performance cycle.

Management by objectives

The SMART method to define objectives

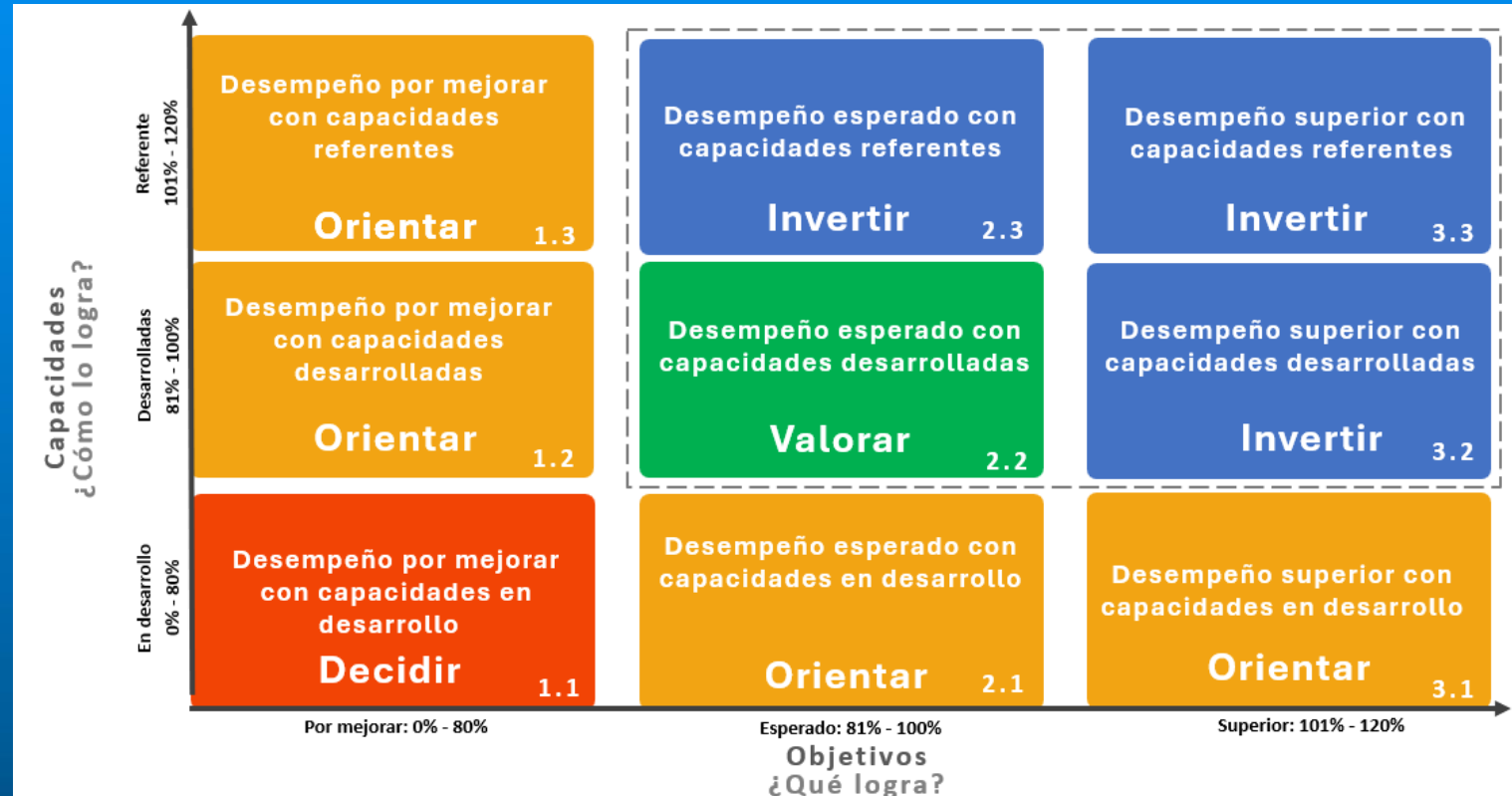
S	SPECIFIC	What do you want to achieve exactly? It should be written without leaving doubts about what to do
M	MEASURABLE	What KPI or indicator can be used to measure your efficiency? In the end, if it is not possible to measure it, it will not be possible to manage its compliance either.
A	ATTAINABLE	Are you proposing a reasonable goal? All objectives must be within the execution capacity
R	RELEVANT	Why is this objective of interest to the company or clients? Every objective must be coherent for the organization, be aligned with its strategy
T	TIMELY	When does this goal have to be achieved? Defining a deadline makes it easier to understand the urgency or priority of the challenge

Multidimensional performance appraisal (e.g. 360 degree feedback)



At the time of evaluating the performance result, each employee performs a self-assessment of their competencies and the results obtained on the agreed objectives; the leader, with this input and the monitoring carried out during the year, evaluates, together with the employee, whether or not the objectives were achieved, and whether the prioritized organizational capabilities were brought into play to achieve them; additionally, it ensures a 360° view by including the performance calibration methodology.

9 box performance matrix



Through this calibration methodology, a multidimensional evaluation is achieved by taking into account in the evaluation of employees, not only the leader's assessment but also the feedback from peers, clients/other leaders with whom they interacted during the year.

Team-based performance appraisal



ISA's CEO shares the Challenges sheet with the Vice Presidents and General Managers, where he prioritizes the objectives of ISA and its Companies and identifies the participation of each one.

Purpose: Provide transparency, alignment and articulation with the business objectives. Employees identify ways to "link" and contribute their individual goals to these goals.

Where do they come from?

Strategic goals and initiatives
Strategic Indicators
Other Projects and Initiatives

Collective construction

The "Conecto" session – Goal Agreement

It is carried out in all areas of the organization

The leader shares with his team the challenges for the year and allows employees to identify ways they can best contribute to those challenges.

The derivation of objectives is practiced as long as it has been previously discussed

Securing:

Focus
relevant contribution

Balance
resource balance

Comprehensive
vision
Assurance



Accompany: This phase of the management cycle enables performance in ISA and its companies to be continuous, through periodic conversations and permanent feedback between the leader and the employee, allowing the identification of progress, achievements, risks, obstacles and making timely adjustments to the objectives initially agreed upon.



