Above All, Everyone Must Benefit

Bio D S.A.

INFORMATION PROTECTION AND SECURITY POLICY

NATIONAL AND INTERNATIONAL APPLICATION VERSION FOR THE SECURITY OF INFORMATION IN TRANSIT, PROCESSING, RECEIPT OR KNOWLEDGE THROUGH ELECTRONIC, INTERNET OR SIMILAR COMMUNICATIONS NETWORKS OR SYSTEMS AND WILL COVER SECURITY TO NATIONALS AND FOREIGNERS.

JANUARY 14, 2021

HISTORY

VERSION	DATE	CHANGES
1.0.0	11/01/21	Versión Inicial del Documento

TABLE OF CONTENTS

PÁG

1. COPYRIGHT

This document on security and privacy of the information of Bio D S.A. It is developed on the basis of the models provided by the Government of the Republic of Colombia / Ministry of information technologies and communications - MinTic. It safeguards the privacy and security of the information that is processed, collected or received from users or participants in the air process on pages and networks in which Bio D S.A. participate and is arranged in accordance with the policies of Information Management, Anti-Corruption, Sarlaf, Code of Business Ethics and all those that complete said internal business regulations in accordance with national and international legal guidelines and especially those set for the countries members of the OECD.

All references to the documents of the Information Security and Privacy Model are rights reserved by the Ministry of Information Technologies and Communications, through the Online Government Strategy, which are provided within this text content and they are kept unchanged in accordance with current regulations.

All references to the policies, definitions or related content, published in the Colombian technical standard NTC ISO / IEC 27001: 2013, as well as to the annexes are rights reserved by ISO / ICONTEC. Bio D S.A. It has made use of the models based on the participation of private entities in the accompaniment processes, provision of mechanisms and models established by the Ministry for the business benefit and the development of technological innovation in the country.

2. AUDIENCIE

This document is prepared by Bio D S.A. based on the models made publicly available by the ICT Ministry available to public entities of a national order, public entities of the territorial order and private entities as a guide to implement the policies outlined in the Information Security Model, as well as government service providers Online and third parties who wish to adopt the Information Security and Privacy Model within the framework of the Online Government Strategy.

3. INTRODUCTION

For Bio D S.A. The mission of safeguarding the information of third parties and its own is framed in the highest standards of commitment both business and each of its members.

The growth of the company's mission both nationally and internationally has led to the expansion of the business on the borders of Colombia through the use of all growth channels: business, foreign trade, customs, through networks, the internet and in general all the mechanisms developed around technology and especially communication technology.

It is for the foregoing that Bio D SA, aware of this commitment to security and privacy, has designed this document of "Information Security and Privacy Policy" hereinafter "The Policy", in order to guarantee national users and international management of the information that as a result of the means of transmission of information became known or processed by the company.

This is why this Policy addresses the implementation of an information security management system (ISMS). This is raised from the description of who, what, why, when and how, around the development of the implementation of the ISMS.

Thus, taking into account the importance that the entity has to define the needs of its stakeholders, and the assessment of the precise controls to maintain the security of the information, this Policy is established that takes into account the general framework of the operation of the entity, its institutional objectives, its missionary processes, and that it is adapted to the specific and particular conditions as appropriate and in turn duly approved, guided and regulated by the business management.

Thus, this policy seeks to be concise, easy to read and understand, flexible, and easy to enforce for all those within scope without exception.

This policy is framed in the articulation of the internal regulations of the company, including those related to Sarlaft, Anti-corruption, Information Management or Habeas Data and the Code of Business Ethics, also complying with the provisions and guidelines of the OECD.

4. PORPUSE

The following document has the special purpose of providing security and privacy to the information that can be the object of receipt, processing, treatment or processing by Bio D S.A. through its electronic channels or information technology in general.

Security is intended to be provided for nationals, foreigners, public entities and private parties, as part of the Information Security and Privacy Model of the Online Government strategy, as established in Decree 1078 of 2015.

5. GLOSSARY

Policy: A high-level corporate statement that describes the entity's position on a specific issue.

Standard: Rule that specifies an action or response to be followed in a given situation. Standards are mandatory guidelines that seek to enforce policies. The standards are designed to promote the implementation of the entity's high-level policies before creating new policies.

