Security Scheme for an Information Management System Developed Under the Framework Laravel with References to the ISO 27001 Standard

Joselin Juarez George[1], M.C. Juan Ramos Ramos[2], M.C. José Juan Hernández Mora[3], Klissman Esquivel Montiel[4]

[1, 2, 3, 4] Tecnológico Nacional de México, Instituto Tecnológico de Apizaco, Carretera Apizaco Tzompantepec, esquina con Av. Instituto Tecnológico S/N, Conurbado Apizaco - Tzompantepec, Tlaxcala, Mex. C.P. 90300

Abstract: ***This article presents the analysis for the implementation of a security scheme, in which are exposed different points of computer security for the implementation of the security scheme of web applications, that involves strategies that cover related processes considering information as a primary asset. This strategy has as guiding axis the establishment of network security, logical security, physical security, hardware security, Laravel's security mechanisms and procedural technologies to detect threats that are vulnerable to the risk of such assets, that is, to help protect and safeguard the data stored and managed by the information management system of statistical variables in the field of justice. The security scheme is aligned with the requirements of ISO 27001, which supports the implementation of an Information Security Management System (IMSS), consisting of measures aimed at protecting information against any threat, in such a way as to ensure the safety of the activities carried out in the organizations.***

Keywords: Security scheme, network security, logical security, physical security, hardware security, Laravel security mechanisms.

1. Introduction

Today, organizations rely on the use of new technologies, which are accompanied by significant risks in information management. This means that your administration has a fundamental role to play, it must already start from an adequate identification of critical elements and, above all, to be clear about the risks involved in devising appropriate strategies to correct security vulnerabilities and to be able to achieve the protection of all types of information, from simple personal data to systems and databases. It is therefore the responsibility of the organizations to enhance the security of the information being handled.

To carry out the implementation of the security scheme in the Information System that was considered as a case of use, the analysis was carried out based on various meetings with users, document queries and observations of the operation of the web system with staff who have a broad knowledge of the activities being carried out, identifying the information processes and techniques used to know and understand the current state that can be applied to carry out processes in the security risk identification phase, determining the likelihood and impact on the criteria of confidentiality, integrity and availability of information, to then establish the security scheme according to the fundamental requirements for determining threats on the basis that may affect the information. Some of the most common threats presented in web systems are:

- Loss of information
- Concurrence or modification of information
- heft, alteration or loss of equipment
- Disclosure of information
- Interaction of services

Among the main factors of insecurity in organizations are network security, logical security, physical security and hardware security. The Laravel Framework presents certain tools that can meet these criteria.

In order to provide satisfactory protection to organizations and avoid risks in authenticating users, it is possible to take into account the Laravel Framework, which is open source for the development of web applications and services. This Framework offers different options to develop a more secure system in different aspects, using the "form request" component that is useful for validating information, delimiting the user and the different values for the database that is used [1].

To develop the proposed security scheme, the requirements and standards of ISO 27001 (Information Security Management) were analyzed. With these elements as a reference, the frequently performed security controls and procedures were implemented, establishing the mechanisms to protect information, reduce risks and threats presented in the system, taking the necessary measures to re-establish the information of the data that were captured.

2. Frame of Reference

2.1 Structure of ISO 27001

Standard ISO/IEC 27001 Information Security Management Systems (IMSS) is the international standard that specifies the requirements for establishing the measures and controls that ensure confidentiality, integrity and availability of information system assets, including hardware, software, firmware, and that information they process, store, and communicate [2].

The central focus of ISO 27001 is to protect the confidentiality, integrity and availability of the organization's information. This is done by investigating what are the potential problems that could affect the information (i.e., risk assessment) and then defining what needs to be done to prevent these problems from occurring (i.e., mitigating or treating the risk) [3].

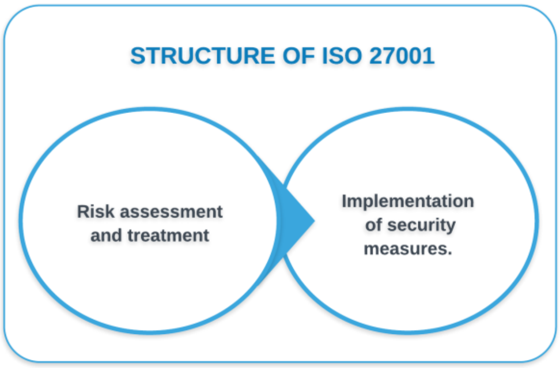

STRUCTURE OF ISO 27001
Risk assessment and treatment
Implementation of security measures.

Figure 1: ISO 27001 structure **[3]**

Through Fig. 1, the main philosophy of the ISO 27001 standard is made known, which is based on risk management: investigate where the risks are and then treat them systematically.

