LÍNEA DIRECTA ASEGURADORA
GROUP

CYBERSECURITY POLICY

Important Information About This Document

Name of the Policy	**Cybersecurity Policy**
Related Section of Línea Directa Group´s Code of Ethics	**3, 4, 10, 14**
Related sections of other policies	**None**
Rules and standards superseded	**Information Security Policy (June 2022)**
Rules and standards repealed	**None**
Related rules and standards	**None**
Business unit or function affected	**All business units of Línea Directa Aseguradora**
Personnel affected	**All Línea Directa Group personnel and service suppliers.**
Main person responsible for monitoring	**CISO (Chief Information Security Officer)**
Approved on	**January 28, 2025**
Effective from	**Not specified**
Version	**Version 1**
Created by	**Corporate Cybersecurity**
Approved by	**Board of Directors**

ÍNDEX

1. Purpose of the Document

Línea Directa Group (hereinafter "Línea Directa" or "the Company") recognizes the strategic importance of its technological and information assets, which represent an essential element in generating and delivering value to its customers and stakeholders. Likewise, cybersecurity is positioned as a key dimension within the Company's Sustainability Plan.

This Policy establishes the general principles, responsibilities, and vision of Línea Directa regarding information security and cybersecurity, with the objective of protecting the confidentiality, integrity, availability, traceability, and authenticity of the systems that host the Company's information, ensuring compliance with legal, contractual, and international cybersecurity standards.

2. Policy Objective

The objective of this Policy is to establish a comprehensive framework for the governance and control of cybersecurity at Línea Directa, providing an adequate level of maturity to manage the Company's cybersecurity threats and risks.

3. Scope

This document applies to all Línea Directa personnel, as well as to suppliers and third parties who access, process, or handle the Company's information. It covers all systems, applications, infrastructures, and assets that store, transmit, or process information.

Additionally, this Policy may be supplemented by various rules, procedures, and standards developed by the Corporate Cybersecurity department.

4. General Principles

Línea Directa establishes the following fundamental principles as the effective foundation for defining an information security and cybersecurity management strategy, as well as for mitigating risks associated with cybersecurity threats:

- **Confidentiality:** Ensuring that information is adequately protected against unauthorized access.

- **Integrity:** Ensuring the accuracy, reliability, and completeness of information, protecting it from unauthorized changes.

- **Availability:** Ensure access to information when required by authorized individuals, processes, or systems.

- **Authenticity:** Ensure the identity of entities (users, systems, etc.) and/or the sources from which the information originates, guaranteeing that such information is genuine and has not been altered. This is related to the principle of non-repudiation.

- **Traceability:** Ensure the tracking of information throughout its lifecycle, allowing the identification of its origin, modifications, and access. This ensures that any change or access to the information can be audited and verified.

5. Cybersecurity Capabilities

The general principles are developed through the following set of cybersecurity capabilities, aligned with market best practices and standards:

- **Govern:** Capabilities related to aligning the Company's cybersecurity principles with all stakeholders, properly managing dependencies, and complying with legal, regulatory, and contractual requirements. This includes establishing, communicating, and prioritizing actions in managing cybersecurity threats and risks; clearly defining and communicating context, roles, responsibilities, and competencies; establishing, communicating, and implementing cybersecurity policies and regulations, ensuring their compliance and maintenance; monitoring the results of cybersecurity risk management; and properly managing cybersecurity risks related to ICT providers.

- **Identify:** Capabilities related to identifying, analyzing, and addressing cybersecurity risks and threats that may compromise the Company's processes, services, and assets, with a particular focus on those essential to Línea Directa.

- **Protect:** Capabilities related to protecting identified assets based on their criticality against cybersecurity threats and risks through:

    - The design and development of secure digital products and services.

    - The implementation of access control mechanisms based on identity and the need-to-know principle.

    - The protection of both internal and external communications.

    - The control of asset operations.

- Cryptographic Key Management.
- Encouraging a strong and appropriate cybersecurity culture within the organization.

- **Detect:** Capabilities related to the detection of cybersecurity threats and vulnerabilities through:
  - Surveillance of digital products and services.
  - Monitoring communications.
  - Supervising technological infrastructure.
  - Detecting and classifying cyber threats and adverse events, both internal and external, that may impact Línea Directa's assets.

- **Respond:** Capabilities related to the establishment, management, and testing of response plans in the event of cybersecurity threats, and communication with stakeholders, including those required by law, regulation, or contracts.

