Introduction

The growing complexity of information systems and potentiality of the infrastructures that support communication between systems, have led to an improvement of the available services and to a larger diversity of them.

However, new issues emerged specially insecurity, as a higher availability ended in the enlargement of the system’s access.

With new and better services, there is a greater necessity of assuring reliability and safety of the systems not only for who makes them available but also to those who use them.

One of the main challenges to face for a safety use of new technologies in complex systems is related to the confidence levels of the users in the systems. There are always problems when these levels are low or users have too much confidence [1]. The lack of confidence causes absence of utilization and the excess of confidence results in mishandling of the systems. Either lack or excess of confidence compromise the security and the profits of the systems [2].

Companies must have an atmosphere of confidence between the different actors. And to have reliability and safety in information systems it becomes fundamental to define coherent access politics and its right implementation. [3]

To assure that systems are consistent, reliable and safe it’s necessary to manage the control of those accesses in an integrated way. An integrated accesses control involves the bottom of an organization, the actors, and the construction of an architectural model completely aligned with the structure, strategy and goals of that organization. It is important to consider all the business processes and to implement the models and access control mechanisms at a technological level.

The recognition of this kind of problems in DIAP of Lisbon, explains the choice of this organization as a case study in the present work.

It became important to delimitate, in the information system, the subject of the accesses control because it coexists with other mechanisms of security. The accesses control only restricts users’ activities of a determined system. Every time a potential user tries to access, there is always a validation to confirm that the user is authenticated. Nevertheless, it required to split the concepts of authentication and accesses control. The accesses control assumes there is already a previous authentication of the user and that it was successful [4]. The accesses control is related to authorizations’ structure in the system. Sometimes the authorization can be the reflex of the organization’s structure, in other situations it can reflect the sensibility level of the various documents and the knowledge of the different users accessing to the documents [5].

To construct the accesses control in an information system, we started from the framework of CEO to the conception of organizational views. The views that allowed to define the organizational architecture were: the organizational view, which contains the strategic vision, mission and internal and external organizational structure, the processes view, which describes the set of business processes and services of the organization; the
application view which represents all the structure of applications and applicational services and the technologic view which regards all the technologic infra-structure. The intention was to characterize all the organizational views, identifying all the concepts, to connect each view with the respective Lankhorst [6] perspectives, according to the common concepts. Therefore, from various points of view, all the concepts related to the accesses control were identified so that the new accesses architecture worked in the alignment of all the perspectives at an accesses control level. These perspectives allowed the mapping of the concepts related to access control with organizational views of the CEO framework.

To construct an access’s architecture based in a methodology which was created from the Lankhorst [6] perspectives, and validate it in a case study, is the main goal of this project.

State of the Art

The research done and consequent analysis of the problem, lead to the proposal of access’s architecture for DIAP of Lisbon, based on the use of the various Lankhorst organizational perspectives [6].

Consequently, through a long revision of the various architectural views, it is possible to conclude that Lankhorst perspectives [6] can be framed in accesses architecture. These perspectives are going to cover the concepts existing in CEO framework and allow the generation of new points of view in each of those views. This means it allows that all aspects present in an organizational architecture are identified and approached. It allows to identify and study all the aspects related to an organizational architecture what was impossible with the CEO framework. Lankhorst [6] perspectives are fundamental to analyze an organizational architecture which is the basis to develop accesses architecture. So, starting with the organizational views we are going to demonstrate how the perspectives identified by Lankhorst [6] can contribute to the development of an access’s architecture.

From the organization view we can obtain all the information relevant to identify and characterize the roles and information related to actor’s restrictions in the organization. This will be necessary to the approach of the accesses control that is going to be defined.

The processes view gives us the main information to identify all the tasks a certain user, who plays a role in the organization, needs to attain his objective.

Identifying all the tasks associated with a business process one can verify which services are used by each user in order to attain his goal within the organization.

This view is also fundamental to identify and validate all the types of permissions and explicit delegations, according to the way each user plays his role within the organization. This allows a correct segregation of functions, preventing potential conflicts within the internal control of the systems. Using this view and the previous one, one can map a set of users who play different roles within the organization, associating a set of restrictions related with the context that is given in this process view, with each one of these users.
The informational view helps us to understand which type of information is used by the organization and how it is aggregated. Thus it is possible to define the types of operations associated with this information that allow manipulating it.

