Information Security Policy

This Policy will be for the protection of the information of internal and external users.

Through the elaboration and implementation of this Policy, OPTIMEN and the General Management establish as an important part:

- The protection of personal data
- Safeguarding the organization's records
- Protection of intellectual property rights
- Documentation of the information security policy
- The assignment of security responsibilities
- Education and training for information security
- Identify, evaluate, and monitor Information Security Risks
- The record of security incidents
- Business continuity management and continuous improvement
- The management of changes that may occur in the company related to security

OPTIMEN is committed to:

- Comply with the controls and policies established in its Information Security Management System.
- Establish and comply with contractual requirements with involved parties.
- Define the necessary safety training requirements and provide it to OPTIMEN staff.
- Prevent and detect viruses or other malicious software, through the development of specific policies.
- Establish the consequences of violations of the security policy, which will be reflected in the contracts and/or confidentiality agreements signed with the involved parties, suppliers, and subcontractors.

The General Management of OPTIMEN will follow the Information Security policies when these are defined by the clients. Whenever there is a need to work on their informatics systems environments, OPTIMEN will require:

- Access to be able to develop software services in accordance with applicable legal and regulatory requirements
- Comply with the contractual requirements with the interested parties and follow the established requirements about consequences of violations of the security policy.

Information Security Objectives

1. Comply with the Annual Training Program
2. Comply with the level of awareness in Information Security
3. Secure and keep Workstations up-to-date with signatures and Antimalware solution
4. Prevent risks that affect Information Security
5. Propose improvements to the Information Security System