PERSONAL DATA PROCESSING POLICY

1. OBJECTIVE

This **Personal Data Processing Policy** (hereinafter the "Policy") aims to regulate the collection, storage, use, circulation and deletion of personal data in **PROQUIMES S.A. Productos Químicos Especializados SA** (hereinafter "**PROQUIMES S.A.**"), providing tools that guarantee the authenticity, confidentiality and integrity of the information.

The Policy is structured following the mandates of the statutory law 1581 of 2012, decrees and other regulations that complement, modify or repeal it.

2. SCOPE

The **PROQUIMES S.A. Policy** covers all the administrative, organizational and control aspects that must be fulfilled by the directors, officials, contractors and third parties that work or have a direct relationship with the Company.

This policy is an integral part of **Plan de manejo de la información PC-GC-001** and have involved the procedures establish in **Gestión de la información PD-GC-002** and **Copia de la seguridad de la información PD-GC-005**.

3. REGULATORY FRAMEWORK OF THE POLICY

- Law 1581 of 2012 through which the General Regime for the Protection of Personal Data was issued.
- Decrees and external circulars that regulate the norm indicated in the previous numeral.
- Constitutional Judgment C-748 of 2011 by means of which the Statutory Law Project for the Protection of Personal Data was declared enforceable.

4. POLICY DEVELOPMENT

PROQUIMES S.A. incorporates respect for the protection of personal data in all its actions. Consequently, it will request from the data entry, authorization for the use of the information it receives for the purposes of its missionary purpose.

PROQUIMES S.A. respects the principles established by law and will attend to the purposes derived from the collection of personal data in its actions and management of personal data.

PROQUIMES S.A. will implement the necessary strategies and actions to give effect to the right enshrined in Statutory Law 1581 of 2012 and other regulations that complement, modify or repeal it.

PROQUIMES S.A. will inform all its users of the rights derived from the protection of personal data.

5. STRATEGIES

5.1 DATA PROCESSING

For the proper processing and protection of personal data, **PROQUIMES S.A.** will supervise the management of these in 3 areas through those responsible for the data that will develop activities in accordance with this policy that has the purpose of developing processes of use, treatment, collection and data protection in accordance with the provisions of Law 1581 of 2012 and other regulations that complement, modify or repeal it, these areas are:

Marketing Area.
Resources and human management area.
Purchasing and logistics area.

5.2 RESPONSIBLE FOR DATA PROCESSING

Those responsible for data processing will be the heads of each of the areas mentioned in numeral 5.1 of this policy or whoever acts on their behalf, and the General Manager. These managers will be the ones who have access and treat the databases where the data collected from third parties by **PROQUIMES S.A.** is stored.

5.3 INFORMATION SECURITY COMMITTEE

The information security committee is appointed by minutes of the Board of Directors and will be made of up to 3 members who are in charge of data processing in the 3 respective areas.

The members of this committee are:

- General Manager
- Administrative and Marketing Director
- HHRR Assistant

The members of this committee will give instructions to the person who is appointed as Information Security Officer.

5.4 INFORMATION SECURITY OFFICER

The information security officer will be chosen by the members of the information security committee. This will ensure compliance with this policy in the activities of the organization and will be in charge of training and disseminating it. This committee will make decisions regarding the updating, modification, application and implementation of this policy as a whole.

The position of Marketing Assistant will have within their duties and scope those assigned as Information Security Officer

5.5 DISSEMINATION AND TRAINING

PROQUIMES S.A. will define the processes for dissemination and training of the content of this Policy through its Information Security Committee.

5.6 INTERNAL ORGANIZATION AND RISK MANAGEMENT

PROQUIMES S.A. will define any action related to the protection of personal data in its Information Security Committee. Within said Committee, the role of Personal Data Protection Officer has been defined, a role that will be within the functional powers of the current Information Security Officer.

6. DEFINITIONS

For the purposes of this document, the following terms and definitions apply:

Privacy Notice: Verbal or written communication generated by the person responsible for the processing of personal data, addressed to the Holder of said data, by which he is informed about the existence of the data processing policies that will be applicable to him, the way of access them and the purposes of the treatment that is intended to be given to personal data.

Authorization: Prior, express and informed consent of the owner of the personal data to carry out the processing of said data.

Databases: Organized set of personal data that is subject to Treatment.