Agile conversations

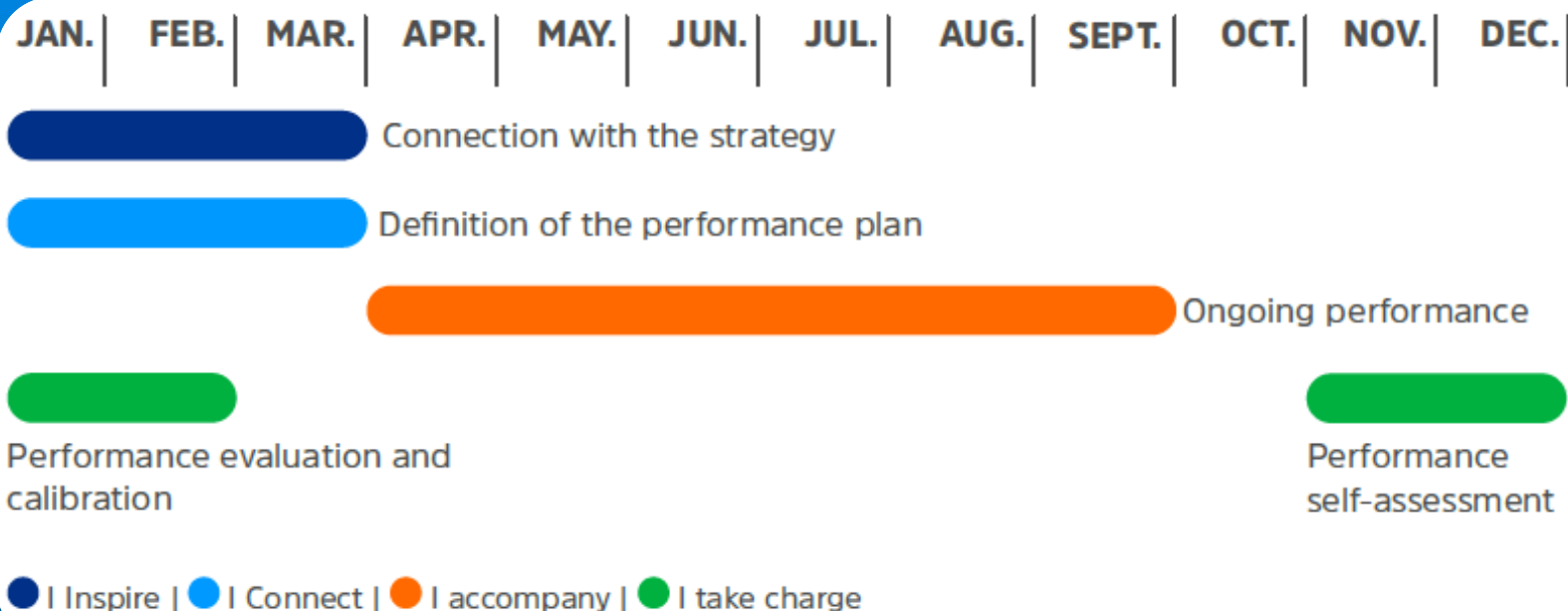
- The communication process between employees and leaders is continuous. (it replaces traditional conversations about performance at a given moment (mid-year, annually)).
- Conversations focused on achievements, objectives, development opportunities, feedback and other operational/tactical requirements.

Additionally, we provide tools to leaders and employees to have continuous performance and development conversations, focused on the following attributes that feedback should have:

- Give and receive permanent, instant and multidirectional feedback.
- Permanent: it is given/received throughout the performance cycle, without needing to wait for a request or an organizational definition to arise.
- Instant: it is given/received right at the moment the actions subject to feedback occur. It does not require preparing a detailed conversation; it is enough to express the related observations clearly and respectfully.
- Multidirectional: it is not linked to levels or roles in the company. It is a practice that involves all of us in the process of collective development.

Performance Appraisal Frequency: Ongoing

Performance annual management cycle





CONEXIONES QUE INSPIRAN

Employee Support Programs

Strategic statements



Work Places

**Flexible
schedule**



Balance care



**Agil and simple
organization**



Leadership

Employee Support Programs

We Promote a True Work-Life Balance

At ISA, we are committed to fostering a real balance between professional and personal life. That's why we offer flexible work arrangements tailored to the diverse needs of our employees, including:

- **Flexible Hours:** Multiple options for start and end times of the workday.
- **Supplementary Telework:** A hybrid model combining days at home and days in the office.
- **Remote Work:** 100% virtual work arrangement.
- **Decentralized Work:** The option to work from abroad for a maximum period of six months.
- **Flexi-Location:** The possibility to work from anywhere within Colombia for up to 21 calendar days per year.

Permanent alternatives



- ☐ Supplementary Telework
- ☐ Autonomous Telework
- ☐ Mobile Telework
- ☐ Remote Work

Temporary alternatives



- ☐ Work from Home
- ☐ Decentralized Work
- ☐ Flexible Location (Flexi-Place)

A temporary alternative means the arrangement has a defined time period and is not permanent.



Flexible Work Statement

The forms of work in the companies of the ISA Group are redefined taking into account the new labor trends and allowing the adaptation of leaders and work teams to a flexible reality leveraged by digital transformation and the globalization of talent.

Flexibility around job sites:

We promote work modalities through which the benefits of remote work are complemented with the benefits of personal interaction

Flexibility around working hours and the development of activities:

We promote flexible working hours and labor contracting modalities that are different from the traditional ones, which allow workers to achieve a balance between personal and professional life, as well as comprehensive knowledge, based on the review of the concept of exclusivity.

Access to global human talent:

We are aware of the globalization of human talent. We analyze and manage the legal framework of the countries where we have a presence to make access to it viable.

Declaration of Workplaces

The work spaces at ISA generate "Inspiring Connections", they are a meeting point that integrates the virtual and physical dimensions of the spaces, taking into account changes in the environment, business challenges, user needs, reflecting the identity and the culture of the ISA Group.

Spaces focused on the user experience: We improve the user experience by permanently identifying their needs, generating self-management solutions. Sensory, eco-friendly and wellness experiences.