Best Practice: A specific security rule or platform that is accepted throughout the industry by providing the most effective approach to a specific security implementation. Best practices are established to ensure that the security features of systems used regularly are configured and managed in a uniform manner, ensuring
a consistent level of security throughout the entity.

Guide: A guide is a general statement used to recommend or suggest an approach to implement policies, standards, good practices. The guides are essentially recommendations that should be considered when implementing security. Although they are not mandatory, they will be followed unless there are documented and approved arguments not to do so.

Procedure: Procedures specifically define the policies, standards, best practices and guidelines that will be implemented in a given situation. Procedures are independent of technology or processes and refer to specific platforms, applications or processes. They are used to outline the steps that must be followed by an agency to implement security related to that specific process or system.

Generally the procedures are developed, implemented and supervised by the owner of the process or the system, the procedures will follow the policies of the entity, the standards, the best practices and the guidelines as closely as possible, and at the same time will conform to the procedural or technical requirements established within the agency where they apply.

6. GENERAL POLICY OF SECURITY AND PRIVACY OF INFORMATION

The general management, understood as, Board of Directors and Administration of the company Bio D SA, understanding the importance of adequate information management, has committed to the implementation of an information security management system (ISMS) seeking to establish a framework of trust in the exercise of their duties with the State and national and foreign citizens, all framed in strict compliance with the laws and in accordance with the mission and vision of the entity. For Bio D SA, the protection of information seeks to reduce the impact generated on its assets, due to the risks systematically identified in order to maintain a level of exposure that allows responding to its integrity, confidentiality and availability, according to the needs of the different stakeholders identified. In accordance with the foregoing, this policy applies to the company as defined in the scope, its officials, third parties, apprentices, practitioners, suppliers and the general public, taking into account that the principles on which the development of the actions or decision-making around the ISMS will be determined by the following premises:

(i) Minimize risk in the most important functions of the entity.
(ii) Comply with the principles of information security.
(iii) Comply with the principles of the administration's activity.
(iv) Maintain the trust of its customers, partners and employees.
(v) Support technological innovation.
(vi) Protect technological assets.
(vii) Establish policies, procedures, and instructions regarding information security.
(viii) Strengthen the information security culture in officials, third parties, apprentices, practitioners and clients of Bio D S.A.
(ix) Guarantee business continuity against incidents.

Bio D S.A. has decided to define, implement, operate and continuously improve an Information Security Management System, supported by clear guidelines aligned to business needs and regulatory requirements. Finally, it is of great help to include the general description of other relevant policies for the fulfillment of the Objectives established within the ISMS project since these are the support on which it is developed; these are:

I- Code of Business Ethics: This compendium contains the general operating guidelines and ethical and honesty parameters of the shareholders, officials, servers, suppliers and in general all the people who are part of Bio D S.A. and those who are related to it.
II- Sarlaft Policy: Compedo of internal norms to guarantee the inanity of business operations and activities in order to avoid any contamination of ill-gotten capital derived from illegal activities or that allow acts such as Money Laundering and terrorist financing.

III- Anticorruption Policy: Compendium of internal regulations that promote the sanity of the company's actions, its transparency in contracting and in general avoid any act aimed at generating bribes, gifts or undue interests in the execution of its processes in general.

IV- Data handling policy or Habeas data. Internal regulations that guarantee the security of the information of the natural persons who provide information for treatment to BioD S.A due to its business operations, supply of goods or services and in general the inanity in the handling of the information called sensitive. It allows the elimination of information or its correction when it should not be treated or is found to contain errors.

Below are 11 security principles that support the ISMS of Bio D S.A.:

1. Responsibilities for information security will be defined, shared, published and accepted by each of the employees, suppliers, business partners or third parties.

2. Bio D S.A. will protect the information generated, processed or protected by business processes, its technological infrastructure and assets from the risk that is generated from accesses granted to third parties (eg: suppliers or clients), or as a result of an internal outsourcing service.

3. Bio D S.A. will protect the information created, processed, transmitted or protected by its business processes, in order to minimize financial, operational or legal impacts due to its incorrect use. For this, the application of controls according to the classification of the information owned or in custody is essential.

