http:d2cigre.org

CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2015 Colloquium
October 08 to 09, 2015
Lima – PERU

D2-03_03

Framework for the development of secure web systems for electrical companies

by

Isai Rojas González – Gabriel Sánchez Pérez

Instituto de Investigaciones Eléctricas – Instituto Politécnico Nacional

(MX)

SUMMARY

Currently, more and more companies are automating their information systems and computer systems based on web technology are frequently used in this process. This may have undesirable effects because more and more cyber attacks occurs through the web platform, in consequence a growing number of companies consider the information security as a crucial aspect to protect their business processes. Companies dedicated to the electricity sector are not immune to this problem, by contrast, due to the implementation of new technology such as the "Smart Grid" puts them in a prone position to be the subject of cyber attacks and that is why the aspect of computer security becomes even more important.

Corporate web portals are part of the solutions most commonly used by companies to provide services all applications that employees, partners, suppliers and others involved in the business, used within the organization as part of their daily work.

This paper presents an alternative of security for the development of corporate web portals and has been called "Framework of security and access control for the development of corporate web portals". The framework is a tool designed to help groups of portal development, to create products that include computer security measures to mitigate the risks of the web system can be violated.

The developed framework is the result of study and analysis of best practices and techniques of secure software development, standards and models of access control, scheme Single Sign-On, and Mexican law on protection of personal data. The solution was designed to be appropriate under the conditions of the environment in which it would be applied, which in this case was the systems development environment form at “Instituto de Investigaciones Eléctricas” (Electrical Research Institute) in Mexico, so that the framework is original and suitable to the software development environment related to electricity sector companies.

During the development of the solution were considered premises that in addition to offer protection, also they propitiate favorable effects for business purposes, such as that fact that the mitigation of security problems is much less expensive if performed in the early stages of any

* Reforma #113 Colonia Palmira, C.P. 62490, Cuernavaca, Morelos, México.
Fax: + 52 777 362 3811 mailbox: 7070 e-mail: irojas@iie.org.mx

process software development, or that use proper of the access control model based on roles strengthens the security of systems and helps reduce the costs of security management.

KEYWORDS

Information Security, Access Control, Secure Software Development, Corporate Web Portals, Electricity Sector Companies.

* Reforma #113 Colonia Palmira, C.P. 62490, Cuernavaca, Morelos, México.
Fax: + 52 777 362 3811 mailbox: 7070 e-mail: irojas@iie.org.mx

1. INTRODUCTION

The energy companies do not escape the constant evolution of Information Technology. However, this momentum so impetuous towards modernization also results in new vulnerabilities and threats that jeopardize the fulfillment of the goals and objectives of the organization. Recently, cybersecurity has become more important due to increasing cyber attacks as they often affect the reputation of businesses and even causing economic losses. As a result, it has become much more important to adopt measures to ensure infrastructure Information Technology.

Therefore, and in a context limited to the protection of information into computer systems in companies of the electricity sector, the need for a reference framework to point the security aspects that must be met in the creation of secure computer systems is observed, particularly in the creation of secure corporate web portals, due to the importance of strategic information that in them is concentrated.

There are several models, specifications, best practices and standards in security that could be used to try to cover all requirements, however, all these elements are separately, in addition, would have to check large volumes of specialized information so that, the main problem is that there is not a reference framework, specifically to the "Instituto de Investigaciones Eléctricas" (Electric Research Institute) and the IT solutions developed therein.

A proposed solution should combine the elements necessary to create corporate web portals that use access control based on roles and attributes, which also has a scheme of Single Sign On (SSO) and compliance with the Mexican legislation for data personal protection. Against this background, the main objective is to specify minimum security guidelines required for the design, construction and implementation of such portals.

To achieve this arises perform study and comparison of best practices, standards, norms and regulations concerning the following topics:

- Secure software development.
- Access Control robust.
- Single Sign On.
- Mexican laws for personal data protection.

The result should be a guide to design and develop corporate web portals with robust security, in a more agile way as it is intended to eliminate the need to consult large volumes of information corresponding to each of the premises established.

