# PROTOCOL FOR THE USE OF THE ITINERE GROUP WHISTLEBLOWERS CHANNEL

## Background

Following the Spanish Criminal Code was reformed in 2010, and Organic Law 1/2015 enacted in March 30th, companies have been required to have control systems that more effectively prevent, detect and react to the risk of any member of the organisation perpetrating a potentially criminal act within their organisation.

The Spanish Public Prosecution Office places special value on disclosure of infractions to the competent authorities by the company itself.

The Whistleblowers Channel enables confidential communication through a simple form that can be filled out and sent subject to the highest standards of integrity, security and confidentiality of user data. Using this channel, potentially irregular activities and behaviours that may breach the code of conduct and/or potential perpetration of a criminal, administrative infraction and/or any other that may entail incurring a risk of a breach that runs contrary to the DNA and the set of values and principles of the ITINERE Group and the companies comprising it can be sent over a secure encrypted SSL connection.

The ITINERE Group Code of Conduct can be consulted on this link:

https://www.grupoitinere.com/wp-content/uploads/IT%C3%8DNERE-GROUP-CODE-OF-CONDUCT-Dic-2019.pdf

**Article 1. Personal scope of application**

The Whistleblowers Channel is open to all employees, workers, clients, suppliers and vendors working with the ITINERE Group that have or may have knowledge of an irregularity committed by any other employee, worker, director, vendor, supplier or, in general, anyone subject to the authority and/or control of any of the companies comprising the Group, acting on the behalf of and to the account of such parties. The following parties fall within its personal scope of application, although the list is not exclusive:

a) persons who are workers in the sense of the prevailing legislation;

b) Shareholders and persons belonging to the bodies for directing, administering or supervising a company, including non-executive members, and volunteers and interns, whether or not they are paid;

c) Contractors, suppliers and/or vendors and any individual or organisation working under the oversight and direction of the above.

**Article 2. Whistleblowing and follow-up procedures**

The procedures for processing and managing the internal complaint to which this protocol refers, will be as follows:

a) Preferentially, the whistlblower should communicate the infraction or irregularity they wish to bring to the attention of the ITINERE Group using the whistleblowing channel on the ITINERE Group website, identifying the informant, since this will facilitate the processing, investigation and efficacy of the Whistleblowers Channel as a tool for detecting potential illicit acts, whether criminal, administrative or breaches of the internal standards and protocols applicable to all members of the ITINERE Group. In all cases, as explained below, when a complaint is lodged, the confidentiality of the whistleblower's identity will be guaranteed, and the prohibition enforced to prevent any retaliation against the whistleblower, as stated in articles 4, 6 and 7 below.

The document ends with details on how to fill in the form and communicate the facts.

b) All complaints communicated over the Whistleblowers Channel will be received by the Itínere Group Compliance Area, which will notify the whistleblower of receipt within a maximum of 7 days. Should the complaint have been communicated verbally (face to face or over the phone), the 7-day period will begin from the signature of the transcription or the complaint document, as shown in the section of "Recording Complaints" below;

c) The Compliance Area will be responsible for a preliminary analysis of the facts, issuing an initial opinion on the entity and truth of the facts. To such end, the Area may request additional information from the whistleblower;

d) Should the facts of the complaint not evince an infraction of ITINERE Group corporate policies or a potentially criminal act or any act that might have an impact on the Group (in criminal, reputational or monetary terms), it will be disallowed and the data contained in the complaint will be immediately erased;

e) Within a maximum of 5 days after acknowledging receipt of the complaint, and whether or not it has been disallowed, the Compliance Area will inform the ITINERE Group Compliance Unit of the content of the complaint;

f) Should the complaint not be allowed for processing, the person to whom the complaint refers or, as applicable, the head of the area affected, when the facts concern an ITINERE Group operating unit, will be given reserved information on the following, always respecting their right to honour, intimacy and dignity:

f.1) Receipt of the complaint.

f.2) The grounds of the complaint.

