1.9.1 Information Security Governance

Ecopetrol has governance mechanisms in place to oversee information security activities, including:

1. A Board of Directors has been formed with the responsibility of maintaining the supervision of information security.
2. There are the Science, Technology and Innovation and Business Risk Committee committees
3. There is an executive role to oversee information security

Therefore, Ecopetrol's Board of Directors has a Technology and Innovation Committee, whose function is to review and monitor the digital strategy with scope for the Ecopetrol Group, as well as the strategy and operating model of computer security, cybersecurity, cyber defense, privacy and data recovery.

This committee is currently made up of Ricardo Rodríguez Yee, Álvaro Torres Macías, Hildebrando Vélez Galeano, Ángela María Robledo Gómez, Tatiana Roa Avendaño, one of these members has high experience in Cybersecurity and information security. This member is Alvaro Torres, he serves as vice president of the Board of Directors and the president of the Audit and Risk Committee of the Board of Directors of Ecopetrol S.A. since March 2024. He is an electrical engineer from the Industrial University of Santander, in Colombia. A specialist in electric power transmission from the Institute National Polytechnique de Lorraine de Nancy, France, he holds a master's degree in electrical engineering, electrical power and computer and systems engineering from Rensselaer Polytechnic Institute in Troy, United States and a PhD in electrical engineering from the same institution.

He currently serves as CEO of Electryon Power Inc. of Canada. He has been Manager – Country Manager of Northland Power Inc. and Electryon Power Inc. (both Canadian companies), Manager of Delphi Capital Partners, President of CONALVIAS, Vice President of Corporate Planning and Equity Portfolio of Empresa de Energía de Bogotá (current Grupo de Energía de Bogotá - GEB), General Manager of SNC Lavalin Inc, Senior Partner, Technical Manager and General Manager of Consultoría Colombiana S.A. - CONCOL. Likewise, as a director in the aforementioned positions, he was a proponent of policies and practices related to cybersecurity and cyber defense. Between 1980 and 2012, he worked as a staff professor at the Faculty of Electrical and Electronic Engineering of the Universidad de Los Andes.

Previously, he was a member of the Boards of Directors of Empresa de Energía de Boyacá – EBSA, Transportadora de Gas Internacional (TGI), Transportadora de Energía de Centroamérica S.A. (Guatemala), Cálidda Energía S.A.C. (Peru), Contugas S.A.C. (Peru), Empresa de Energía de Cundinamarca (EEC), companies of GEB, ITANSUCA, OPAIN, Incubadora de Empresas Innovar (COLCIENCIAS), SOFTEC and alternate member of the Board of Directors of PROMIGAS.

According to the positions held, he has experience in: i) energy industry; (ii) energy transition; (iii) administration, senior management and leadership; (iv) financial matters; (v) enterprise risk management; (vi) human resources and/or talent development; (vii) legal issues and/or ECP-PUBLIC INFORMATION corporate governance; (vii) technology and/or

innovation; (ix) health, safety and/or environment (HSE); (x) sustainability; (xi) **cybersecurity**; (xii) climate change and (xiii) business strategy and/or project management. As a member of Ecopetrol's Board of Directors, he receives regular training on ethics, compliance, and risk management issues.

His duties as a board member include reviewing and monitoring the digital strategy with scope for the Ecopetrol Group, as well as the strategy and operating model of computer security, cybersecurity, cyber defense, privacy and data recovery. (Check profile at the following link: 251202+Perfil+Álvaro+Torres+ENG.pdf)

In addition to the above, Ecopetrol has also appointed an executive position to oversee information security and it is Sergio Andrés Moreno Acevedo who was appointed Corporate Vice President of Science, Technology and Innovation of Ecopetrol as of July 28, 2025. He is a Systems Engineer from the Industrial University of Santander, with a specialization in Technology Management. He has more than 25 years of experience in transformation, digital strategy and innovation, having held key roles in companies with global projection. He has led digital transformation initiatives. His career includes positions of high responsibility with multiple achievements in the optimization of processes from a tactical, operational and strategic point of view, contributing to operational efficiency and service experience. Their skills in transformational leadership, strategic planning, adaptability, critical thinking, innovation, and problem solving stand out.

