FRAMEWORK FOR THE DEVELOPMENT OF SECURE SYSTEMS FOR ELECTRICAL COMPANIES

Presented by:

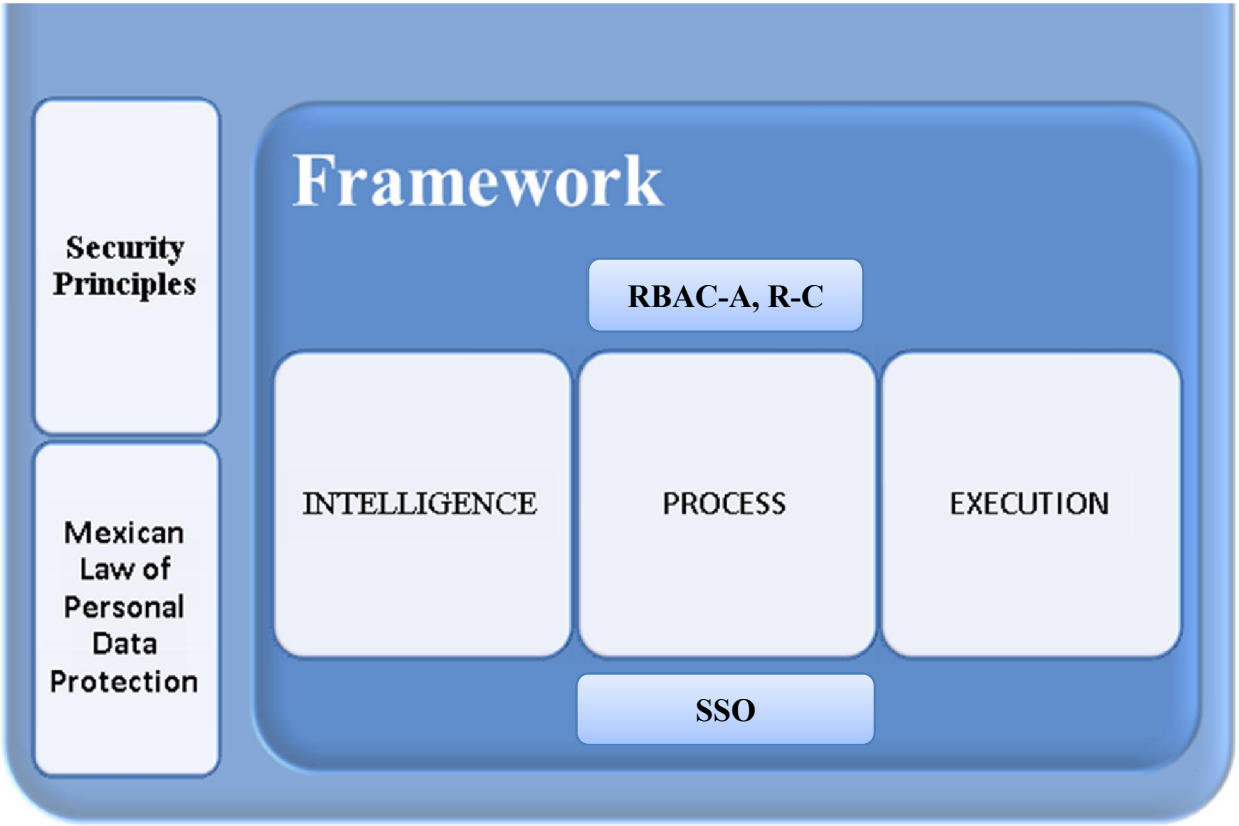
Isai Rojas González

Instituto Nacional de Electricidad y Energías Limpias (México)

November, 2015

CONTENT:

