CEST Centro de Estudos Sociedade e Tecnologia
USP Universidade de São Paulo
Bulletin - Volume 1, Number 9, March/2017

Information Security in the Public Administration

Vera Kerr

In the last decades, we have witnessed the emergence of the information society as a result from the constant technological evolution that brought together deep changes in interpersonal relationships.

With the progress of the information and communication technology and the arising of the Internet, the Public Administration has also become the target for these deep transformations, facing the huge challenge of digital inclusion within the governmental environment.

> It is imperative that the public servant behaves properly when dealing with open public data and especially with confidential public data when using information and communication technologies.

However, providing new technologies without due guidance and control has generated, for the public agency and servants involved, civil and even criminal responsibility, as court decisions have revealed. The reason is because the Public Administration is subject to external attacks or even illegal actions carried out by its own public servants or by other people strange to its office work force by means of new technologies usage. Not mentioning that the public agency, besides working with public data, that is, with information accessible to the society, it also works with legal secrecy protected data. Therefore, it is imperative that the public servant behaves properly when dealing with open public data and especially with confidential public data when using information and communication technologies. For such, it is indispensable to implement an information security strategic planning within the governmental environment. Such measure is focused on divulging good practices standards related to the servant's rights and duties, to the access and use of data, and to the penalties related to its violation.

In this sense, according to the instructions proposed by the Institutional Security Office of the Presidency of the Republic (GSI/PR), the bodies and entities integrating the Administration System of the Information Technology Resources (SISP) should elaborate the information and communication security policy, implement it and enable the servants to comply with it. It is also fundamental that, in the event of an attack, invasion, or violation of the information technology system, the servant should know what minimal care must be taken to preserve the information and the proof till an expert arrives. Nonetheless, it is important to outline that both the information security regulation and the systematic auditing, though indispensable, are not enough to solve the problem. This is because the human being still continues to be the most vulnerable link in the security chain. Training programs consisting of training and awareness of public servants, as mentioned before, are essential to reduce the social engineers' actions and mitigate the vulnerabilities of the system.

The Court of Auditors of the Union (TCU), in its Judgements 1603/2008 and 2308/2010, recommends the elaboration of information and communication security policy, as well as a complementary regulation referring to the Federal Public Administration body or entity where they are implemented. The recommendation documented in item 9.1.3 of Judgement 1.603/2008 – TCU – Plenary to the superior ruling bodies consists in:

“Guidance over the importance of Information Security management, promoting actions, including through the standardization, aimed at establishing and/or improving business continuity management, change management, capacity management, information classification, incident management, risk analysis, the specific area for the Information Security management, Information Security policy, and access control procedures.”

Apart from the above-mentioned judgements, there are other decisions by the Court of Auditors of the Union (TCU) related to several governmental institutions that went through auditing process and that shall implement security policies. In order to facilitate easy access and promote a safety culture in the Public Administration environment, the Information and Communication Security Department of the GSI/PR provides in its website a compilation of the current legislation to serve as a reference for the work of jurists, public servants, technicians, and specialists in the area. There are standards from ISO/IEC 27000-family that deal with the management of information security, being a reference for bodies or entities of the Federal Public Administration, direct and indirect, such as: ISO 27001 – which establishes a System of Information Security Management; and ISO 27002 – which is a Code of Practices for the Information Security Management; and ISO 27005 – which describes the management of risks in Information Security. Besides these standards, there are still the ISO/IEC-international standards, like, for example, the ISO/IEC 15408-standard (*Common Criteria*), which has the objective to assess the IT security, among others.

Concerning the structure of the information and communication security management, the GSI/PR recommends that the governmental bodies should have:

I. Information and Communication Security Committee;

II. Information and Communication Security Manager; and

III. Incident Treatment-and-Response Team.

Due to its importance, the General-Coordination for Information Security of the Department of Logistics and Information Technology of the Ministry of Planning (SLTI/MP) recommends that the structure of the information and communication security of the body or entity should be defined in the institutional organization chart at strategic level with the involvement of all the areas of the organization. Moreover, it further establishes that the referred structure should address the issue at strategic (security committee), tactical (board of directors) and operational (work groups and specific information and communication security teams, such as IT security and property security) levels.

It is therefore seen that the mere acquisition of new technologies does not necessarily represent higher efficiency and security towards the services performed by managers and public servants. It is necessary to implement strategic planning on information security within the environment of Public Administration. Likewise, it is imperative to qualify the public servant, user of new technologies, on the related good practices and standards in order to create a corporate culture concerning the responsible, secure, and ethical use of these tools according to the current legislation, in an educative, preventive, and collaborative manner.

Vera Kerr, *lawyer, doctorate student at Escola Politécnica da Universidade de São Paulo, and researcher at CEST-USP.*

Coordinator: Edison Spina

This article is a result of the author’s ascertainment and analysis, without compulsorily reflecting CEST’s opinion.