Soluciones innovadoras en energía | Instituto de Investigaciones Eléctricas

LIMA 2015 SC D2
TUTORIALS & COLLOQUIUM

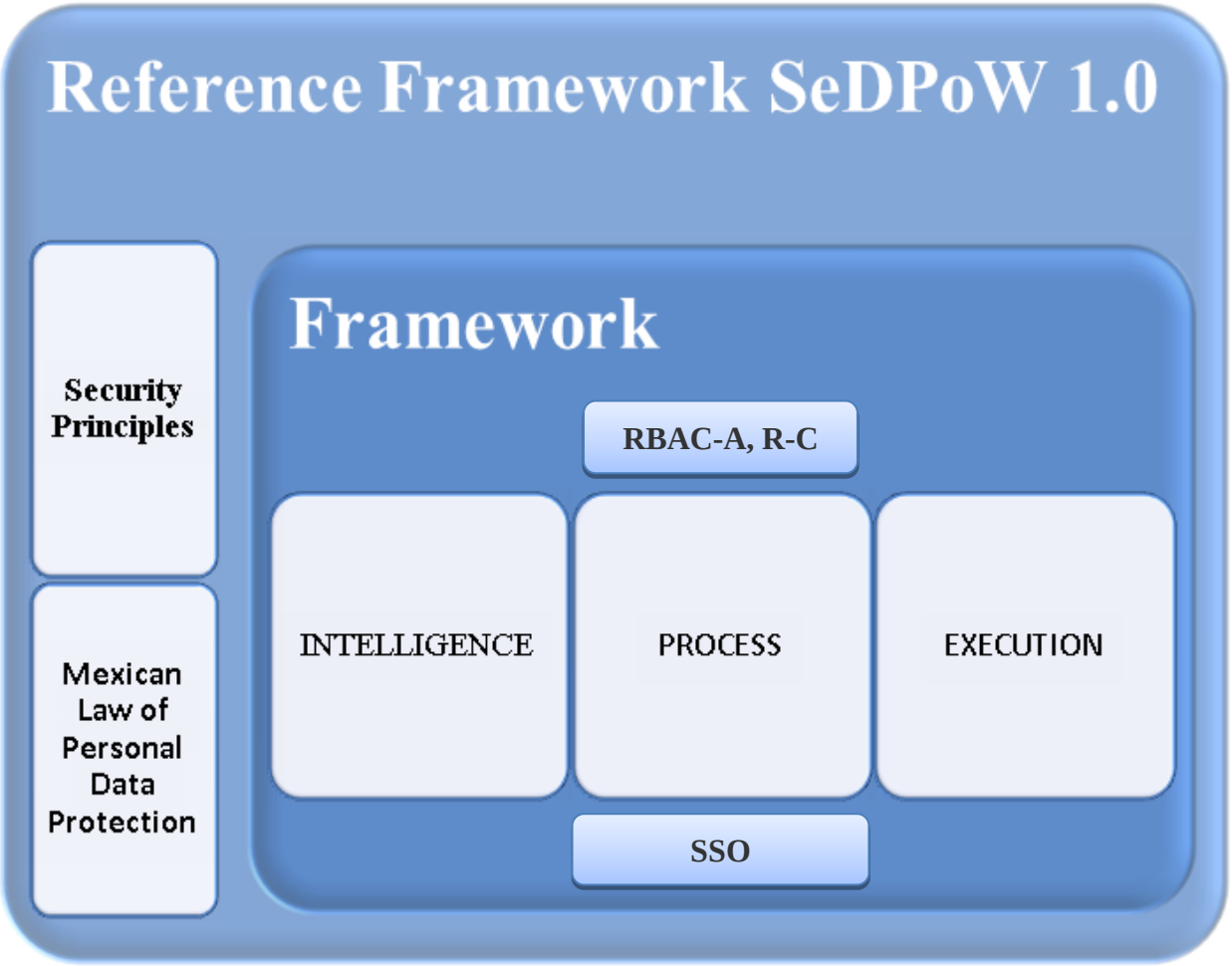
FRAMEWORK FOR THE DEVELOPMENT OF SECURE WEB SYSTEMS FOR ELECTRICAL COMPANIES

Presented by:
Isai Rojas González
Instituto de Investigaciones Eléctricas (México)