Liquid and flexible spaces for EVERYONE: Our spaces are versatile and dynamic, prioritizing their democratization to respond to different ways of working, where users can choose according to the work dynamics required. Spaces for different forms of work: concentration areas, individual work spaces, spaces for informal interaction, spaces for disconnection, spaces for creativity.

Spaces for the development of Capacities: They promote the development of organizational capacities: adaptability, networking, digital transformation and innovation through different forms of collaboration and interaction: (virtual / physical / hybrid)

Collaboration rooms: spaces for formal interaction, co-creation, rituals, videoconference rooms, etc.



Balance Care Statement

At Grupo ISA we are sure that our well-being is linked to that of everyone, therefore we are co-responsible as an organization, leaders and employees to promote the care of the balance between personal and work life, leveraging the strategy of attraction, motivation and permanence of our workers, as well as your physical, mental, emotional and spiritual health.

Balance care actions promote co-responsibility: We design and implement measures aimed at achieving a balance between personal and work life, empowering leaders and employees in the application and validity of the same.

Balance care actions respond to the needs of workers: The fundamental axis of these measures are the workers, that is why we identify their needs and structure and implement different alternatives based on them, and monitor their results.

Balance care actions are consistent and respond to the characteristics of the business: We ensure the coherence of the measures to be implemented and the reality of the business, preserving the continuity of the processes and their operational excellence.

Balance care actions are aligned with the market and the labor legislation of each geography: We seek to standardize the measures for all the companies in the group, but we adapt to the cultural and legal realities of each geography as required.

Telecommuting

Concept

Definition

Observations

Applicable positions

Between 80 and 98%
of the charges

- VP: agreement with President.
- Boss and employee define in common agreement, boss signs format approving inclusion in the program.

Telecommuting days

2 / 3 days

- Possibility of taking any day of the week and may be consecutive. The bosses define a specific day for the team on which no one on their team has telecommuting.
- Employees in work commission, the definitions of Telecommuting do not apply to them.

Workplace assignments

According to SST area protocols

- The place of work must be the principal residence, which must be evaluated by the SST area. Once the main address of all those registered is evaluated, a second address may be evaluated for employees who request it.

Telecommuting
Assistance

An economic aid is delivered

- It is awarded monthly.

Other considerations:

- Possibility of income semi-annually (June - December).
- possibility of withdrawal at any time.

Figures:

- Close to 90% of the population of ISA has Supplementary Telecommuting
- The measure has been implemented in the subsidiaries, about 80% of our employees have this type of work.

Work halftime



At ISA we offer the possibility of choosing the part-time working day (in those positions that allow it). This day allows us to satisfy some of our workers' time needs and provides support to caregivers.

Childcare services or financial contributions

At ISA, workers who have children are granted various economic contributions:

- Fixed amounts in money for study in nursery school.
- Reimbursement of expenses, derived from the hiring of a person for the maintenance and care of the children.

Family leave or payments for any physical or mental health condition

At ISA, financial support is provided for employees' children, as well as for a sibling with a disability who is financially dependent on the employee.

Paternity or maternity leave



Parental Support and Leave at ISA

At ISA, we provide financial recognition for the birth or adoption of an employee's child. Additionally, employees may receive **between two and five extra paid business days** of leave, in addition to the legally mandated time off.

We offer the following parental leave benefits:

- **Primary caregiver paid parental leave:** 23 weeks
- **Non-primary caregiver paid parental leave:** 2 weeks

Maternity and paternity leave are granted in accordance with the legislation of each country where we operate. All ISA companies comply with applicable legal requirements, and some go further by offering **an additional 2 to 8 weeks of paid leave**, fully covered by the employer.

Paternity or maternity leave

Promoting Work-Life Balance at ISA

ISA and its companies implement targeted and differentiated actions to promote a healthy balance between personal, family, and professional life for our employees.

Parental Leave

We respect and apply the parental leave legislation of each country where we operate. We recognize that there are significant differences in the number of leave days granted to mothers and fathers under national laws. For this reason, we are continuously reviewing potential alternatives to help ensure greater balance during this important life stage.

Additional Measures in Colombia

In some of our companies in Colombia, employees—both women and men—are granted 3 days of leave for the birth or adoption of a child, in addition to what is established by law.

In 2025, we launched **Autonomous Telework**, a flexible work arrangement designed to support parents in staying close to and caring for their baby during **the child's first year of life**.



Lactation/Breastfeeding Facilities

We have lactation rooms that offer intimacy and privacy for breastfeeding, these rooms are quiet and pleasant spaces with all the comfort conditions and equipment for the conservation of breast milk while it is taken home for the baby's use.

These rooms can be used by any person regardless of the type of contractual relationship they have during the working day, mothers can use it at any time of the day and have an additional hour a day to breastfeed their baby up to six months of age.



Childcare and contributions

Breastfeeding and Parental Leave Benefits at ISA

At ISA, mothers are granted **1 to 2 hours of daily breastfeeding** leave to meet their baby's nutritional needs during working hours.

Regional Highlights:

- ISA Energía Brasil:
 - For birth or adoption, the company provides an additional 60 days of paid leave for mothers and 15 days for fathers, on top of what is mandated by law.
- ISA Energía Chile:
 - For birth or adoption, the company grants an additional 1 week of paid leave for fathers, beyond the legal requirement.

Acciones Realizadas 

Medidas de conciliación



Nuevo Beneficio:

Teletrabajo autónomo

Tendrás la oportunidad de realizar tus labores desde casa de manera permanente y, ocasionalmente, desde nuestras instalaciones.

¿Quiénes podrán disfrutarlo?

- Las madres podrán disfrutar de este beneficio después de la licencia de maternidad y hasta que el hijo/hija cumpla el primer año de vida.
- Asimismo, los padres podrán acceder a esta modalidad desde la finalización de la licencia de paternidad hasta que el hijo/hija cumpla seis meses de vida.
- Podrán hacer uso de este beneficio las personas con discapacidad, las cuales tengan una restricción que les impida desplazarse y prestar el servicio desde la sede.