f.3) The department and third parties, if any, about which the complaint was made.

f.4) Their right, if this is deemed necessary or advisable, to take legal advice at their own cost.

f.5) How to exercise their rights to access, rectification, suppression, limitation, challenge and portability of their personal data and not to be subjected to automated decision-making.

g) The identity of the whistleblower will never be disclosed;

h) However, if the ITINERE Group Compliance Unit deems there to be a risk that notifying the object of the complaint could compromise the investigation, the Unit may resolve to postpone the communication for up to one month from when the complaint is received (extendible by one more month) or until such risk disappears, whichever comes first. Within a maximum of 3 months from the submission of the acknowledgement of receipt to the whisteblower, the ITINERE Group Compliance Unit;

i) The Compliance Unit will initiate suitable investigations into the content of the complaint. To such end, it will delegate in one of its members to carry out due diligence to reveal denounced facts. The Compliance Unit may decide to bring in external help to check out possible infractions;

j) Once the investigation has concluded, the Compliance Unit, at the proposal of the instructor and in light of the evidence, may:

j.1) Definitively archive the complaint.

j.2) Propose disciplinary measures.

j.3) Pass on the complaint, with the facts and evidence from the investigation, to the State Public Prosecution Office, Judges and Courts or Security Corps.

k) Disciplinary measures will be applied by the person or department to which such duties are attributed.

**Article 4. Duty of Confidentiality**

1. The ITINERE Group guarantees maximum confidentiality regarding the whistleblower's identity. The whistleblower's identity will not be disclosed without express consent to anyone who is not authorised to manage the Whistleblower Channel. It will not be disclosed to the party about which the complaint is made. No other information will be disclosed from which the whistleblower's identity might be deduced directly or indirectly. All parties apprised of the complaints made through the channels established by the Board of Directors for the ITINERE Group are obliged to maintain professional secrecy regarding the whistleblower's identity.

2. The sole exception to the previous section would be the disclosure of the whistleblower's identity when, in light of the investigation, it becomes necessary to submit the facts to a judicial authority, the public prosecution office or the State security corps. In such cases, the whistleblower will be informed before their identity is disclosed, unless such information might compromise the court proceedings or investigation.

**Article 5. Recording Complaints**

the ITINERE Group will keep a record of all complaints received, which will be stored only during the period required and in a manner proportionate to requirements.

When the whistleblower uses the telephone or recorded voice media, the ITINERE Group will be entitled to document the verbal complaint in one of the following manners, with the previous consent of the whistleblower:

a) By recording the conversation in a robust, accessible format, or

b) By the person in charge of processing the complaint making a complete, verbatim transcription of the conversation. The ITINERE Group will offer the whisteblower the chance to check, and rectify the transcription of the call and accept it with their signature.

In cases where the whistleblower uses an unrecorded telephone conversation or voice messaging, the ITINERE Group will be entitled to have the staff responsible for processing the complaint document the verbal complaint as a detailed transcript of the conversation, although the whistleblower will be able to check, rectify and accept this transcript before signing it.

When a person requests a meeting with the ITINERE Group staff in charge of managing the Whistleblower Channel, complete, exact records will be kept of the meeting on a robust, accessible:

a) By recording the conversation in a robust, accessible format, or

b) Through detailed minutes of the meeting drawn up by the staff responsible for processing the complaint, duly read, and where applicable, rectified and then signed by the whistleblower.