4. Bio D S.A. will protect your information from threats posed by staff.

5. Bio D S.A. It will protect the processing facilities and technological infrastructure that supports your critical processes.

6. Bio D S.A. will control the operation of its business processes, guaranteeing the security of technological resources and data networks.

7. Bio D S.A. will implement access control to information, systems and network resources.

8. Bio D S.A. It will ensure that security is an integral part of the life cycle of information systems.

9. Bio D S.A. will guarantee through proper management of security events and weaknesses associated with information systems an effective improvement of its security model.

10. Bio D S.A. will guarantee the availability of its business processes and the continuity of its operation based on the impact that events can generate.

11. Bio D S.A. will guarantee compliance with established legal, regulatory and contractual obligations. Failure to comply with the Information Security and Privacy policy will bring with it the legal consequences that apply to the Entity's regulations, including what is established in the regulations that correspond to the national and territorial Government in terms of Information Security and Privacy. it means

7. PHASES OF IMPLEMENTATION AND OPERATION OF THE INFORMATION SECURITY POLICIES

The implementation and compliance of information security policies require compliance with a series of phases that are established in this policy. These phases are aimed at Bio D S.A. After the approval, implementation and socialization of this policy, maintain the internalization of it so that its effective use by all officials, contractors and / or third parties related to the company guarantees its fulfillment and purpose.

IMPORTANCE OF INFORMATION SECURITY POLICIES

For Bio D SA, taking into account its growth and respect for the dignity and safety of people related to the business environment from the beginning of its operations, it is important to have security policies since they are the ones who will guide personal behavior and professional staff, contractors or third parties on the information obtained, generated or processed by the entity, likewise the policies will allow Bio D SA carry out its activities under the best security practices and comply with the legal requirements to which the entity is obliged to comply.

PRECEDING PHASES EXECUTED IN THE IMPLEMENTATION OF INFORMATION SECURITY POLICIES

1. Design, discussion, assembly, approval and updating of the Policy:
Bio D S.A. certifies that it has executed the design, discussion and assembly of its information security and privacy policies: In this phase, Bio D S.A. He made the areas responsible for the creation of the policies, including the operational, administrative and legal advisory areas in order to structure, write, review and approve them; whereby this phase was brought to fruition. Verification and investigation operations were carried out on the following aspects:

- Justification of the policy creation: The need for Bio D S.A. was identified. of creating the information security policy and the control to which its implementation refers was determined. This justification is immersed in the need to guarantee national and foreign users the security of their data or information that could be received by the systems of Bio D S.A. in general communication processes, including those related to communication networks, social networks and in general any mechanism that allows access, crossing or obtaining information.

- Scope: The scope was determined: The population, areas, processes or departments to which this Policy applies have been defined as, any natural or legal person that provides or provides information that is understood as "sensitive information", whether national or foreign, its obligation is predicated on any related person, official, shareholder, supplier or similar, clients or people who access or provide direct information or people related to Bio D

SA in all departments or administrative, operational units or even people linked by services or companies that provide them

- Roles and Responsibilities: The operational administrative units of the company will be responsible for keeping this policy up to date and for verifying its application and compliance, including the sanctions derived from its violation. The general management will verify compliance with the updating and application of the policies against the management or administrative, financial, treasury, systems unit and in other operations that have access to third party information.

- Policy review: This policy will be reviewed and updated every year in June. For the update, the related regulations that are updated or issued by the Government or Congress of the Republic will be taken into account. The updates will be submitted to the evaluation processes by the board of directors who will verify their applicability, the wording and will make suggestions on the development and creation of the same.

- Approval of the Policy: The approval of this Policy has been executed by the company's board of directors and its updates will also be approved by it.

2. Compliance: This policy is firm and duly approved by the units designated for said function at the business level. It is mandatory for all officials, shareholders or people related to the company for all types of business activity, especially all those related to the movement or transfer of information, reception and processing thereof by electronic means.

3. Communication: This policy has been socialized and disseminated at all business levels. It has also been transmitted and will be transmitted to contractors and / or third parties of the Entity. It is also arranged on the official page of Bio D S.A. for public awareness.