Cultura

Alejandro Estévez Neira
Analista de Proyectos Corporativos TE - ISA



Otras miradas

Desde que terminé mi licencia de paternidad el 30 de diciembre de 2023, he estado disfrutando del beneficio de teletrabajo en modalidad de autónomo, un beneficio que se extiende por seis meses debido al nacimiento de mi hija. Esta flexibilidad ha sido un regalo invaluable que me ha permitido estar presente y comprometido con mi familia en un momento crucial de sus vidas.

Este tiempo ha sido fundamental para forjar lazos más fuertes con mis hijos y ejercer plenamente mi paternidad. He sido testigo de cada hito en su crecimiento, he tenido la oportunidad de consolarlos en momentos de dificultad y de celebrar sus logros. Este regalo es algo que valoraré para siempre.

Además, quiero destacar que esta experiencia de teletrabajo no ha afectado mi desempeño laboral. Al contrario, me ha permitido organizar mi tiempo de manera más eficiente, manteniendo un equilibrio saludable entre mis responsabilidades profesionales y mi compromiso con mi familia.

CONEXIÓN TALENTO | isa

Quality of life

We have our Balance your life program through which we promote the physical, mental, emotional and spiritual health of employees and their families.

Equilibra
tu vida

isa

CONEXIONES QUE INSPIRAN

We take care of our talent

through of physical, mental, spiritual and emotional health

Through the Equilibra tu Vida (Balance your Life) ecosystem, the comprehensive care of people and healthy work environments are promoted. In 2025, the well-being ecosystem positively impacted

Allies such as ARL, Eps, health policy, compensation fund, prepaid medicine and employee fund

Physical, sports, cultural activities, active breaks and physiotherapy

- 6,856 family members
- More than 71,000 engagements
- 5,000 active users
- 9,000 activities,
- Thereby establishing well-being as a catalyst for the employee experience.

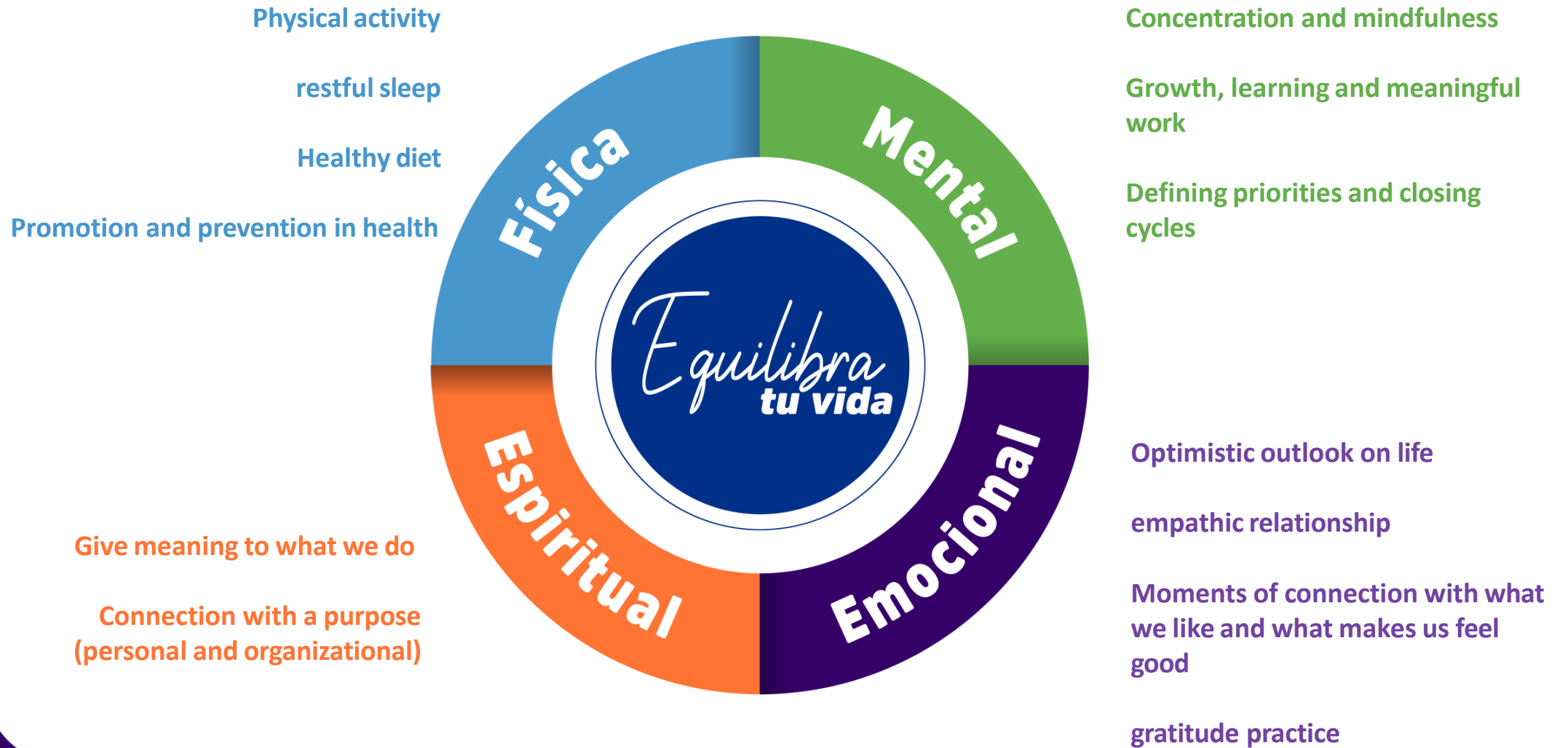
In addition, psycho-social risk assessments were conducted to evaluate factors that could impact the physical and mental health of the teams; the 2025 results showed favorable performance:

- Workplace factors: population at low risk or no risk.
- Non-work factor: low risk.
- Stress-related symptoms: medium risk.

Our findings helped strengthen programs and targeted specialized support, promoting holistic well-being through initiatives in mental health, leadership, and healthy habits, as well as channels for providing timely psychological support and care.

The logo for 'Equilibra tu vida' is displayed on a white rectangular background. The word 'Equilibra' is written in a large, elegant, dark blue script font. Below it, the words 'tu vida' are written in a smaller, bold, dark blue sans-serif font.

