KEDRION
BIOPHARMA

SECURITY POLICY AND PRIVACY FOR THE PROCESSING OF INFORMATION

Table Of Contents

1. INTRODUCTION

KEDRIÓN COLOMBIA S.A.S (hereinafter **KEDRIÓN)** has implemented an Information Security Policy, in response to the identification of responsibilities and objectives that an organization must draw as Responsible for the Processing of Personal Data, in order to provide adequate protection of information assets, and to reduce the risks that may lead to disclosure, modification, destruction or misuse of these.

This Information Security Policy is made up of standards, procedures and verification and control tools, with the purpose of guiding and strengthening the human, technical and administrative measures that allow **KEDRIÓN**, manage the information under the principle of security, and guiding criteria in the identification and management of security and privacy risks.

2. OBJECT

This document establishes the guidelines to ensure compliance with the principles of confidentiality, integrity, availability, legality, purpose, freedom, veracity and/or quality, security, transparency, access, and circulation of information for the Treatment of personal data and management of information carried out by [1] **KEDRIÓN,** in such a way that allows the organization to maintain and strengthen the information security posture.

3. SCOPE

These guidelines apply to all collaborators, suppliers and / or third parties, who have access to **KEDRIÓN's** information assets**.**

4. REGULATORY FRAMEWORK

Article 15 of the Political Constitution of Colombia – All persons have the right to their personal and family privacy and to their good name, and the State must respect them and ensure respect for them." In the same way, they have the right to know, update and rectify the information that has been collected about them in databases and in archives of public and private entities.

Statutory Law 1581 of 2012 - Imparts provisions for the protection of personal data, which aims to "develop the constitutional right that all people have to know, update and rectify the information that has been collected about them in databases or files (...)".

Law 1273 of 2009 – Modifies the Criminal Code and creates a new protected legal asset called "protection of information and data".

[1] Law 1581 of 2012, article 4°.

Statutory Law 1266 of 2008 - Dictates general provisions of habeas data and regulates the handling of information contained in personal databases, especially financial, credit, commercial, services and from third countries.

Law 1032 of 2006 (copyright and related rights) - Amending articles 257, 271, 272 and 306 of the Criminal Code (article 271. violation of economic rights of copyright and related rights).

Law 527 of 1999 (Access and Use of Data Messages) - By means of which the access and use of data messages, electronic commerce and digital signatures is defined and regulated, and certification entities are established, and other provisions are issued.

Decree 1074 of 2015 - By means of which the Single Regulatory Decree of the Commerce, Industry and Tourism Sector is issued. It partially regulates Law 1581 of 2012 and gives instructions on the National Registry of Databases. Articles 25 and 26.

Decree 1377 of 2013 - By which Law 1581 of 2012 is partially regulated, which constitutes the general framework for the protection of personal data in Colombia.

CONPES 3701 of 2011 - "National Policy Guidelines for Cybersecurity and Cyberdefense".

CONPES 3854 of 2016 - "National Digital Security Policy".

ISO/IEC 27001 – International standard applicable to information security management systems.

ISO/IEC 27002 – International standard that condenses good practices in information security management.

5. GLOSSARY

Asset: Refers to any information or element related to the treatment of this (systems, supports, buildings, people) that have a value for the organization.[2]

Information asset: resource or element that contains information with value for the organization due to its use in some process, or that is directly or indirectly related to the activities of the company: hardware software, people (roles), physical (facilities, file storage area, data processing centers), intangibles (image and reputation). [3]

Threat: Potential cause of an unwanted incident that could cause damage to a system or organization. [4]

[2] ISO 27000
[3] ISO 27001
[4] ISO 27000

Computer threat: Any circumstance, event or person that has the potential to cause damage to a system in the form of theft, destruction, disclosure, modification of data or denial of service[5].

Antivirus: A category of security software that protects a computer from viruses, usually through real-time detection and through system scanning, which quarantines and removes viruses.[6]

Risk analysis: The process of understanding the nature of risk and determining its level of risk.[7]

Data anonymization: delete or replace some names of persons (natural or legal), addresses, contact information, identification numbers, nicknames, or position with other data to avoid the identification of persons and preserve the confidentiality of the information[8].

Authentication: technical mechanism that ensures that a person or entity is correct[9].