Personal Data: Any information linked or that can be associated to one or several determined or determinable natural persons. “Personal data” must then be understood as information related to a natural person (person individually considered).

Public Data: It is the data that is not semi-private, private or sensitive. Public data is considered, among others, the data related to the marital status of people, their profession or trade and their quality as merchant or public servant. Due to its nature, public data may be contained, among others, in public records, public documents, gazettes and official bulletins, and duly executed judicial sentences that are not subject to confidentiality.

Sensitive Data: Corresponds to that data that affects the privacy of the Owner or whose improper use can generate discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership of unions, social organizations , human rights or that promotes the interests of any political party or that guarantees the rights and guarantees of opposition political parties as well as data related to health, sexual life and biometric data.

Data Processor: Natural or legal person, public or private, that by itself or in association with others, performs the processing of personal data on behalf of the controller.

Responsible for the Data Processing: Natural or legal person, public or private, that by itself or in association with others, decides on the database and/or the Treatment of the data.

Owner: Natural person whose personal data is processed.

Transfer: The transfer of data takes place when the person in charge and/or in charge of the processing of personal data, located in Colombia, sends the information or personal data to a recipient, who in turn is responsible for the treatment and is located inside or outside from the country.

Transmission: Processing of personal data that implies the communication of these inside or outside the territory of the Republic of Colombia when its purpose is to carry out a treatment by the person in charge on behalf of the person in charge.

Data Processing: Any operation or set of operations on personal data, such as collection, storage, use, circulation or deletion.

Data Protection Officer: It is the role within **PROQUIMES S.A.**, whose function will be the surveillance and control of the Policy under the control of the Security Committee.

7. GUIDING PRINCIPLES

Principle of Legality in terms of Data Processing: Data processing is a regulated activity that must be subject to the provisions of the law and the other provisions that develop it.

Principle of Purpose: Data Processing must obey a legitimate purpose in accordance with the Political Constitution and the law, which must be informed to the Owner.

Principle of Freedom: Data Processing can only be exercised with the prior, express and informed consent of the Holder. Personal data may not be obtained or disclosed without prior authorization, or in the absence of a legal or judicial mandate that relieves consent.

Principle of Veracity or Quality: The information subject to Data Processing treatment must be truthful, complete, exact, updated, verifiable and understandable. The processing of partial, incomplete, fractional or misleading data is prohibited.

Principle of Transparency: In Data Processing, the right of the Holder to obtain from the person responsible for said treatment or the Manager, at any time and without restrictions, information about the existence of data that concerns him must be guaranteed.

Principle of Access and Restricted Circulation: Data Processing is subject to the limits that derive from the nature of the personal data and the constitutional and legal provisions. In this sense, the treatment can only be done by persons authorized by the Owner and/or by the persons provided for in the Law. Personal data, except for public information, may not be available on the Internet or other means of dissemination or mass communication, unless the access is technically controllable to provide knowledge restricted only to the Holders or authorized third parties in accordance with the aforementioned law.

Security Principle: The information subject to Data Processing by the responsible or person in charge referred to in the law must be handled with the technical, human and administrative measures that are necessary to grant security to the records, and avoid their adulteration, unauthorized or fraudulent loss, consultation, use or access.

Principle of Confidentiality: All persons involved in the processing of personal data that are not of a public nature are obliged to guarantee the confidentiality of the information, even after the end of their relationship with any of the tasks that comprise the treatment, and may only Provide or communicate personal data when it corresponds to the development of the activities authorized by the Law and in its terms.

8. SPECIAL CATEGORIES OF DATA

8.1 SENSITIVE PERSONAL DATA

Sensitive data are those data that affect the privacy of the owner or whose improper use may generate discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership of unions, social organizations, of human rights or that promotes the interests of any political party or that guarantees the rights and guarantees of opposition political parties, as well as data related to health, sexual life and biometric data.

PROQUIMES S.A. will restrict the processing of sensitive personal data to what is strictly essential and will request prior and express consent on the purpose of its processing.

8.2 PROCESSING OF SENSITIVE PERSONAL DATA

Data classified as sensitive may be used and processed when:

The Holder has given his express authorization to said treatment, except in cases where, by law, the granting of said authorization is not required.

