
	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

## TABLE OF CONTENTS

1.	OBJECTIVE.....	2
2.	GENERAL CONDITIONS .....	2
2.1	Scope .....	2
2.2	Terms and definitions.....	2
2.3	Associated documents .....	2
2.3.a	Normative references .....	2
3.	DEVELOPMENT .....	3
3.1	Information Security Components .....	3
3.1.a	People .....	3
3.1.b	Technology .....	4
3.1.c	Processes.....	4
3.1.c.1.	Secure Information Management Cycle .....	4
3.1.c.1.1.	Information classification.....	8
3.1.c.1.1.1.	Non-Confidential Information.....	9
3.1.c.1.1.2.	Information confidentiality .....	11
3.1.c.1.1.3.	Information classification guidelines .....	12
3.1.c.1.2.	Information processing .....	13
3.1.c.1.2.1.	Labeling the information .....	13
3.1.c.1.2.2.	Access to Electronic and Physical Information .....	14
3.1.c.1.2.3.	Identification and securing of electronic sheets.....	15
3.1.c.1.2.4.	Storage of Electronic and Physical Information .....	15
3.1.c.1.2.5.	Distribution and Transmission of Information .....	16
3.1.c.1.2.6.	Final and secure disposal of information .....	16
3.1.c.1.3.	Risk analysis .....	16
3.1.c.1.4.	Implementation of the Mitigation Plan .....	16
3.1.c.1.5.	Follow-up.....	16
3.2	Responsibilities of Users Regarding Information and Technological Resources .....	16
3.2.a	Responsibilities of users with regard to information and technological resources .....	17
3.2.a.1.	Technical-Scientific Publications .....	17
3.2.a.2.	Copyright .....	17
3.3	Legal Liability and Consequences .....	17
4.	CONTINGENCIES .....	18
5.	ANNEXES.....	18

## Illustration and table content

Figure 1 - Ecopetrol S.A. appropriation model.....	4
Figure 2 - Secure Information Management Cycle of Ecopetrol S.A .....	5
Figure 3 - Classification or categorization of information.....	9
Figure 4 - Classified or reserved information, according to the Transparency Law .....	12
Figure 5 - Classification and labelling of digital media information.....	13
Table 1 - Some Media on Which Information May Be Submitted, Stored, or Transferred .....	5
Table 2 - Matrix of Roles and Responsibilities in the Secure Information Management Cycle .....	8
Table 3 - Document under construction is Confidential .....	12

	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

## 1. OBJECTIVE

Present the management guidelines on Information Security with reference to the applicable regulations and standards adopted in Ecopetrol S.A., in order to establish the principles, criteria, responsibilities, conducts and practices required for the protection of information assets, promoting their proper treatment and seeking to reduce exposure to the risk of leakage or loss. This is based on the guidelines of the codes of Ethics and Good Governance of the Company.

## 2. GENERAL CONDITIONS

### 2.1 Scope

These guidelines apply to Ecopetrol S.A. and contractors who have access to Ecopetrol information. For the companies of the Business Group, this manual can be taken as a reference.

### 2.2 Terms and definitions

**Computer Crime:** cybercrime or cybercrime is any unlawful action that is carried out in the digital environment, digital space or the Internet. In view of the widespread use and utilization of new technologies in all spheres of life (economy, culture, industry, science, education, information, communication, etc.) and the growing number of users, as a result of the digital globalization of society, crime has also expanded to this dimension.

**Encryption:** Encryption is a method of protecting data that involves altering data until it is unreadable. Data is converted from plaintext to ciphertext using a method called an algorithm. Whoever wants to access the encrypted data must first decode it with the correct decryption key.

**Data Lost Prevention:** DLP or data loss prevention is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.

<https://ecopetrol.sharepoint.com/teams/gentepila/glosariocorpo/SitePages/Glosario.aspx>.

### 2.3 Associated documents


#### 2.3.a Normative references

##### Internal:

- Circular responsibility in the use of information.
- Manual for the processing of personal data at Ecopetrol S.A.
- Security guide for computer systems and services.
- Guide to the proper use of email.
- Operation Guide for Functional Leaders and/or Executors of Information Systems Controls.

##### External:

- Political Constitution of Colombia of 1991, Article 15.
- Law 1581 of 2012, "By which general provisions for the protection of personal data are issued".