2.2 Security informatic

Information security is responsible for the discipline of rules, procedures, methods and techniques aimed at ensuring a secure and reliable information system for information systems. To address the security of a system, it is necessary to know the following:

- The elements that make up a system. Information can be obtained through interviews with the users responsible for the organization's system.
- Hazards affecting the system, whether accidental or caused by the users themselves. They are deduced from the data provided from the tests and samples on it.
- Measures to be taken to identify, prevent, prevent, reduce or control risks. With this information it is decided which security services and mechanisms would reduce the possible risks.

Computer security is the medicine for designing standards, procedures, methods and techniques to achieve a secure and reliable information system [4].

In Fig. 2, you can observe the identification of the properties of computer security, analysis and irrigation controls, in addition to the elements of analysis, services and mechanisms of each one of the controls. Each of the controls presented are considered in the implementation of the final security scheme.

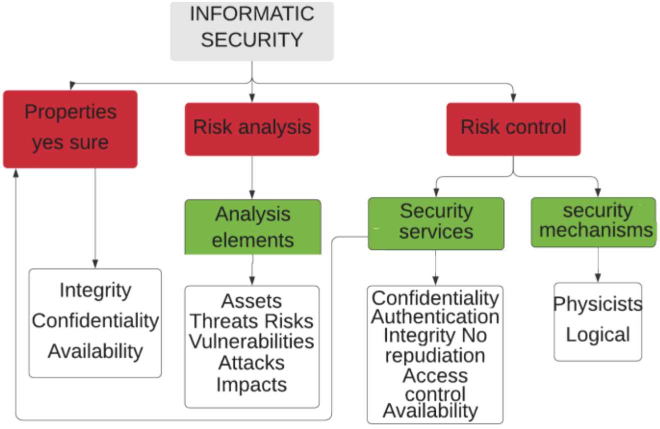


Figure 2: Computer security and components [4]

2.3 Security of Laravel

One of the main components of the Laravel Framework that it offers in terms of security, is the Middleware. This component is responsible for analyzing and filtering HTTP calls on the server. In addition, it can be used to verify that it is a registered user and thus avoid security measures problems.

Laravel offers security mechanism that allows to use in web applications, which are:

- Identification
- Authentication
- Encryption
- Roles Service
- Limitations
- Location and time
- Access control list
- Limitation on user interfaces

Laravel's security protocols are fundamental to building robust applications that must be implemented in organizations to identify the different technological risks that may violate information systems. These risks can be classified as internal or external threats; the former is generated by internal organizational factors and the latter by external factors.

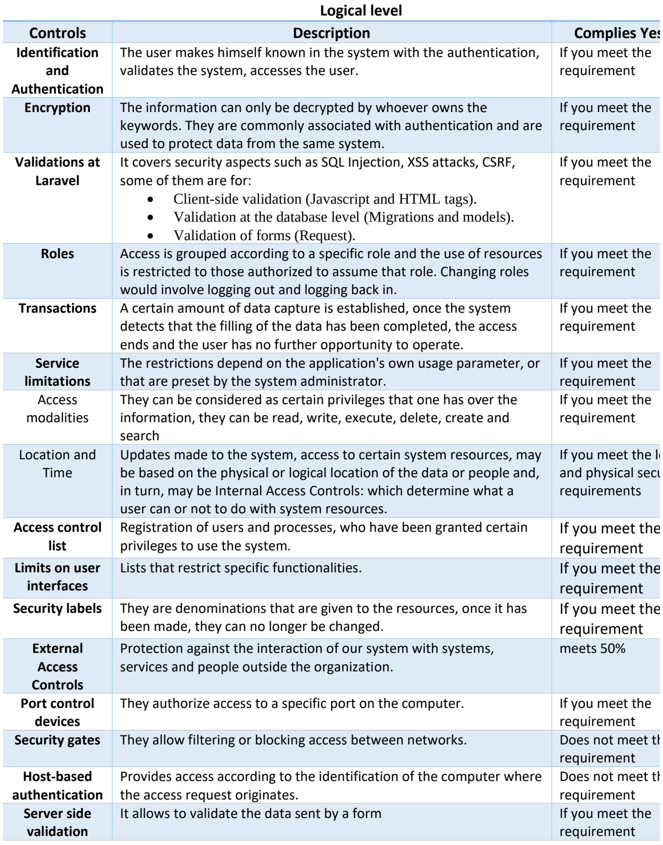
3. Análisis y definición del Marco de seguridad

3.1 Squama basic

Analyzing the logic, physical and network security elements present through the Laravel Framework determines the need to evaluate each of the components. In case it does not comply with requirements, it will be necessary to analyze various technological tools that can be used and be able to correct the vulnerabilities presented in the web system developed under the Laravel Framework.

