Information Security Risk Management

Regulatory Compliance Management

According to the established Compliance Manual of the Personal Data Protection Law, the Regulatory Compliance Officer has the responsibility of:

- Ensure compliance with the Personal Data Protection Law (from now on, "LPDP").
- Report to the Board of Directors and Chief Executive Manager on implementing the adopted procedures to comply with the LPDP.
- Ensure procedures and controls to guarantee that the Bank's collaborators comply with the adopted decisions and the entrusted functions for the LPDP compliance.
- Guide the Bank employees regarding the importance of complying with the LPDP. Also, with the responsibilities that arise in the event of non-compliance. Comply with the policies and guidelines indicated in the Regulatory Compliance Management Manual.

The Regulatory Compliance Management is reflected in the 2021 Annual Work Program for Regulatory Compliance. This document details activities focused on strengthening compliance with personal data protection within Interbank.

Information Security Risk Management

According to the Information Security Policy, the Information Security Risk Management is responsible for incorporating the general requirements established by the Law on Personal Data Protection in Information Security and other related regulations.

Thus, within the Information Security Policy, the following are specified as general requirements for the processing of personal data:

Management of personal data

- The use, collection and retention of personal data should be minimized to what is strictly necessary to meet business objectives. Furthermore, the

treatment of personal data should be risk-oriented and comply with local regulations at the same time.

- The treatment of personal data stored, processed or transmitted by Interbank will comply with Law No. 29733, Personal Data Protection Law.
- The collection of personal data by fraudulent, unfair or illegal means is prohibited.
- Personal data must be collected for a specific, explicit and lawful purpose.
- All processing of personal data must be adequate, relevant and not excessive for the purpose for which they were collected.
    - For personal data processing, Interbank must adopt technical, organizational and legal measures that guarantee its security and prevent its alteration, loss, treatment or unauthorized access.
    - Personal data must be kept in a way as to guarantee its security and only for the time necessary to fulfil the purpose of its treatment.

The management of personal data is carried out through the Information Security Committee. Interbank's Board of Directors appoints an Information Security Committee, which comprises members of the organization's Senior Management.

The personal data management results are periodically reported to the Global Risk Management Committee.