Summary of the General Policies on Security of the Information

Blumar and Affiliates

Policy

The purpose of the General Policy on Security of the Information is to establish the general directives for the protection of the information assets used in the processes of Blumar.

General Purpose

Confer continuance to the operational processes of Blumar, protecting the information assets from internal and external threats attempting against the confidentiality, integrity and availability.

Security of the Information

It is the group of preventive and reactive measures of the organizations and technological systems that permit to safeguard and protect the information (physical or digital) from malicious attacks seeking to maintain the confidentiality, integrity and availability of the information.

THE THREE FUNDAMENTAL PILLARS OF THE SECURITY OF THE INFORMATION

Confidentiality: Level or classification of the information in accordance with the capacity of access for authorized persons.

Integrity: Level of protection of the wholeness and accuracy of the information.

Availability: Level of certainty of the accesses of users authorized to the information and the associated assets.

RESPONSIBILITIES

Responsibility of the Collaborators

To comply with what has been formalized in the policy and apply same both in his (her) working environment and outside, and in addition comply with the obligation to alert his (her) supervisor and /or information security committee in a timely and appropriate manner in respect of any incident affecting the confidentiality, integrity and availability of the information.

Responsibility of the Suppliers

Comply with the information security requirements that Blumar defines, such as:

- Comply with the levels of service established;
- Count with the mechanisms of continuance of businesses to ensure the availability of the services;
- The conditions of confidentiality and non-disclosure of information must be complied with even after the termination of the services contract;
- Notice must be provided to Blumar in respect of any emergency affecting the security of the information that may occur.

RECOMMENDATIONS

Even though new threats may appear every day, these recommendations must always be followed by workers and suppliers:

- Maintain antivirus software installed and activated;
- Ser precavido a la hora de visitar sitios web fijándose siempre en que sean sitios seguros y cuenten con el protocolo https.
- Never open links sent by electronic mail of unknown origin;
- Never open files attached to electronic mails of unknown origin;
- If you travel with a computer, always take it as hand baggage and do not leave it visible in automobiles or public places;
- Maintain the sources of information confidential with mechanisms of control of access and out of the reach of those who are no supposed to have access to it;
- Block the computer when it is left unattended;
- Do not keep written access keys in places that are visible or of easy access such as agendas, under the keyboard, etc.;
- Only use software authorized by the company
- Refrain from using external storage devices such as pendrives, external hard disks, etc., in computers connected to the Blumar network that do not comply with the minimum requirements of security, or of unknown origin, or which have been used in a computer that does not count with the necessary security measures;
- The physical or digital information that is no longer needed must be destroyed by means of shredders or the safety erasing of same.