	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

- Law 1712 of March 6, 2014, Law on Transparency and the Right of Access to National Public Information.
- Law 1915 of July 12, 2018, Copyright and Intellectual Property Law
- Article 269F of Law 1273 of 2009, Computer Crimes.
- Article 34, paragraph 5 of Law 734 of 2002 Single Disciplinary Code for Public Servants.
- Decree 1008 on Digital Government Policy
- Sarbanes-Oxley Act of 2002 – Section 404
- Resolution 500 of 2021, establishes the guidelines and standards for the digital security strategy.
- Law 1952 of 2019 - General Disciplinary Code
- Law 527 of 1999 - Electronic Commerce and Data Messages
- Law 599 of 2000 - Colombian Penal Code

### 3. DEVELOPMENT

#### 3.1 Information Security Components


##### 3.1.a People

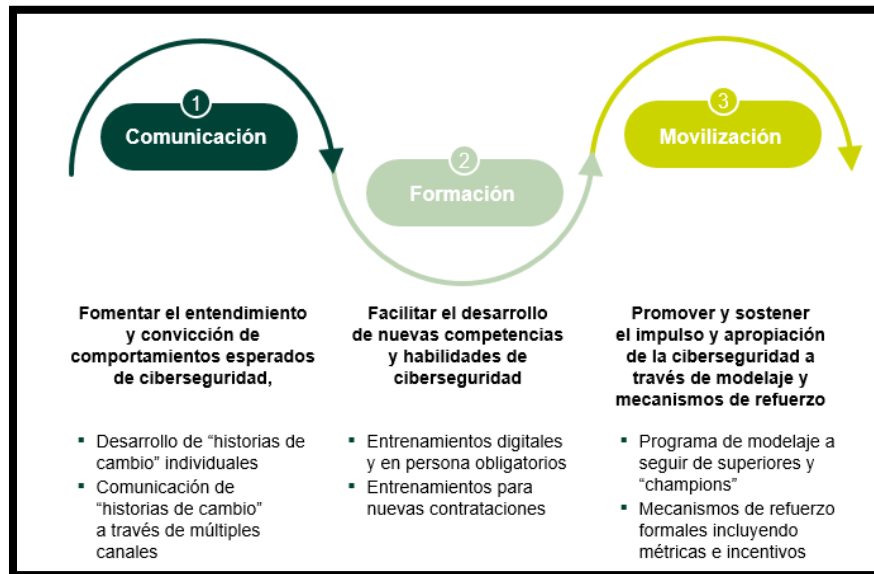
People and their behaviors regarding the processing of information are a critical factor in preserving its confidentiality, integrity and availability.

The information security model at Ecopetrol S.A. works with people to raise awareness and internalize practices and behaviors for the protection and assurance of information.

Employees, collaborators, contractors, allies, suppliers, interest groups, subsidiaries and associates must remain informed and sensitive to adopt behaviors that protect information, in such a way as to minimize the risks of leakage or loss of information. These behaviors are of two types: the first is habits, that is, the "mechanical" actions that are executed to protect the Information (for example: blocking the computer session when absent from the workplace); and the second type refers to behaviors that require a level of prior knowledge to execute it (for example: knowing the process of making backups).

The program of awareness and appropriation of practices has been developed through the three dimensions of the appropriation model of Ecopetrol S.A.

	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>



**Illustration 1 - Ecopetrol S.A. appropriation model**

### 3.1.b Technology

Ecopetrol S.A. has a series of tools focused on reducing or mitigating the risk of leakage and/or loss of information, therefore, depending on the risk analysis carried out on the critical information units, tools are installed to mitigate risks:

- Hard Drive Encryption
- File encryption
- Antivirus on computers and mobiles
- Data Lost Prevention Tools
- Content Control
- Other


### 3.1.c Processes

#### 3.1.c.1. Secure Information Management Cycle

Information is an asset that has critical value and as such must be disclosed and protected within the parameters established in the political constitution and the law.

Information related to the company's business activities must be classified according to its confidentiality basis, processed by the persons in charge of the company and deleted when it has served its purpose; the foregoing allows establishing mechanisms for the protection of the Information against loss, destruction, unauthorized disclosure, in accordance with legal and business requirements.

The Information is stored, presented and transferred in different media:

	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

Medium	Examples
Physics	Printed documents
	Research Records
	Photographs
	Books
Electronics	Mobile devices
	Computer equipment
	USB and external drive
	Videos
	Images
	Email messages
	Files in different formats such as Documents, electronic sheets or presentations
	Cloud Storage Services
	Instant messaging services
	Artificial intelligence systems
Other media	Social Media
	Knowledge of officials and contractors
	Conversations
	Work meetings

**Table 1 - Certain means by which Information may be presented, stored, or transferred**


Next, the cycle of secure management of the Information of Ecopetrol S.A. is diagrammed, which allows to guide the proper management of the Information.



**Illustration 2 - Secure Information Management Cycle of Ecopetrol S.A**

Information goes through different stages from the moment it is generated or acquired, to the moment of its final disposal. It is important that, regardless of the medium in which it is found, the information must be properly treated and protected.

