



## **Synthesis of Information Security Policy**

Our Information Security policy establishes the rules to guarantee the confidentiality, integrity and availability of the information, in addition to protecting it against any threat.

The policy provides that the Company must:

- a) Comply with the strategy and institutional regulations of the area of Information Security.
- b) Provide the resources, processes, training and tools to maintain the function of Information Security in the Company.
- c) Have the following elements of Security Information:
  - i. Security assessments regarding the infrastructure.
  - ii. Analysis of Information Security risks.
  - iii. A monitoring scheme for critical information assets as defined within the Company.
  - iv. A procedure for the management of Information Security incidents.

The institutional regulatory dispositions of the area regarding Security of Information must:

- a) Be formalized, disseminated and be easily accessible by all employees.
- b) Be updated in accordance with the Company's operations.

Infrastructure security assessments must:

- a) Be carried out at least annually.
- b) Include insight tests, vulnerability scans and review of applications, among others.

The Security Information risks detected in the Information Security risk analysis must:

- a) Be clearly identified and updated.
- b) Be reported to the owner of the information.
- c) Have plans to mitigate, transfer, accept or eliminate them.
- d) Be evaluated based on the probability of occurrence and impact for the Company.
- e) Be adjusted according to public sources and internal monitoring of threats to the Company's infrastructure, the industry, and the technological community in general.

Information Security incidents must have a procedure for their attention in accordance with the provisions of the Information Security Incident Management policy.

The monitoring of critical information assets must have:

- a) An alert scheme.
- b) The activities to respond to Information Security alerts resulting from the monitoring.



Failure by any employee to comply with the provisions of the Information Security policy shall subject such employee to the administrative sanctions established in the current Code of Ethics of the Company and its Internal Labor Regulations.