**PROTECTION MEASURES**

**Article 6. No retaliation allowed**

The ITINERE Group guarantees absolute protection against any form of direct or indirect retaliation, expressly forbidding any retaliatory measures from being taken, encouraged or tolerated. Thus, the ITINERE Group will prevent any whistleblower from suffering retaliation, threats or attempted retaliation in general relating to use of the Whistleblower Channel and more particularly, will not allow:

a) suspension from their job and salary, dismissal, severance or equivalent measures;

b) demotion or refusal of deserved promotion;

c) change of job, relocation of workplace, wage reduction or change of working hours;

d) refusal of training;

e) negative performance assessment or references regarding performance at work;

f) imposition of any disciplinary proceedings, reprimand or other punishment, including fines.

g) coercion, intimidation, bullying or ostracism;

h) unfair or unfavourable treatment or discrimination;

i) failure to convert a temporary employment contract into an open-ended one when the worker has legitimate expectations of being offered a more permanent job;

j) failure to renew or early cancellation of a temporary employment contract;

k) damages in general, including reputational damage, especially in social and corporate media, or monetary looses, including loss of business and income;

l) blacklisting under informal or formal sectoral agreements that could mean the whistleblower may not find future employment in the sector;

m) early termination or cancellation of contracts for goods or services;

n) cancellation of licences or permits;

o) dissemination of any medical or psychiatric information known to the ITINERE Group that may undermine or breach the whistleblower's right to honour and dignity as a person.

**Article 7. Protection against retaliation**

In no event will disclosure of facts that could be infractions of the ITINERE Group Code of Conduct, its corporate policies or criminal law over the Whistleblower Channel be considered a breach of the non-disclosure agreement the whistleblower may have signed.

Cases in which the acquisition or access to the information is in itself criminal are excepted from the above.

**Article 8. Processing of personal data**

1. Personal data ensuing on use of the Whistleblower Channel will be employed exclusively to investigate and process the facts of the complaint, in compliance with the requirements of Constitutional Act 1/2015, 30 March, Constitutional Act 3/2018, 5 December, on Personal Data Protection and guarantee of digital right, EU Regulation 2016/679 and EU Directive 2016/680. No personal data will be gathered that are not manifestly pertinent to a specific complaint. If such data are gathered without intent, they will be eliminated without undue delay.

2. The data facilitated over the Whistleblower Channel will not be assigned; they will be incorporated into a file held by the Company for managing the Whistleblower Channel and for the purposes of processing, investigating and resolving the case. Whistleblowers will be informed of the ends and uses to which their personal data are processed. The data will be conserved for the time necessary for the processing, management and/or investigation of the facts of the complaint.

3. ITÍNERE INFRAESTRUCTURAS S.A. will be:

3.1. Controller of personal data of employees of ITÍNERE DE INFRAESTRUCTURAS, S.A.

3.2. Joint controller for the processing of personal data of employees of the subsidiaries comprising the ITINERE Group that may arise from this protocol regarding the use of the Whistleblower Channel.

4. The grounds for processing personal data stemming from the use of the Whistleblower Channel are legitimate when:

4.1 Consent has been given by the interested party for one or more ends;

4.2 It is necessary to protect vital interests of the interested party or other parties;

4.3 It is necessary in order for the responsible party to comply with a legal obligation;

4.4 It is necessary to satisfy prevailing legitimate interests of the responsible party or third parties to which the data are communicated;

5. The Company will adopt adequate technical and organisational measures to guarantee the security of the personal data received over the Whistleblower Channel in order to avoid their alteration, loss or unauthorised processing or access. These measures will be in keeping with the state of current technology, the nature of the data and the risks to which they may be exposed.

