linea directa

LÍNEA DIRECTA GROUP

INFORMATION SECURITY POLICY

28/06/2022

Important information about this document

Name of the Policy	**INFORMATION SECURITY POLICY**
Related section of Línea Directa Group's Code of Ethics	**10**
Rules and standards superseded	**Security Policy January 2015**
Rules and standards repealed	**Security Policy January 2015**
Related rules and standards	**Code of Ethics of the Línea Directa Group, Compliance Policy, Regulations of the Board of Directors**
Business unit or function affected	**All business units of the Línea Directa Group**
Personnel affected	**All Línea Directa Group personnel and service suppliers.**
Main person responsible for monitoring	**CISO (Chief Information Security Officer)**
Approved on	**28 June 2022**
Effective from	**28 June 2022**
Version	**V1**
Created by	**Security**
Approved by	**Board of Directors**

CONTENTS

1. Introduction

The Security Policy of the Línea Directa Group ("Línea Directa") establishes the organisational and procedural framework to develop, implement, control, review, maintain and improve the Information Security Management System to provide the appropriate level of security to preserve and/or mitigate the risks to Línea Directa's information assets, based on ISO/IEC 27001 and ISO/IEC 22301 reference standards. The Company places special emphasis on the protection of information assets as a result of its strong commitment to technology, digitalisation and the implementation of direct channels to reach their customers. Basing business operations on these technologies entails an intrinsic security risk that must be addressed.

2. Scope

All personnel and persons providing services to Línea Directa are obliged to comply with the provisions of this Policy, as well as to promote its application and collaborate in the management and improvement of Information Security and Business Continuity.

Likewise, any service or product contracted from a third party may imply that such product or service is under the scope of this Policy, to the extent that this service may affect the security and/or continuity of the information or processes of Línea Directa. In this regard, Línea Directa's contracts will include this obligation, and the Information Security area must determine the security measures to be adopted and complied with by each supplier or third party, ensuring periodic review of their compliance.

3. General principles

Línea Directa undertakes to ensure information security and cybersecurity in its daily operations by considering the following principles on which ISO 27001 information security is based:

- Confidentiality: Ensuring that the information is accessible only by authorised recipients (persons, processes or devices).

- Integrity: Ensuring that information has not been modified, and that its integrity is maintained both at rest and when it is processed or transmitted from origin to destination.

- Availability: Ensuring that information can be reliably accessed at the time that any person, entity or process requires it.

4. Commitments and obligations

Línea Directa is committed, as a cornerstone of its Security Policy, to compliance with the legal, regulatory and sectoral framework applicable to it in accordance with the activities carried out. Within this framework, Línea Directa undertakes the following commitments:

- Security must be considered part of normal operations, being present and applied in all Línea Directa's processes.
- To plan and carry out a security-related risk assessment for all assets of the organisation, establishing the necessary security controls to minimise risks to acceptable levels.
- To provide employees, customers and collaborators included in the scope of this Policy with adequate security measures in the information systems owned by Línea Directa and made available to them for the provision of the corresponding service. In the event that the third party uses its own information systems, it must comply with the appropriate security measures determined by Línea Directa's Security area.
- To appropriately limit access to its information systems, ensuring the traceability of such access, as well as the actions performed on them.
- To manage all security incidents, seeking their successful resolution in the shortest possible time, taking all appropriate measures to resolve or mitigate the effects of the incident. These incidents shall be documented and notified to the relevant and affected bodies through the procedures to be established for this purpose.
- To hold security awareness campaigns and training programmes for all employees.
- To maintain up-to-date inventories of the services and the information assets that support them, their owners or holders and the risks and effects of their non-confidentiality, integrity and availability, enabling continuous risk analysis to manage them.
- To understand the value of information for Línea Directa, specifying methods for classifying it according to its level of importance for the organisation, carrying out the associated processes for its processing, storage, transmission, declassification, access, reproduction and destruction, according to its level of classification.

Línea Directa may take appropriate measures to prevent or mitigate behaviour or actions that breach this Policy, resulting in a threat to security or a violation of legal regulations and/or contractual agreements to which the Group is bound.

5. Governance model

Línea Directa must have a Security Committee in charge of managing all activity aimed at preventing, safeguarding and strengthening the security of information assets. Information security management will be included in Línea Directa's Internal Control review programme to ensure its monitoring.

Línea Directa guarantees that the information security management programme is kept updated, reviewed, tested and improved periodically, at least annually and in the event of significant changes in regulations, people, facilities, processes, suppliers, markets, technology or organisational structure.

The Information Security function belongs to the IT Security department through the CISO (Chief Information Security Officer), within the Technology-Security area of Línea Directa Aseguradora.

The IT Security department undertakes to continuously improve the programme, which shall consist of defining objectives on a regular basis, and to report at least annually to Management on the status of the programme, so that the results can be monitored.

The CISO shall report at least annually, or as circumstances dictate, to the Audit and Compliance Committee on the monitoring of the information security programme and any related issues that the Committee deems relevant. This Committee shall report to the Board of Directors with the same frequency for appropriate supervision.

6. Communication

This Policy shall be communicated to the members of the Board of Línea Directa and will be available to the organisation's stakeholders through the intranet and the corporate website.

7. Updating clause

The responsibility for periodically reviewing this Policy, at least once a year, and in any case when there is a change of any kind that implies its updating or modification, lies with the

Security Committee, which shall assess whether the content of this Policy continues to be suitable to allow its application in accordance with the established guidelines. Proposals for updates will be submitted to the Board of Directors for approval, following a report from the Audit and Compliance Committee.