Advising and collaboration by:
Gabriel Sánchez Pérez
Instituto Politécnico Nacional (México)

CONTENT:

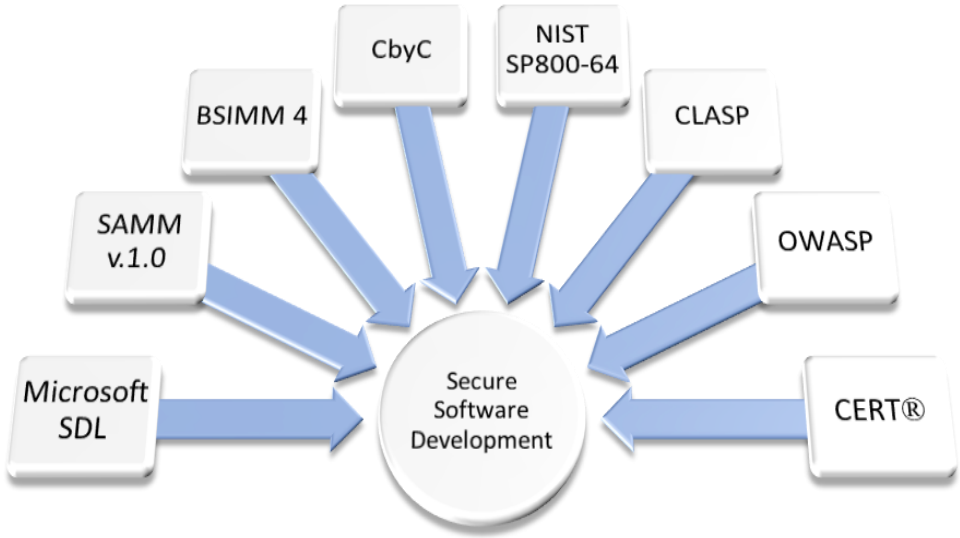
- Elements considered to develop the reference framework
- Reference Framework SeDPoW 1.0:
  - Security Principles
  - Security Framework
  - Access Control Model
  - Single Sing On Recommendations
  - Mexican Law Compliance
- Conclusion
- Special Report (Q&A)



Elements considered to develop the reference framework

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 systems development environment of the Electrical Research Institute in Mexico, such that the framework also is suitable to the software development related to electricity sector companies.



SSO RBAC ABAC

- **Federal Law on Protection of Personal Data Held by Individuals (LFPDPPP)**
- **Federal Law of Transparency and Access to Public Government Information (LFTAIPG)**

Components of the Reference Framework SeDPoW 1.0

1) 9 Security principles

2) A security framework to the software development with 27 activities of security grouped in 9 practices through 3 domains

3) A role-attribute based access control model (role centric)

4) A set of recommendations about Single Sing On

5) A set of recommendations for Mexican law compliance on data personal protection

1) Security Principles of SeDPoW 1.0

1. **Keep yourself informed**. More information = more probabilities to reduce the vulnerabilities.
2. **Avoiding mistakes**. The errors in the software development become vulnerabilities
3. **Keep a schema simple**. The complexity increase the attack surface of a system.
4. **Validate the data inputs**. To prevent the malicious code injection.
5. **Security by default**. The system must be closed by default and opening them as needed
6. **The least privilege**. To any entity to assign only the privileges needed for realize its job, not more.
7. **Defense in Depth**. Different security layers.
8. **Develop incrementally**. A little modules are easier to review and secure them
9. **Ethical perspective of attacker**. In this way the developer thinks different and try to protect its development.

Note: The security principles must be considered every moment, even in all activities done before and after of development process.