4. Monitoring: The monitoring of compliance with policies in electronic communication mechanisms networks will be in charge of the systems department. However, the operating units of the company will be responsible for the information that is processed, processed and received for the purpose of their on-air processes. The systems units and management will keep a record of the possible claims, updates, recommendations or PQRS that are received or promoted in order to maintain and update the policy.

5. Maintenance: The maintenance and updating, different from the annual review that must be carried out, will be in charge of the systems unit and the company administration who will execute the modifications of this policy together with the legal unit and external consultants.

6. Withdrawal: This policy will be in force until the administration or management bodies of the company determine it and always while there are operations related to electronic, internet or related communication platforms. In case of opting for the withdrawal of the policies, the conditions and motivation for such decision will be recorded in an official document of the company.

8. SPECIFIC POLICIES FOR THE IMPLEMENTATION OF INFORMATION SECURITY CONTROLS

This policy determines recommendations for information assurance mechanisms and actions that guarantee the application of the security and privacy objective for the company, its shareholders, officials, suppliers, clients and in general any person or company that links or provides their information. in any type of business relationship.

The recommendations are not exhaustive and have been designed in order to be transversal to the corporate Information security objective.

The recommendations set out in the following points in this policy document imply direct actions by the company and acts or ways of acting of those who are related to it with the aim of avoiding risks to the detriment of information security.

8.1 ORGANIZATION OF INFORMATION SECURITY

Information security, in relation to the updating of this policy, the implementation of the information protection mechanisms, campaigns and special actions that are implemented for each protection case, will be in charge of the Security Steering Committee of the "CDSI" Information.

The CDSI will be composed of:

a) Its president will be the Manager or Financial Director or whoever he or she delegates for the execution of the committee's management activity, scheduling its meetings and guiding the precursors to be executed.

b) They will be members of the CDSI, two (2) elected officials of the administrative groups that are in charge of the control of industrial security, one, and the other information controller in charge of the control activities in the policies of handling information of people natural or habeas data.

- Goals:

The objectives of the CDSI will be:

1. Keep the information security and privacy policy updated. For this process, you may request the accompaniment of the company's legal advice area.

2. Receive requests and complaints or PQRS related to information security or privacy issues that are sent to the company through electronic means of communication.

3. Resolve in the first instance the claims and sanctions against officials who are determined to be responsible for the violation of the security or privacy of the information.

4. Request to the general manager or legal representative the necessary complaints about acts of violation of the security or privacy of the information that were brought to the attention of the authorities because they contain aspects that are considered criminal or criminal.

5. Coordinate continuous improvement programs for information security mechanisms.

6. Verify compliance with the processes and actions of the information security programs.

7. All the additional ones related to the information security and privacy policy that are not specifically indicated in this policy but that will require improvement actions.

8.2 ASSET MANAGEMENT

Asset Management is understood as the processes or actions aimed at the identification by the officials or servers of the company in relation to the limits and procedures regarding the identification, use, administration and responsibility regarding the Information assets.

a) Identification of Assets: At least once a year, and before October, the officials determined by the Information Security Steering Committee "CDSI" will carry out the identification and / or update of the inventory within the company of Information Assets.

Regarding information assets, including personal information, sensitive business data, contracts, identification documents, and all those that are determined under this criterion, it must be determined which person within the organization is responsible for their management, management , care, storage and especially the transmission or use of the same for commercial purposes, research for any purpose related to the ordinary course of business activities.

b) Information retention table: Each person in charge will prepare an information retention table in which they will indicate, (i) the type of information, (ii) who originates it, (iii) its destination or type of processing to the that will be submitted and (iv) the term or time in which it will be kept

contained or collected before being erased or eliminated from the business files.

c) **Classification of Assets:** Classified as assets according to the type of information and its destination, the criticality, sensitivity and reserve thereof will also be determined in the documentary retention tables.

The classification of the criticality, sensitivity and confidentiality of the information will be graduated in accordance with the provisions of Law 1581 of 2012, Decree 1377 of 2013, Law 1712 of 2014, Decree 103 of 2015, among others and all those that may apply accordingly. according to the nature of the entity generating the information, the person and their nationality if necessary.