The treatment is necessary to safeguard the vital interest of the Holder and he is physically or legally incapacitated. In these events, the legal representatives must grant their authorization.

The treatment refers to data that is necessary for the recognition, exercise or defense of a right in a judicial process.

The treatment has a historical, statistical or scientific purpose, or within the framework of improvement processes, as long as the measures leading to the suppression of the identity of the holders are adopted.

8.3 PERSONAL DATA OF CHILDREN AND ADOLESCENTS

Minors are the owners of their personal data and therefore are bearers of the corresponding rights. In accordance with the provisions of the Political Constitution and in accordance with the Code for Children and Adolescents, the rights of minors must be interpreted and applied in a prevailing manner. Therefore, they must be observed with special care. As stated in Ruling C-748 of 2011, the opinions of minors must be taken into account when processing their data.

PROQUIMES S.A. then undertakes, in the processing of personal data, to respect the prevailing rights of minors. The processing of personal data of minors is prohibited, except for those data that are of a public nature.

9. CLASSIFICATIONS OF INFORMATION AND DATABASES

The databases are classified as follows:

9.1 CONFIDENTIAL DATABASES:

They are databases or electronic files with confidential information which deals with the business model of **PROQUIMES S.A.** in the case of financial data, personnel databases, databases with sensitive information on managers, suppliers, formulas, investigations, processes, procedures and R&D projects. In general, reference is made to databases containing information related to the Know How and the operation of **PROQUIMES S.A.**

9.2 DATABASES WITH SENSITIVE INFORMATION:

These are the data that affect the privacy of the Holder or whose improper use can generate discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership of unions, social organizations, human rights or that promotes the interests of any political party or that guarantees the rights and guarantees of opposition political parties as well as data related to health, sexual life and biometric data. At **PROQUIMES S.A.**, access to this type of information is restricted and will only be known by an authorized group of officials.

9.3 DATABASES WITH PUBLIC INFORMATION:

They are the databases that contain public data classified as such according to the mandates of the law or the Political Constitution and that are not classified as semi-private, private or sensitive data. The data relating to the marital status of people, their profession or trade, their quality as a merchant or public servant and those that can be obtained without any reservation are public, among others. Due to its nature, public data may be contained, among others, in public registries, public documents, gazettes and official bulletins, duly executed judicial sentences that are not subject to reservation, social networks and publicly accessible websites.

10. OBLIGATIONS AND RIGHTS OF HOLDERS

The Holders of personal data have the following rights:

To access, to know, to update and to rectify your personal data against **PROQUIMES S.A.** in its capacity as data controller.

By any valid means, request the authorization granted to **PROQUIMES S.A.**, except for the cases in which the Law exempts the authorization.

Request information from **PROQUIMES S.A.**, upon request, regarding the use it has given to your personal data.

To Go to the legally constituted authorities, especially the Superintendence of Industry and Commerce (SIC) and present complaints for violations of the provisions of current regulations, prior to the consultation process or request before the person responsible for the treatment.

Modify and revoke the authorization and/or request the deletion of personal data when the current constitutional principles, rights and guarantees are not respected in the treatment.

To have knowledge and free access to your personal data that has been processed.

11. DUTIES OF PROQUIMES SA IN RELATION TO THE PROCESSING OF PERSONAL DATA

PROQUIMES S.A., will keep in mind that personal data is the property of the people to whom they refer and that only they can decide on them. **PROQUIMES S.A.** will use said data only for the activities of the ordinary course of the company within its corporate purpose and legal relations with its contractors, clients, employees and/or suppliers, subject in all cases to current regulations on the Protection of Personal Data. (Law 1581 of 2012 through which the General Regime for the Protection of Personal Data was issued.).

12. INFORMATION PROCESSING POLICIES

12.1 GENERAL INFORMATION ABOUT THE AUTHORIZATION

PROQUIMES S.A. will request authorization for the processing of personal data by any means that allows it to be used as evidence. Depending on the case, said authorization may be part of a broader document, such as a contract or a specific document for that purpose. In any case, the description of the purpose of data processing will also be reported through the same specific or attached document. **PROQUIMES S.A.** will inform the owner of the data, the following:

Specific request for the required data.
The treatment to which your personal data will be subjected and the purpose of this.

- Assist rights as Owner.
  Available channels for queries, requests and/or claims.