For Ecopetrol S.A., the Secure Information Management Cycle is established taking into account the following stages:


	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

- a) **Classification:** Ecopetrol S.A. adopts the confidentiality basis for classification. To develop this stage, two activities must be carried out as follows:
  - a. Identification of the Information Units: It consists of listing the Information Units of the selected Process according to a defined source.
  - b. Information Classification: It consists of applying the criteria defined in this manual to assess the previously identified units.
- b) **Risk Analysis:** It consists of the identification of the level of exposure to the risk of Leakage or Loss of Information using Ecopetrol S.A.'s risk analysis methodology. and formulate the treatment actions required for risk mitigation.
- c) **Treatment:** Ecopetrol S.A.'s Information must be duly protected from unauthorized access, modification, transmission or final disposal, regardless of the medium in which it is found; processing actions must be defined to manage the Information at the following times: Labeling, Access, Transport, Storage and Secure Final Disposal. See paragraph 5.1.b.1.2. - Processing of the Information in this manual.
- d) **Implementation of the treatment plan:** It consists of implementing the general actions defined in the treatment plan. This implementation is the responsibility of the area that owns the Information and must follow a previously established schedule where the responsible parties and the start and end dates are identified.
- e) **Monitoring:** It consists of the subsequent measurement of the effectiveness and sustainability of the actions of the mitigation plan implemented.

During the execution of the secure management cycle, there are different roles that intervene in the specific activities that make up each stage. The responsibilities of each role in relation to these activities have been set out in a RACI matrix described in Table 2 and the description of each role is mentioned below:

**Responsible for the Information:** The person responsible for the Information is established as the executive or owner of the process where it was generated, obtained, acquired, transformed or controlled, either through officials of Ecopetrol S.A. or by contractor personnel who support the process. Your responsibilities with respect to information are:

- Its responsibility is to control the generation, classification, processing and adequate protection of the Information.
- Classify and periodically review the Information, following the defined guidelines and establish treatment plans in accordance with said Information.
- Manage and process the Information according to its rating, value and criticality.
- Establish the users within its area who may have access to the Information and the privileges for its Processing, as well as periodically verify the access restrictions and qualification levels of the Information, in line with the Information Security and Privacy regulations of Ecopetrol S.A.
- Ensure the filing of the Document containing the qualified Information in accordance with current documentary standards.
- Ensure that risk management actions are complied with, to preserve the confidentiality, integrity and availability of the Information.
- Maintain and periodically review the effectiveness of the appropriate security measures in accordance with current regulations for the protection of physical and electronic Information.

	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

**User of the Information:** It is the official of Ecopetrol S.A. or the natural or legal person contractor who has been authorized by the Responsible for the Information to Process the same. Such Processing must be carried out in accordance with the powers expressly defined by the Information Controller.

The User of the Information is responsible for:

- Know the criteria for rating the Information according to the parameters defined in item 5.1.b.1.1 Classification of Information.
- Support the Information Owners in determining the protection requirements and control mechanisms of each rating category.
- To treat it preserving its qualification, in accordance with contractual or legal obligations and/or functions.
- Ensure its use in accordance with the Confidentiality Basis and take the necessary actions to maintain it at the level at which it has been rated.

**Custodian of Information:** It is the area of Ecopetrol S.A. that has the archiving and surveillance of the information generated by the areas that may be in physical or digital media.

Both the person responsible, the User, and the Information Custodian must be attentive to identify and report any breach of the Information Security standards and procedures established by the entity.


**Legal Advisor:** It is the official of Ecopetrol S.A. or person authorized to issue the concept by which the motivation of the classified and/or reserved Information is constitutionally or legally based.

**Cybersecurity and Cyber Defense Manager:** This is the Ecopetrol S.A. official who leads and defines together with his work team the guidelines, guidelines, procedures and guides that stipulate the proper treatment of Information in Ecopetrol S.A. in compliance with the rules and laws that apply.

**Liaison professionals:** Contacts of the areas that support the identification, assessment and implementation of the defined treatment plan.

	Activity	Information Controller	User of the information	Custodian of information	Legal	Cybersecurity and Cyber Defense Manager	Liaison professionals
Classification	Define and disclose guidelines related to managing the risk of leakage or loss of critical information	I				A, R	
	Information Classification Training	I	I	I	I	A, R	R
	Identification and listing of Information Units	R, A	C, I	C, I	I	C, I	R
	Classify the units of information	R, A	C, I	C, I	I	C, I	R
	Verify the motivation and issue a legal concept, if applicable	To	C, I	C, I	R	I, R	
	Formalize the information units to the Vice-Presidency of	R					R



	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

	Activity	Information Controller	User of the information	Custodian of information	Legal	Cybersecurity and Cyber Defense Manager	Liaison professionals
	Science, Technology and Innovation						
Treatment	Preparation of Standard Treatment Plan	C, A	C	C		I, R	
	Validation and approval of the proposed Treatment Plan	R, A	I	I		I, C	R
	Standard Treatment Plan Execution	A, R	R	R		I, R	R
Risk Analysis	Provide verbal or written information requested for the preparation of the risk analysis	A, R	C	C		I	R
	Document and execute risk analysis	To	I, C	I, C		C, R	
	Develop mitigation plan in accordance with the risk analysis and initial standard activities and incorporate them into the report	C, I	I	I		A, R	R
	Formalize the final risk analysis report and treatment plan.	R	C	C		A, I	R
Treatment Plan Implementation	Execute mitigation plan	A, R	R	I		I, R	R
	Monitoring of the mitigation plan and work plan	To	I	I		I, R	
Follow-up	Planning for follow-up	I, C	I, C	I, C		A, R	R
	Running the Follow-Up	C, I, A	I, C	I, C		I, R	R
	Preparation and delivery of follow-up results	I	I	I		A, R	R


