ABSTRACT ISO 27001

First of all, it is necessary to define what ISO IEC 27000 consists of. It is a standard developed with the objective of establishing a standard for information security management within organizations. By this we mean the requirements needed to establish, implement and maintain these systems.

This standard was published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint subcommittee of ISO and IEC, ISO/IEC JTC 1 / SC 27. So far its modifications have been minimal, but the possibility is not ruled out, because as the technology industry is constantly changing and seeking innovation, hacking methods and social engineering as well.

This standard arose because a need was found in all sectors since we live in a world that is constantly connected, where information begins to prevail as one of the most precious goods, being already considered an asset. For this reason, both public and private organizations that are in constant interaction with data in any of its formats such as text chains, images, audio, etc.

Additionally, information security is not restricted only to this as such, but also to the infrastructure where it is stored. That is to say, its physical means, also in the facilities where it is located (the offices, DataCenter, or any enclosure that was conditioned for this work). By being aware of this, we can begin to see the need to take action with respect to people who have access to these facilities, the signage that should be placed in these places taking into account that the less visible and less marked it is, the more difficult it will be for malicious people to find it.

But not only can we focus our efforts on making the infrastructure secure, but we must also focus on choosing a person in whom we can place a very high degree of trust for positions involving direct manipulation of information. In addition, the organization's employees will have to be kept aware of the policies since they are usually the ones who are most exposed, besides playing a fundamental role and without their commitment and due compliance with the rules, the rest will have been in vain. The company must be committed to educating its employees about information security, it must try to stay ahead of the game so that everything is done efficiently.

It must also be stipulated the corrections or sanctions that correspond to the people who do not comply with the action plans that were being implemented.

As mentioned above, the equipment is treated as property, but like many others it must be constantly maintained in order to comply with the fundamental principles of computer security, which are: integrity, availability and confidentiality. This need is based on the fact that at the moment in which an equipment that stores information fails, it can be catastrophic for the company and great amounts of money, the confidence of its users and many things more can be lost. So to minimize the margin of error, precautionary measures are taken with the equipment

For all the above, it is necessary that companies have a fixed path when choosing which rules to adopt, this is where standardization comes into play. ISO 27001 gives companies the possibility to certify quality levels that can serve as proof to their users and to any entity that wants to verify if their information will be safe in that company. In short, the standard can be taken as a manual of good information security practices.

The standard is divided into different sections, these are classified so that most of the fields that compromise data security are covered. That is to say, it is segmented in specific subjects that demand the implementation of security controls of the information.

In a slightly more specific way it is possible to give some examples of the topics covered:

a. Access control

b. Classification of information

c. Physical and environmental security

d. End-user-oriented topics, such as:

a. Acceptable use of assets

b. Desktop and clean screen policy

c. Transfer of information

d. Mobile and teleworking devices

e. Restrictions on installation and use of the software

e. Backup copies

f. Transfer of information

g. Protection against malicious code

h. Management of technical vulnerabilities

i. Cryptographic controls

j. Communications security

k. Privacy and protection of personal data information

l. Relationships with suppliers