12.2 GUARANTEES OF THE RIGHT OF ACCESS

PROQUIMES S.A. will guarantee the right of access, prior accreditation of the identity of the owner, legitimacy, or personality of his representative, making available to him/her, without any cost or expense, in a detailed manner, the respective personal data.

12.3 INQUIRIES

The holders of the personal data or their successors in title may request the personal data that rests in the database of **PROQUIMES S.A.** Consequently, **PROQUIMES S.A.** will

guarantee the right of consultation, providing the Holders of personal data, all the information contained in the individual record or that is linked to the identification of the Holder.

Regarding the attention to requests for consultation of personal data, **PROQUIMES S.A.** guarantees:

Enable electronic means of communication or others that it considers pertinent.
Establish forms, systems and other methods.
Use the customer service or claims services that are in operation.

Regardless of the mechanism that is implemented for the attention of consultation requests, these will be attended to within a maximum term of ten (10) business days from the date of receipt. In the event that a query request cannot be answered within the term indicated above, the interested party will be informed before the expiration of the term of the reasons why no response to their query has been given, which, in no case may exceed five (5) business days following the expiration of the first term.

Queries made regarding personal data must be sent by email to the following address **protecciondedatos@proquimes-sa.com**.

12.4 CLAIMS

The Owner or his successors in title who consider that the information contained in a database must be corrected, updated or deleted, or when they notice the alleged breach of any of the duties contained in the Personal Data Protection regulations, may present a complaint to the data controller.

The claim must be submitted by the Owner of the personal data, filling out the Claim form for the Processing of Personal Data that may be requested by sending an email to the address **protecciondedatos@proquimes-sa.com**. In this format, the Holder must indicate if he wishes his data to be updated, rectified or deleted or if he wishes to revoke the authorization that had been granted for the processing of personal data. For the purposes of claims, the Holder must take into account the provisions of article 15 of law 1581 of 2012.

If the claim is incomplete, the Holder can complete it within five (5) business days following receipt of the claim so that the failures can be corrected. After two (2) months from the date of the request without the applicant submitting the required information, it will be understood that the claim has been withdrawn.

In the event that the person who receives the claim is not competent to resolve it, they will transfer it to the appropriate person within a maximum term of two (2) business days and inform the interested party of the situation.

Once the complete claim is received, the maximum term to address it will be fifteen (15) business days from the day following the date of receipt. When it is not possible to address the claim within said term, the interested party will be informed of the reasons for the delay and the date on which their claim will be addressed, which in no case may exceed eight (8) business days following the expiration of the first finished.

PARAGRAPH 1: In the event that between the company and the claimant there is a validly executed contract or legal act that is in force, the request will be denied.

12.5 RECTIFICATION AND UPDATE OF DATA

PROQUIMES S.A. may rectify and update, at the request of the Holder, the information of the latter that turns out to be incomplete or inaccurate in accordance with the procedure and the terms indicated above. In this regard, **PROQUIMES S.A.** will take into account the following:

In requests for rectification and updating of personal data, the owner must indicate the corrections to be made and provide the documentation that supports their request.

PROQUIMES S.A. has full freedom to enable mechanisms that facilitate the exercise of this right, as long as it does not harm the Owner of the data. Consequently, electronic means or others that **PROQUIMES S.A.** considers pertinent may be enabled.

PROQUIMES S.A. may establish forms, systems and other methods, which will be made available to interested parties on the website or request them by email to **protecciondedatos@proquimes-sa.com**.

12.6 DELETION OF DATA

The Owner of personal data may request **PROQUIMES S.A.**, the deletion (elimination) of their personal data when:

- Consider that they are not being treated in accordance with the principles, duties and obligations provided for in current regulations.
- They have ceased to be necessary or pertinent for the purpose for which they were collected.
- The period necessary for the fulfillment of the purposes for which they were collected has been exceeded.

The deletion implies the total or partial elimination of personal information in accordance with what is requested by the Holder in the records, files, databases or treatments carried out by **PROQUIMES S.A.**

The right of deletion is not an absolute right and the person responsible for the processing of personal data may deny the exercise of this right when:

- The Owner of the data has a legal or contractual duty to remain in the database.
- The deletion of data hinders judicial or administrative actions related to tax obligations, the investigation and prosecution of crimes or the updating of administrative sanctions.
- The data is necessary to protect the legally protected interests of the Owner to carry out an action based on the public interest or to comply with a legal obligation acquired by the Owner.