Equilibra
tu vida



- Functional Fitness (physical conditioning and special classes)
- Individual physical training plans
- Basic Motor Adventures (children)
- Physical challenges (youth)
- Senior Fitness (older adult)
- Physiotherapy: consultation, telerehabilitation, ergonomic advice, awareness and musculoskeletal health
- Healthy eating and restful sleep



- Concentration techniques and stress management
- Challenges and mind games
- Exchange of experiences: what you know is useful to others... (languages, hobbies)
- Reading clubs, cinema forums and gatherings
- Time management and productivity programs



- Celebrations
- meetings and conversations
- Activities for the family group
- New masculinities

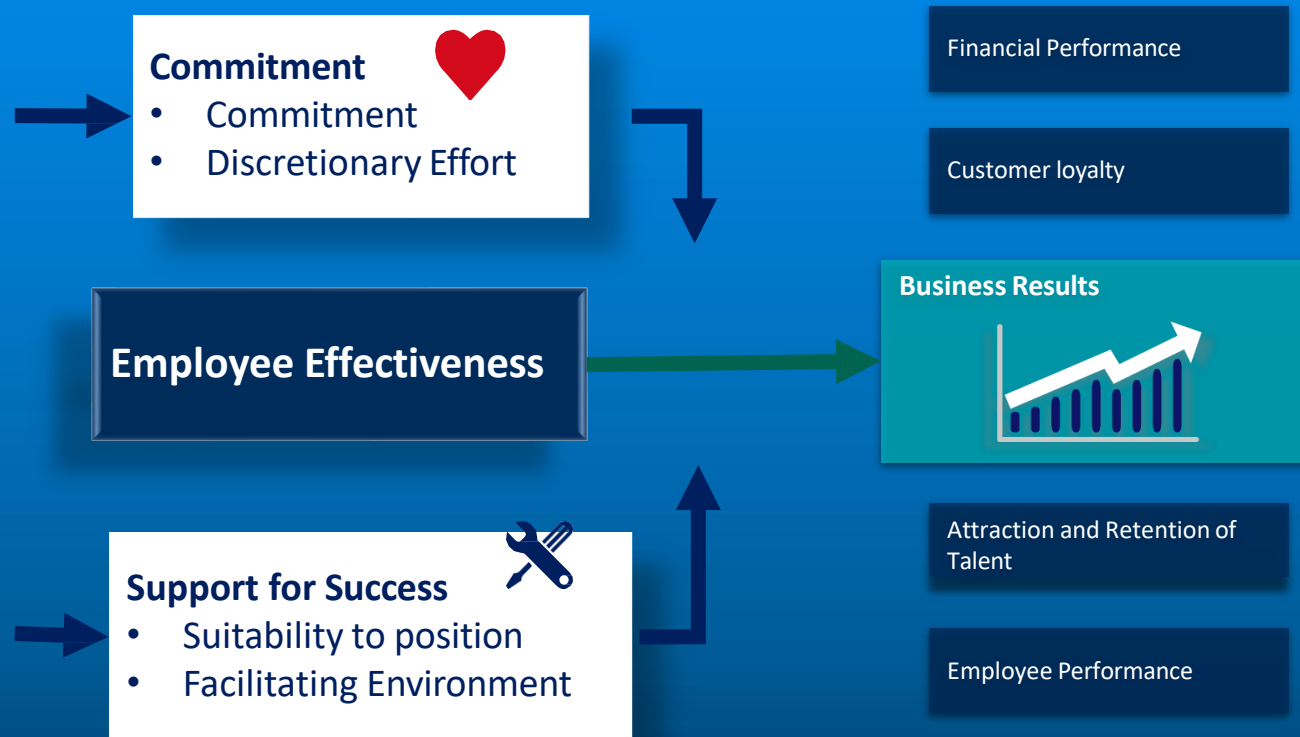


- IKIGAI Program (Life Project)
- Encounters with the soul
- Agreements to access connection and purpose programs

Trend of Employee Wellbeing

Trend of Employee Wellbeing

Korn Ferry's conceptual model posits climate favorability based on level of commitment and support for success



Conceptual differences of the measurements

Criterion	Korn Ferry® (2022-2024)	Great Place to Work® (GPTW) (2025)
Conceptual framework	Model of engagement and organizational effectiveness based on the favorability of working and organizational conditions.	Model based on trust relationships between leaders, colleagues and the organization
Dimensions and Factors assessed	Engagement: commitment, discretionary effort, quality and customer orientation, clarity and direction, trust in leaders, compensation, leader skills, development opportunities, recognition, purpose and organizational capabilities, and balance and reconciliation. Support for success: job fit, enabling environment, autonomy and empowerment, change, collaboration, training, structure and processes, performance management, innovation, resources, and health and safety.	Credibility: information, accessibility, coordination, delegation, vision, reliability, honesty. Respect: development, recognition, collaboration, work environment, personal life. Fairness: equity in compensation, equity in treatment, impartiality, justice in the treatment of people, ability to appeal. Camaraderie: fraternity, hospitality of the place, hospitality of the people, community. Pride: Pride in personal work, team pride and organizational pride. Overall appreciation as an employer
Calculation of Results	Comparative statistical approach, based on employees' favorability levels.	Quantitative assessment based on multivariate comparison with reference or comparable groups, establishing excellence thresholds (8 levels).
External comparability	For 2024 in Latin America: - 95 companies - approx. 900,000 participants	For 2024 globally: - 22,000 organizations - 180 countries – approx. 20 million employees For 2024 in Colombia: - 350 organizations – approx. more than 700 thousand employees
Certification	Does not issue certification	Issues certification by the Great Place to Work institute (GPTW) and in Colombia endorsed by ICONTEC, meaning that the organization meets international standards to be recognized as an excellent place to work.

Note: The Work Environment measurement assesses the internal experience of employees, while Merco evaluates the reputation and external appeal of the organization as an employer with various stakeholder groups.

Korn Ferry's conceptual model posits climate favorability based on level of commitment and support for success

97% Percentage of employees who responded to the survey

- **Favorability Index:** Improved from **83% (2024)** to **86% (2025)**, exceeding the target of 80%.
- **NPS:** Increased from **58 (2024)** to **71 (2025)**, well above the positive threshold.
- **Work Environment Index:** Achieved **73**, rated as **Outstanding**, surpassing the target of **Very Satisfactory**.