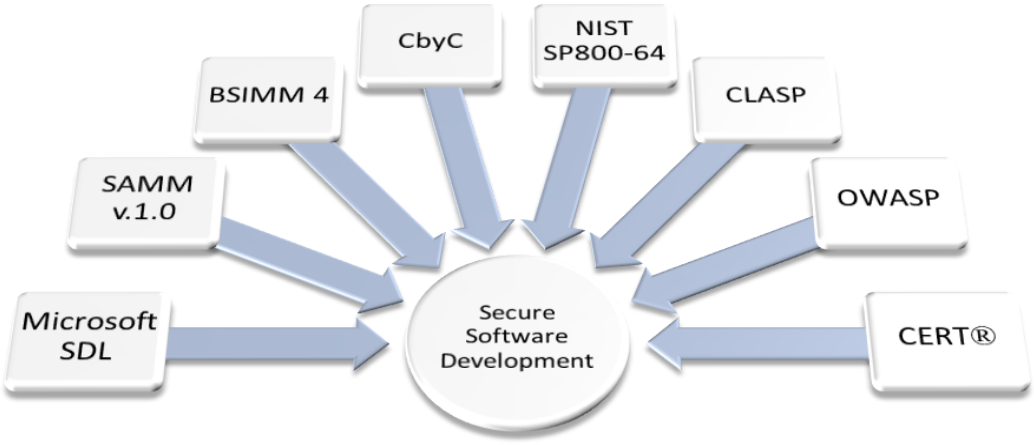
The solution proposed has been named "Framework of security and access control for the development of corporate web portals", all this as result of in-depth investigation about the theoretical framework of the needed concepts and the qualitative evaluation of the different options that were found, in order to obtain the necessary knowledge to define adequate solution to the established runtime environment and that meets the requirements requested.

2. DEVELOPMENT OF THE PROPOSED SOLUTION

The first step was to define the characteristics of the environment in which it is proposed to implement the reference framework, to do this was important because it will allow delimiting every component of the proposed solution.

Aspect	Actual condition	Implications
Budget allocated for security into software development	Practically is null and the future budget is conditional on obtaining tangible results of the security implementation.	Implementing mechanisms and security controls of very low cost.
Personnel involved in the software projects he has been formally trained in techniques for secure software development	Insufficient to cover the different security roles for software development.	The activities to be undertaken should be assigned to a minimum of roles specialized in security. It should use the available staff participation and foment the formation of new security specialists.
Formal method of software development	The organization has several software development teams using different methods for manufacturing of systems.	The solution must be flexible and be able to be applied to different development methods.
Is there any method currently for develop secure software and building corporate web portals?	No.	In case of using a maturity model, the starting point must be the most basic level.
Is there a way to have tools, methods, training and advisors in security even if these have a cost?	At the moment only be used items and services that their use is free of cost.	If necessary, use support tools that are freeware, promote self-training, forums free advice and methods that are not owners.
Development teams are willing to invest time in security activities	Not unless it is strictly necessary or higher order.	Activities should be simple and quick to implement. Awareness programs should be established for all personnel involved.
Policies, rules, regulations or standards of security	General security policies ISMS under development	The reference framework should consider the current security policy

Under the context previously defined, the next step was selecting a set of the most important and recognized techniques for the secure software development. Then were selected 8 techniques that are of the most used due their effectiveness and the prestige of institutions that they created them.

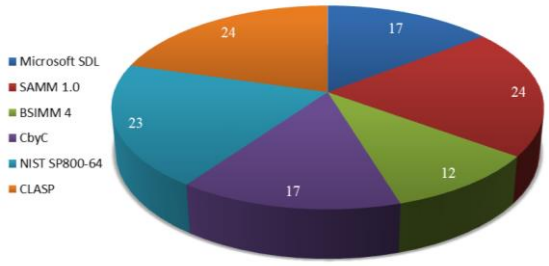


Techniques used to development secure software

The characteristics of the selected techniques were observed and studied in order to identify their elements and which are their strengths and weakness.