He works as CTO (Chief Technology Officer), DPO (Data Protection Officer) and Chief CISO (Chief Information Security Officer) at Ecopetrol S.A. In the development of these functions, he directs the organization's cybersecurity and cyberdefense strategy, aligning its actions with the vision and objectives of the business strategy. (check profile at the following link: Perfil-Sergio-Andres-Moreno.ingles.pdf)

Governance oversight is maintained given that Ecopetrol has two senior management committees made up of members of the board of directors whose functions are associated with cybersecurity issues, which are presented below:

1. **The Technology and Innovation Committee**: as part of its functions, it monitors the cybersecurity strategy of the Ecopetrol Group (GE). (Consult the Committee's internal regulations at the following link: https://www.ecopetrol.com.co/wps/wcm/connect/399038c3-2227-44f4-90bb-c0575e3eec7b/GOC-R-013+Internal+regulations+of+the+Technology+and+Innovation+Committee+of+the+Board+of+Directors+of+Ecopetrol+S.pdf?MOD=AJPERES&CVID=pGUi6ym)

2. **Audit and Risk Committee:** as part of its functions, it supervises the risks associated with cybersecurity threats. (Consult the Committee's internal regulations at the following link: https://www.ecopetrol.com.co/wps/wcm/connect/fa3d64d2-1e53-4f42-82ed-ebc1cd1ff2cd/GOC-R-014+Internal+regulations+of+the+Audit+and+Risk+Committee+of+the+Board+of+Directors+of+Ecopetrol+S.A_.pdf?MOD=AJPERES&CVID=pGUivrS)

1.9.2 Information Security Policy

Ecopetrol, due to issues of Management Systems and document structure, has a single normative document called **"Comprehensive Policy"** whose content shows the intentions and direction of the organization, formally expressed by Senior Management. It shows the criterion of action chosen in compliance with the strategic framework that generally frames the actions at the institutional level.

Within the same line of document management, it has Circulars, manuals, guides, procedures, instructions, among others. Where the regulatory guidelines of Cybersecurity and Information Security are immersed, among these Ecopetrol has the **Information Security Manual**, which serves as the information security policy, this manual is applicable to the company and to contractors with access to information, which defines guidelines and standards based on the Code of Ethics and Good Governance. This manual establishes principles, criteria and responsibilities to protect information assets, ensure their proper treatment and reduce the risk of leakage or loss, in compliance with regulations and standards adopted by the organization.

In line with these guidelines, Ecopetrol maintains a firm commitment to the integrity, protection and responsible management of data, in addition, assigns individual responsibilities to all personnel, ensuring that employees and suppliers comply with corporate standards and actively contribute to information security. (See the manual at the following link: cti-m-005-information-security-manual.pdf)

It should be clarified that for the supervision and response capacity to threats to information security, Ecopetrol within its regulatory framework has the **Cyber Incident Management Guide** that aims to establish actions and general guidelines for the attention of cybersecurity incidents in Information Technology and/or Operation Technology, that allow Ecopetrol S.A. and Grupo Empresarial to quickly and effectively manage service activities and reduce the levels of risk and impact of these.

On the other hand, the corresponding continuous investment in information security systems is included in the strategy of the Cybersecurity program.

1.9.3 Information Security Management Program

Ecopetrol has a program that supports the management of Information Security and Cybersecurity with continuous investments aligned with the 2040 Strategy, which requires reaching higher levels of maturity in cybersecurity and information security, with the aim of protecting Ecopetrol's value against threats and cyberattacks. To this end, Ecopetrol has developed a cybersecurity strategy based on the following four (4) pillars:

1. **Digital trust:** Promote excellence, innovation and cyber collaboration, putting the customer, the Ecopetrol Group and the supply chain at the center of actions.
2. **Cyber resilience:** Strengthen the capacity to respond to cyberattacks and ensure continuous monitoring of cyber activities, covering intelligence, visibility, response and recovery.

3. **Efficiency and Consolidation:** Protect data and privacy, establish ethical guidelines, and ensure the safe use of artificial intelligence.

4. **Industrial protection:** Incorporate security measures that optimize the comprehensive protection of information and industrial infrastructure, promoting defense and collaboration.

   Therefore, within the management of these pillars there are different topics, among them:

- Business continuity plans related to information security
- Information Security Vulnerability Analysis
- Internal audits of IT infrastructure and/or information security management systems
- Independent external audit of IT infrastructure and/or information security management systems
- Escalation process for employees to report incidents, vulnerabilities, or suspicious activity
- Information Security Awareness Training
- Disclosure of the total number of breaches that occurred in the last fiscal year

The management of the aforementioned topics is described below:

From cybersecurity practices aimed at securing and responding to cyber incidents, Ecopetrol actively contributes to the protection of critical infrastructures and has a robust framework for cyber incident management, which establishes the official process for the identification, analysis, classification, treatment and closure of cybersecurity incidents. This process is led by the Security Operations Center (SOC), and the Incident Response Team (CSIRT). It is important to note that, during the year 2025, the total number of breaches occurred was 0 (zero), which means that there were no cyber or information security incidents.