General Table of Historical Results - ISA and its Companies				
	2022	2023	2024	2025
	Korn Ferry (Qualtrics) Favorability Index			Great Place to Work Trust Index (Emprising)
Favorability Index	84%	83%	83%	86%
Target	Above 76% favorability, corresponding to the Strength level			Above 80%
NPS	GPTW NPS Methodology			GPTW NPS Methodology
	61	62	58	71
Target	Above 51 - Quality Zone ; the company has more promoters and neutral respondents than detractors			Positive index above 0
Work Environment Index	This index does not apply under the KF methodology			GPTW Work Environment Index
Numerical Index	N/A	N/A	N/A	73
Rating Scale				Outstanding
Target				Higher than Very Satisfactory

Rating scale



Job satisfaction (external motivation, e.g. I am satisfied with my job)



Purpose (internal motivation, e.g., my work has a clear sense of purpose)



Company culture at ISA and its companies

The employee feedback shown below was obtained through the Great Place To Work® Trust Index® survey

LEARN MORE

94 % of ISA and company employees say this is a great place to work compared to 86% of employees at companies in the market .



Source: Great Place To Work® Colombia National Climate Study in 2024

97%

I receive good treatment, regardless of my position in the organization.

98%

I feel proud when I see what we've accomplished

98%

I feel proud when I say that I work for this organization.

98%

I feel good about the way we contribute to the community

98%

People are treated fairly regardless of their sexual orientation

Stress (e.g., I feel stressed at work most of the time)

Objective

To assess the psychosocial risk factors affecting employees at ISA in order to identify potential stressors in the work environment, promote mental well-being, and implement targeted interventions that enhance occupational health, productivity, and overall organizational climate

- Analyze the results of the psychosocial risk assessment to identify key risk factors and areas of concern.
- Use the findings to design and implement targeted action plans aimed at mitigating risks, improving working conditions, and promoting employee well-being.
- Communicate the outcomes transparently with employees and ensure continuous monitoring and evaluation to foster a healthy and sustainable work environment.

Objective plant for measurement 1,431

Total coverage 85.8%

Results by factors:

- Intra-workplace: low risk
- Outside of work: low risk
- Stress-related symptoms: médium risk

Privacy Protection

Scope of privacy management and personal data protection

ISA has the Personal Data Protection Guide – Interconexión Eléctrica S.A. E.S.P., a document that adopts the internal manual of policies and procedures to ensure compliance with Law 1581 of 2012, its complementary regulations, and the handling of inquiries and complaints related to the protection of personal data. This guide establishes guidelines to guarantee the right of individuals to know, update, and rectify the information collected in databases or files, as well as the protection of their privacy.

The guide applies to personal information registered in the databases of the data controller, and its guidelines are of mandatory and strict compliance for ISA, its administrators, and employees. Likewise, the guide recognizes the figure of the Personal Data Processing Administrator, understood as the natural or legal person, public or private, that processes personal data on behalf of ISA, including suppliers, clients, and other third parties.

In line with the above, ISA extends its privacy and personal data protection standards to its value chain. The ISA Group's Code of Conduct for Suppliers covers ISA and its affiliates, and defines the fundamental non-negotiable criteria that must be met by all suppliers contracted by the ISA Group. Knowledge of this code is a prerequisite for contracting and, by accepting the contractual conditions, suppliers commit to complying with its provisions.

The Code of Conduct for Suppliers establishes that suppliers must properly manage and use the information they have access to during the execution of the contract, especially when it concerns confidential or personal information. Additionally, ISA and its companies may verify compliance with this code through various mechanisms during the execution of the contract.

For more information, consult the following public documents:

Personal Data Protection Guide – Interconexión Eléctrica S.A. E.S.P.

<https://isaasprods-d87a26cb809c1f43d1f1-endpoint.azureedge.net/blobisaasprods27f2ae9b77/wp-content/uploads/2021/04/PERSONAL-DATA-PROTECTION-GUIDE-242.pdf>
ISA Group's Code of Conduct for Suppliers https://isaasprods-d87a26cb809c1f43d1f1-endpoint.azureedge.net/blobisaasprods27f2ae9b77/wp-content/uploads/2021/09/CodigoConducta_ISA_ingles.pdf

Person or department designated as responsible for privacy issues



Hugo Nicolás Genoni

Chief Risk and Compliance Officer

ISA has designated officers for the management, implementation, and oversight of matters related to privacy and personal data protection.

In accordance with the Personal Data Protection Guide – Interconexión Eléctrica S.A. E.S.P., the Compliance Officer is responsible for handling requests, inquiries, and complaints related to personal data protection, as well as ensuring the effective implementation of the guide, compliance with applicable regulations, and the adoption of good personal data management practices at ISA.

Additionally, ISA has corporate oversight in this matter through Hugo Nicolás Genoni, a member of ISA's Audit and Risk Committee, a Board of Directors committee, who is the primary person responsible for ensuring the protection of privacy within ISA and its companies.

Personal data owners and other stakeholders may channel requests, inquiries, or complaints related to privacy and personal data protection through the channels established by ISA:

- Email: protecciondatospersonales@ISA.com.co- Address: Calle 12 Sur No. 18-168, Medellín, Colombia- Service line: 018000941341

Resume of Hugo Nicolás Genoni – ISA

Link: [RESUME OF THE EXECUTIVE Nicolas Genoni – ISA](#)

Integration of privacy into risk management and compliance

The management of privacy and protection of personal data at ISA is aligned with the corporate model of comprehensive management of risks, compliance, internal control, and information security. Under this approach, the risks associated with the processing of personal data are managed as part of the company's operational, technological, compliance, and reputational risks.

The protection of personal data is mainly related to the risks of cybersecurity and information technology, due to the need to protect the confidentiality, integrity, availability, and appropriate use of personal information. It is also linked to compliance risks, insofar as the company must ensure compliance with the applicable regulations regarding data protection, privacy, handling of data subjects' rights, and contractual obligations with third parties.