Components identified in each scheme

Scheme	Development process	Madurity model	Security principles	Framework
Microsoft SDL	✓	-	-	-
SAMM v.1.0	-	✓	-	✓
BSIMM 4	-	✓	-	✓
CbyC	✓	-	✓	-
NIST SP800-64	✓	-	-	-
CLASP	✓	-	✓	-
OWASP	-	-	✓	-
CERT®	-	-	✓	-



Minimum security activities identified in each scheme

With the knowledge obtained were established the first concepts of the reference framework, in specific the components denominated framework and security principles. To define the security principles was used a qualitative comparison such as it was done with the framework concepts, in the comparison were considered advantages and disadvantages rescuing the most relevant concepts.

Concepts identified	For each scheme, the principle of security related to the concept identified			
	CbyC	CERT	OWASP	CLASP
Easiness	✓ principle 6	✓ principle 4	✓ principle 9	-
Avoiding mistakes	✓ principles 1, 2, 5	✓ principle 2	✓ principles 5, 10	-
Validate inputs	-	✓ principle 1	-	✓ principle 9
Security by default	-	✓ principle 5	✓ principle 2	✓ principle 5
Principle of least privilege	-	✓ principle 6	✓ principle 3	✓ principle 7
Defense in depth	-	✓ principle 8	✓ principle 4	✓ principle 6
Reduce attack surfaces	-	-	✓ principle 1	✓ principle 4

To define de access control model were considered two existing models whose characteristics are convenient for desired model of corporate web portals in which is necessary the use of the concepts of roles and attributes, such that it was studied the model of Role Based Access Control (RBAC), and the model of Attribute Based Access Control(ABAC). The comparison was done considering the advantages and disadvantages of each model and for each possible combination between them:

- Using RBAC and ABAC without combination
- RBAC-A, Dynamic Roles
- RBAC-A, Attributes-Centric
- RBAC-A, Role-Centric

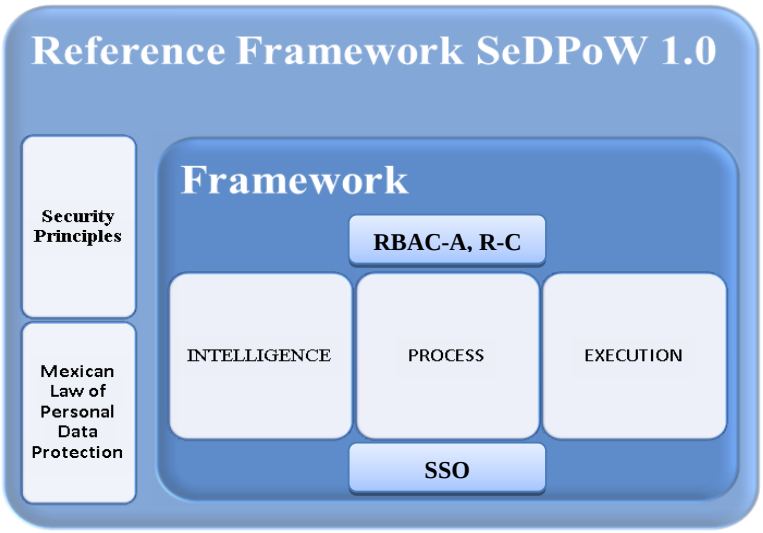
In the case of recommendations of Single Sign On were studied the premises and concepts of the model in order to take those that are the most adequate to be incorporated in the reference framework according with the defined context.

Finally, the legal aspect was considered by the study of two laws of data personal protection in Mexico, they are the “Ley Federal de Protección de Datos Personales en Posesión de

Particulares" (Federal Law on Protection of Personal Data Held by Individuals) and the "Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental" (Federal Law of Transparency and Access to Public Government Information). From both laws were taken the precepts concerning, directly or indirectly, to the Information Technologies.

3. RESULTS

Based on the knowledge gained and preset conditions of the application environment was defined the Framework for the development of secure web systems.



3.1 Security principles

Are the premises about how to carry out the activities that integrate the security practices.

- Keep yourself informed.
- Avoiding mistakes.
- Keep a schema simple.
- Validate the data inputs.
- Security by default.
- The least privilege.
- Defense in Depth.
- Develop incrementally.
- Ethical perspective of attacker.