In addition, there is also a procedure for employees to report alerts, cybersecurity events, suspicious emails (phishing/spam) or unwanted emails through 2 channels: the help desk system and the corresponding email for this purpose. It should be clarified that this procedure was disclosed internally. (It can be consulted at the following link https://files.ecopetrol.com.co/web/eng/learn-how-to-report-cybersecurity-alerts-events.pdf)

Ecopetrol also has Technical Vulnerability Management where the official process for identifying, analyzing, prioritizing, remediating and verifying vulnerabilities in IT infrastructure, software, telecommunications and prioritized applications is defined.

Aligned with the continuity of processes and the business, in accordance with the provisions of the guidelines and manuals for business continuity management in Ecopetrol S.A., an annual cycle is carried out for the processes or functions and facilities critical to business continuity (risks, BIA, strategy, plan and tests) that allows the Company to incorporate capabilities to operate in contingency in the event of interruption incidents. Operational continuity plans (OCPs) are updated at least annually in a planned, systematic and rigorous manner, and in the event of organizational or environmental changes that imply adjustments to key premises, adjustments are made to increase their effectiveness, including the review of the response structures to interruption incidents and their escalation. if necessary to a business crisis.

Operational continuity plans are generally approved and for the Vice Presidency of IT Science and Technology they are tested two (2) times a year, favoring the strengthening of the responses of the teams required to respond to interruptions.

On the other hand, cybersecurity management at Ecopetrol is based on the principles of the company's Comprehensive Policy, with special emphasis on the pursuit of operational excellence, adequate risk management and continuous improvement of processes and information and data assurance. The strategic direction of cybersecurity falls to the Corporate Vice Presidency of Science, Technology and Innovation (VTI), whose objective is to ensure digital excellence, optimize efficiencies and strengthen protection against cyber threats.

The Company has the ideal personnel for the development of activities associated with cybersecurity, incorporating the necessary talents for their management. Similarly, it generates appropriation actions in order to sensitize and prepare personnel about possible situations that threaten normal operation. To this end, it has a Cybersecurity Appropriation Program, through which strategies and actions are implemented that tend to a change in user behavior, and generate safe practices that reduce exposure to risk. It also offers a wide range of cybersecurity courses, assigned in each employee's annual learning plans, along with endomarketing, mobilization and training campaigns. It also has a network of Cyber Guardians[1] that help disseminate good practices within the Company's management and subsidiaries (see appropriation management in the following link 2025 Closing Report.)

At Ecopetrol, people represent a fundamental factor, since their behaviors in the treatment of information are decisive in preserving its confidentiality, integrity and availability. The company's information security model promotes awareness and internalization of practices and behaviors aimed at the protection and assurance of information. Therefore, employees, collaborators, contractors, allies, suppliers, stakeholders, subsidiaries and associated companies must remain informed and committed to adopting behaviors that safeguard information, thus minimizing the risks of data leakage or loss.

In addition, it is important to mention that Ecopetrol carries out internal and external audits of the IT infrastructure and/or information security management systems. Ecopetrol periodically comprehensively reviews its cross-cutting cybersecurity process, identifying risks, controls and assessments and then carrying out an evaluation to determine its sufficiency and correct operationality.

Internal audit reviews are executed by the Corporate Internal Audit Department who, through the general audit plan, plan review exercises that involve aspects of process, security, infrastructure,

[1] A cyberguardian is a collaborator within an organization who, without necessarily being a technical expert in computer security, acts as a liaison between the cybersecurity team and the rest of the employees. Their role is to promote digital security from the behavior of workers, raise awareness of good practices and help identify and mitigate risks in their work area.

controls and tests. During 2025, five (5) audits were carried out with a focus on cybersecurity and IT infrastructure and OT issues, such as:

- Audit of cybersecurity management in Refining Operation Technologies (OT).
- Audit of cybersecurity incident management.
- Audit of the management of cloud technology services.
- Audit of the Information Technology control environment at Ecopetrol Brasil (follow-up), Ecopetrol USA Inc.- Monitoring Audit of the Information Technology control environment)

Additionally, the company receives independent external audits and verifications (Consult audit certificate from one of the related external auditing entities at the following link: https://files.ecopetrol.com.co/web/eng/external-audit-certificate-swift.pdf), carried out by different control entities such as tax auditing, management tests, superintendencies, among others. These audits, executed by specialized firms, comprehensively cover the science, technology and innovation process, emphasizing topics such as IT infrastructure, cybersecurity, access management, configurations, etc. Additionally, they take into account the controls defined for the process both in design and operation. We currently receive by 2025 the following formal external audit exercises involving the CT+i process, such as:

- **Tax Audit** (with coverage of the year),
- **SWIFT** (Swift Customer Security Controls Framework Verification)
- **AEGR** (Verification of compliance with Resolutions of the Superintendence of Residential Public Services.)