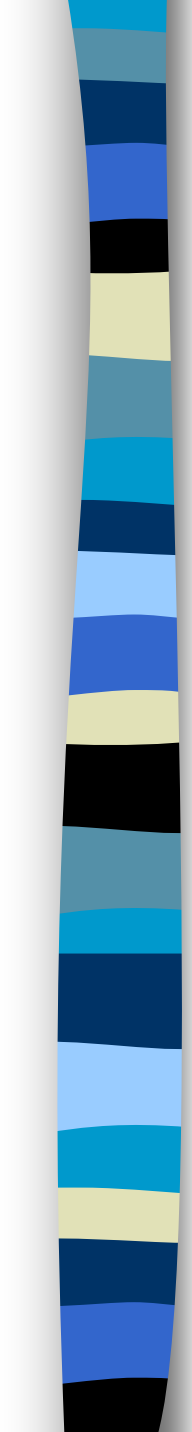


The Siena Municipality Programmatic Document for Security





Based on the results achieved by the risk analysis in terms of the identification of threats, the evaluation of vulnerabilities and the identification of safeguards, it is advisable to take actions on those factors that are typically related to security, in the broadest sense of the word, both as a physical and as a logical entity, and to the security of the Administration itself.

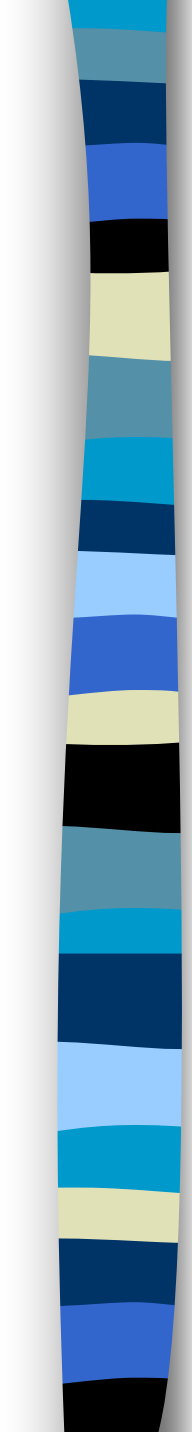




Security means adopting technical-infrastructurel, technological, organizational, procedural, educational and regulatory measures capable of:

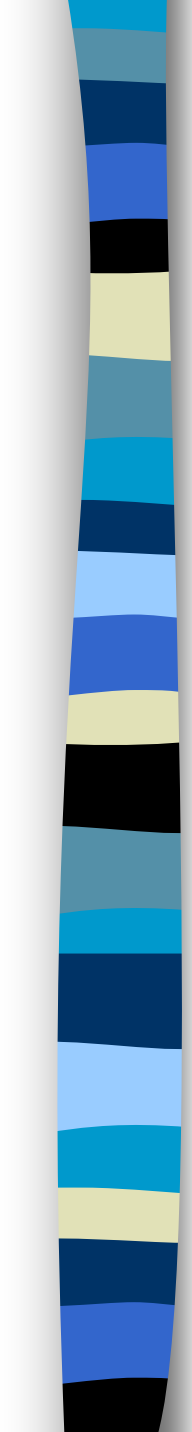
- Limiting damages of any kind, both tangible and intangible, direct or indirect, that the Administration may sustain.
- Guaranteeing availability and access to the information at any time and in any place.





On this basis, a number of modifications to the **infrastructures** have been envisaged, mainly connected to the development of the electric supply for workstations that provide services to the public, visitor access control systems in the various administrative premises in town, air conditioning and intrusion-detection systems, and fire prevention and control in the server rooms.





As for the solutions to be adopted in the **information technology** field, the following actions have been envisaged:

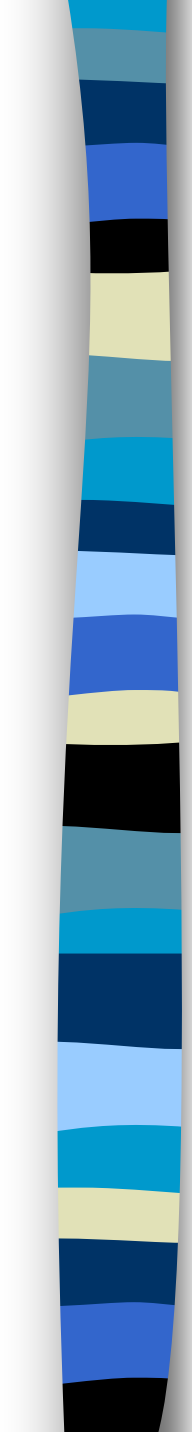
- Selectively introduce data encryption techniques in order to guarantee data integrity and privacy as specifically imposed, as observed above, by the minimum security measures for privacy protection.
- Enhance controls on access to information resources, auditing and preventive maintenance of those resources.
- Improve security measures on the information system architecture in order to increase security levels in the whole system every time a change is introduced into the network.
- Formally create an inventory of the IT resources and a knowledge base for the recording of events that have caused interruptions of service.