3.2 Framework

It was integrated with 3 domains composed by 9 security practices that frame the activities to develop secure web systems.

INTELLIGENCE	PROCESS	EXECUTION
Training and guidance (TG)	**Initial planning (IP)**	**Operating configuration (OC)**
Continuous improvement (CI)	**Secure design (SD)**	**Transfer of responsibility (control and safekeeping) (TR)**
Knowledge retention (KR)	**Secure construction (SC)**	**Obtaining knowledge (OK)**

This is the complete framework including the activities of each security practice.

INTELLIGENCE	PROCESS	EXECUTION
Training and guidance (TG) TG1. Train to the staff of software development in computer security. TG2 Promote culture of security.	**Initial planning (IP)** IP1. Include the participation of security advisors for the initial planning of the project. IP2. Identify all high-level IT assets. IP3. Classify information to be processed and stored in the portal. IP4. Obtain information about the threats and informatics attacks most relevant of the moment.	**Operating configuration (OC)** OC1. System final configuration. OC2. Identify and gather security recommendations.
Continuous improvement (CI) CI1. Identify and document each opportunity of improve the reference framework. CI2. Periodically analyze improvement opportunities.	**Secure Design (SD)** SD1. Disseminate the information obtained in the IP4 activity among members of the development team. SD2. Perform a quick risk analysis of IT assets identified. SD3. Determine what are the security requirements SD4. Incorporate security requirements in the high-level design and architecture of the corporate portal. SD5. Define security tests for the portal in its totality. SD6. Incorporate security requirements in the detailed design. SD7. Define security tests for each module.	**Transfer of responsibility (TR)** TR1. Establish formal agreements. TR2. Transfer the system control. TR3. Formally deliver the system.
Knowledge retention (KR) KR1. Create knowledge repositories. KR2. Keep repositories updated.	**Secure construction (SC)** SC1. Programming each module using best practices. SC2. Validate the programming of each module. SC3. Execute the security tests of each module. SC4. Execute security tests of the portal in its totality (global tests)	**Obtaining knowledge (OK)** OK1. Gathering empirical data.

3.2.1 Access Control model

After studying different strategies to combine the access control models, it was proposed, such as part of this reference framework, the combination denominated RBAC-A Role-Centric. The concept of this access control model is divided in two processes: Assignation and Execution.

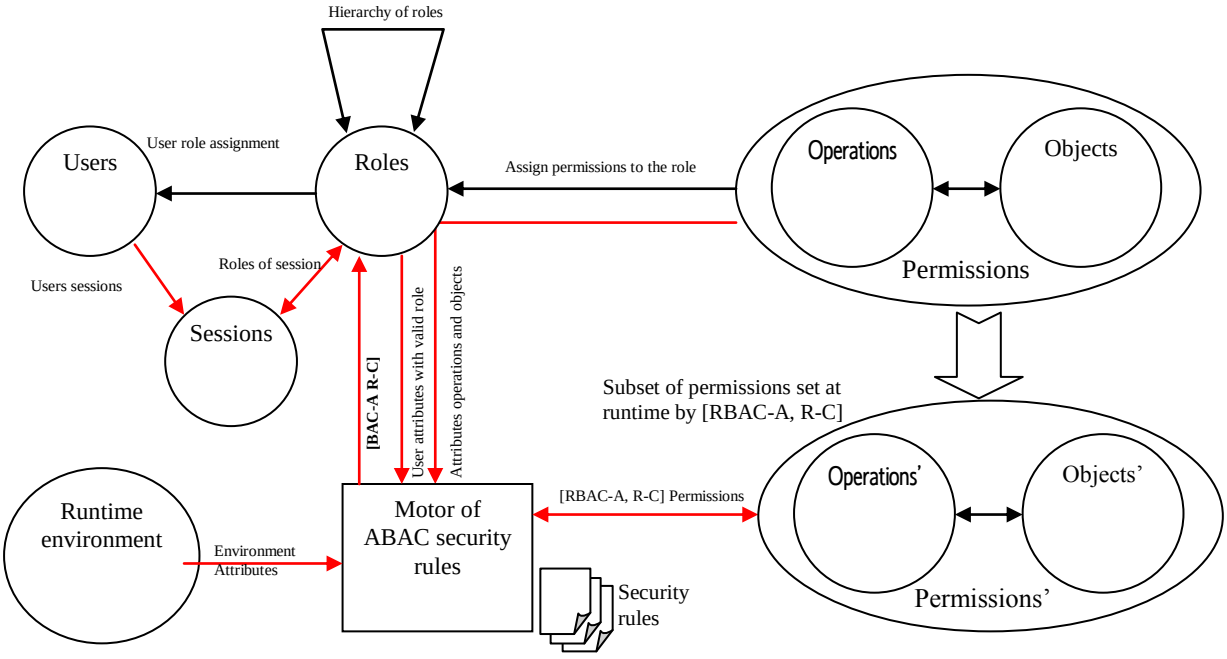
Assignation process:

1. The role is defined.
2. The permissions, on operations and objects (system resources), are assigned to the corresponding roles according with definition of functions.
3. The corresponding roles are assigned to each user.

Execution Process:

1. The user gains a valid session to request access to the system.
2. The user with a valid session requests access to the resources through its assigned role.

3. If the user role is valid, then its attributes are sent to the motor of security rules ABAC together with the attributes of the operations and the objects associated with the user role and the attributes of the execution environment (ABAC's characteristic). If the user does not have a valid role the request for access to resources is denied.
4. The attributes of the user, of the environment and of the resources are all evaluated in the ABAC security motor, basing on the previously set rules of security that are applicable to the access request.
5. If the evaluation of attributes produces a response of authorized access, then a subset of the permissions assigned to the role is indirectly provided to the user through its role. If the evaluation of the attributes with security rules produces a response of unauthorized access, then the access request is denied.



The considerations concerning the implementation of this model must be used into "Process" domain of the framework, this in order that the aspects defined here are part of the design and construction of the corporate web portal.

3.2.1 Single Sing On recommendations

The following aspects and recommendations of security must be considered to realize the activities “Secure design” and “Secure construction” into the “Process” domain of the framework for secure development.

- Sending credentials must be made indirectly.
- Sending credentials must be made on demand.
- Another recommendations:
  - The user credentials must be stored in such a way as to be unintelligible.
    - Use ciphers.
    - Use Hash methods (It is recommended to use stronger methods than MD5)
  - The credentials must be stored into an environment trusted and protected (Preferably at the server).
  - You must ensure that only the authorized process can read and write to the repository user credentials.

- The transference of credentials between domains must always be through secure communication channels.
- Always use POST method instead of GET method.
- Whenever possible send the credential information in encrypted form.

3.3 Recommendations to comply with laws protecting personal data in Mexico

After studying the content of the Federal Law on Protection of Personal Data Held by Individuals (LFPDPPP) and of the Federal Law of Transparency and Access to Public Government Information (LFTAIPG), the following basic concepts were identified that they must be considered in the framework of security for the development of corporate web portals.

Into the "Process" domain, in the security practice denominated "initial planning" is very useful consider the definition and classification of data personal.

- **Protection of information.**

  Refer to LFTAIPG: (Article 3, part XIV), (Article 20, part III & VI), (Article 21) and LFPDPPP: (Article 2, part I & II), (Article 9, 11 & 19)

- **Data classification and protection levels.**

  Refer to LFTAIPG: (Article 3, part II) and LFPDPPP: (Article 3, part V & VI).

  Data classification by security level required: "Recomendaciones del IFAI sobre medidas de seguridad Aplicables a los sistemas de datos personales" (IFAI recommendations on security measures applicable to systems of personal data).

The following references of the law should be considered into the security practice "Transfer of responsibility" of the "Execution" domain in order to they will be useful to issue precautions to the company that will be responsible for the corporate web portal has been developed.

- **Misdemeanours and responsibilities**. Every organization and enterprise that they have informatics systems that process data personal, they must adopt the corresponding measures to avoid committing crimes and misdemeanors to the protection data laws in México. Refer to LFTAIPG: (Article 63) and LFPDPPP: (Article 20 & 36), (Article 63, part XI)

- **Penalties**. Regarding the penalties that are applied when there is a violation of laws data personal protection, Refer to LFPDPPP: (Article 64, part III & IV), (Article 67, 68 & 69)

All the information described above about the legal aspect also should be considered in the "Intelligence" domain in order to foment the security culture.