- **Recover:** Capabilities related to the resilience of Línea Directa's assets to recover from the impact of adverse cybersecurity events and return to normal operations as quickly as possible, while identifying lessons learned to prevent future recurrence of such events.

All these capabilities will be implemented through a Cybersecurity Strategy that defines and deploys the Company's action framework aligned with market best practices.

6. Governance Model

The Company will have a Digital Operational Resilience Technical Team, composed of experts who support the Permanent Risk Committee and report quarterly to the Audit Committee and periodically to the Board of Directors. Their responsibilities include:

- Proposing and monitoring the digital operational resilience strategy and overseeing the Cybersecurity Strategy, its progress, and the Company's maturity level.

- Monitoring the state of cybersecurity threats and ICT-related risks.

The cybersecurity function resides within the Corporate Cybersecurity Department, led by the CISO (Chief Information Security Officer), and is part of Línea Directa's Technology and Cybersecurity area.

7. Responsibilities

Línea Directa defines the following cybersecurity responsibilities:

7.1 Board of Directors

- Approve and oversee the Company's Cybersecurity Strategy, as well as the Cybersecurity Policy and mission.
- Assume ultimate responsibility for managing the Company's ICT-related risk.
- Allocate and periodically review the adequacy of the budget and resources designated to meet the needs of the Cybersecurity Strategy and digital operational resilience.
- Stay informed and possess sufficient knowledge and capabilities to understand and assess ICT-related risks and cybersecurity threats, and their potential impact on the Company.

7.2 Technology and Cybersecurity Management

- Promote and support the establishment of technical, organizational, and control measures that ensure the implementation of the general cybersecurity principles.
- Foster a cybersecurity culture within the Company.
- Establish communication channels to stay informed about serious ICT-related incidents and their repercussions, as well as the response, recovery, and corrective measures.
- Approve the document specifying the scope of threat-based penetration testing.

7.3 Corporate Cybersecurity Department

- Implement mechanisms for detecting anomalous activities and define alert and escalation thresholds, as well as response and incident management plans for cybersecurity.
- Plan and manage the definition and execution of advanced threat-based penetration tests on production systems every three years.
- Define a cybersecurity incident recovery plan that includes the most relevant incident scenarios for Línea Directa.

- Apply mechanisms to limit access to the Company's information and ICT assets, and establish a set of policies, procedures, and controls focused on access rights to ensure proper administration.
- Ensure the security of Línea Directa's digital assets.
- Annually review the Cybersecurity Strategy, Cybersecurity Policy, and the rules and procedures included in the Company's cybersecurity regulatory framework, or upon any significant internal or external change, to protect the general cybersecurity principles.
- Develop awareness and training content specifically related to cybersecurity and technology risk management, as well as specialized training required for the cybersecurity area and ICT risk management.

7.4 Employees and Collaborators

- Comply with all policies, procedures, and rules derived from this Policy.
- Participate in cybersecurity training and awareness initiatives.
- Protect information and assets by preserving access and preventing any unnecessary disclosure or communication, using them only for authorized purposes.
- Classify information according to the information classification and handling policy.
- Report any potential incidents, breaches, or security violations as soon as possible.
- Safeguard access credentials, not disclosing them to third parties and using them only to access corporate applications.

7.5 Data and System Owners

- Define classification levels for their information assets.
- Authorize and periodically review access rights and roles for the systems and data under their ownership.
- Ensure the application of appropriate security controls.
- Participate in risk assessments and security reviews.

- Collaborate in defining security measures and requirements for systems, data, and recovery needs.
- Support investigations of security incidents.
- Ensure compliance with security policies for their assets.

7.6 Consequences of Non-Compliance

Any violation of this policy or the rules and procedures derived from it may result in the adoption of measures in accordance with applicable regulations.

8. Cybersecurity Mission

Línea Directa's mission is to ensure the general principles of cybersecurity (confidentiality, integrity, availability, authenticity, and traceability) by committing to the following:

8.1 Regulatory Compliance

- **Cybersecurity Regulatory Compliance:** A Cybersecurity Regulatory Framework will be developed and published, aligned with the main applicable regulations and based on market standards and best practices, according to the Company's needs.
- **Review and Update:** The Regulatory Framework will be reviewed at least once a year, as well as when serious ICT-related incidents occur or significant changes take place within the Company.

8.2 Cybersecurity Risk Management

- **Identification of Cybersecurity Risks:** Vulnerabilities, threats, and cybersecurity risks in systems and the information they handle will be identified.
- **Assessment, Analysis, and Mitigation of Cybersecurity Risks:** Criteria will be defined for identifying and assessing cybersecurity risks, along with action plans to remediate and mitigate identified weaknesses and prioritize mitigation measures.