2) Security Framework of SeDPoW 1.0

Domains

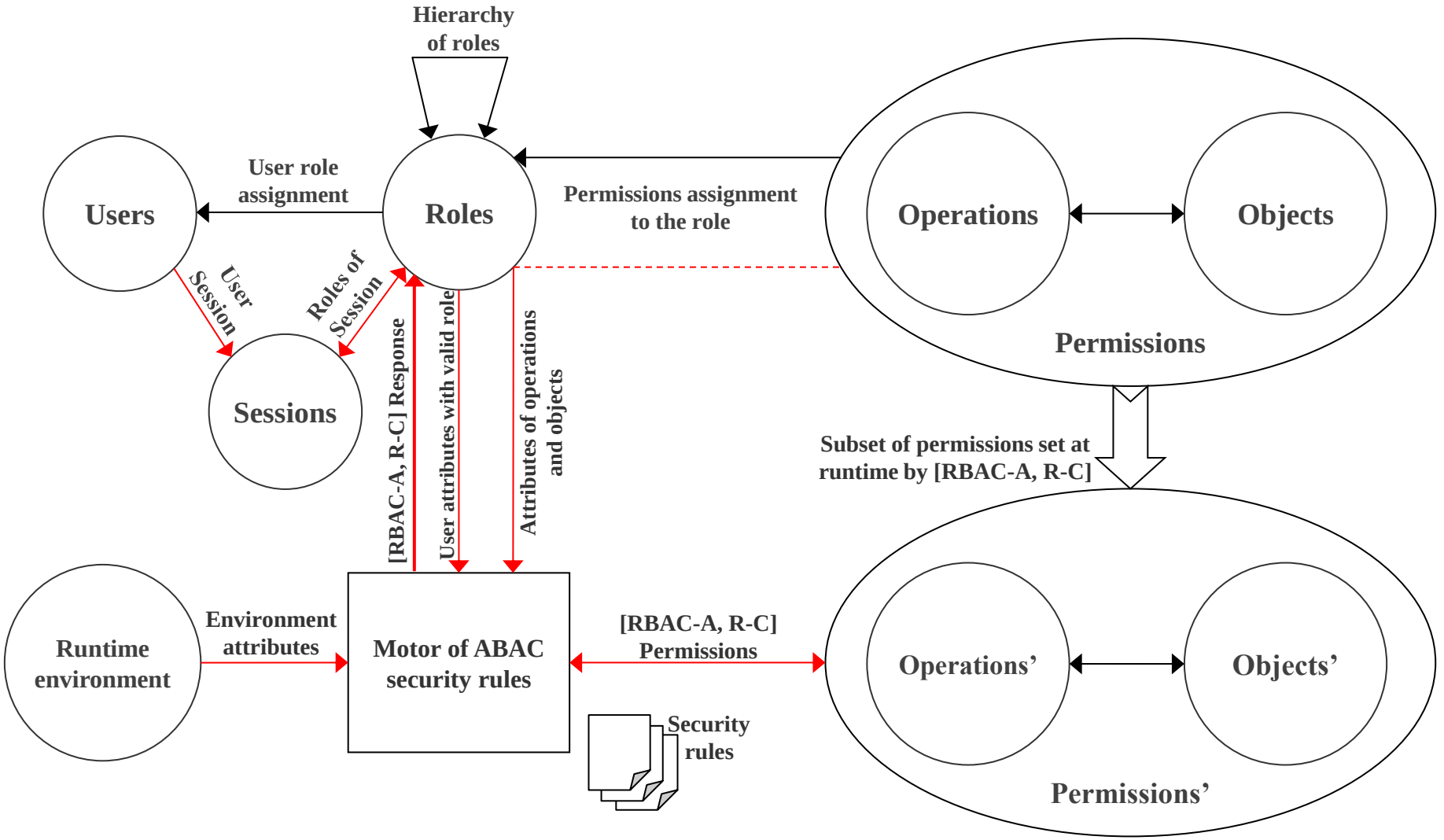
Security Practices

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)

2) Framework SeDPoW – Security Activities

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) Access Control Model of SeDPoW 1.0
RBAC-A, R-C



4) Single Sing On recommendations of SeDPoW 1.0

- Sending credentials must be made indirectly and on demand.
- The user credentials must be stored into an environment trusted and protected (preferably at the server) and in such a way as to be unintelligible.
  - Use ciphers and hash methods (It is recommended to use stronger methods than MD5)
- 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.
- If is necessary to send the credential information in a encrypted form.