12.7 REVOCATION OF AUTHORIZATION

Any holder of personal data can revoke, at any time, the consent to the treatment of these as long as it is not prevented by a legal or contractual provision. For this, **PROQUIMES S.A.** will establish simple mechanisms that allow the Owner to revoke their consent.

There are two ways in which consent can be revoked:

- Regarding the totality of consented purposes, that is, that **PROQUIMES S.A.** must completely stop processing the data of the Holder.
- On certain consented purposes such as for advertising or market research purposes. In this case, **PROQUIMES S.A.** must partially stop processing the data of the Holder. Other purposes of the treatment are then maintained that the person in charge, in accordance with the authorization granted, can carry out and with which the Owner agrees.

12.8 CONTRACTS

In labor contracts, **PROQUIMES S.A.** will include clauses in order to authorize in advance and generally the processing of personal data related to the execution of the contract, which includes the authorization to collect, modify or correct, at future times, personal data of the headline. It will also include the authorization for some of the personal data, if necessary, to be accessed by third parties with whom **PROQUIMES S.A.** has contracts for the provision of services or of any other type, for the performance of tasks related to the contract. This Policy will be mentioned in these clauses.

In contracts with third parties, when the contractor requires personal data, **PROQUIMES S.A.** will provide said data as long as there is prior and express authorization from the owner for this transfer. Given that in these cases third parties are in charge of data processing, their contracts will include clauses that specify the purposes and treatments authorized by **PROQUIMES S.A.** and precisely delimit the use that said third parties may give to the data.

12.9 TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

The transfer of personal data to third countries will only be carried out when there is corresponding authorization from the Holder.

13. GENERAL RULES APPLICABLE

- **PROQUIMES S.A.** establishes the following general rules for the protection of personal and sensitive data, such as in the care of databases, electronic files and personal information:

- **PROQUIMES S.A.** will guarantee the authenticity, confidentiality and integrity of the information.
- The Security Committee will be the one whose objective will be to execute and design the strategy so that this Policy is complied with.

- **PROQUIMES S.A.** will take all the necessary technical measures to guarantee the protection of existing databases. In cases where the infrastructure depends on a third party, it will ensure that the availability of information, as well as the care of personal and sensitive data, is a fundamental objective.

- Audits and controls will be carried out periodically to guarantee the correct implementation of Law 1581 of 2012 and its regulatory decrees.

- It is the responsibility of the employees and collaborators, contractors, shareholders and members of the board of directors of **PROQUIMES S.A.** to report any incident of information leakage, computer damage, violation of personal data, commercialization of data, use of personal data of children or adolescents, identity theft, or conduct that may violate the privacy of a person.

- **PROQUIMES S.A.**, in order to guarantee the protection of personal information, will adopt, in its transactional portals, all the mechanisms to guarantee the confidentiality of the information. For this you can adopt technological security mechanisms such as security software, digital signatures, SSL certificates, Hypertext Transfer Protocol Secure (HTTPS), as the necessary tools to safeguard and protect the entity's databases.

- The education and training of officials, suppliers and contractors will be a fundamental complement to these Policies.

- The Data Protection Officer must identify and promote the authorizations of the Holders, the privacy notices, the notices on the entity's website, awareness campaigns, claim legends and other procedures to comply with the law. 1581 of 2012 and other regulations that complement, modify or repeal it.

14. FUNCTION OF PROTECTION OF PERSONAL DATA WITHIN PROQUIMES SA

14.1 THOSE RESPONSIBLE

The person responsible for the processing of personal data is "the natural or legal person, public or private, who decides on the basis of data and/or data processing". In this way, the person in charge is the one who defines the purposes and means of the processing of personal data and guarantees compliance with the legal requirements.

In the case of **PROQUIMES S.A.**, the person responsible for adopting the necessary measures for the proper treatment of personal data is the Personal Data Protection Officer.

14.2 THE PERSONS IN CHARGE

The person in charge of the processing of personal data is "the natural or legal person, public or private, who processes personal data on behalf of or on behalf of the data controller". This assumes that, for each data processing, their respective managers have been defined and that they act by precise instruction of a person in charge.