Information assets considered as industrial secrets will have special treatment. These must be classified and identified both in their extension, type and especially in front of their manager. The transfer, delivery, copy or use of this information may only be authorized by the General Management of the company.

d) **Information Labeling:** Those responsible for the information in each case, must label, label or name the information assets in the electronic systems within containment folders with security systems and access codes.

e) **Return of Assets:** The information assets that are disposed of for use, treatment, processing or simple archiving or containment, once they complete their life cycle and usability, must be returned to their generator, eliminated from the archives or destroyed according to the case. In these situations, the assets should be indicated in the retention tables as eliminated or destroyed. Temporary or service officials who have access to information recognized as an information asset must sign the receipt and return of the information before the immediate boss or controller of the contract. The controllers of contracts or heads, must verify in any case that the respective contracts or confidentiality agreements subscribed prior to the delivery of the information exist.

f) **Management of removable media:** The immediate managers or contract controllers will have the obligation to assign or verify the permissions that are granted to users and / or officials for the use of removable media, understanding as removable media all those electronic devices that store information and can be extracted from computers.

The use of these removable mechanisms and the procedures used to transfer information to them, as the case may be, will be authorized. Information assets that are considered “industrial secrets” may only be copied in removable mechanisms or media with the express authorization of the General Management.

g) **Disposal of assets:** Information assets that are used for processing, analysis, or any activity related to it, must be returned to their storage mechanisms or deposit sites. In cases where after use or due to the passage of time, the information is not useful, it must be destroyed, eliminated or returned to its originator. For these cases, the destruction of electronic information assets will be verified by the management or systems unit or the administrative management, leaving a record of said procedure. In cases of physical destruction, they will be carried out with the supervision of the administrative management or whoever is deciding, leaving the respective act. The returns of information that are executed before the generators, must contain a record with the receipt of the same by the receiver.

h) **Mobile devices:** The installation, assignment, modification, expansion or any activity for the processes related to access to wireless networks, will be the sole responsibility of the company's systems unit. The assignment of corporate chats and / or emails of the entity through the use of this type of device will be assigned by the immediate managers and requested to the business systems unit. Said deliveries, use or access will be determined in the respective contracts, labor, service or of the nature that is required for the link.

   In any case, the officials, contractors or people who have access to these mechanisms for the treatment of Information Assets will be responsible for the protection and use of the information stored on mobile devices. The immediate managers will have the obligation at least once a year to confirm the proper use of the mechanisms and the review of the storage stability and proper disposal thereof to guarantee, protect, mitigate, supervise and monitor the risks associated with access. and unauthorized disclosure of information.

8.3 ACCESS CONTROL

The company, through its area managers, will enforce the guidelines that this policy sets in relation to the security and privacy of information.

The application of protection mechanisms, limits and procedures against administration and responsibility, related to access to information, regardless of whether these accesses are electronic or physical; Policies related to access control are mandatory for compliance by all company officials and contractors, who by signing their employment contracts, services or whatever their relationship, declare their acceptance and compliance.

In any case, this policy duly socialized and published through the mechanisms of socialization of business information oblige at least:

a. Access control with username and password: The mechanisms for controlling access to networks, applications, and / or information systems of the entity will always be applied, determining who are responsible and the formal authorization procedures for creation, modification, suspension or deletion of users (ID) and passwords.

b. Economic responsibility for damages: They will be responsible not only for the purpose of protecting the information, but also for the means they use so that this purpose is fulfilled. The officials will be financially liable for the damages caused to the company by the misuse of the information. Its improper use, aimed at the sale of industrial secrets, sale of formulations, procedures or negotiation of internal or third-party commercial information, will be reported to the Colombian criminal authorities.

   Contractors or third parties who eventually or permanently have access to company information, will also be financially responsible for the damages caused to the company or third parties.

c. Provision of access control: The people who are authorized and assigned with controls of entry to information, emails or company networks must respond for the inappropriate use of said keys when they are known or used by third parties due to negligence. The assignment, modification, revision or revocation of rights and / or privileges will be verified or ordered by the heads of unit.