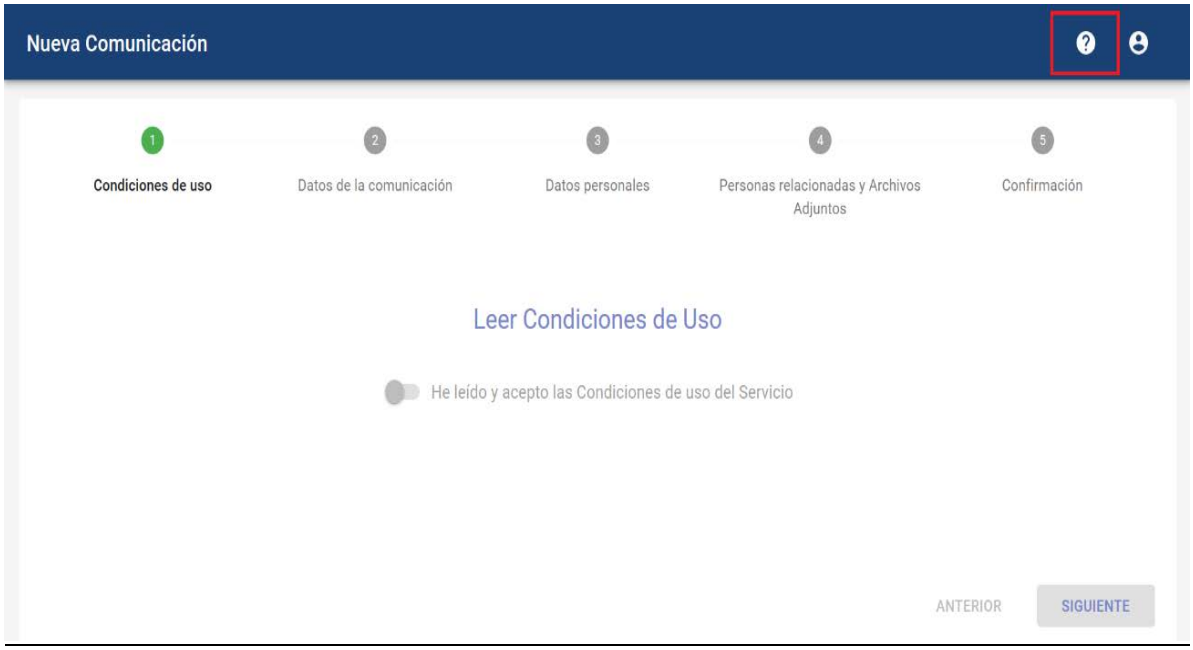
6. Users of the Whistleblower Channel will ensure the personal data provided in their queries or complaints are true, exact, complete and up to date. These data will be cancelled as soon as the investigations have concluded, except in cases in which they are required for government or judicial purposes. Likewise the Company will keep these personal data blocked during the periods in which the complaints or the internal investigations they trigger evince potential legal liabilities.

7. Whistleblowers who have been identified by using the Whistleblower Channel have their rights guaranteed to exercise access, rectification, challenge, limitation, portability and suppression over their personal data, through written communication addressed to the Compliance Area at dpd@grupoitinere.com accompanied by a photocopy of their national identity document (or equivalent for foreign nationals) indicating the right they wish to exercise.

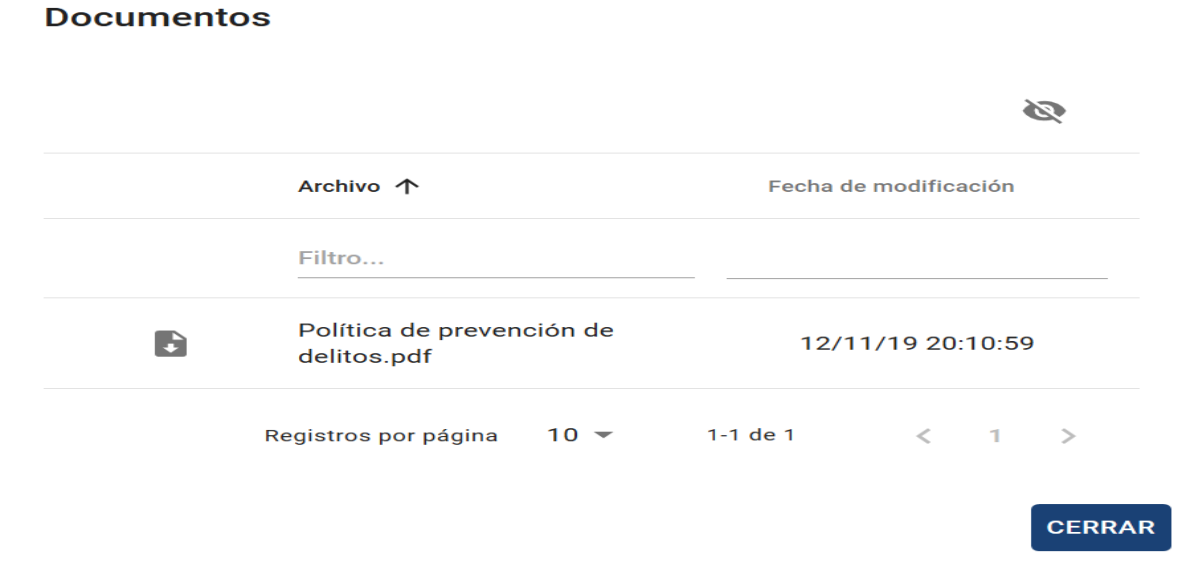
8. They also have the right to present a complaint to the Spanish Data Protection Agency. More information is available on the Data Protection Agency's website www.aepd.es.