**Table 2 - Matrix of Roles and Responsibilities in the Secure Information Management Cycle**

### 3.1.c.1.1. Information classification

Information security consists of the preservation of the following criteria of the information that is managed in the systems and processes involved in its processing and in charge of the people who operate them within Ecopetrol S.A., whether they are officials or contractors. The information security triad is described below:

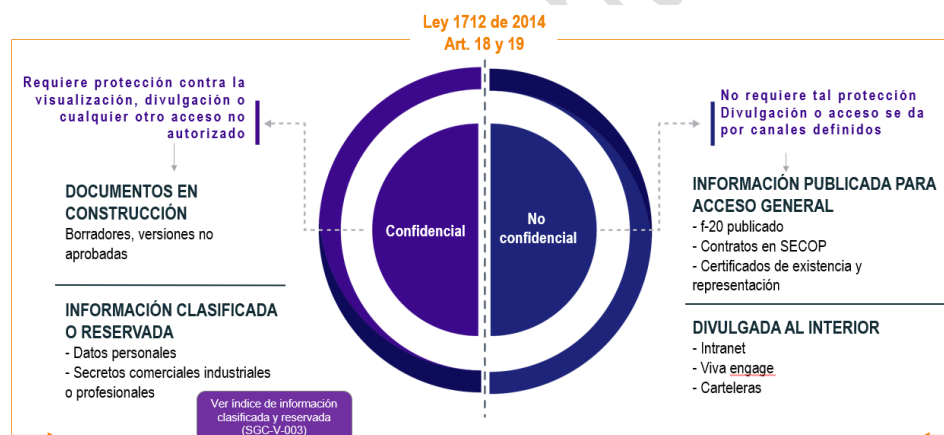
- **Confidentiality:** It consists of protecting information against viewing, disclosure or any other unauthorized access. Confidential information must be protected by means of suitable mechanisms of processes, people and tools (technological or other applicable to physical media). Its access must be limited, enabling it only to those individuals who actually need that information to perform their tasks ("need to know basis"). If confidentiality is affected (for example, through unauthorized disclosure or access), it can have negative impacts on the company.



	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

- **Integrity:** Ecopetrol S.A.'s Information must be accurate, consistent and complete from its creation to its final disposition and may only be modified by persons expressly authorized to do so. The lack of integrity of the Information can expose the Company to incorrect decision-making and cause failures in processes, financial losses or damage to the image.
- **Availability:** The information must be available at the time, in the medium and format that is required, as well as the resources necessary for its use. The non-availability of the Information may result in failures in the processes, financial losses and image of the Company.

The categorization of information is carried out under a confidentiality approach. When categorizing the information in its charge, **each area separates confidential information from that which is not**, for this purpose, Ecopetrol S.A. has been using as a guiding criterion the one provided for in the Law on Transparency and Access to Information<sup>1</sup>. This regulation defines that entities may deny access that may be requested to **classified and reserved**<sup>2</sup> information and **documents under construction**<sup>3</sup>. In addition, the Constitutional Court specified that, in the case of companies in which the State has a stake, "... in relation to their own activity, industrial or commercial, they are not in a duty to provide information with respect to said activity."<sup>4</sup>. Therefore, the categorization of information that each of the areas makes with respect to the information in their charge is the starting point for protecting confidential information.



**Illustration 3 - Classification or categorization of information**

### 3.1.c.1.1.1. Non-Confidential Information


There are multiple reasons why certain Ecopetrol information is intended to be public and therefore its nature is opposite to that of what is considered confidential.

<sup>1</sup> Law 1712 of 2014 or that which modifies or replaces it.

<sup>2</sup> Law 1712 of 2014, Articles 6 (letters c, d and e), 18 and 19

<sup>3</sup> "Document under construction: Preliminary and non-definitive information, typical of the deliberative process (sic) of an obligated subject in its capacity as such, will not be considered public information." Law 1712 of 2014, Article 6 (literal k).

<sup>4</sup> Judgment C-734 of 2013, paragraph five of the operative part

	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

- These may include regulatory obligations derived from its nature as a mixed economy company. For example, aspects of transparency and access to public information about the entity (e.g., the entity's website), contracting aspects (e.g., SECOP, when applicable), regulatory aspects applicable to the entity's activity (e.g., advertising rules of the National Hydrocarbons Agency or other entities), among others.
- Other mandatory aspects may arise from its status as an issuer of securities, in Colombia or on the New York Stock Exchange. This includes, for example, financial reporting (e.g. F20) or disclosure of relevant information.
- Likewise, there is information specific to the company's operations or initiatives, which is intended to be known by different stakeholders. For example, calls for the Ecopetrol Bachelor's program, open innovation challenges, among others.
- There is information that is part of the company's communications strategy or other announcements aimed at the public, on its website, its social networks, among others.