Authenticity: The property that an entity is what it claims to be[10].

Back up: refers to a backup of information.

Mailbox: Storage space reserved on an e-mail server for the purpose of storing email, contacts, calendar, and more.

Communication channel: medium used for the transmission of information, for example: cabling, fiber optics and the atmosphere.

Computer center: space where the resources necessary for the processing of the information of an organization also called data center by its Anglo-Saxon term are concentrated.

Cybersecurity: capacity of the State to minimize the level of risk to which citizens are exposed, in the face of threats or incidents of a cyber nature[11].

Cyberspace: both physical and virtual environment composed of computers, computer systems, computer programs (software), telecommunications networks, data and information that is used for interaction between users[12].

Reliability: person or thing that can be trusted.

[5] Ministry of Technologies and Communications - Guide for the Implementation of Information Security.
[6] Ministry of Technologies and Communications - Guide for the Implementation of Information Security.
[7] ISO 27000
[8] http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/Estandares-Proteccion-Datos-Personales espanol.pdf
[9] ISO 27001
[10] ISO 27001
[11] CONPES 3701
[12] Resolution CRC 2258 of 2009

Confidentiality: ownership of information from not being made available or disclosed to unauthorized individuals, entities, or processes[13].

IT control: The policies, procedures, practices, and organizational structures designed to keep information security risks below the level of risk assumed. Control is also used as a synonym for safeguard or countermeasure, it is a measure that modifies the risk reducing the probability or impact of the event[14].

Criteria for technology acquisition: minimum conditions or requirements to consider when implementing and/or acquiring technology.

Biometric data: unique physical parameters of each person that prove their identity and are evidenced when the person or a part of it interacts with the system (e.g., fingerprint or voice)[15].

Sensitive personal data: those 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 trade unions, social organizations, human rights or that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties as well as data related to the health, sex life and biometric data[16].

Private data: data that due to its intimate or reserved nature is only relevant to the owner. [17]

Public data: data qualified as such according to the mandates of the law or the Political Constitution and all those that are not semi-private or private, in accordance with the law. Data contained in public documents, duly enforceable judicial judgments that are not subject to confidentiality and those relating to the civil status of persons are public. [18]

Semi-private data: semi-private data is data that is not intimate, reserved, or public and whose knowledge or disclosure may interest not only its owner but a certain sector or group of people or society in general, such as financial and credit data of commercial activity or services. [19]

Availability: ownership of information to be accessible and usable when required by an authorized entity. [20]

Information security event: An identified occurrence of status in an information system, service, or network that indicates a potential security breach, control failure, or unidentified condition that may be relevant to information security. [21]

[13] NTC-ISO/IEC 27001
[14] ISO 27000
[15] Law 1581 of 2012
[16] Decree 1377 of 2013.
[17] Law 1266 of 2008.
[18] Law 1266 of 2008.
[19] Law 1266 of 2008.
[20] NTC-ISO/IEC 27001

Key management: these are controls that are performed by managing cryptographic keys. [22]

Information Security Incident Management: The process for detecting, reporting, evaluating, responding, dealing with, and learning from information security incidents. [23]

Risk management: coordinated activities to direct and control an organization with respect to risk, including the identification, assessment, and treatment of risks. [24]

Habeas data: right to access personal information found in files or databases; implies the possibility of being informed about the data recorded about oneself and the power to correct them. [25]

Technological infrastructure: elements of hardware, software and communications that support the operation of the different services of the entity, among which are: work equipment, laptops, printers, scanners, camcorders, wifi, operational systems, office tools and internet among others.

Impact: the cost to the company of an incident -of whatever scale-, which may or may not be measured in strictly financial terms -e.g., loss of reputation, legal implications, etc.[26]

Information Security Incident: A single event or series of unexpected or unwanted information security events that possess a significant probability of compromising business operations and threatening information security. [27]

Integrity: the property of safeguarding the accuracy and completeness of information. [28]

Inventory of assets: list of all those resources (physical, information, software, documents, services, people, intangibles, etc.) within the scope of the Information Security Management System, which have value for the organization and therefore need to be protected from potential risks. [29]

Business continuity plan: Plan aimed at allowing the continuity of the main missionary or business functions in the event of an unforeseen event that endangers them. [30]