   The privileges of use of information or control of it, such as those related to people linked to the company's systems unit, will be authorized by the general management.

d. Password Management: Passwords will be for personal and non-transferable use. The improper use of passwords that allows the loss, improper

transmission or misuse of the information asset will be the responsibility of the official or contractor assigned with the password. Passwords should avoid the use of combinations that are easy to locate or that allow easy identification, such as identification numbers, names of relatives, children or similar. The use of low security passwords will be the responsibility of the person assigned with security.

e. Security Perimeters: The information considered as an information asset must remain within the business facilities, be they those located at the Mansilla plant or in the offices that are eventually located in the city of Bogotá. People who have information for processing will ensure that it is not transferred to different locations. The extraction of information or transfer of it outside the facilities will be the responsibility of whoever executes said act and the damages caused by this improper process will be financially covered by the official against the company or injured third parties.

8.4 NO REMOVAL

Officials may not claim for their benefit the ignorance of external risks or risks of damage to the company or third parties. It is clearly stated that whatever information is accessed, it is considered an information asset whose improper treatment entails direct and collateral damage to third parties.

To this end, anyone with access to information assets must ensure that it can be demonstrated:

a. Traceability: All access to information must be duly reported, leaving a follow-up of the creation, origin, reception, delivery of information and other processes to which the information may be submitted.

b. Retention: The information accessed must be analyzed and defined in terms of the period of use or usefulness. Once this period has expired, those responsible must execute the processes of return, erasure or destruction.

c. Audit: The administration and especially the Information Security Steering Committee "CDSI" will ensure the execution at least once a year of an audit process to verify the management of information assets.

d. Electronic exchange of information: it can only be carried out when said activity is duly authorized by the administration of the company and especially if the information comes from a third party, it must be duly authorized for its delivery, transmission and use.

8.5 PRIVACY AND CONFIDENTIALITY

The Information Security and Privacy Policy is mandatory for all shareholders, officers, employees, contractors or any related to the company. The treatment of the information assets of the company will be subject in any case, and especially those that are considered as industrial or commercial secrets, to confidentiality and privacy in their treatment and use.

The following conditions and aspects of information security and privacy will be taken into account:

a. Scope of application: The application will be executed within the company, outside it in its application, at the national level against contractors, suppliers, clients or related parties and at the international level under the same conditions.

b. Exception to the scope of application of the personal data treatment policies. In the case of information assets that are considered confidential and that due to acts of authorities or their public disclosure become public knowledge, said information will no longer be considered confidential.

c. Principles of the processing of personal data:

- Principle of Legality: The processing of personal data must be subject to the provisions of current regulations.

- Principle of purpose: simepres when information is requested or received from a third party in a process, the purpose of the processing of personal data must be indicated, which must be informed to the owner.

- Principle of freedom: The treatment can only be done with the prior, express and informed consent of the owner of the data.

- Principle of truthfulness or quality: The information to be processed must be truthful, complete, exact, updated, verifiable and understandable.

- Principle of transparency: Guarantee the owner of the data the right to obtain information that concerns him / her from the person in charge of the treatment.

- Principle of access and restricted circulation: The treatment may only be done by persons authorized by the owner or by persons provided for in current regulations.

- Principle of security: The information subject to treatment must be handled with the technical, human and administrative measures that are necessary to

guarantee security, avoiding its adulteration, loss, consultation, use or unauthorized or fraudulent access.

- Principle of confidentiality: All persons who participate in the Processing of Personal Data must guarantee the reservation of said information.

d.Rights of the Holders: The following shall be the rights of the holders:

1. Know, update and rectify your personal data.

2. Request proof of your authorization for the processing of your data personal.

3. Be informed about the use that is given to your personal data.

4. Revoke the authorization and / or request the deletion of your personal data from the databases or files when the owner considers it, as long as the services or products that gave rise to said authorization are not in force with the bank.