Although the information is intended to be public, its dissemination must be carried out through the channels defined for this purpose, according to the respective process. By way of illustration, there is the **Procedure for Disclosure of Relevant and Non-Relevant Information**, the **Ecopetrol Group's Corporate Guide for Communications Management** or some rules of the procurement process on the publication of **the Electronic System for Public Procurement**. Therefore, until the area in charge authorizes and/or makes the respective publication, these are documents under construction.

a) Public or published information for general access


There is information that by law is public or rests on publicly accessible sources. For example, the identification data of the company and its representatives can be found in the company's certificate of existence and representation, which is administered by the Chamber of Commerce. The Transparency Law defines "publish or disclose" as "making available in a form of general access to members of the public and includes printing, broadcasting, and electronic forms of dissemination."

In the event of a request for access to information that is available in open access sources (whose publication has been authorized by the competent area), the area in charge may indicate that the information is already public and indicate to the requester how to access it (e.g., by providing the respective link, when applicable).

b) Information Disclosed Within the Company

Table 3 outlines some examples of information disclosed within the company. To these can be added information on physical billboards, information presented in talks or training, face-to-face or virtual, among other spaces with a vocation for internal dissemination.

- Even if it is non-confidential information, the open and indiscriminate distribution of the content is not enabled.
- Please note that there may be aspects of communications, image, rights of disclosure, among other aspects that are pertinent.

	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

- The scope of disclosure of the information is defined by the areas in charge of communications or the respective information, so they are the ones who determine whether it can be published externally.

#### 3.1.c.1.1.2. Confidential Information

As indicated above, categorizing information as confidential requires having the respective support.

##### a) Documents under construction

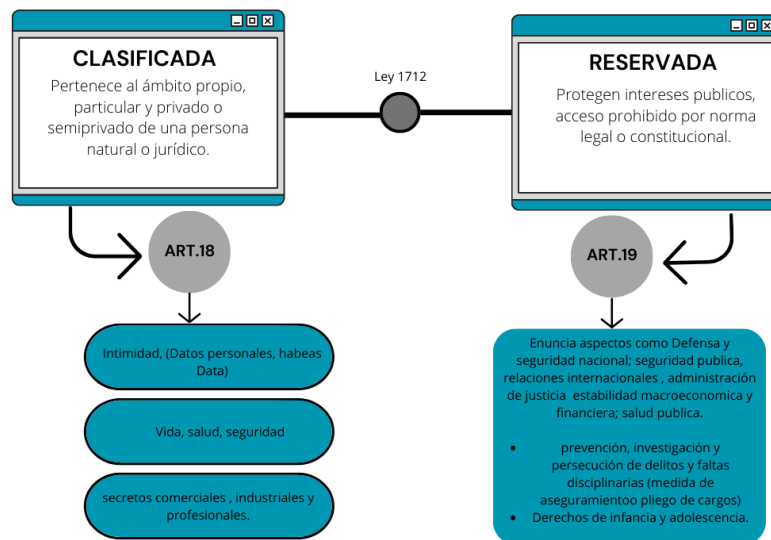
There it was stated, for example, that the Transparency Law states that documents under construction are not considered public information. Unless the area in charge authorizes the publication or sharing of them, they may invoke this legal basis to protect the confidentiality of such information, for example, in the face of access requests or disclosure initiatives (See Table 3).


##### b) Classified or reserved information

The Transparency Law allows the protection of classified or reserved information. As stated, their access may be denied in a reasoned manner, under the grounds provided for in those regulations. On this basis, the areas have constructed the **index of classified and reserved information** outlined in this document. There, the areas indicate the normative provisions that support this categorization of information.

Therefore, based on the law and supported by the practical reference of said index or other document management instruments, the area in charge of the respective information can support the confidential nature of the information that corresponds to these categories.

**El artículo 6 de la ley de transparencia prevee dos excepciones al acceso a la información pública en poder o custodia de un sujeto obligado.**



	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

#### Illustration 4 - Classified or reserved information, according to the Transparency Law

In the case, for example, of the protection of the right to privacy, the rules highlight that access to personal data requires authorization from the owner of the information or that one of the exceptions enshrined in Articles 6 and 10 of Law 1581 of 2012 occurs. In the same sense, there is information associated with the protection of information classified by its commercial, industrial or professional nature. In the same way, it was noted above that the Constitutional Court (Judgment C-734 of 2013) defined details to the scope of advertising in entities with state participation, dealing with issues associated with their own, industrial or commercial activity.

Given the multiplicity of document types and processes that are managed within Ecopetrol, each area is responsible for categorizing the information that corresponds to these categories. Depending on the particularities of each topic, in some cases it will be called, for example, privileged information, with a basis for the relevant financial regime. In others, it is, for example, a matter of confidentiality of medical records. In disciplinary proceedings, the corresponding procedural reserve. Each area, from the domain of the subject in charge, supports confidentiality to categorize the information in its charge and protect it appropriately.