8.3 Cybersecurity in Third Parties

- **Preliminary Assessment**: Cybersecurity requirements will be defined for ICT third parties before establishing contractual relationships.
- **Contracts and Agreements**: The inclusion of clauses related to cybersecurity measures will be ensured in contracts with ICT providers.
- **Ongoing Supervision**: Monitoring, compliance reporting, and performance evaluation of ICT third parties will be conducted to ensure compliance with contractual cybersecurity obligations.
- **Third-Party Incident Response Plan**: Specific procedures will be defined to manage cybersecurity incidents involving ICT providers.

8.4 Cybersecurity Asset Management

- **Cybersecurity Asset Inventory**: A register of assets related to cybersecurity will be defined and kept up to date.
- **Asset Protection**: Cybersecurity measures will be implemented throughout the lifecycle of identified and registered assets (planning, development, implementation, and maintenance/operation).
- **Information Labeling and Classification**: Rules will be defined to identify and classify the Company's information assets.
- **Information Controls**: Specific cybersecurity controls will be implemented based on information labeling and classification mechanisms.
- **Secure Disposal**: Mechanisms will be established for the secure destruction of information, applied according to its classification level.

8.5 Vulnerability and Patch Management

- **Vulnerability Identification**: Tools and processes will be deployed for periodic scanning to detect and address vulnerabilities.

- **Vulnerability Assessment**: Vulnerabilities will be prioritized and assessed based on their criticality, ensuring the availability of both technical and human capabilities to collect and analyze such information.

- **Patch Management Plan**: Mechanisms will be in place to apply updates and security patches to the Company's assets and systems.

- **Monitoring, Validation, and Continuous Improvement**: Post-patch verification will be conducted, and a continuous monitoring process will be defined to identify new vulnerabilities.

- **Penetration Testing**: Threat-based and advanced penetration tests will be conducted on systems supporting essential or important functions.

8.6 Access Management

- **Identity Control**: Access control requirements will be defined for information systems, aligned with the classification of the information they contain and the risk profile of the ICT asset.

- **Authentication and Authorization**: Strong authentication mechanisms will be implemented for remote network access, privileged user access, and access to ICT assets supporting critical, important, or public-facing functions.

- **Least Privilege Principle**: The assignment and use of privileged access rights will be restricted and controlled, based on the need-to-know principle.

- **Privileged and Non-Privileged Account Management**: Formal procedures will be defined for user onboarding, offboarding, and modifications.

- **Access Monitoring**: Access logs will be implemented for systems and data to ensure traceability of user actions. Additionally, asset owners will periodically review access rights.

8.7 Cybersecurity Awareness and Training

- **Training Programs**: Training programs and initiatives will be developed in cybersecurity, applicable to employees, ICT providers, and management, with a level of complexity appropriate to their roles and responsibilities.

- **Simulations and Exercises**: Periodic attack simulation exercises and campaigns will be conducted targeting employees and external users of the Company to raise awareness and provide training in cybersecurity.

- **Awareness Campaigns**: Cybersecurity awareness campaigns will be developed for both employees and ICT providers to reinforce best practices and foster a cybersecurity culture.

8.8 Encryption and Cryptography

- **Key Management**: Secure procedures will be defined for the generation, storage, replacement methods in case of loss, compromise, or damage, and deletion of cryptographic keys.
- **Encryption of Sensitive Data**: Methods for encrypting information both in transit and at rest will be defined and implemented.
- **Review of Cryptographic Algorithms**: Periodic reviews of cryptographic techniques will be conducted in accordance with best practices, technological advancements, and emerging threats.

8.9 Threat Management

- **Threat Identification**: Proactive identification of cybersecurity threats will be carried out based on reliable sources of information and intelligence, complemented by the use of early detection tools.
- **Threat Analysis and Response**: The potential impact of each previously identified threat will be assessed to define plans for management, response, and mitigation.

8.10 Incident Management

- **Detection and Notification**: Mechanisms will be defined to identify and report incidents both internally and to involved third parties and supervisory bodies, identifying the roles and personnel responsible for carrying out these actions.
- **Analysis and Prioritization**: The scope and severity of incidents will be assessed, recording all necessary information for subsequent analysis.
- **Incident Response**: Action plans will be defined to contain and respond to incidents and to restore the availability and integrity of affected systems as quickly as possible.
- **Lessons Learned**: Post-incident analyses will be conducted to improve affected controls and processes, as well as to identify patterns and enhance response plans.