Note: These aspects and recommendations must be considered into the practices “Secure design” and “Secure construction” of the “Process” domain.

5) Mexican law compliance

Personal Data Protection

This information must be considered into the “Initial planning“ security practice of the "Process" domain.

- **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: IFAI recommendations on security measures applicable to systems of personal data.

This information should be considered into the security practice “Transfer of responsibility” of the “Execution” domain.

- **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)

Note: All these information should be considered in the “Intelligence” domain in order to foment the security culture.

Conclusion

The use of the reference framework allows to provide extra value to web systems that are developed under this scheme, its essence agile and lightweight facilitates that the development teams can incorporate the recommendations of security into their software development processes and into their software products.

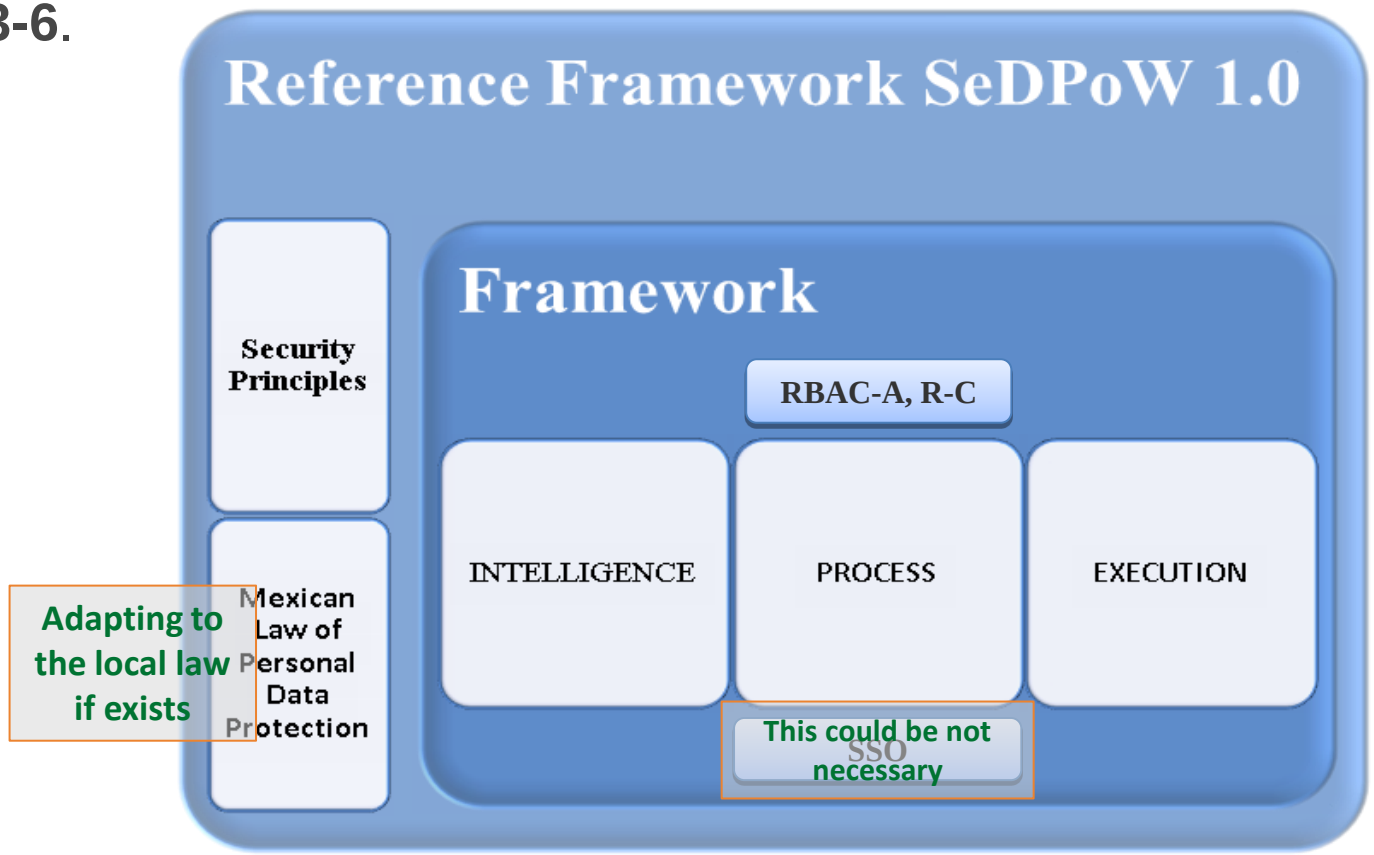
Special Report Q3-5

Q3-5. Can we learn from this approach to secure the installed base, particularly legacy systems?

A3-5. The reference framework is focused on adding security activities to the process of software development, however, the model is flexible and modular and it can be applied to legacy systems. With the replacing the software development process by a process for maintaining and improvement of systems and with slight adjustments to the activities of the "Process" domain and in this way you can use the framework to incorporate security aspects, as much as the legacy systems allow because these systems were not designed thinking about security and it will not be the same like in the new systems.