These risks are managed through defined responsibilities, internal controls, information security guidelines, periodic monitoring, identification of vulnerabilities, follow-up on action plans, and escalation to the corresponding corporate bodies, including the Compliance, Risk, Internal Audit areas, and the Audit and Risk Committee, as applicable.

In this way, ISA integrates privacy and the protection of personal data within its corporate system of risk management and compliance, ensuring that the associated risks are identified, assessed, monitored, and addressed in a cross-cutting manner across its operations and companies.

Measures against breaches of privacy and personal data protection

ISA has internal and contractual mechanisms to manage breaches related to privacy, confidentiality, and personal data protection. These mechanisms apply both to employees and to suppliers, contractors, and third parties who, in the course of their duties or contractual relationships, have access to personal or confidential information.

In the case of employees, breaches are managed in accordance with the disciplinary procedure established in the Internal Labor Regulations. This procedure guarantees the verification of the facts, the right of defense, the disclosure of evidence, and the application of sanctions according to the severity of the conduct. Offenses may be classified as minor or serious, considering criteria such as the harm caused to the company, the repetition of the conduct, and the circumstances of time, manner, and place in which the breach occurred.

In this context, conduct such as misuse, unauthorized access, disclosure, loss, alteration, irregular processing, or negligent handling of personal data or confidential information may trigger the following measures:

1. Verification of the conduct or possible breach

ISA reviews the facts, conduct, or omissions related to the possible breach of legal, contractual, regulatory, or internal obligations regarding privacy, confidentiality, and personal data protection.

2. Summons and hearing of explanations

When the case involves an employee, the corresponding summons is issued so that they may present their explanations, provide information, and exercise their right of defense within the disciplinary procedure.

3. Disclosure and review of evidence

The company makes the employee aware of the evidence supporting the process, guaranteeing due process and the possibility of contesting or supplementing it.

4. Classification of the offense

The breach is assessed and classified as a minor or serious offense, according to the applicable disciplinary scale and the nature of the conduct.

5. Assessment of severity criteria

To determine the applicable sanction, ISA considers the harm caused to the company, including financial, operational, or reputational impacts; the repetition of the conduct; and the circumstances of time, manner, and place of the breach.

6. Application of disciplinary sanctions

When applicable, disciplinary sanctions are applied in accordance with the Internal Labor Regulations and the defined internal procedure.

7. Record of offenses and sanctions

ISA may keep a record of the offenses committed and the sanctions applied, in order to identify repetitive or recurring conduct and consider them in possible subsequent processes.

8. Civil, labor, or third-party liability

The application of a disciplinary sanction does not exempt the employee from the civil or labor liability that may arise from the breach toward ISA or toward affected third parties.

9. Contractual measures against suppliers and third parties

When the breach involves suppliers, contractors, or third parties, ISA may invoke the contractual clauses on confidentiality and personal data protection.

10. Compensation for damages

In the event of disclosure, unauthorized use, or processing contrary to what was contractually agreed, third parties may be required to compensate for the damages caused, including lost profits, whether the breach occurs intentionally or through negligence.

11. Corrective actions and strengthening of controls

ISA may define corrective actions to mitigate the impact of the breach, correct its causes, reinforce controls, and prevent the recurrence of similar events.

12. Legal actions, when applicable

Depending on the severity of the breach, ISA may initiate the corresponding legal actions or claims, in accordance with the applicable regulations and current contracts.

In this way, ISA has a framework of action that allows it to manage breaches of privacy and personal data protection through disciplinary, contractual, corrective, and legal measures, applicable according to the nature of the relationship with the person or third party involved and the severity of the case.

Confidentiality and data protection clause – Third Party Contracts

CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES

LAS PARTES se obligan a cumplir a cabalidad con lo dispuesto en las normas sobre protección de datos personales. Así mismo, cada una de **LAS PARTES** se obliga a guardar reserva de la información que le sea entregada por la otra parte, o a la que tenga acceso en desarrollo del presente Contrato, con independencia del medio en el cual se encuentre soportada. En cumplimiento de la obligación de reserva cada parte deberá: **a.** Utilizar la información suministrada por la otra parte para la labor encomendada; comprometerse, además, a utilizar todos los medios a su alcance para garantizar la más estricta confidencialidad respecto de dicha información, y hacer extensivo dicho deber de confidencialidad a cualquier persona que, por su relación con él, deba tener acceso a dicha información, para el correcto cumplimiento de sus obligaciones. **b.** Abstenerse de reproducir, modificar, hacer pública o divulgar a terceros la información objeto del presente compromiso, sin previa autorización escrita de la parte que se la reveló. LAS PARTES reconocen que la información entregada por la otra parte le pertenece a ésta o al tercero que haya autorizado a la parte receptora para suministrar la información confidencial. Por ello, se obligan mutuamente a resarcir los perjuicios por daño emergente y/o lucro cesante que llegare a ocasionar la revelación, divulgación o utilización realizada de cualquier forma distinta a la definida en el presente Contrato, ya sea de forma dolosa o culposa. El presente compromiso de confidencialidad tendrá vigencia desde la fecha de la firma del Contrato y hasta cinco (5) años más después de la terminación del mismo.

Therefore, they are mutually obligated to compensate for the consequential damages and losses and/or loss of profits that may be caused by the disclosure, dissemination or use made in any manner other than that defined in this Agreement, whether intentionally or through negligence. This confidentiality commitment shall be in effect from the date of signing of the Contract and for five (5) additional years after its termination.

firmas del Contrato y hasta cinco (5) años más después de la terminación del mismo.
culposa. El presente compromiso de confidencialidad tendrá vigencia desde la fecha de la
de cualquier forma distinta a la definida en el presente Contrato, ya sea de forma dolosa o

Audit – ISA personal data protection assessment

Third-party audits on compliance with the privacy policy

ISA conducts assessments with specialized third parties to verify the effectiveness of controls related to privacy, personal data protection, and information security.

In 2025, ISA had the support of the specialized firm **Safe-U** to carry out a **Red Team** exercise, aimed at evaluating the effectiveness of physical and digital security controls at the company's various sites. The objective was to perform a controlled, intrusive, and persistent exercise to identify vulnerabilities that could affect the protection of information and personal data.