14.3 DUTIES OF PERSONS IN CHARGE

PROQUIMES S.A. distinguishes between Internal Manager and External Manager. The internal Managers are employees and collaborators of **PROQUIMES S.A.** While the external ones are natural or legal persons who process data that the entity provides them to carry out an assigned task (suppliers, consultants, etc.).

14.4 THE INTERNAL DEPLOYMENT OF THE DATA PROTECTION POLICY

From the adoption of this Policy, **PROQUIMES S.A.** will establish:

- **Terms and conditions of use of external computer tools**: Self-regulation of the principles and rules enshrined in Law 1581 of 2012, specifically aimed at protecting the right of habeas data of clients, users and in general any natural person who interacts with a computer application (element that manages information, whether physical or electronic).
- **Data Protection Officer:** In compliance with the legal duty enshrined in article 17 of Law 1581 of 2012, regarding the need to assign direct responsibilities to a subject within the Organization, the role of Data Protection Officer is created. Personal, headed by the Information Security Officer, who, taking into account what is defined by the Security Committee, will articulate all actions for the effective compliance of the Personal Data Protection Policy in **PROQUIMES S.A.**

The most important duties of the Safety Committee are the following:

1. Guarantee the Owner, at all times, the full and effective exercise of the right of habeas data.
2. Request and keep, under the conditions provided in this law, a copy of the respective authorization granted by the Holder.
3. Duly inform the Holder about the purpose of the collection and the rights that assist him by virtue of the authorization granted.
4. Keep the information under the necessary security conditions to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.
5. Guarantee that the information provided to the person in charge of the treatment is true, complete, exact, updated, verifiable and understandable.
6. Update the information, communicating in a timely manner to the person in charge of the treatment, all the news regarding the data that has previously been provided and adopt the other necessary measures so that the information provided to it is kept updated.
7. Rectify the information when it is incorrect and communicate what is pertinent to the person in charge of the treatment.
8. Provide the Data Processor, as the case may be, only data whose treatment is previously authorized in accordance with the provisions of the law.
9. Demand from the person in charge of the treatment at all times, the respect of the security protocols and privacy of the information of the Owner.
10. Process inquiries and claims formulated in the terms indicated in the law.
11. Inform the person in charge of the treatment when certain information is under discussion by the Owner, once the claim has been filed and the respective process has not been completed.
12. Inform at the request of the Owner the use given to their personal data.
13. Inform the data protection authority (SIC) when there are violations of the security codes and there are risks in the administration of the information of the Holders.
14. Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce (SIC).

15. THE NATIONAL REGISTRY OF DATABASES

In accordance with the provisions of Decree 886 of 2014, which regulates article 25 of Law 1581 of 2012, **PROQUIMES S.A.** will independently register in the National Database Registry, each of the databases that contain personal data. whose treatment is carried out by the Company (articles 2 and 3 of Decree 886 of 2014), identifying each of these databases according to the purpose for which they were created (article 9 Decree 886 of 2014).

PROQUIMES S.A. databases, it will indicate its company name, tax identification number, as well as its location and contact information of the person responsible.

PROQUIMES S.A. will indicate in the National Database Registry the company name, tax identification number, location and contact of those in charge of the treatment of its databases (article 7 of Decree 886 of 2014).

Finally, **PROQUIMES S.A.** must update the registered information in the National Database Registry when substantial changes are made to it.

16. VALIDITY AND UPDATE

This Policy enters into force as of its approval by the Information Security Committee and its update will depend on the instructions of said Committee.

The actions leading to the protection of personal data will be articulated within the Information Security Committee, which will carry out semi-annual reviews of the correct execution of the Policy jointly with the Company's Data Protection Officer.

The approved version of this Policy will be published on the official website of **PROQUIMES S.A.**

It is a duty of the employees and collaborators of **PROQUIMES S.A.**, to know this Policy and carry out all the acts leading to its compliance, implementation and maintenance.

This Personal Data Protection Policy was approved in a session of the Security Committee of **PROQUIMES S.A.** on the second (02) day of the month five (05) of two thousand and twenty-three (2023).

17. ANNEXES - REFERENCES

- Plan de manejo de la información PC-GC-001
- Gestión de la información PD-GC-002
- Copia de la seguridad de la información PD-GC-005.