Risk treatment plan: document that defines the actions to manage unacceptable information security risks and implement the necessary controls to protect it. [31]

---

[21] ISO 27001
[22] ISO 27000
[23] ISO 27001
[24] NTC-ISO/IEC 27001
[25] Political Constitution of Colombia, article 15
[26]ISO 27000
[27] ISO 27000
[28] NTC-ISO/IEC 27001
[29] ISO 27000
[30] ISO 27000

Process: set of interrelated or interacting activities that transform inputs into outputs. [32]

Information Asset Manager: Identifies an individual, a designated position, process, or working group charged with defining the controls, development, maintenance, use, and security of assigned information assets, who may designate custodians of the information asset and authorize users to access the information asset.

Risk: The possibility that a particular threat could exploit a vulnerability to cause loss or damage to an information asset. It is usually thought of as a combination of the probability of an event and its considerations.[33]

Responsible for the treatment: 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. [34]

Information security: preservation of the confidentiality, integrity, and availability of information. [35]

Owner of the information: natural or legal person to whom the information that rests in a database refers and subject to the right of habeas data and other rights and guarantees referred to in this law. [36]

Traceability: quality that allows all actions carried out on information or an information processing system to be unequivocally associated with an individual or entity. [37]

Vulnerability: weakness of an asset or control that can be exploited by one or more threats. [38]

6. GENERAL POLICY ON INFORMATION SECURITY AND PRIVACY AND DIGITAL SECURITY

KEDRIÓN, understanding the importance of proper information management, is committed to protecting, preserving, and managing the confidentiality, integrity, availability, and non-repudiation of information, through comprehensive risk management, implementation of physical and digital controls, to prevent incidents, and complying with legal requirements. For this reason, **KEDRIÓN** has defined and implemented an Information Security and Privacy Policy, considering the following aspects:

6.1. Protect information assets, through policies, procedures, and instructions on information

[31] ISO 27000
[32] ISO 27000.
[33] ISO Guide 73:2002
[34] Law 1581 of 2012
[35] NTC-ISO/IEC 27001
[36] Law 1266 of 2008
[37] ISO 27000
[38] ISO 27000

security, considering the useful life cycle of the data.

6.2. Apply access controls to the information created, processed, transmitted, or safeguarded by the business processes, to minimize financial, operational or legal impacts due to incorrect use of this, taking into account the classification of the information to which it is Treated.

6.3. Mitigate the risk of vulnerability in information security, in the execution of the processes and activities of **KEDRIÓN**, through an adequate management of security events and risks associated with the processing of personal data and information management.

6.4. Comply with the principles (Availability, Integrity, and Confidentiality) of information security.

6.5. Strengthen the culture of information security within the organization.

6.6. Periodically verify compliance with information security policies.

6.7. Comply with established legal, regulatory, and contractual obligations.

7. SPECIFIC INFORMATION SECURITY AND PRIVACY POLICIES

7.1. INFORMATION SECURITY ROLES

In response to the organizational structure of **KEDRIÓN,** the person in charge of verifying compliance and monitoring the measures established in the Security and Information Security Policy will be the Legal Representative.

7.2. ASSET MANAGEMENT

7.2.1. Liability to information assets:

7.2.1.1. Strive for the security and quality of information, following criteria of confidentiality, integrity, availability, effectiveness, efficiency, reliability, and compliance, as collaborators, suppliers and / or third parties with whom **KEDRIÓN** has a relationship in the ordinary course of business.

7.2.1.2. Comply with defined information security policies and controls to ensure the preservation of confidentiality, integrity, availability of the organization's information assets, and information retrieval.

7.2.1.3. It is forbidden to make modifications to the information assets, without prior, express and written authorization to do so.

7.2.1.4. It is forbidden to use **KEDRIÓN's** information assets for purposes other than the fulfillment of the organization's own activities.

7.2.1.5. Make the inventory of all information assets, which must be assigned to a responsible,

7.2.1.6. Periodically update all information assets, with guidelines related to access restrictions.

7.2.1.7. Be responsible for the use and protection of the assets of the information, as in charge of this, while it is in its physical custody or digital.