#### 3.1.c.1.1.3. Information classification guidelines


- When categorizing information, the area in charge must establish whether or not the information is confidential.
- If it is, the area must make the analysis and have the respective support.
- The index of Classified and Reserved Information and other associated document management elements are references that the areas must keep updated. Therefore, they are reference points for consultation when categorizing certain information.
- Given the wide variety of topics and types of information managed by Ecopetrol, the analysis of each area is decisive, in light of the rules that govern its activities and processes. These may even involve temporal aspects when they are decisive for confidentiality.

Theoretical scenario	Temporal aspect	Confidentiality support
Information that is intended to be public (e.g. communication or text of relevant information)	Assume that the document is in the process of being prepared and internally validated (draft)	Document under construction Law 1712 of 2014, Article 6 (literal k).

**Table 3 - Document under construction is Confidential**

- There is information about the company that, by regulatory provision or decision of the company, is intended to be disclosed.
- When analyzing whether or not the information is confidential, validate whether it is public information (or that it should be of that nature) or if it is already published for general access.
- The publication and form of disclosure of information must be authorized following the rules that apply (see, for example, the **Procedure for Disclosure of Relevant and Non-Relevant Information**).
- To classify information in digital media, the classification and labeling tools defined by the organization (confidentiality - sensitivity) provided in the Office 365 suite must be used, as follows:

#### a) Non-Confidential Information:

	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

**Tag:** ECP-NON-CONFIDENTIAL

**Subtag:** ECP – public (Public information or published for general access)

**Sublabel:** ECP – Internal Disclosure (Information Disclosed Within the Company)

b) Confidential Information

**Tag:** ECP - Confidential

**Sublabel:** ECP information under construction

**Sublabel:** ECP classified and/or reserved information



**Illustration 5 - Classification and labelling of digital media information**

#### 3.1.c.1.1.4. Email Classification Guidelines


- For e-mail messages, these must include at the bottom, after signing, the legends (automatic disclaimers) in both Spanish and English described in the guide for the proper use of e-mail
- For email messages, these must be labeled according to the confidentiality assessment.
- When high-security transmission channels are needed, the secure file transfer tool provided by the organization should be used

#### 3.1.c.1.2. Information processing

The processing of Information refers to the activities that people carry out with the Information. Some of these actions, but not limited to, are: Labeling, Access, Storage, Distribution, Transmission and Final Disposal, which will be discussed below, in accordance with the level of confidentiality defined by Ecopetrol S.A.

##### 3.1.c.1.2.1. Labeling the information

As a result of the qualification of the Information, the area/process gives a high level of confidentiality, the labeling of the Information must be carried out as follows:

	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

- **For paper documents**, they will be labeled "CONFIDENTIAL" or "NOT CONFIDENTIAL" and may be stamped or marked with ink that cannot be easily erased on the upper central margin of the sheet; for cases where the document has more than one sheet, the total number of pages that compose it must be specified. the last blank page will also be marked if applicable.


When the documents contain information related to the privacy, health or safety of people, classified as "CONFIDENTIAL" they may be labeled as "PERSONAL DATA".

- **For electronic documents** they must be labeled with the corresponding degree of confidentiality which will automatically assign a watermark or footer. There must be no uncontrolled copies of documents classified as "CONFIDENTIAL" information.
- **For storage devices** such as CDs, DVDs, among others, that require to be marked with some type of indelible ink, the title of the information it contains and the label "CONFIDENTIAL" or "NOT CONFIDENTIAL", as the case may be, must be placed.

#### 3.1.c.1.2.2. Access to Electronic and Physical Information

- Persons who access "CONFIDENTIAL" Information must have the authorization of the person responsible for the Information.
- Officials or collaborators who treat the Information that is "CONFIDENTIAL" must have confidentiality agreements in force.
- Access to Information that has been classified and labeled as: "CONFIDENTIAL", must be limited to those officials or third parties duly authorized by the Company to comply with their labor and/or contractual responsibilities.
- The leader of the area/process must request from whoever manages the sites and periodically (according to the needs of the area or at least every three months) a list of the users who have permission to the folders where "CONFIDENTIAL" Information is stored and thus validate against the allowed users and notify the service if there is any modification to keep it updated. Additionally, other corporate sites and applications, such as SharePoint, OpenTex, among others, should be verified.
- For access to the information recorded in the information systems and processes, the provisions of the documents must be followed, in particular the guidelines, responsibilities and control practices:
  - Guide for Integrated Risk Management in the Ecopetrol Group
  - Operation Guide for Functional Leaders and/or Executors of Information Systems Controls.
  - Guide to Segregation of Duties Management in Information Systems
- The consultation and loan of documents and file files generated (regardless of whether it is electronic or physical) in the areas/processes filed and kept in the Management Archives and in the Central Archive of Ecopetrol S.A., must follow the guidelines of the "Instructions for the consultation and loan of documents and files".