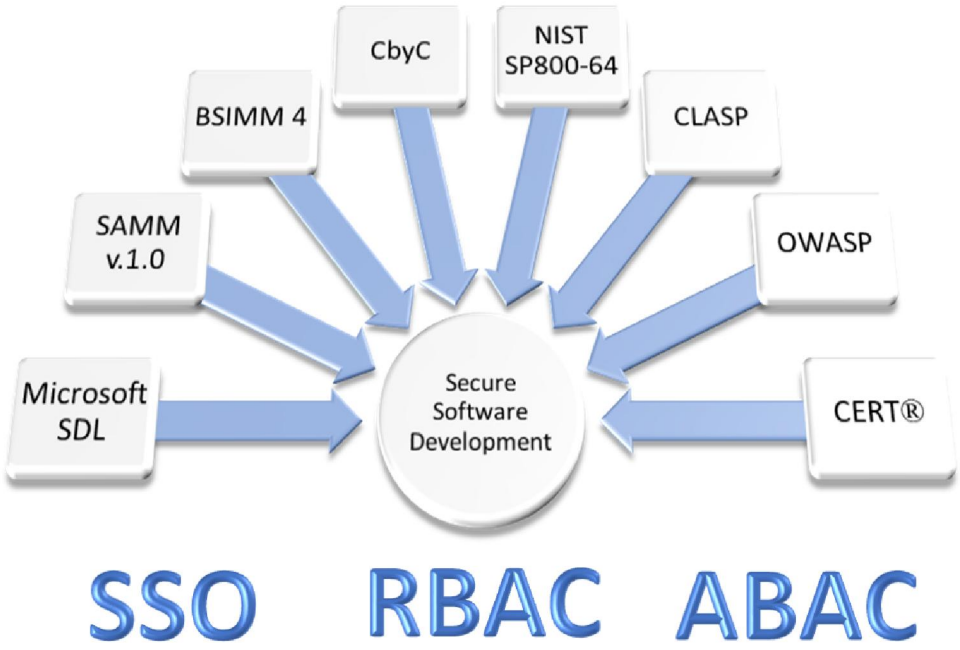
- **Elements considered to develop the reference framework**
- **Reference Framework:**
  - **Security Principles**
  - **Security Framework**
  - **Access Control Model**
  - **Single Sing On Recommendations**
  - **Mexican Law Compliance**
- **Conclusion**



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 National Institute of Electricity and Clean Energies in Mexico, such that the framework also is suitable to the software development related to electricity sector companies.



- **General Law for the Protection of Personal Data in Possession of Obligated Subjects (LGPDPPSO)**
- **Federal Law of Transparency and Access to Public Information (LFTAIP)**

INEEL

Aspects considered

Aspect	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 systems?	Beginning.	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

Reference Framework – Components

- 9 Security principles
- A security framework with 9 practices through 3 domains
- A role-attribute based access control model (role centric)
- A set of recommendations about Single Sing On
- A set of recommendations for Mexican law compliance on data personal protection

Framework – Security Principles

1. Keep yourself informed.
2. Avoiding mistakes.
3. Keep a schema simple.
4. Validate the data inputs.
5. Security by default.
6. The least privilege.
7. Defense in Depth.
8. Develop incrementally.
9. Ethical perspective of attacker