Next, the various controls are displayed, as well as the logical level related to ISO 27001 and the result of the compliance analysis.

Subsequently, the analysis of the logical level controls of the Laravel Framework was carried out, allowing the evaluation of the requirements of each of its components, identifying those that, if they comply and those that do not, then correct them with tools according to the system (Fig. 3).



Logical level

Controls	Description	Complies Yes
Identification and Authentication	The user makes himself known in the system with the authentication, validates the system, accesses the user.	If you meet the requirement
Encryption	The information can only be decrypted by whoever owns the keywords. They are commonly associated with authentication and are used to protect data from the same system.	If you meet the requirement
Validations at Laravel	It covers security aspects such as SQL Injection, XSS attacks, CSRF, some of them are for: • Client-side validation (Javascript and HTML tags). • Validation at the database level (Migrations and models). • Validation of forms (Request).	If you meet the requirement
Roles	Access is grouped according to a specific role and the use of resources is restricted to those authorized to assume that role. Changing roles would involve logging out and logging back in.	If you meet the requirement
Transactions	A certain amount of data capture is established, once the system detects that the filling of the data has been completed, the access ends and the user has no further opportunity to operate.	If you meet the requirement
Service limitations	The restrictions depend on the application's own usage parameter, or that are preset by the system administrator.	If you meet the requirement
Access modalities	They can be considered as certain privileges that one has over the information, they can be read, write, execute, delete, create and search	If you meet the requirement
Location and Time	Updates made to the system, access to certain system resources, may be based on the physical or logical location of the data or people and, in turn, may be Internal Access Controls: which determine what a user can or not to do with system resources.	If you meet the l and physical secu requirements
Access control list	Registration of users and processes, who have been granted certain privileges to use the system.	If you meet the requirement
Limits on user interfaces	Lists that restrict specific functionalities.	If you meet the requirement
Security labels	They are denominations that are given to the resources, once it has been made, they can no longer be changed.	If you meet the requirement
External Access Controls	Protection against the interaction of our system with systems, services and people outside the organization.	meets 50%
Port control devices	They authorize access to a specific port on the computer.	If you meet the requirement
Security gates	They allow filtering or blocking access between networks.	Does not meet th requirement
Host-based authentication	Provides access according to the identification of the computer where the access request originates.	Does not meet th requirement
Server side validation	It allows to validate the data sent by a form	If you meet the requirement

Figure 3: Functional requirements (own source)

The computer security controls mentioned in Fig. 2 were taken into account for the analysis of the requirements that were found in the organization, to carry out the implementation of the proposed security scheme.

Through Fig. 4 you can see the final security scheme, specifying the security of web applications, based on hardware security, logical security, physical security and network security, taking into account the aspects of security incorporated by it. Framework Laravel, taking into account IT security controls and those of ISO 27001.

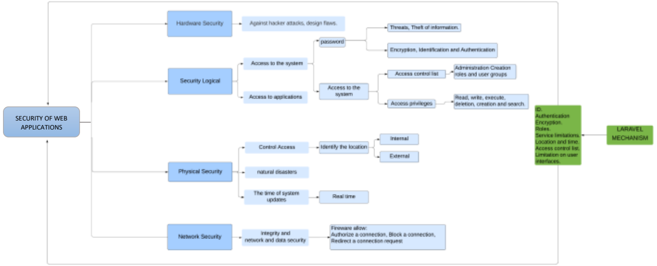

SECURITY OF WEB APPLICATIONS
Hardware Security
Against hacker attacks, design flaws.
Security Logical
Access to the system
password
Threats, Theft of information.
Encryption, Identification and Authentication
Access to the system
Access control list
Administration Creation roles and user groups
Access privileges
Read, write, execute, deletion, creation and search.
Access to applications
Physical Security
Control Access
Identify the location
Internal
External
natural disasters
The time of system updates
Real time
Network Security
Integrity and network and data security
Fireware allow: Authorize a connection, Block a connection, Redirect a connection request
ID. Authentication Encryption. Roles. Service limitations. Location and time. Access control list. Limitation on user interfaces.
LARAVEL MECHANISM

Figure 4: Security Scheme (Own source)

3.2 Additional tools

The tools described below complement the security criteria that are not covered by Laravel and that are required through ISO 27001.

3.2.1Pwned Passwords

It is a tool that is used to correct system vulnerabilities. It helps that the passwords created in the system are not vulnerable to any situation or that they are used in other places outside the system. It is recommended to change passwords periodically to avoid information leaks in the system [5].

3.2.2Tool Have I been Pwned

Have I been pwned, it allows to check if the email address has been filtered in one of these attacks. It is very useful if you want to check the security of different passwords for each website and they are no longer vulnerable for any type of user or person who wants to do any type of action or fraud on the system [6].