7.2.1.8. Report any security incidents that may occur, such as: misuse, alteration and/or unauthorized disclosure.

7.2.2. Asset identification

The information assets that **KEDRIÓN** has are made up of: information related to the constitution and composition of the organization, and three (3) databases called: "kedrión clients", "kedrión suppliers" and "kedrión payroll".

The identification of the information assets that **KEDRIÓN** has, is carried out manually given the size of the organization.

7.2.3. Labelling of information

To identify the nature and type of personal data and in general, information, with respect to which Treatment is carried out; The following classification should be considered:

7.2.3.1. **Public Information:** It is all information that an obligated subject generates, obtains, acquires, or controls in its capacity as such. Literal b) of Article 6 of Law 1712 of 2014.

7.2.3.2. **Classified Information:** It is that information that being in the possession or custody of an obligated subject in its capacity as such, belongs to the own, private, and private or semi-private scope of a natural or legal person, so that its access may be denied or excepted, if it is the legitimate and necessary circumstances and the particular or private rights enshrined in article 18 of Law 1712 of 2014.

7.2.3.3. **Sensitive information:** Sensitive data is understood to be those that affect the privacy of the Holder or whose improper use may generate discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership of trade unions, social organizations, human rights or that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties as well as data relating to health, sex life and biometric data.

7.2.3.4. **Reserved Information:** It is that information that being in the possession or custody of an obligated subject in its capacity as such, is exempted from access to citizenship for damage to public interests and under compliance with all the requirements enshrined in article 19 of Law 1712 of 2014.

The person responsible for verifying the understanding and proper classification of the information will be the Legal Representative of **KEDRIÓN.**

7.2.4. Disposition of assets

To establish rules for the acceptable use of the identified information assets and the infrastructure intended for the processing of the information, the necessary restrictions in the

management of the information will be documented, in accordance with the protection requirements determined by the type of information and its classification.

The authorized **KEDRIÓN** collaborators involved in the processes that manage and process the information assets will be registered.

The guidelines and procedures of IT operation in **KEDRIÓN** will establish the actions in the management of any mobile and reusable means that will be transported or decommissioned from the organization. Once the media is removed, measures will be taken to ensure that the information is not recoverable, these activities must be recorded, documented, and reported to those responsible for the processes of backup and recovery of information.

The transportation of means with missionary information or associated with the contractual object of the organization must be through duly certified specialized service providers. Prior authorizations for the transfer or disposal of media must be registered and available for subsequent consultation. The formats used for the storage of the information according to its classification and risk assessment must be current standards in the market both in the encryption and in the location of the information, this to facilitate its recovery, therefore, the follow-up to the periodic exercises of recovery of backups will evaluate the effectiveness of the restoration and the technological validity to the infrastructure of "*BackUp*".

7.3. ACCESS CONTROL POLICY

7.3.1. Objective

Establish the definitions of access to authorized users to systems, applications, and other technological resources, exercising the assignment, modification, revocation and management of permissions under the following guidelines:

7.3.1.1. Minimum privilege.
7.3.1.2. The strict need to fulfill the assigned functions.
7.3.1.3. Dual control set on role and profile flows.
7.3.1.4. Consistency between access rights and information classification policies of systems and networks.
7.3.1.5. The security requirements of each of the applications.
7.3.1.6. All information related to applications.
7.3.1.7. Applicable law and contractual obligations regarding the protection of access to data and services.
7.3.1.8. The access profiles of base users, common to each category of jobs.
7.3.1.9. Manage access rights in a distributed and network environment, which recognize all types of available connections.
7.3.1.10. Periodic review of access rights.

7.3.2. Assignment of Permissions and/or assignment of passwords

The permissions will specify what actions can be performed on the information (creation, reading, deletion, modification, copying, execution, etc.). As a rule, the minimum privilege will always be granted in the establishment of permits.

The assignment of passwords will be controlled through a formal management process, using the following flow:

7.3.2.1. Require users to sign a statement committing to keep their personal passwords secret.
7.3.2.2. Ensure that users change the initial passwords assigned to them the first time they log in. Temporary passwords, which are assigned when users forget their password, should only be provided after the user is identified.
7.3.2.3. Generate temporary passwords to start users. Third party involvement or the use of unprotected e-mail messages (plain text) in the password delivery mechanism should be avoided and users should acknowledge receipt when they receive it.