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

Framework – Security practices

Domains

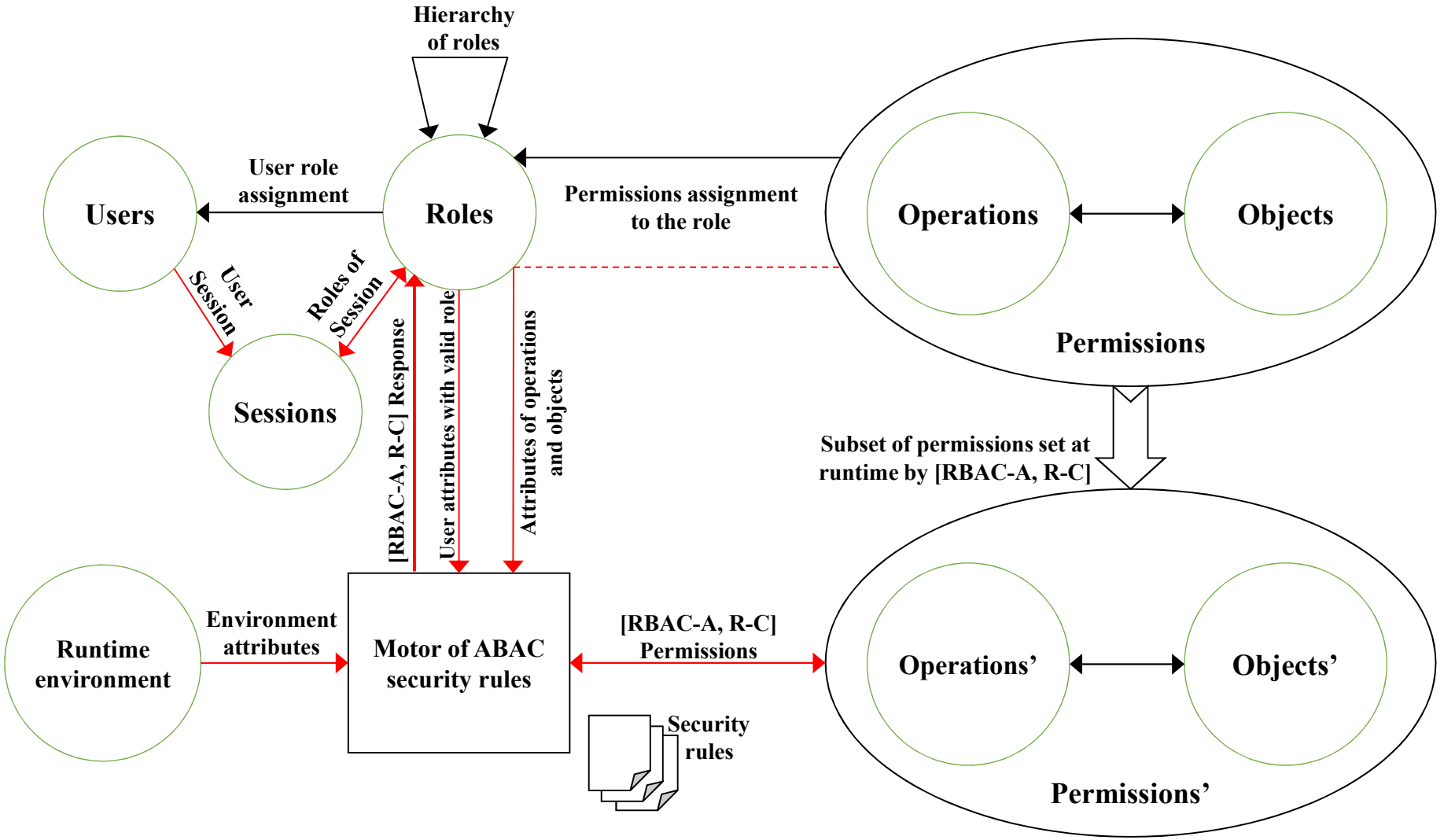
Security Practices

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)

Framework – 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&OT assets. IP3. Classify information to be processed and stored in the system. 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 system. SD5. Define security tests for the systen 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 system in its totality (global tests)	**Obtaining knowledge (OK)** OK1. Gathering empirical data.

Framework – Access Control Model (RBAC-A, R-C)



Framework – Single Sing On recommendations

- 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 SHA1)
- 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.

Mexican law compliance

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

- **Protection of information.**

  Refer to LFTAIP and LGPDPPSO

- **Data classification and protection levels.**

  Refer to LFTAIP and LGPDPPSO

  Data classification by security level required: INAI 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 LFTAIP and LGPDPPSO

- **Penalties**. Regarding the penalties that are applied when there is a violation of laws data personal protection, Refer to LGPDPPSO

