



Synthesis of Information Security Incident Management Policy

This policy regulates the information security incident management process.

The policy provides that the Company must:

- a) Have the necessary resources and infrastructure to identify and inform of possible Incidents of Information Security.
- b) Have defined the technical and organizational roles to give attention to and mitigate the reported Information Security Incidents.
- c) Establish the appropriate communication channels to deal with Information Security Incidents.
- d) Define mechanisms that allow the Company to be informed on issues of Information Security, in order to know how to act in the event of an Information Security Incident.

Information Security Incidents must:

- a) Be managed by an Information Security Incident response team.
- b) Have an information security incident management process.
- c) Be classified according to their type and impact.
- d) Be duly documented in order to keep a record and follow up.

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