	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

- For access to the Management and Central Archive files, the persons authorized to access the "CONFIDENTIAL" Information and comply with the Document Management regulations must be verified.

#### 3.1.c.1.2.3. Identification and securing of electronic sheets


- Electronic sheets with "CONFIDENTIAL" information or with personal information that have or do not have an impact on financial reports (SOX and non-SOX) must be treated in accordance with the **"Instructions for the identification and assurance of electronic sheets with an impact on financial reporting", in chapter 3.3.2. Control activities on electronic sheets.** Considering the key controls mentioned below:
  - ✓ The owner of the process, owner of the sheet and/or person designated by the owner of the process, must determine an official repository where they store the electronic sheets (sharepoint/teams/others).
  - ✓ Organize the electronic sheets in a repository structure with restricted access to people who, due to their functions, require it (reading, creating, modifying).
  - ✓ Quarterly review the users with access to the electronic sheets and defined repository, to corroborate that only authorized users have access, otherwise you must request the correction of the identified exceptions.
  - ✓ Protect the formulated cells of the electronic sheet in order to prevent unauthorized modification of the information contained therein
- For electronic sheets that contain or manage personal information, the risk analysis of information flows must be carried out in accordance with the document **Instructions for the preparation of risk analysis of information flows** and validate the relevance of their report to the SIC<sup>5</sup>.

#### 3.1.c.1.2.4. Storage of Electronic and Physical Information

- The electronic information of a "CONFIDENTIAL" nature in each area/process must be kept in the corporate repositories designated by the Company for this purpose and the Information Controller must periodically review and update the permissions to said repositories.
- In the event that the physical information needs to be transferred to the custody of the Archive service, each owner must take into account the criteria defined in the Document Retention Tables (TRD) of the corresponding agency, available in the official repository, as well as the permissions for its access.

<sup>5</sup> Superintendence of Industry and Commerce



	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

#### 3.1.c.1.2.5. Distribution and Transmission of Information

- The Data Controller, in the event of distributing and/or transmitting Information, must send it duly labeled or labeled and informing its recipient of the treatment that this level of confidentiality requires.
- When "CONFIDENTIAL" matters are discussed in meetings between officials or between officials and third parties, it must be done taking into account secure means of communication authorized by the Company.
- In the event of sharing "CONFIDENTIAL" Information with a third party, the legal support of the area must be consulted beforehand to clarify contractual issues and the scope of applicable laws.
- For cases in which it is required to SHARE INFORMATION (regardless of the format) "CONFIDENTIAL", the collaborative and secure tools provided by the organization must be used.

#### 3.1.c.1.2.6. Final and secure disposal of information

- To delete "CONFIDENTIAL" Information, written authorization must be obtained from the head of the area to which the Information Controller belongs. The disposal process depends on the storage medium in which it is located (printed or digital).
- The final disposition must be in accordance with document retention tables and their corresponding procedures.

### 3.1.c.1.3. Risk analysis

It consists of identifying the level of exposure to the risk of cyberattacks and leakage or loss of information using Ecopetrol S.A.'s risk analysis methodology,<sup>6</sup> and formulate the treatment actions required for risk mitigation. During this stage, the treatment plan that brings together the required actions as a result of said risk analysis and the initial actions proposed in accordance with the analysis carried out during the treatment stage must be completely defined.

### 3.1.c.1.4. Treatment Plan Implementation


It consists of implementing the general actions defined in the treatment plan. This implementation is the responsibility of the area that owns the Information and must follow a previously established schedule where the responsible parties and the start and end dates are identified.

### 3.1.c.1.5. Follow-up

It consists of verifying compliance with the actions of the defined treatment plan and generating alerts if required.

## 3.2 Responsibilities of Users with regard to information and technological resources

<sup>6</sup> Strategic Risk Assessment Matrix - ECP-UGR-F-008

	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

Information security technologies are articulated with business architectures and fulfill their life cycle, implementation, operation, maintenance and output, in accordance with the strategy established by the Cybersecurity and Cyber Defense Management.

### 3.2.a Responsibilities of users with regard to information and technological resources

The protection of Ecopetrol S.A. Information identified as "CONFIDENTIAL" is the responsibility of the officials or contractors who, during their position, have access to it or have it under their care.

#### 3.2.a.1. Technical-Scientific Publications

In order to carry out technical-scientific publications, the provisions of the current technical-scientific publication procedure must be complied with, these must have the endorsement of the technical authority and the manager of the area corresponding to their role before their dissemination.

#### 3.2.a.2. Copyright


Ecopetrol S.A. protects and exalts Copyright both for printed works and for the protection of the Software used by its officers and contractors. Therefore, without prejudice to the regulatory obligations on copyright protection, the following are the guidelines in relation to copyright:

1. Use only properly licensed software.
2. In presentations, documents, reports and other documents used by officials and/or contractors for the work of their position, the source from which the information was extracted must be mentioned.
3. Refrain from making partial or total copies of books, articles, reports and other documents; that are not permitted by copyright law.
4. The Information of Ecopetrol S.A. is the property of the Entity, therefore, it may not be used for any purpose other than that established and required in the execution of the tasks corresponding to its charge. Therefore, it may not be used as a source of information for promotional, commercial, among other issues.