5. File complaints with the administrative entity in charge of the protection of personal data.

e.Owner's authorization: The company will ensure that in the processes of access to information or electronic mechanisms in which third-party information is accessed, they may indicate that they authorize the access, use and treatment thereof. The mechanisms must be conciliatory with the processes of authorization of use of the information of natural persons contained in the policies of information management and habeas data.

f.Duties of those responsible for the Treatment: Those responsible and / or in charge of the processing of personal data must:
. feed holding tables,
. classify the risks of information
. guarantee the delivery of the information requested in the audits
. locate and process authorizations for the use of information
. verify the proper use of removable mechanisms
. guarantee the destruction, erasure or return of the information

g.Cryptographic controls: The company, whenever it contracts mechanisms for the use of information assets in electronic form, will verify that the contracts that are signed have a guarantee for the assurance of the confidentiality and authenticity of the information that circulates or is generated through the different information systems.

h.Confidentiality controls: The company will ensure that any official, contractor, linked or person who has access to the business information assets signs a confidentiality commitment or agreement. Through this, every official, contractor and / or third party linked to the company, must sign a commitment not to disclose the internal and external information that they know about the company, as well as that related to the functions they perform in it. The signing of the agreement implies that the information known by any official, contractor and / or third party, under no circumstances should be revealed by any electronic, verbal, written or other means, neither totally nor partially, without prior authorization.

The policy should indicate from when the confidentiality agreement is signed, as well as its validity.

8.6 INTEGRITY

The integrity in the management of the information assets will be declared compromised and accepted after being read by the officials,
contractors and / or third parties that are part of the company at the signing of their contracts.

This refers to the complete and comprehensive management of both internal and external information, known or managed by them.

In this way, all verbal, physical or electronic information must be adopted, processed and delivered or transmitted integrally, coherently, exclusively to the corresponding persons and through the corresponding means, without modifications or alterations, unless so determined by the authorized persons. and / or responsible for said information.

In the case of a contractual relationship, the Commitment of administration and integral and integral management of internal and external information will be part of the clauses of the respective contract, under the name of the Information Integrity Clause. In each case it will be established that confidentiality will be maintained for the duration of the contract, whatever its nature, plus an additional period that in each case will be established by the administration in accordance with the risk generated by the information accessed.

8.7. AVAILABILITY OF THE SERVICE AND INFORMATION

Bio D S.A. in accordance with business continuity and in order to ensure, recover or restore the availability of the processes that support the Information Security Management System and missionary processes of the company, in the event of a security incident of the information, provides that the information must always be contained with the following parameters or aspects:

- Availability levels: The company will ensure compliance with the levels of availability of services and information agreed with clients, suppliers and / or third parties based on the needs of the company, the level agreements of goods and services offered and evaluations of risks.
- Recovery plans: Bio D S.A. It will arrange recovery plans that include the availability needs of the business.
- Interruptions: Bio D S.A. It will ensure the management of service maintenance interruptions that affect its availability. For this purpose, in each case, it will contract with the providers of communications services or of communications technology processes through networks or the Internet that this is possible.

- Service Level Agreements: In the contracts that are subscribed for services of transmission or handling of information in networks or via the internet, Bio D S.A. It will ensure that the responsibilities for service interruptions are determined in the service level agreements (ANS).
- Segregation of environments: Bio D S.A. It will guarantee that in the contracts that are subscribed for services of transmission or handling of information in networks or via the Internet, the segregation of environments is established to minimize the risks of putting changes and new developments into operation in order to minimize the impact of unavailability of service during development, testing and production phases.
- Change Management: The information management processes contracted by Bio S.A. or that are eventually provided directly, must include change management so that the steps to production minimally affect availability and are carried out under controlled conditions.

8.8 REGISTRATION AND AUDIT

This information security and privacy policy ensures the maintenance of evidence of activities and actions that affect information assets.

Thus, the following aspects are established as mandatory:

• Responsibility: The Office of Internal Control or whoever takes its place or is delegated by the administration for such purposes will have the duty to execute, in parallel to the audits that the Information Security Steering Committee executes "CDSI", audit processes periodically to the systems and activities related to the management of information assets, as well as the responsibility of said Office to report the results of the audits to the Board of Directors.
• Storage of records: The records of the audits of both the Information Security Steering Committee "CDSI" and the Office of Internal Control will be delivered to one of the administrative or financial managements for safekeeping and delivery to the administration and board of directors in the assignments of said administrative body. Audit logs should include all security event log and monitoring information.
• Regulations: The audit will be carried out in accordance with the regulations and legal requirements applicable to the nature of the company.
• Compliance guarantee: The administrative bodies such as the Board of Directors or Management must state in their annual reports the results of the information asset audit processes.