This assessment made it possible to review information exposure scenarios, unauthorized access, detection and containment capabilities, as well as opportunities for improvement in the defense and protection mechanisms implemented by ISA.

As a result, ISA strengthens its privacy, personal data protection, and information security controls, managing the corresponding findings and action plans.

Internal audits on compliance with the privacy policy
ISA conducts internal assessments to verify the effectiveness of controls related to privacy, personal data protection, information security, and internal control.

In 2025, **ITGC** controls were internally evaluated through management testing, with the support of **BDO Audit S.A.S. BIC** as independent auditor. These tests were related to the assessment of the internal control system under **SOX** and included controls associated with access management, cybersecurity, change management, and operational continuity.

These controls are relevant to personal data protection, as they help preserve the **confidentiality, integrity, and availability** of information. The assessment evidenced coverage of technical risks in areas such as access management, cybersecurity, change management, and operational continuity, and is complemented by **SOC 1 Type 2** reviews for providers such as SAP.

Based on these internal assessments, ISA identifies opportunities for improvement, follows up on findings, and strengthens controls associated with privacy, personal data protection, and information security.

Rights of data subjects over their personal data

ISA recognizes that personal data subjects, including customers and other stakeholders, have the right to decide on the processing of their personal information, in accordance with applicable regulations and the procedures defined by the company. To this end, ISA requests authorization for the collection, use, retention, processing, and disclosure of personal data, except in cases exempted by law, and provides channels for data subjects to exercise their rights over the information the company retains in its databases.

Data subjects may exercise the following rights:

Decide how their personal data is collected, used, retained, and processed

Data subjects may know the purposes of the processing of their personal data and exercise control over the information that ISA collects, uses, retains, processes, or shares, in accordance with the authorization granted and applicable regulations.

Grant prior consent for the processing of their personal data

ISA requests authorization to collect, use, retain, process, and disclose personal data, except in cases where the law permits processing without prior authorization. This authorization may be granted by physical, electronic, or other means that allow for subsequent consultation.

Revoke the authorization granted

Data subjects may revoke the authorization for the processing of their personal data when there is no legal or contractual duty requiring ISA to retain them or continue processing them.

Request access to the data retained by ISA

Data subjects may consult and access the personal data held in ISA's databases, as well as request information about how it has been used.

Request the correction or updating of their personal data

Data subjects may request the updating, rectification, or correction of incomplete, inaccurate, outdated, or misleading information.

Request the deletion or removal of their personal data

Data subjects may request the deletion of their personal data when they consider that it is not being processed in accordance with applicable regulations or when it is no longer necessary for the authorized purposes, provided there is no legal or contractual duty of retention.

Request the transfer of their data to other service providers

When legally, technically, and contractually appropriate, data subjects may request that their information be delivered or transferred in accordance with the mechanisms enabled by ISA and applicable regulations. This request will be handled under criteria of security, traceability, identity verification, and protection of the confidentiality of the information.

Submit inquiries, requests, or complaints

Data subjects may submit requests related to the processing of their personal data through the channels defined by ISA for personal data protection.

In this way, ISA allows data subjects to exercise control over the manner in which their personal data is collected, used, retained, processed, updated, deleted, transferred, or shared, strengthening transparency and the protection of privacy in its relationship with customers and other stakeholders.

How personal information is protected

ISA protects personal information through guidelines, procedures, and controls aimed at preserving the confidentiality, integrity, and availability of the data. The company recognizes that personal data is information and an intangible asset, so its processing is subject to internal policies and procedures on information security, personal data protection, internal control, and risk management.

The protection of personal information is strengthened through:

Information security policies and procedures

Personal data is managed under internal security, privacy, and data protection guidelines, in order to prevent unauthorized access, misuse, loss, alteration, disclosure, or improper processing of the information.

Access controls and cybersecurity

ISA implements controls aimed at protecting the systems, platforms, and repositories where personal data is stored or processed. These controls include access management, cybersecurity, change management, and mechanisms to protect operational continuity.

Physical and digital security assessments

In 2025, ISA carried out a Red Team exercise with the support of the specialized firm Safe-U, aimed at evaluating the effectiveness of physical and digital security controls, including controls related to personal data protection.

Assessment of internal technology controls

ISA evaluates ITGC controls related to access management, cybersecurity, change management, and operational continuity. These controls help protect the confidentiality, integrity, and availability of personal and confidential information.

Review of critical technology providers

The company complements its controls with reviews applicable to critical third parties, including assessments such as SOC 1 Type 2 for relevant providers, where appropriate.

Training and data protection culture

ISA strengthens information protection through internal training. In 2025, 97% of new hires at ISA completed the training on personal data protection, information security, and responsible information handling.

Monitoring, findings, and action plans

Internal and third-party assessments make it possible to identify vulnerabilities, review the effectiveness of controls, manage findings, and define corrective or preventive actions to strengthen personal data protection.

In this way, ISA protects personal information through a comprehensive approach that combines policies, technology controls, physical and digital security, audits, third-party reviews, training, and continuous improvement.

Use of personal data for secondary purposes and internal training

ISA manages personal data under the principles of purpose, necessity, transparency, and accountability. The company collects and processes only the information necessary to fulfill defined purposes that are authorized or permitted by law, avoiding the use of personal data for purposes other than those for which it was originally collected.

Use of personal data for secondary purposes

ISA does not use personal data for secondary purposes. In line with this approach, the percentage of data subjects whose personal data is used for purposes other than those originally reported or authorized is 0%.

Limitation of the purpose of processing

Personal data is processed solely for clearly defined purposes, necessary for the development of the corporate purpose, the fulfillment of legal, contractual, or regulatory obligations, and the purposes authorized by the data subjects.

Principles applied to the processing of personal data

The management of personal data is carried out under the principles of purpose limitation, data minimization, accountability, and traceability, ensuring that personal information is not used beyond the purpose originally reported.

Internal training and awareness

As part of ISA's commitment to information security and the protection of personal data, new employees must complete training on personal data protection during their onboarding process.

Training coverage 2025

In 2025, **97% of new hires at ISA completed the training on personal data protection**, strengthening the secure, responsible, and appropriate handling of personal information.



isa

2024

Energía
Vida
Transición