## 3.3 Legal Liability and Consequences

Because the improper use of Ecopetrol S.A.'s resources may cause the leakage or loss of sensitive information of the entity and this is considered an asset of the company; its impact on integrity, availability or confidentiality may be considered as a fraud event, which entails consequences for the Entity and for the persons involved in the event.

Failure to comply with this manual may be subject to sanctions that may reach the termination of the employment contract in the case of workers, without prejudice to the legal actions (criminal, disciplinary, civil) that may be appropriate, according to applicable laws in force. In the case of suppliers, the clauses established in the contracts that mediate their relationship with Ecopetrol S.A. apply.

	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

#### 4. CONTINGENCIES


N/A

#### 5. ANNEXES

N/A

#### VERSION LIST

Previous Document			
Version	Date dd/mm/yyyy	Document Code and Title	Changes
1	14/04/2011	ECP-DTI-M-067 Secure Information Management Manual	Incorporated into the information security manual.
1	01/04/2012	PDO-G-001 Guide to the proper use of social networks	Incorporated into the information security manual.
2	31/05/2012	PDO-G-002 Mobile Device Liability Guide	Incorporated into the information security manual.
2	09/10/2014	IDO-G-016 Guide for the classification of Ecopetrol S.A.'s information according to its level of treatment.	Incorporated into the information security manual.
1	28/05/2015	PDO-I-028 Instructions for Protecting Ecopetrol S.A.'s Information	Incorporated into the information security manual.
1	07/09/2015	PDO-G-005 Guide to the responsibility of users in the access and use of information and computer resources of Ecopetrol S.A.	Incorporated into the information security manual.
1	12/05/2016	PDO-M-011 Information Security Manual	First version of the document
1	29/09/2023	SGY-M-002 - INFORMATION SECURITY MANUAL	New Document
1	01/07/2020	SSI-M-00X - INFORMATION SECURITY MANUAL Code Update Adjustment to the new GCY Management structure Updating of terms and technologies referred to The ECP Wi-Fi Visitor Connection Policy was included The numeral 3.3.g of "use of external storage media" was eliminated, because it was included in the SGY-G-002 guide	

	<b>Information Security Handbook</b>		
	<b>Vice-Presidency of Science, Technology and Innovation Cybersecurity and Cyber Defense Management</b>		
	<b>CODE CTI-M-005</b>	<b>Elaborated 06/12/2024</b>	<b>Version: 6</b>

1	17/11/2023	SGY-M-002 - INFORMATION SECURITY MANUAL Code Update Adjustment to the new GCY Management structure Updating of terms and technologies referred to The ECP Wi-Fi Visitor Connection Policy was included The numeral 3.3.g of "use of external storage media" was eliminated, because it was included in the SGY-G-002 guide Numeral 5.1.b.2.3 Distribution and Transmission of Information was included the classification and labeling tools in Office 365 Change of coding and management system.
<b>New Document</b>		
<b>Version</b>	<b>Date dd/mm/yyyy</b>	<b>Changes</b>
2	20/06/2024	Update of the chapter on classification of information and adjustment in guidelines, inclusion of guidelines for non-SOX electronic sheets
3	20/06/2024	Inclusion of non-SOX electronic sheet guidelines validated with administrative management
4	31/07/2024	Update on Tag Taxonomy
5	08/11/2024	Update of chapter 3.1.c.1.2.3 Identification and securing of electronic sheets
6	06/12/2024	Update of the Confidentiality Label of this document.

<b>For more information on this document, please contact the person who prepared it, on behalf of the responsible agency:</b>	
<b>Prepared by:</b> Daliris Milena Maldonado <b>Mailbox:</b> <a href="mailto:daliris.maldonado@ecopetrol.com.co">daliris.maldonado@ecopetrol.com.co</a> <b>Dependency:</b> Vice-Presidency of Science, Technology and Innovation	
<b>Reviewed</b>	<b>Approved</b>
<b>ERICA ALEXANDRA REINA CEBALLOS</b> Cybersecurity Professional <b>Registration No. E0287174</b> Vice-Presidency of Science, Technology and Innovation	<b>ELKIN FERNEY QUINTERO GOMEZ</b> Cybersecurity and Cyber Defense Manager <b>Registration No. E0307304</b> Vice-Presidency of Science, Technology and Innovation

Electronically signed document, in accordance with the provisions of **Decree 2364 of 2012**, which regulates Article 7 of Law 527 of 1999, on electronic signatures and other provisions are issued.  
To verify compliance with this mechanism, the system generates an **electronic report that shows the traceability of the review and approval actions by those responsible**. If you need to verify this information, request such a report from Service Desk.