**USE OF THE ITINERE GROUP WHISTLEBLOWER CHANNEL**

Whistleblowers must complete the following 5 steps: At any moment, it is possible to consult the support documentation made available to the whistleblower on this channel:

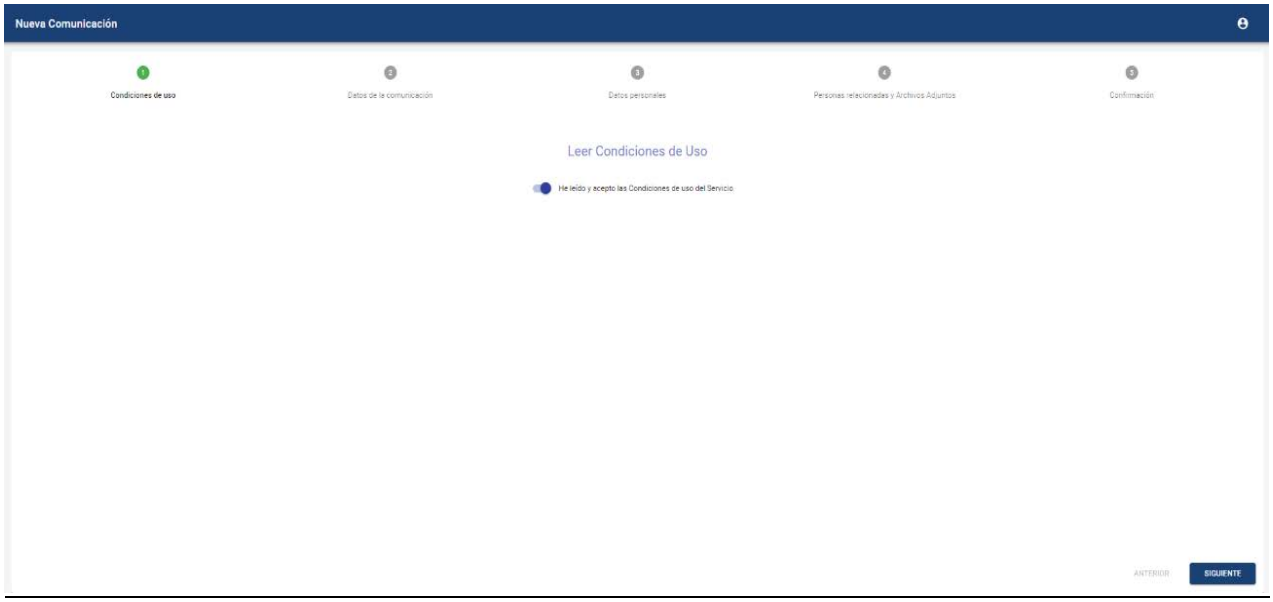



Clicking on the button opens a dropdown menu of documents. Should there be no document, the link to this user manual will appear.



