



Synthesis of Policy Regarding Safeguarding of Information Systems

Our Information Systems Safeguarding Policy regulates the security of the Company's Information Systems.

The policy provides that Information Systems must:

- a) Be used only for the purposes that they were assigned to.
- b) Comply with the security standards established by the Company.
- c) Have:
 - i. A user identifier for each Information System.
 - ii. Authentication mechanisms established by the Company.
 - iii. Profiles and access privileges granted according to the functions and responsibilities of the end user.
 - iv. A scheme of backup and recovery of information, according to the requirements and needs of the business.
 - v. Robust cryptographic keys, if applicable.
 - vi. A control of different versions for developments.
 - vii. An inventory of closed-source third-party software versions. Test environments different from the productive ones.
 - viii. Mechanisms that ensure the support and maintenance of the same, as well as its infrastructure.
- d) Have audit tracking mechanisms enabled.
- e) Be monitored as established by the Company.
- f) Be protected against malicious software.
- g) Have encrypted communication links to send and receive information classified as restricted and very restricted.

The identifiers of users and passwords with administrator privileges in the Information Systems, such as databases, operating systems, applications and security infrastructure and systems, should be protected in an electronic access control vault.

The information contained in the Information Systems must be disclosed only and with prior authorization, for any of the following reasons:

- a) Operability and business continuity.
- b) Investigation of possible incidents of information security.
- c) Rescue or preservation of the security of the Company's Information Systems.

The information transmitted in the Information Systems between different points and that requires a high level of availability, must have redundant communication links.

The Information Security risks detected in the Information Systems must have a remediation plan to mitigate them.



It is strictly prohibited to:

- a) Copy information from the Information Systems from a productive environment to a different one, without previously applying data masking processes to desensitize the information.
- b) Make use of Information Systems to store, create, download or transmit personal or public information of an obscene, offensive, illegal, abusive, harmful, vulgar, irrelevant or questionable nature.

Failure by any employee to comply with the provisions of the information Systems Safeguarding Policy shall subject such employee to the administrative sanctions established in the current Code of Ethics of the Company and its Internal Labor Regulations.