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

Finally…

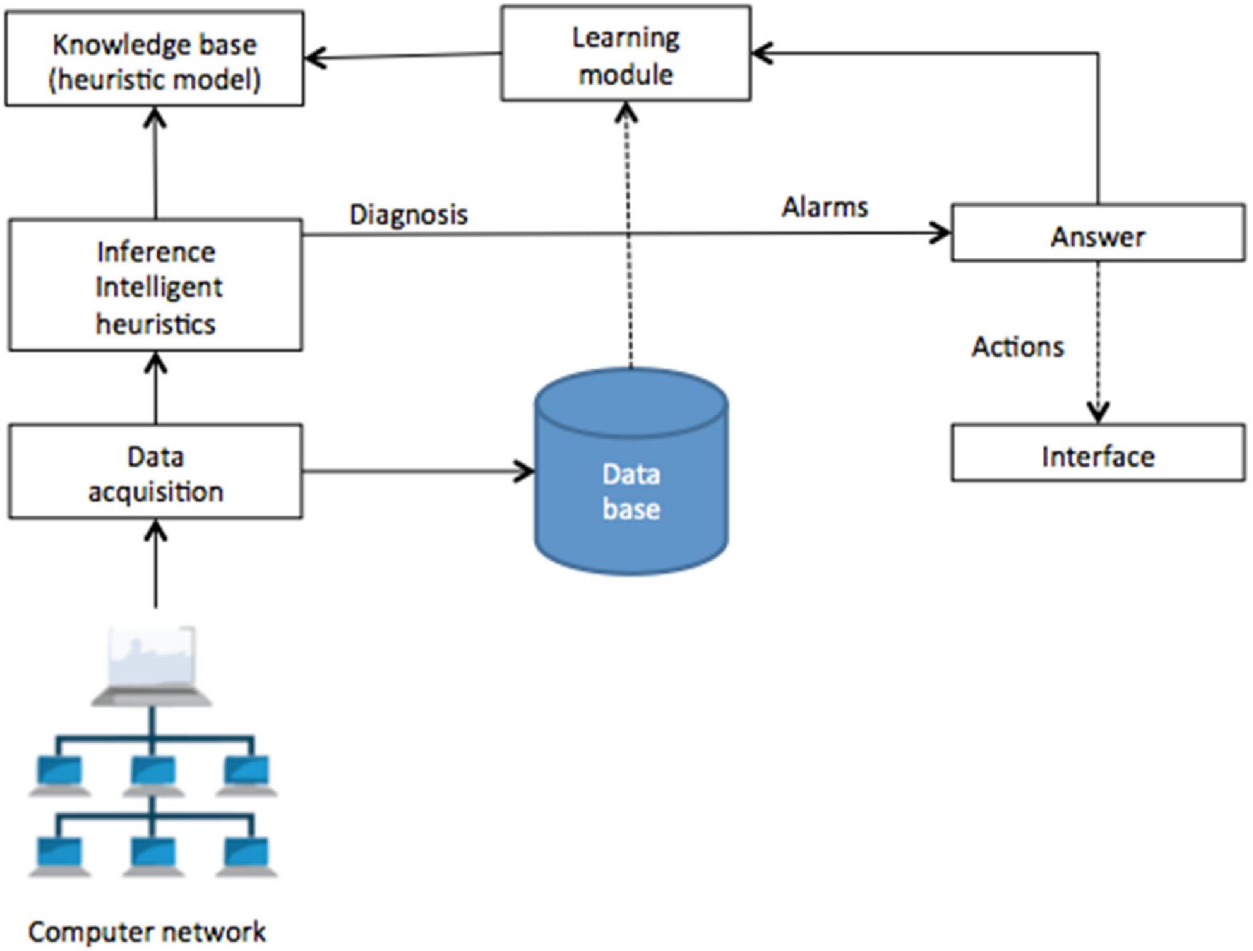
The use of the reference framework allows to provide extra value to the systems that are developed under this scheme, its essence agile and lightweight facilitates that the development teams incorporate the recommendations into their development processes.

Considering…

- Currently, the framework is under revision with the aim of incorporating a protection scheme through the use of Artificial Intelligence for the detection of malicious incidents of cybersecurity in the data network in which the system is implemented.

- With this scheme is intended to prevent cybersecurity attacks, both those who are already known as well as those who use new techniques, this through the use of AI techniques

Model for the Intrusion Detection Systems using Artificial Intelligence



Framework – Some acronyms

- LGPDPPSO: Acronym in spanish of General Law for the Protection of Personal Data in Possession of Obligated Subjects.
- LFTAIP: Acronym in spanish of Federal Law of Transparency and Access to Public Information
- 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.

INEEL
Instituto Nacional de Electricidad y Energías Limpias

THANKS FOR YOUR ATTENTION

www.ineel.mx

Isai Rojas González
Investigador Especialista en Seguridad Informática
Gerencia Tecnologías de la Información
División Tecnologías Habilitadoras
Tel. (777) 3623820
Tel. Com. (777) 3623811 ext. 7070
irojas@ineel.mx

Gustavo Arroyo Figueroa
Gerente de Tecnologías de la Información
División Tecnologías Habilitadoras
Tel. (777) 3623820
Tel. Com. (777) 3623811 ext. 7166
garroyo@ineel.mx