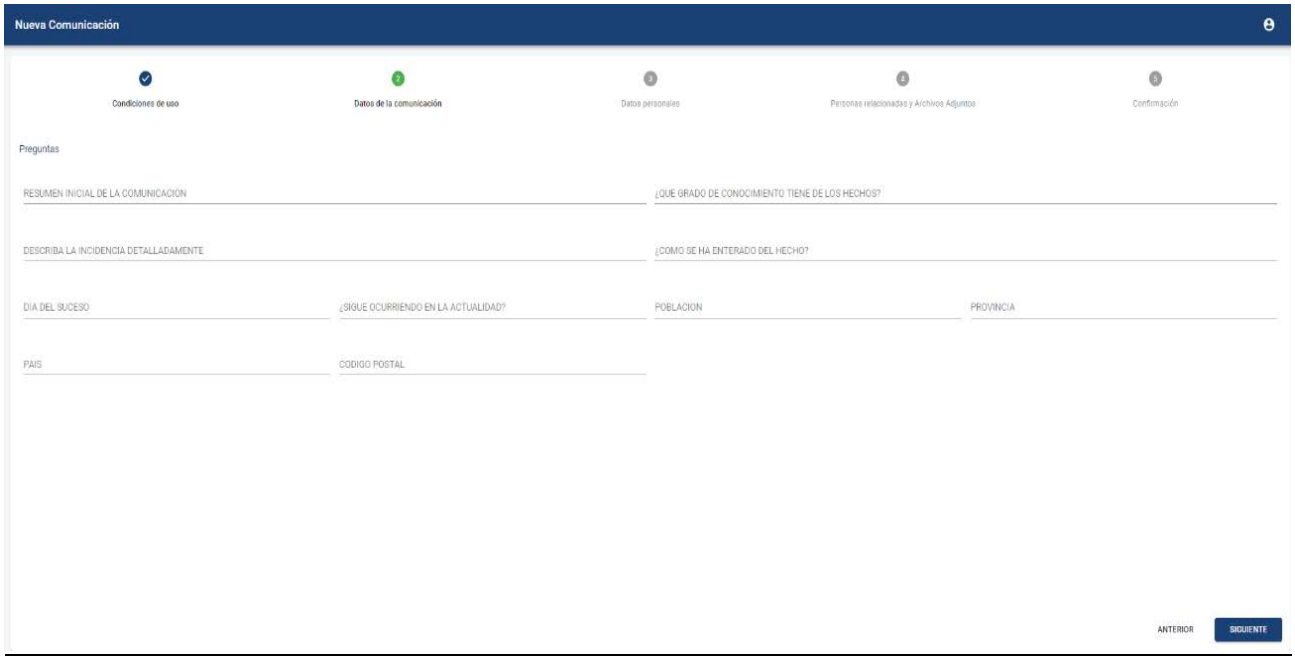
## 1- Acceptance of conditions of use.

It is mandatory to read the conditions of use of the channel to continue with the procedure.