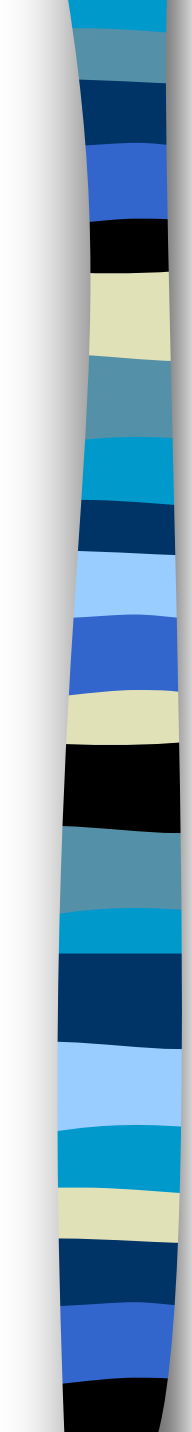
From the **organizational** point of view the following actions need to be taken:

- Adopt the security life-cycle in full as a standard reference model for security
- Identify and appoint a security manager, a password and encryption keys keeper, a system and network administrator, etc
- Increase the permanent staff in the technical department dedicated to the information system management
- Introduce a system for the treatment of personal data that makes it possible to monitor all information related to these issues, such as the relationship between server, databank name, type of treated data, purpose of the treatment, owner, manager, group or employees, security measures adopted, etc.



- 
- Introduce a security management system that makes it possible to follow all aspects of these issues through standardized reference models.
 - Introduce an internal structure or use a third-party service for the management of computer-related incidents (IRT-Incident Response Team)
 - Use security cabinets to store back-up copies and internal documentation.

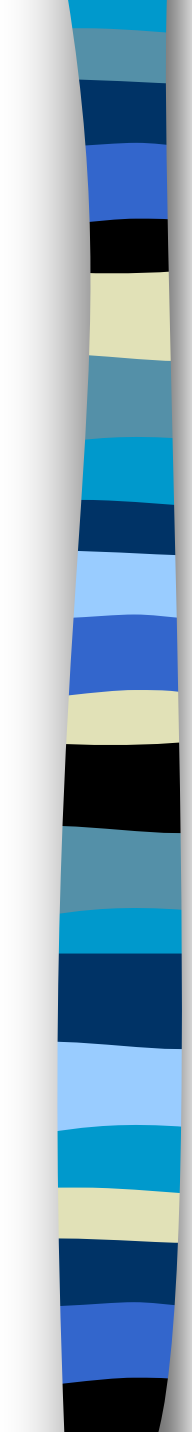




As regards the **procedural** aspects, it is advisable to classify the data, define security policies and prepare an emergency and contingency plan.

In addition to the courses already attended by the employees and the CED and Service Centre staff, further **training** needs to be planned with a view to make the Administration staff aware of information security and privacy issues, as well as specific courses on the Programmatic Document for Security and on security policies.

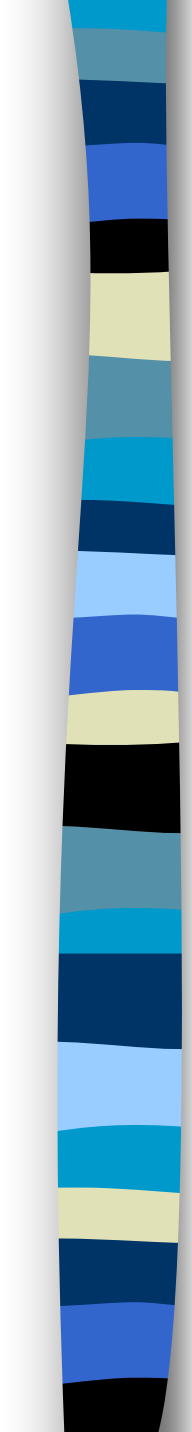




In connection to the **regulatory** aspects, the following actions can be suggested:

- Review and, if necessary, change the legal ownership of data banks and the ownership of data treatment tasks
- Review and adjust the minimum measures dictated by the Code on the protection of personal data (Legislative decree 196/03), with regard to the treatment of personal data through both electronic and non-electronic systems (manual treatment).





And again in regulatory terms, it is necessary to comply with the rules of the information protocol about documentation and archives management and it is advisable to conform to the "provisional rules and regulations about security of the Internet sites belonging to the Central Administration and to the public authorities" (Norme provvisorie in materia di sicurezza dei siti Internet delle Amministrazioni Centrali e degli Enti Pubblici).





AMTEC

Alberto Bianchi

AMTEC spa

Una società ELSAG-FINMECCANICA





Gianluca Daino

Department of Information Engineering

University of Siena