7.3.3. Creating/modifying/deleting user accounts

To allow access to **KEDRIÓN's** information systems, the procedure must be followed to manage the creation/modification/deletion of users' access accounts, indicating who should authorize it. Detail the identifying data of the same, the actions that are allowed and providing them with the corresponding access credentials that must be delivered confidentially to their owners. It will also include parameters such as password expiration and appropriate locking procedures. The user must be informed of these requirements when handing over the credentials, as well as the Password Policy.

7.3.4. Privileged accounts

The Information Officer shall limit and control the assignment and use of privileges. Multi-user systems that require protection against unauthorized access should provide for a controlled privilege assignment through a formal authorization process.

The following steps should be considered:

7.3.4.1. Identify the privileges associated with each asset that requires user access, such as operating system, database and application management system, and the categories of personnel to which products should be assigned.
7.3.4.2. Assign privileges to users based on usage need and event per event.
7.3.4.3. Maintain an authorization process and a record of all assigned privileges. (Note: Privileges should not be granted until the formal authorization process has been completed.)
7.3.4.4. Establish a period of validity for the maintenance of privileges, after which they will be revoked. (Note: There must be NO users without an effective date)
7.3.4.5. Promote the development and use of system routines to avoid the need to grant privileges to users.

7.3.5. Authentication mechanisms

To establish the appropriate authentication mechanisms to allow access to the organization's information, aspects such as the following will be considered:

7.3.5.1. Use internal authentication mechanisms or those based on third-party authentication services
7.3.5.2. Technologies that can be used: web authentication, directory services, LDAP.
7.3.5.3. Factors of authentication mechanisms (one or several): (*i*) something we are (through biometric techniques), (ii) something we know (through passwords), (*iii)* something we have (through personal devices, cryptographic *tokens*).

7.3.6. Event Log

The necessary mechanisms must be established to record the relevant events, guaranteeing their conservation and authorized access in the management of the organization's information. Likewise, its will conveniently record who accesses the information, when, how and for what purpose.

7.3.7. Permission Review

The owners of the information assets that correspond to the application services will establish the periodic requirements for the evaluation of the permissions, including the privileged users.

7.3.8. Revocation of permissions

In compliance with the procedures of management of users based on the requests of the owners of the assets, sufficient and necessary actions will be taken to revoke the privileges, permissions, and accesses of any user, who for reasons of transfers or disassociation requires such revocation. Technical mechanisms should be provided for compliance, registration, and follow-up.

7.4. CONTROLS AGAINST MALWARE

KEDRIÓN shall establish detection and prevention controls for protection against malicious software, establishing and executing appropriate security awareness procedures and system access controls.

Controls will be applied such as:

7.4.1. Prohibit the use of unauthorized software.
7.4.2. Evaluate the risks related to obtaining files and software from or through external networks, or by any other means, indicating the protection measures to be taken.
7.4.3. Install commercially available advanced virus detection and repair software to

permanently examine information and computing assets by any workstation, server, or infrastructure

7.4.4. Keep systems updated according to the releases generated by their manufacturers.

7.4.5. Establish procedures to verify all information related to malicious software issued by validated channels and entities.

7.5. CLEAN DESK

This policy aims to safeguard the information assets associated with workstations and computer equipment through the actions of maintaining a clean workplace and unexposed information processing data, to reduce the risks of unauthorized access, leakage or damage of information during and after the working day.

Workstations must be configured session lock, which must be activated automatically maximum after one hundred and eighty seconds or three minutes of inactivity and will be necessary to enter the session, write the user's password.

Whenever a user is absent from his work computer, he must lock the session by pressing the **Windows key + the L key** to avoid risks of unauthorized access.

Passwords should not be written on sticky notes on the desktop or any other visual medium or kept in view of others.

When sending documents to be printed, the printed document should be immediately removed from the printer.

At the end of the workday, documents and media containing **KEDRIÓN's** missionary fulfillment information should be kept in a safe place under lock and key**.**

7.6. REMOTE ACCESS

Users will be able to remotely access information assets through a VPN connection platform. Authorization must be requested for access. In any situation, such access will be managed by the personnel assigned for it and may only be intended to support technological equipment or information systems, review operating errors or provide security and / or monitoring services.