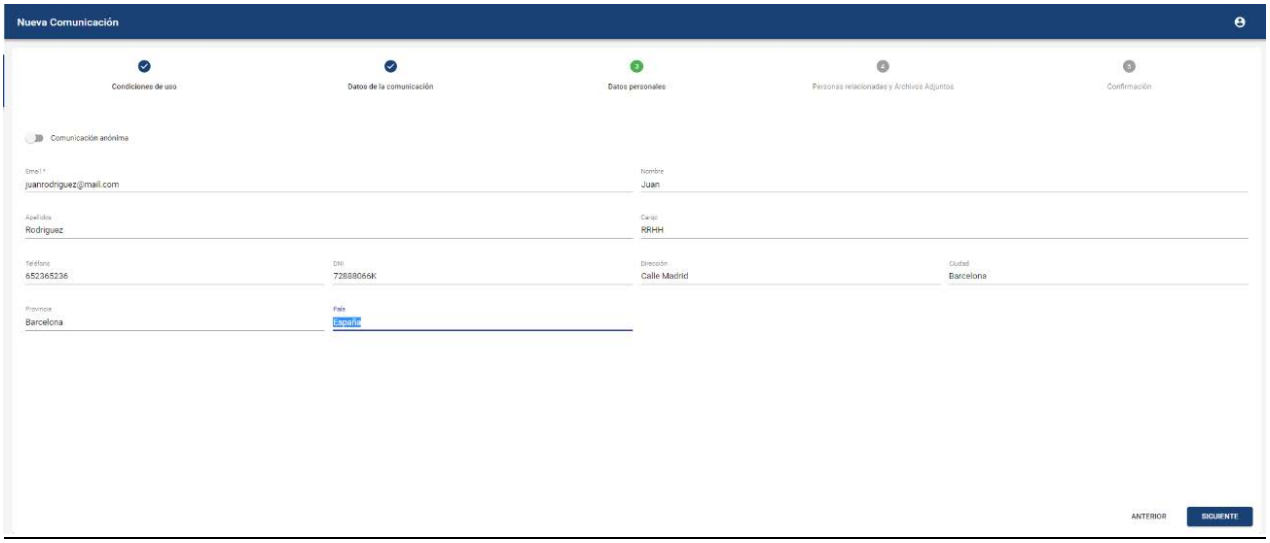

## 2 - Communication data

General form in which to **submit the complaint**.



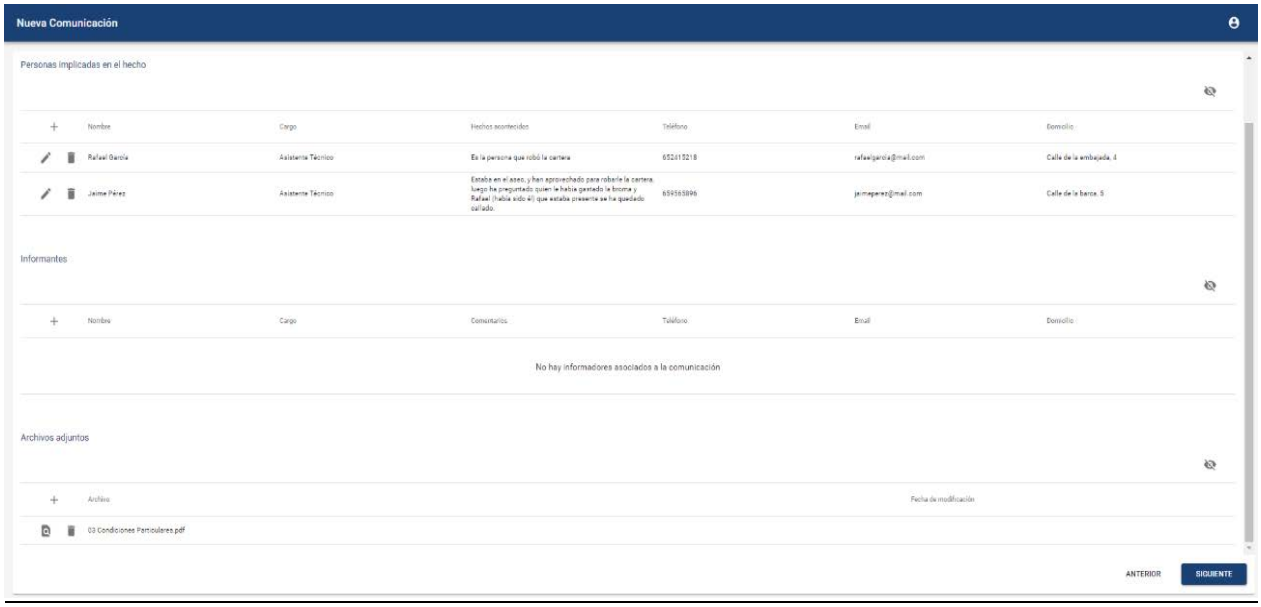
## 3 - Personal data

Personal data of the **whistleblower**




## 4 - Parties involved in the facts or with further information plus attached files

This provides space to report on the parties pertaining to the complaint communicated and persons who may have further information, and to attach files that may provide proof or evidence of the denounced facts.