4. CONSIDERATIONS

- The process of selection, creation and adaptation of safety guidelines, was conducted using engineering of information security, to build the reference framework, appropriate to the needs of the company, was not reinvented anything, the best of what existed was obtained.

- Two of security requirements are from a previously established model for the Corporate Portals Development in the "Instituto de Investigaciones Eléctricas" (Electrical Research Institute): Role Based Access Control and Single Sign On.

- It was decided not to use a maturity model for this initial version of the framework because the intention is to establish a light and agile implementation, if a maturity model is established then implementation of the framework will require a greater investment of time, effort and resources. Therefore, it must be assumed that the defined security activities are located in the most basic level of maturity like a start point

- The recommendations are flexible and can be included in different software development processes to get secure web applications.

- Both the model specification of access control as the schema Single Sign On are defined only conceptually in a high level without going into the details of a formal or mathematical specification, since for purposes of this study, it was enough to high-level conceptual model to show the reference of what is necessary as access control scheme.

- The framework focuses primarily on the circumstances and activities are controlled by the developer company (development environment, internal policies, internal models of development and internal infrastructure development) and left somewhat aside security activities to be performed on matters which are not within its competence such as infrastructure where reside the system: security of network operating environment, physical facilities, security policies, etc..

5. CONCLUSIONS

At the end of this research we were able to obtain a framework of security and access control, for the development of corporate web portals, which concentrates a series of safety recommendations regarding the design and the construction of corporate web portals, regarding the model access control and to the legal compliance with data protection in Mexico.

Using the reference framework will allow to provide extra value to corporate web portals that are developed under this scheme, its essence agile and lightweight will facilitate that the development teams incorporate the recommendations into their software development processes.

Other relevant aspects were identified during the course of this work. Following are described those conclusions:

- In companies, it is very important to have a framework for information security which must be integral and must have the support of senior management of the organization.

- Are increasingly frequent the cyber-attacks through the web and therefore businesses worldwide are investing more resources to implement security in their information systems.

- When software is produced, mitigating security concerns is much less expensive if done in the early stages of any software development process.

- Promote information security culture among people of a company contributes greatly to prevent security flaws in information systems.

- A combined scheme of access control based on roles and access control based on attributes, allows for a more robust model for access control.

5.1 Projects for the future

The following is a suggested list of research and development projects whose implementation would contribute to enriching the actual work done.

- Define and add a maturity model for the reference framework defined in this research.
- Create quick security guidelines for designing, coding, testing, configuration and implementation of a corporate web portal.
- Define and establish a model standardized of software creation for the development process of secure portals web for the "Instituto de Investigaciones Eléctricas" (Electric Research Institute).
- Define the detailed specification for the access control model: [RBAC-A, Role-Centric] and for the scheme: Single Sign On.
- Define and implement quality metrics to measure the effectiveness of the security activities and they also can be used as indicators aligned to the business strategy of the company.
- Add activities for the complete fulfillment of standards and policies about information security, this will allow that the reference framework to be ready for any plan of certification and accreditation.

There is still much work to be done, however the result of this research is a tool that represents a step towards a stronger information security culture in the computer systems in energy sector companies in Mexico.

GLOSARY

Microsoft SDL: Security Development Lifecycle de Microsoft.

SAMM v.1.0: Software Assurance Maturity Model version 1.0.

BSIMM 4: Building Security in Maturity Model version 4.

CbyC: Correctness by Construction.

NIST SP800-64: Security Considerations in the System Development Life Cycle.

CLASP: Comprehensive, Lightweight Application Security Process.

OWASP: Open Web Application Security Project.

CERT®: Recomendaciones de seguridad del CERT del SEI de la Universidad Carnegie Mellon.

RBAC: Role Based Access Control.

ABAC: Attribute Based Access Control.

SSO: Single Sign On.

RBAC-A: Combination between RBAC with ABAC.