A record of the accesses that have been made through the VPN must be kept for traceability purposes and subsequent review if required.

VPN access must be associated with user management and follow the same guidelines for creation, modification, revocation, change and monitoring.

7.7. NON-REPUDIATION

The security and privacy policy includes the ability not to repudiate for users to avoid having taken any action. At least the following aspects must be included:

7.7.1. Traceability: The policy will ensure that through the traceability of the actions, the creation, origin, reception, delivery of information and others are monitored.
7.7.2. Retention: The policy must include the retention or storage period of the actions performed by users, which must be reported to the officers, contractors and / or third parties of the organization.
7.7.3. Audit: The policy will include conducting ongoing audits, as a procedure to ensure that the parties involved deny having taken any action.
7.7.4. Electronic exchange of information: The policy will include, where applicable, that electronic information exchange services are a guarantee of non-repudiation.

7.8. PRIVACY AND CONFIDENTIALITY POLICY

7.8.1. Objective

Describe the policies of Treatment and Protection of personal data that must be applied, in accordance with current regulations.

7.8.2. Principles of Personal Data Processing[39]

7.8.2.1. Principle of Lawfulness: The processing of personal data must be subject to the provisions of current regulations.
7.8.2.2. Principle of purpose: Indicate the purpose of the processing of personal data, which must be informed to the owner.
7.8.2.3. Principle of freedom: The treatment can only be done with the prior, express, and informed consent of the owner of the data.
7.8.2.4. Principle of veracity or quality: The information to be treated must be truthful, complete, accurate, updated, verifiable and understandable.
7.8.2.5. Principle of transparency: Guarantee the owner of the data the right to obtain information concerning him from the person in charge of the treatment.
7.8.2.6. 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.
7.8.2.7. 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.
7.8.2.8. Principle of confidentiality: All persons involved in the Processing of Personal Data must guarantee the confidentiality of such information

[39] Statutory Law 1581 of 2012 "General Regime for the Protection of Personal Data".

7.8.3. Confidentiality Agreement

In order to preserve the confidentiality and privacy of the information handled in **KEDRIÓN**, the confidentiality agreement implemented with collaborators, contractors and / or third parties will be used, in those events in which the information that is being treated deserves it.

7.9. INFORMATION AVAILABILITY POLICY

7.9.1. Recovery plans

To guarantee the continuity of services in the event of possible unwanted events that interrupt the operation of **KEDRIÓN's** processes, those that may cause interruptions in IT operations processes must be identified, for example, equipment failures, interruption of electrical power, flooding of facilities, and others that affect **KEDRIÓN's** information assets.

Assess risks to determine the impact of such outages, both in terms of magnitude of damage and recovery period, critical resources, impacts produced by an outage, acceptable or permitted outage times should be identified, and recovery priorities should be specified.

7.9.2. Service Level Agreements

The IT area and the Legal area will review existing contracts or agreements with service providers, considering the following guidelines:

7.9.2.1. Comply with the Information Security Policy.
7.9.2.2. Confidentiality agreement for information that is shared transmitted or managed.
7.9.2.3. Description of the contracted services Expected level of service according to the nature of the service contracted with the due fines for non-compliance with the agreed levels.

7.9.3. Segregation of environments

Development, test, and operations environments shall be separated according to the following definitions:

7.9.3.1. Run development and operations software in different operations environments, computers, or directories.
7.9.3.2. Separate development and testing activities into different environments.
7.9.3.3. Prevent access to compilers, editors, and other system utilities in the operating environment.
7.9.3.4. Use independent authentication and authorization systems for different environments, as well as access profiles to the systems.
7.9.3.5. Prohibit users from sharing passwords on these systems. The interfaces of

the systems will clearly identify to which instance the connection is being made.

7.9.3.6. Define owners of the information for each of the existing processing environments.

7.9.3.7. Development personnel will NOT have access to the operating environment.

7.9.4. Change Management

Procedures for controlling changes in the operational and communications environment should be defined. Any changes must be previously assessed for technical and safety risk aspects. It must be ensured that changes in the operational and communications components do not affect the security of these or the information they support.

The change procedures shall assess the potential operational impact of the planned changes and verify their correct implementation. The Information System Manager shall maintain an audit trail containing all relevant information on each change implemented.