Q3-6. Which part of this framework do you suggest to advice to other EPUs and how could they implement it?

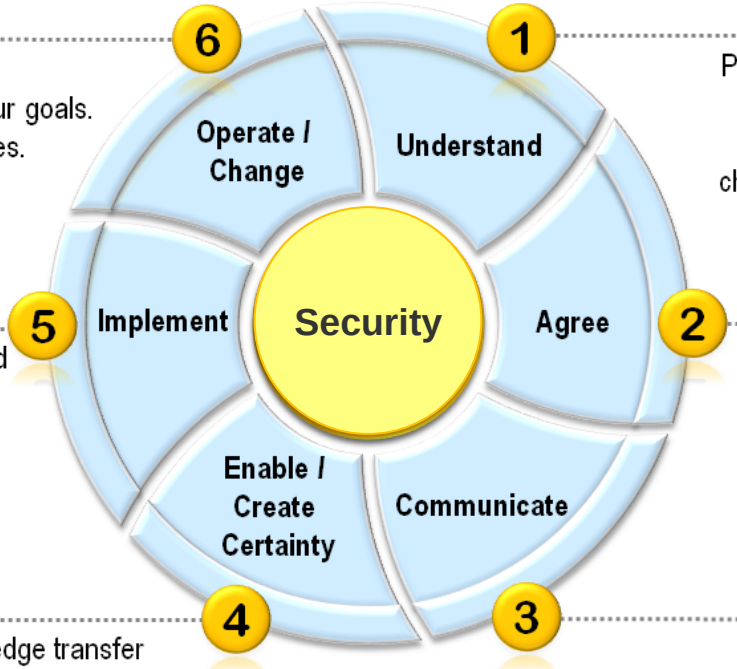
A3-6.



Special Report Q3-6 (Cont.)

Q3-6. Which part of this framework do you suggest to advice to other EPUs and how could they implement it?

A3-6. Change Management, awareness and diffusion



6 — Attend change process and make necessary changes to achieve your goals. Consider experiences of employees. Adjust procedure and motivate employees.

1 — Point of departure, mission, goals, needs of changes and understanding of histories of changes. Become acquainted with organization and situation of affected employees.

5 — Stringent project management and implementation of arranged changes. Remove and conquer obstacles.

2 — Declare dimension and implementation of changes with early involvement of affected employees.

4 — Long-term management of knowledge transfer and security towards affected employees to implement and operate changes successfully in a sustainable way.

3 — Communicate changes, required activities, advantages and improvements regularly to affected employees.

Soluciones innovadoras en energía | Instituto de Investigaciones Eléctricas

ISAI ROJAS GONZÁLEZ

Tel.: +52 (777) 3 62 38 11
Extension: 7070
E-mail: irojas@iie.org.mx
@MISTI_RGI

LIMA 2015 SC D2
TUTORIALS & COLLOQUIUM

THANKS FOR YOUR ATTENTION

And don't forget...

In cybersecurity the worst that you can do it is doing nothing !!