RBAC-A, R-C: Combination between RBAC with ABAC and Role–Centric.

LFPDPPP: Federal Law on Protection of Personal Data Held by Individuals (initials in Spanish).

LFTAIPG: Federal Law of Transparency and Access to Public Government Information (initials in Spanish).

IFAI: "Instituto Federal de Acceso a la Información" (Federal Institute for Access to Information). It is a Mexican government dependence that regulates the public information access and the protection of people data personals

BIBLIOGRAPHY

[1] Isai Rojas González. (2012, December) "Marco de Referencia de Seguridad y de Control de Acceso para el Desarrollo de Portales Web Corporativos" (Tesis para obtener grado de Maestría). Instituto Politécnico Nacional, México D.F.

[2] NIST. (2011, October) ROLE BASED ACCESS CONTROL (RBAC) AND ROLE BASED SECURITY. [Online]. http://csrc.nist.gov/groups/SNS/rbac/

[3] Alan C. O'Connor and Ross J. Loomis, "2010 Economic Analysis of Role-Based Access Control," Research Triangle Institute International, Report prepared to the NIST.

[4] Isai Rojas and Martín Santos, "Arquitectura de un Portal Corporativo", Boletín IIE, no. 4, pp. 127-133, Octubre-Diciembre 2007.

[5] Microsoft. (2010, February) Security Development Lifecycle. Implementación simplificada del proceso SDL de Microsoft.

[6] Pravir Chandra and Team OWASP. (2005, March) Software Assurance Maturity Model versión 1.0. Documento guía para integrar seguridad en el desarrollo de software.

[7] Gary McGraw, Sammy Migues, and Jacob West. (2012, September) Building Security In Maturity Model versión 4. Estudio de iniciativas de seguridad.

[8] Anthony Hall and Rod Chapman. (2004, January) Correctness by Construction. Metodo de construcción de software seguro.

[9] NIST. (2008, October) Security Considerations in the System Development Life Cycle. Special Publication 800-64 Revision 2.

[10] OWASP. (2012, September) Proyecto CLASP. [Online]. https://www.owasp.org/index.php/Category:OWASP_CLASP_Project

[11] OWASP. (2011) OWASP website - The Open Web Application Security Project. [Online]. https://www.owasp.org/

[12] OWASP. (2005, July) Una Guía para Construir Aplicaciones y Servicios Web Seguros. Edición 2.0 Black Hat, versión en español.

[13] DesarrolloWeb.com. (2012, September) Guía para el desarrollo de aplicaciones web seguras. Normas y conceptos para hacer aplicaciones web seguras. [Online]. http://www.desarrolloweb.com/articulos/996.php

[14] CERT Software Engineering Institute Carnegie Mellon. (2012, September) Top 10 Secure Coding Practices. [Online]. https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices

[15] David F. Ferraiolo and Richard D. Kuhn, "Role Based Access Control," in 15th National Computer Security Conference, Baltimore, 1992, pp. 554-563.

[16] David F. Ferraiolo, Richard Kuhn, and Ravi Sandhu, "RBAC Standard Rationale: Comments on a Critique of the ANSI Standard on Role Based Access Control," IEEE Security & Privacy, vol. 5, no. 6, pp. 51-53, 2007.

[17] D. Richard Kuhn, Edward J. Coyne, and Timothy R. Weil, "Adding Attributes to Role Based Access Control," IEEE Computer, vol. 43, no. 6, pp. 79-81, June 2010.

[18] ANSI/INCITS. (2004, February) Role Based Access Control. Standard 359-2004.

[19] InCommon. (2011, October) Single Sign-On Concept. [Online]. https://spaces.internet2.edu/display/InCCollaborate/Single+Sign-On+Concept

[20] The Open Group. (2011, October) Introduction to Single Sign-On. [Online]. http://www.opengroup.org/security/sso/sso_intro.htm

[21] Ley Federal de Transparencia y Acceso a la Información Pública, June 11, 2002.

[22] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, July 05, 2012.

[23] IFAI. Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales. [Online]. http://ifai.org.mx/pdf/ciudadanos/cumplimiento_normativo/datos_personales/Recomendaciones_SDP.pdf