

Robocall Mitigation Program (RMDB)

1.	Purpose	3
2.	Scope	4
3.	Definitions.....	5
4.	Grounds for Certification (Option 3)	6
5.	Reasonable Steps to Mitigate Robocalls	7
5.1.	Customer Due Diligence	7
5.2.	Knowledge of Upstream Providers.....	7
5.3.	Traffic Analysis and Illegitimate Traffic Detection Systems.....	7
5.4.	Technical Access Control Measures	7
6.	Commitment to Cooperate with Traceback Requests.....	9
7.	Statement on Prior Proceedings or Investigations	10
8.	Validity and Updates	11
9.	Signature	12
10.	Revision History	13

1. Purpose

This document establishes the **robocall mitigation program** (*Robocall Mitigation Program*) of Irontec, Internet y sistemas sobre GNU/Linux, S.L., prepared to comply with the regulations of the Federal Communications Commission (FCC) of the United States regarding call authentication (STIR/SHAKEN) and robocall mitigation.

Its purpose is to serve as the basis for the company's certification in the Robocall Mitigation Database (RMDB) under Option 3 (without STIR/SHAKEN implementation), and to provide stable documentation of the controls applied by the company in its voice traffic switching activity to destinations in the United States.

This document describes the procedures and controls that the company applies transversally to any client to which it provides voice traffic switching services to destinations in the United States.

2. Scope

The program applies to all voice traffic that the company originates to destinations in the United States through its international transit providers, regardless of the client, site, or country from which such traffic is routed.

It covers the entire service delivery chain: from the contracting and verification of the client to the delivery of traffic to the international operator responsible for termination in the United States.

3. Definitions

- **FCC (Federal Communications Commission):** regulatory body for telecommunications in the United States.
- **RMDB (Robocall Mitigation Database):** the FCC's public database in which voice service providers that originate, carry, or process traffic destined for the United States must register.
- **STIR/SHAKEN:** technical call authentication framework that verifies the legitimacy of the number originating a call.
- **Voice Service Provider (VSP):** a voice service provider that serves end users directly or serves other providers.
- **FRN (FCC Registration Number):** unique identifier assigned by the FCC through the CORES system, required to submit any application to the FCC.
- **CORES (Commission Registration System):** the FCC's registration system through which the FRN is obtained.
- **Traceback:** the process of tracing the origin of a call, requested by the FCC, law enforcement authorities, or the industry consortium (Industry Traceback Group).
- **Robocall:** an automated, mass call, typically unsolicited, that may constitute a fraudulent, abusive, or illegal practice.

4. Grounds for Certification (Option 3)

Irontec, Internet y sistemas sobre GNU/Linux, S.L. certifies that it has not implemented the STIR/SHAKEN authentication framework anywhere in its network.

This is because the company operates as a foreign voice service provider and does not control the network infrastructure required to implement STIR/SHAKEN on traffic destined for the United States. In the company's operating model:

- Voice traffic originates and is managed on the company's own switching platform, to which clients connect via SIP trunks.
- This traffic is then routed to interconnection providers and, similarly, to an international voice transit operator, which delivers it to its final destinations in the United States.
- The company does not have its own SPC (Service Provider Code) token, nor call-signing infrastructure on the U.S. public network, as it is not an operator domiciled in the US, nor does it have direct access to NANP numbering resources.

Consequently, call authentication via STIR/SHAKEN is beyond the company's direct technical control, which justifies certification under Option 3, complemented by the mitigation program described in the following section.

5. Reasonable Steps to Mitigate Robocalls

The company systematically applies the following controls to all its clients, regardless of the specific case or project:

5.1. Customer Due Diligence

Before enabling any SIP trunk or numbering for a client, the company applies the following controls:

- Verification of the identity and activity of the contracting client (company name, tax identification, and details of the company that actually contracts the service).
- Execution of a service agreement that identifies the intended use of the traffic and the client's obligations regarding the lawful use of communications.
- Review of the use case declared by the client and its consistency with the traffic patterns observed once the service is in production.

5.2. Knowledge of Upstream Providers

- The company selects as its international transit and termination providers, operators that have their own robocall mitigation programs and comply with their regulatory obligations in the jurisdictions where they operate.
- It maintains a direct, documented contractual relationship with these providers, with operational communication channels for resolving quality, fraud, or anomalous traffic incidents.
- The company periodically reviews the regulatory requirements imposed by its transit providers and adapts its operations accordingly.

5.3. Traffic Analysis and Illegitimate Traffic Detection Systems

- Monitoring of call detail records (CDR) and SIP signaling to track traffic routed to international destinations, including the United States.
- Review of anomalous traffic patterns (unusual volumes, abnormally short average call duration, concentration of attempts toward specific numbering ranges) indicative of fraudulent traffic or robocalls.
- Setting capacity limits per client and per trunk, so that a sudden increase in traffic can be detected and contained.
- Use of proprietary traffic analysis tools to investigate incidents reported by clients, providers, or regulatory bodies. No external analytics provider is used

5.4. Technical Access Control Measures

- Authentication of SIP trunks using client-specific credentials and, where applicable, IP address access restriction.

- Ability to immediately suspend a specific trunk or client upon detection of suspicious traffic, without affecting other clients on the platform.
- Full traceability of the internal origin of each call (client, trunk, and originating site), enabling precise responses to tracing requests (traceback).

6. Commitment to Cooperate with Traceback Requests

Irontec, Internet y sistemas sobre GNU/Linux, S.L. undertakes to respond fully and within a maximum of twenty-four (24) hours to any traceback request from the Federal Communications Commission (FCC), law enforcement authorities, or the industry consortium for call tracing (Industry Traceback Group), as well as to cooperate with such entities in investigating and stopping any illegal robocall activity that uses its services to originate calls.

7. Statement on Prior Proceedings or Investigations

As of the date of this certification, the company has not been the subject, in the preceding two (2) years, of any formal proceeding, investigation, or action by the FCC, law enforcement authorities, or any other regulatory body, with findings of actual or alleged infringement related to the transmission, facilitation, or concealment of illegal robocalls, spoofing practices, or a deficient robocall mitigation certification or program description in the RMDB.

8. Validity and Updates

This mitigation program will be reviewed and, where applicable, updated within ten (10) business days following any material change to the information contained herein, and will be recertified annually, before March 1 of each year, as required by FCC regulations (47 CFR § 64.6305).

9. Signature

Name and title: Ignacio Urigüen Echeberria, CEO

16076780X
IGNACIO
URIGUEN (R:
B95274890)

Firmado digitalmente
por 16076780X IGNACIO
URIGUEN (R: B95274890)
Fecha: 2026.08.14
13:15:21 +02'00'

10. Revision History

VERSION	SIGNIFICANT CHANGES FROM THE PREVIOUS VERSION
0	Initial version of the document