8.9. INFORMATION SECURITY INCIDENT MANAGEMENT

Bio D S.A. will apply the same mechanisms for processing events and PQRS established in the information management or habeas data policy.

In said policy, the corrective measures to be applied in solution of the third party or injured party will be analyzed and will also take into account the analysis of continuous improvements derived from the individual analysis of the events, incidents and information security vulnerabilities that are verified.

It will be directed to any person who uses or has authorized access to any information system. The procedures will additionally consider the following parameters for their preparation:

• It must be approved by senior management, thus certifying the commitment to the process.
• Overview: The following will be reported: errors in information management, loss of information, improper or illegitimate use of information (unauthorized), failures in the purpose of using the information, complaints from third parties that feel that their rights are violated against the management of sensitive or personal information, cases that due to their incidence must be known.
The means for reporting failures or PPQRS will be through written or verbal report to company officials.
• Define Responsible Parties: The reports that are generated will be received by the information controller or the official who receives them and will be forwarded to the Information Security Steering Committee "CDSI". The procedure and deadlines will be the same content in the information management or habeas data policy. The processes, their analysis and results must be contained in the proceedings, highlighting the security vulnerabilities that are identified.
• Legal Aspects: The cases in which situations are identified that should be reported to the authorities by acts of officials, contractors or third parties, these will be processed through the General Management or a legal representative who will be responsible for making the complaint with support of the legal unit.

8.10. INFORMATION SECURITY TRAINING AND AWARENESS

This policy will be known to all officials, contractors or those linked to the company. Its purpose is focused on training staff on issues related to information security, the purpose of which is to reduce vulnerabilities and threats related to human resources.

The senior management of Bio D S.A. declares its unrestricted commitment to the protection and permanent design of the mechanisms that are necessary for the protection of the security and privacy of the information.
All officials must be trained in the information asset security mechanism and especially those engaged in commercial work that make use of their own or external electronic information transfer platforms.

This policy refers especially to compliance with the parameters described in the policies of good business practices defined by the OECD and is especially implemented within the continuous improvement processes defined in corporate governance.

9. CONTACT

The data controller with respect to our website is Bio D S.A., Facatativá Terminal de Combustibles Sabana Mancilla 253051.

Cundinamarca, . Puede contactarse mediante escrito dirigido a Bio D S.A., Facatativá Terminal de Combustibles Sabana Mancilla 253051 o mediante email a atencionalcliente@biodsa.com.

If you have any questions about our information security and privacy policies, please contact the Information Controller.

10. CURRENT MEANS OF INFORMATION HANDLING

10.1. WEB SERVER INFORMATION

Bio D S.A server provides the current operating server where our website is hosted.

Our server automatically stores the IP address that you use to access our website as well as some about your visit such as the pages visited, required information, the date and time of the request, the origin of your access to our website (eg the website or URL line (link) that sent you or referred you to our website), and the version of your browser and operating system.

10.2. TRANSFER AND STORAGE OF YOUR INFORMATION

Bio D S.A. makes use of a third-party email provider / user of the management tool for the storage of emails and messages that you send us.

Our third party provider is https://mailchimp.com/es/.

- Email provider (s); Es Mailchimp. its privacy policy can be found at the address https://mailchimp.com/es/.

- Provider of the User Service system: The provider is Zendesk Inc.

- The IT service provider is Shipping Easy and Microsoft Azure. Your privacy policy can be found at: y.com/hc/en-us/articles/115003637406-Privacy-Policy https://privacy.microsoft.com/en-us/privacystatement

- Hosting provider: It is Network Solutions Your privacy policy can be found at: https://www.networksolutions.com/

- Our service providers are located in Colombia.

Information storage country for international cases: Canada and the United States of America

Safeguard(s) used: our third party hosting provider has self-certified its compliance with the EU-U.S. Privacy Shield.

10. VALIDITY.

This policy is effective as of January 14, 2021.