The change control procedures shall cover the following points:

7.9.4.1. Risk assessment of the possible impact of such changes.
7.9.4.2. Formal approval of proposed changes.
7.9.4.3. Planning of the change process – Detail engineering.
7.9.4.4. Test of the new scenario.
7.9.4.5. Communication of details of changes to all relevant persons.
7.9.4.6. Identification of responsibilities.
7.9.4.7. Return activities in the event of unforeseen events.

7.10. REGISTRATION AND AUDIT

The person responsible for carrying out the audit and recording of the evidenced findings will be the Legal Representative of **KEDRIÓN** or its formally designated delegate.

The audit will be carried out every six months, and a record of the findings that are evidenced must be drawn up, in such a way that a consecutive record of compliance with this obligation is administered.

7.11. INFORMATION SECURITY INCIDENT MANAGEMENT

7.11.1. Risk level of the security incident[40]

The level of risk shall be calculated in relation to the risk posed by the security incident to the Data Subjects, as follows:

[40] Superintendence of Industry and Commerce, Security Incident Management Guide, 2020.

LOW RISK: The security incident is unlikely to have an impact on people, and if it does, it would be minimal.
MEDIUM RISK: The security incident may have an impact on people, but the impact is unlikely to be substantial
HIGH RISK: The security incident can have a considerable impact on the people affected.
SERIOUS RISK: The security incident can have a critical, extensive, or dangerous impact on the people affected.

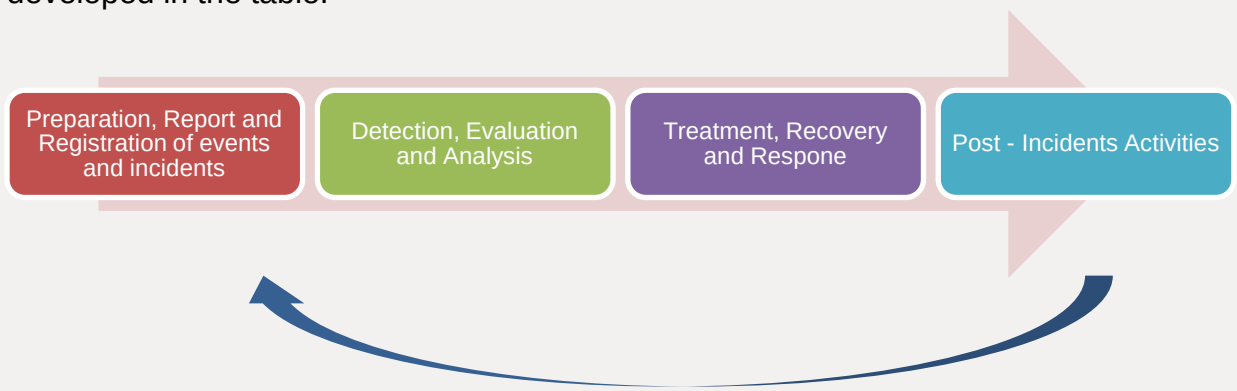
7.11.2. Response protocol in the handling of security violations or incidents

This protocol seeks to have a structured and planned guideline that allows to adequately handle security incidents associated with the processing of Personal Data in **KEDRION** to:

7.11.2.1. Properly manage the technological events associated with the processing of Personal Data
7.11.2.2. Manage security incidents associated with the processing of Personal Data
7.11.2.3. Integrate the procedures for attending events associated with the processing of Personal Data

Events and incidents associated with the processing of Personal Data may occur at any stage of **KEDRIÓN's** data lifecycle. It is important to consider that "the probability of a security breach materializing is never zero, and the longer it elapses, the greater the probability of an incident occurring."[41]

The protocol for managing security incidents associated with the processing of Personal Data will be developed according to the following phases in a cyclical manner, as shown in the image and developed in the table: [42]



Incident Management Life Cycle

[41] Spanish Agency for the Protection of Personal Data. *"Risk management and impact assessment on personal data processing"*. Madrid, 2021. Page 46.
[42] https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf, page 2.