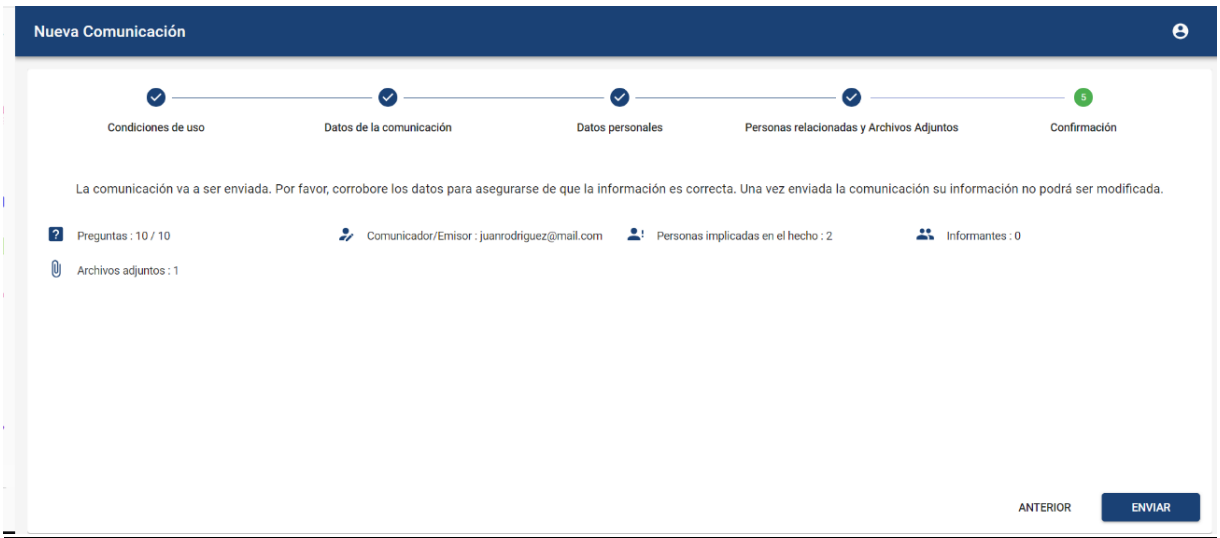
Example for inputting a party implicated in the matter:


The files attached to the communication must in any of the following formats:

.7z, .ac3, .avi, .bmp, .bpm, .bpmc, .csv, .doc, .docx, .dot, .jpeg, .jpg, .mgr, .mkv, .mov, .mp3, .mp4, .mpp, .mpt, .msg, .odg, .odp, .ods, .odt, .pdf, .png, .pps, .ppsx, .ppt, .pptx, .rar, .rtf, .txt, .vsd, .vst, .wmv, .xls, .xlsm, .xlsx, .zip

## 5 - Confirmation

Overview of the complaint to be sent.



## 6 - Username and Password

Once the report is communicated, the system will provide a username and password. THESE ARE FOR EXCLUSIVE USE BY THE WHISTLEBLOWER. IT IS VERY IMPORTANT TO **CONSERVE YOUR USERNAME AND PASSWORD** IN ORDER TO ACCESS THE DENOUNCEMENT AFTER IT HAS BEEN LODGED. YOU CANNOT ACCESS WITHOUT YOUR USER NAME AND PASSWORD


This platform provide two-way communication between the Compliance Department and the whistleblower. Should it be necessary, the whistleblower can receive communications in emails, receiving an alert. It is important to keep in mind that communications will be received at the email address indicated by the whistleblower.

After receiving the alert, the whistleblower must use their user name and password to access the platform and check the content of the communication on it. The communication may be of various kinds, including:

- Request for further information.
- Notification of changes in the status of the proceedings (pending, processing, under investigation, resolved).
- Posting of documents by the platform manager.
- Request for personal interview.
- Others.