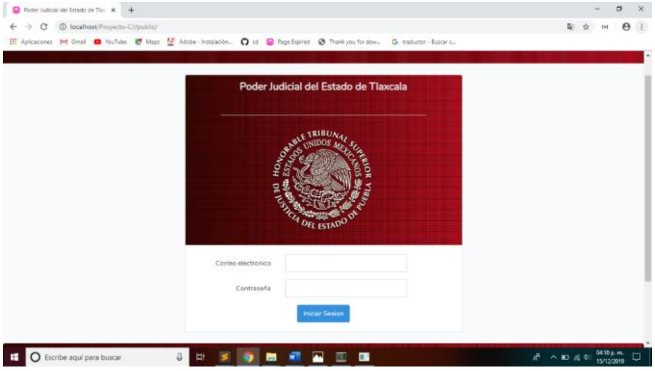
4. Tests

The application case for verification of the Integrity Scheme proposed was an information system related to statistical variables in the area of justice delivery.

In Fig. 5 you can see the login that complies with the validation of the user authentication, to provide confidentiality of the information that is managed within the system and to be able to enter the various sections that it comprises, guaranteeing security, privacy and integrity of user data.

In the image shown above, the implementation of the Laravel Framework in terms of security is presented, applying it in the authentication to new users.

They can access the system in a browser since the authentication drivers already contain the logic (through its features) to authenticate existing users and store new users in the database, when the user successfully authenticates, he will be redirected at system startup.


Poder Judicial del Estado de Tlaxcala

Correo electronico

Contraseña

Iniciar Sesion

Figure 5: Login validation
(Own source)

5. Conclusion

Implementing security in web applications taking ISO 270001 as a reference is a good strategy to define a security scheme.

The construction of the proposed security scheme and its implementation in the referred application case allowed putting into practice the principles established by the ISO 27001 standard, taking into account the security elements provided by the Marco Laravel.

Together, these two tools allowed defining and generating measures that give certainty to an organization for the management and use of its information, improving the administration and use of the systems, monitoring computer security controls, improve user access control and security measures, to avoid vulnerabilities within the work environment and identify threats that may threaten information.

References

[1] Dayle Rees & Antonio Laguna. (2013-02-06). Desarrollo deaplicaciones con el Framework de PHP Laravel para principiantes. Leanpub: Code Happy.

[2] Francisco Nicolás Javier Solarte, Edgar Rodrigo Enríquez Rosero, Mirian del Carmen Benavides Ruano. (Diciembre 2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica ESPO, Vol. 28, N. 5, 492-507, 16.

[3] Antonio Jose Segovia. (2013). ¿Que es la norma ISO 27001?. 21/03/2020, de 27001 Academy Sitio web: https://advisera.com/27001academy/es/que-es-iso-27001/

[4] Purificacion Aguilar López. (2010). Seguridad Informatica. Ciclos Formativos: EDITEX.

[5] Troy Hunt. (1/Marzo/2015). Pwned Passwords. 20/02/2020, de CLOUDFLARE Sitio web: https://haveibeenpwned.com/Passwords

[6] Troy Hunt. (15/Marzo/2015). have I been pwned?. 20/02/2020, de CLOUDFLARE Sitio web: https://haveibeenpwned.com/

Author Profile

Joselin Juarez George is currently studying for a master's degree in Computer Systems at the Instituto Tecnológico de Apizaco, graduated from Engineering in Information and Communication Technologies in 2018 at the same institution, having a specialty in the area of computing in 2011. She is currently studying a master's degree in Computer Systems in Software Engineering from the TecNM / Instituto Tecnológico de Apizaco.

Juan Ramos Ramos has a degree in Computer Science from the Instituto Tecnológico de Apizaco, from 1993. He is also a Master in Computer Science and Telecommunications from the Instituto de Estudios Universitarios, A.C.; he works as a full-time professor at the TecNM / Instituto Tecnológico de Apizaco in the area of Systems and Computing, teaching at the undergraduate and postgraduate level, in the areas of Programming and Software Engineering.

José Juan Hernández Mora has a Doctor of Teaching Excellence degree from the University of Los Angeles, 2019. He also has a degree in Computer engineer from the Universidad Autónoma de Tlaxcala, from 1994. Master in Computer science at the National Center for Research and Technological Development of the TecNM, 2003. Research professor at the Tecnológico de Apizaco del TecNM. Teacher of the Master of computer systems of the TecNM / Instituto Tecnológico de Apizaco.

Klissman Esquivel Montiel currently a student of the master's degree in computer systems at the Technological Institute of Apizaco, graduated as an engineer in information and communication technologies at the same institution and a computer technician specialized in the area of database and distributed systems. He is currently studying a master's degree in Computer Systems in Software Engineering from the TecNM / Instituto Tecnológico de Apizaco.