STAGE	DESCRIPTION
Preparation, Report and Registration of security events and incidents associated with the processing of personal data	It allows **KEDRIÓN** to be able to respond to incidents associated with the processing of Personal Data and, in addition, to develop a way in which vulnerabilities can be detected, evaluated and managed, that is, technical and organizational measures to be able to face an incident associated with the processing of Personal Data, in order to mitigate the risks.
Detection, Evaluation and Analysis	**Detection** is responsible for the identification and management of elements that alert about an incident, provides information about the future occurrence of the same and affects the preparation of procedures to mitigate its impact. To this end, **KEDRIÓN** must: i) define a list of sources generating events that allow the identification of a security incident associated with the processing of personal data, ii) seek strategies so that the incident does not spread and generate more damage. The strategies vary according to the type of incident associated with the Processing of personal data, iii) define the level of priority, the criticality of impact -the current impact and the future impact-, in order to implement adequate attention to security incidents associated with the processing of personal data. Regarding the **evaluation** of an incident, the level of impact according to **KEDRIÓN's** risk analysis and classification of information assets must be considered, depending on its infrastructure, risks and criticality of its assets. Finally, to determine more accurately the classification of the incident in the analysis of security breaches, it must be considered: (i) The technological component focused on security controls and measures, (ii) The assessment of risks to the rights and freedoms of individuals.
Containment, Eradication, Recovery and Response	**Containment** allows timely decisions to be made to prevent the spread of the incident and thus reduce damage to IT resources and loss of confidentiality, integrity and availability associated with the processing of personal data.

STAGE	DESCRIPTION
	Eradication is the stage in which traces that could have left the cause of the incident and that involve the occurrence of a new one must be eliminated if they remain active. It is essential to have the technical and human resources to correctly preserve the possible evidence that serves to locate the person responsible for the incident, if any. Finally, **recovery** is the elimination of traces left by the incident associated with the Processing of personal data and the subsequent restoration of the affected system and / or services. It is important to keep in mind that in case an incident seriously affects, the BCP (Business Continuity Plan) or the DRP (Disaster Recovery Plan) can be activated.
Post-Incident Activities	The post-incident activities are composed of the report of the Incident associated with the Processing of personal data, the verification of the lessons learned, the design and implementation of technological, disciplinary and criminal measures if necessary as well as the registration in the knowledge base to feed the indicators.

7.11.3. Points or contact persons

If the security and / or privacy of the information managed by **KEDRIÓN** is at risk of a security incident, you should immediately contact the Legal Representative of the organization:

Representative Legal: Juan Carlos Beltrán Gonzalez

Contact Number: +57 3173657453

Email: j.beltran@kedrion.com

7.11.4. Incident Report

KEDRIÓN, as Responsible for the Processing of Personal Data, is obliged to adopt the necessary security measures at its disposal to prevent unauthorized access and alteration of Personal Data. However, in the event of a violation of the security codes, it will inform the SIC of this circumstance, in accordance with the guidelines established within the organization.

For this, the personnel in charge of making the report to the SIC will be the Legal Representative of **KEDRIÓN.**

7.11.5. Documentation and/or internal record of the incident

If an incident of security and / or privacy of **KEDRIÓN's** information occurs, the Legal Representative must keep a documentary record, with the following information:

7.11.5.1. Overview of the circumstances of the security incident
7.11.5.2. Compromised information and/or data
7.11.5.3. Category of information subjects
7.11.5.4. Date and time of the security incident and/or the discovery of the security incident
7.11.5.5. Investigations carried out by the person in charge
7.11.5.6. Corrective measures implemented
7.11.5.7. Proof of the report made to the SIC, when necessary
7.11.5.8. Proof of the communication made to the holders of the Information, if applicable
7.11.5.9. Risk level assessment

7.12. Information security training and awareness

KEDRIÓN, through its Legal Representative, must inform the other members of the organization of this Information Security and Privacy Policy, periodically raising awareness about the importance of the principle of security in the Treatment of information that is carried out by the organization, and the implications that would bring the breach of it.
Of the sensitizations that are made within the organization, a record will be drawn up stating: date of realization, theme, and participants.

8. VALIDITY

This policy is effective from the date of its approval. The modifications made to the policies described here will give rise to a new version of the document.

Given in Bogotá D.C. on the twenty-second (22nd) day of August, two thousand and twenty-two (2022).