The application view is essential to identify the type of services provided by the applications and to define the set of privileges that will be associated with the access control rules of each application. Besides, this view is important to help us understanding the definition of the accesses control module – centralized or decentralized. Gathering this view with the other ones one can define the set of privileges which will be mapped in a certain user, according to the role he plays, and associate that set of privileges with the respective operations to realize considering the informational entities that he is going to manipulate.

The technological view allows identifying access control mechanisms one need to implement, according to the existing infrastructure. Together with the other views, we can identify a set of mechanisms which will support an access control policy that is going to be defined considering the concepts identified in the previous views.

To conclude the state of the art, we analyzed a set of models, mechanisms and access policies in order to find the best solution to the problem we identified. This analysis allowed us to identify different ways of managing access control in an information system.

Access control management can be done at different levels of the organization. Its study led us to the identification of aspects related to access control in the different organizational views.

The RBAC approach [9] guarantees the integration of all these aspects and concepts. With RBAC [9] one can map a certain user (“WHO”) into a role delegating a group of permissions (“WHAT”) according to a certain context (“WHEN”). This allows developing a set of tasks related to a certain information source (“WHERE”).

Besides, the case studied has also a lot of characteristics identified bellow. The organization studied “DIAP de Lisboa” belongs to Public Ministry and to the Justice’s sector. This type of organizations has a strong control and a well defined set of rules related to its organizational and hierarchical structure, categories and functions. Thus, the law was used as an important source of information to obtain categories and functions of the organization. Another relevant aspect was the validation of the information available through the contact with some cooperators from DIAP, who were available to provide the rest of the information needed. RBAC [9] was the chosen approach. It integrates the set of concepts used in this work and fits the characteristics of the studied case.
Nowadays it is difficult to define properly the processes in order to analyze, design and implement security system’s architectures. So it becomes difficult to verify if they are implemented in the organization’s architecture [7].

According to Wimmel [8], it’s necessary to develop policies about the use of formal models and integrate security in the software development cycle. It’s also necessary to develop formal conceptual models applicable to aspects related with security that can be easily understood by people from other areas. Actually, the development of security and access control systems has an important technologic basis. It is supported by information and the definition of how and to whom it must be available, without considering other organizational views.

The construction of access architecture guarantees a greater consistency and security between applications since the access control is drawn in an integrated way, considering the different organizational views and respective perspectives. An integrated access control implies the contribution of all the concepts related to access control, identified in the different views that compose an organizational architecture.

Then, the solution is based on the CEO framework use, which supported the characterization of the different Lankhorst perspectives [6]. Its alignment allowed the construction of a set of access control rules.

It allowed also the construction of a set of access control rules using the RBAC approach [9] to convert that set of rules into access models and policies. The analysis of the different organizational views and perspectives led to a set of practices and methodologies to the construction of access architecture aligned with the organization. The final solution permits a constant adaptation between access control system and the changes in the organization structure.

With this methodology it is possible to separate the access management module from other modules to guarantee identification, validation and access control, separately.

We propose the definition of an identification module and the validation out of the organic structure, strongly integrated with the system slope, using the Single Sign-On technology.

In this context, access management should happen at the application level, adapted to the application specificity. Access management uses the group of user’s module, built from the organic structure, to identify the access users, but has an internal structure in each application. There are different policies of access control. Each application should use the solution that fits better its needs.

The solution we propose permits that groups of users are used to different goals, e.g. access control and communication, heterogeneity of access control policies re-using organic structure and groups of users modules.

This methodology also allows supporting the attribution and explicit delegation of privileges to face unexpected situations and guarantee flexibility of access control management.
The attribution and delegation in applications mean to add privileges explicit rules. These rules are active during a certain period of time and are valid if the user who delegates keeps the delegated privileges. This second technique makes a more accurate attribution of privileges possible, but demands a greater number of changes.

**Validation**

The proposed methodology was validated by constructing a set of access control modules, according to the RBAC approach [9], integrated in the applicational architecture of “DIAP de Lisboa”. This set represents a final example of the DIAP’s access architecture.

The new access architecture makes the separation between access management and other modules possible.

The access architecture allows the attribution and explicit delegation of privileges. It simplifies the resolution of unexpected situations and guarantees flexibility in access control management.

**Conclusions**

This work may contribute to the development of new methodologies which include the CEO framework. We hope it contributes to (1) the development of standard models according to the organizational views; (2) the extension of the existing modulation tools to new access control concepts in these views; this should allow a clearer identification of the different approaches and an enrichment of the information systems at access control management level; (3) the creation of a more integrated and complete evidence supporting the internal management of organizations access control; the description of this architecture should permit the elaboration of a complete model to support the different views of an organization.

**References**


