

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

GRADE WORK PRIOR TO OBTAINING THE TITLE OF ENGINEERING IN COMPUTER SYSTEMS

SCIENTIFIC ARTICLE

THEME:

"Elaboración del Plan de Gestión de Seguridad de Información en base a la metodología MAGERIT para el Gobierno Autónomo Descentralizado Municipal de Antonio Ante (GADMAA)"

AUTHOR:

Erika Alexandra Varela Recalde

TUTOR:

Ing. Pablo Andrés Landeta López

Ibarra - Ecuador

2015

.

ELABORACIÓN DEL PLAN DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN BASE A LA METODOLOGÍA MAGERIT PARA EL GOBIERNO DESCENTRALIZADO MUNICIPAL DE ANTONIO ANTE (GADMAA)

Erika Alexandra VARELA RECALDE
Carrera de Ingeniería en Sistemas Computacionales, Universidad Técnica del Norte, Av.17 de Julio 5-21 y Gral. José María Córdova, Ibarra, Imbabura, Ecuador

e-mail: evarela02@gmail.com

RESUMEN: *La información es un recurso fundamental para el desarrollo del GADMAA, de manera que uno de los objetivos prioritarios de dicha Gobernación será el aseguramiento de dicho activo.*
Al Departamento de Sistemas y Tecnologías del GADMAA se le es complicado llevar un control sobre el aseguramiento de la información, ya que no cuentan con una metodología que les permita proteger de manera adecuada la información.
El proyecto consta de tres partes para el aseguramiento de la información: elaboración del plan de seguridad de información en base a la metodología MAGERIT, levantamiento de procedimientos e implementación de Seguridad Perimetral con la ayuda de un firewall.

PALABRAS CLAVE: Plan de seguridad de información, Metodología MAGERIT, Seguridad Perimetral, firewall.

ABSTRACT: *Information is a vital resource development GADMAA so that one of the priority objectives of the Government is the assurance that asset.*
The Department of Systems and Technologies GADMAA will be is difficult to keep tabs on the information assurance because they do not have a methodology that enables them to adequately protect the information.
The project consists of three parts for information assurance: development of information security plan based on the methodology MAGERIT lifting procedures and implementation of perimeter security with the help of a firewall.

KEY WORDS: Information Security Plan, Methodology MAGERIT, Perimeter Security, firewall.

1. INTRODUCTION

Decentralized Autonomous Municipal Government of Antonio Ante, is a public entity that is responsible for promoting the integral development of the community antenna, providing efficient services and quality, framed in participation, equity and transparency. The Department of Systems and Technologies, provides technical support in the area of information to different administrative units, in addition to updating all computer systems used in the Municipality to maintain technological force.

Information is a vital resource development GADMAA so that one of the priority objectives of the Government is the assurance that asset.

Currently the Department of Systems and Technologies GADMAA will be is difficult to keep tabs on the information assurance because they do not have a methodology that enables them to adequately protect the information.

This degree project will help identify vulnerabilities and risks they are exposed daily information handled by the municipality of Antonio Ante, thus helping to prevent future threats that may arise in the development of their activities.

.

2. MATERIALS Y MÉTHODS

1.1 Software and Hardware used

1.1.1 Software

To implement the firewall perimeter security tool the following applies:

In implementing the firewall free software tool Shoreline (Shorewall) is used,

Operating system for Centos 6.5 server.

1.1.2 Hardware

- Implementation of the firewall:
- 1 Centos server
- 1 Swtch
- 1 router
- 2 network cards

1.2 MAGERIT Methodology

To develop a Risk Management Plan Information Security is necessary to apply a methodology Information Security; in this case the Methodology Analysis and Risk Management Information Systems (MAGERIT) applies. This methodology consists of four stages: Assets, Threats, Impact-risk and Safeguards.

Activos.- component or functionality of a system of information capable of being deliberately or accidentally attacked with consequences for the organization. It includes information, data, services, applications (software), equipment (hardware), communications, administrative resources, physical resources and human resources.

Amenazas.- potential of an incident which may cause damage to an information system or an organization Causa.

Impact-risk environments.- is called impact to the extent of the damage on the active derivative of a threat; and the risk is the measure of the likely damage to a system. Knowing the impact of threats on assets derived directly without further risk to take into account the probability of occurrence.

Salvaguardas.- Son medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

3. RESULTS

Significantly, the results were favorably satisfactory, achieving generate a receipt of the information through the firewall.

As mentioned above the project consists of three parts:

Development of information security plan based on MAGERIT methodology and implementation procedures Uprising Perimeter Security with the help of a firewall.

- Security Plan based on information MAGERIT: It aims to help the Department of Systems and Technology to identify potential threats.

  Identify outstanding assets held by the GADM-AA.

Activo: ***Nombre del Activo Principal***
(*Detalle de los activos*)

Tabla 1: Identification of active

- Detail the threats to which they are exposed assets through a list that presents the methodology used by tables that highlight the level of degradation and the probability of occurrence of the threats found.

Valor	Descripción
MA	Muy alta
A	Alta
M	Media
B	Baja
MB	Muy baja

Table 2: Niveles de degradación

.

Valor	Descripción
MF	Muy Frecuente
F	Frecuente
N	Normal
PF	Poco frecuente
MPF	Muy poco frecuente

Table 3: Niveles de Probabilidad de Ocurrencia

- Estimated impact and probability of risks occurring threats found.

Probabilidad de Ocurrencia Amenazas	Degradación: Probabilidad de ocurrencia	MB	B	M	A/MA
		Impacto			
		Insignificante	Bajo	Medio	Alto
PF/MPF	Improbable	Bajo	Bajo	Bajo	Medio
N	Posible	Bajo	Medio	Medio	Alto
F	Probable	Bajo	Medio	Alto	Alto
MF	Muy Probable	Medio	Medio	Alto	Alto

Table 4: Values Impact Matrix

Probabilidad de ocurrencia		Impacto			
		Muy Bajo	Bajo	Medio	Alto / Muy Alto
		1	2	3	4
Improbable	1	1	2	3	4
Posible	2	2	4	6	8
Probable	3	3	6	9	12
Muy Probable	4	4	8	12	16

Table 5: Numerical equivalence of the impact matrix

Riesgo	Desde	Hasta
Alto	9	16
Medio	4	8
Bajo	1	3

Table 6: Hazard Scale

Probabilidad	Descripción	Frecuencia Trimestral
Muy Probable	Se espera que ocurra en la mayoría de las circunstancias	1
Probable	Podría ocurrir muchas veces.	0,75
Posible	Podría ocurrir algunas veces	0,5
Incierto	No es muy probable que ocurra	0,3
Improbable	Sólo podría ocurrir en casos excepcionales	0,1

Table 7: Probability values Matrix

- For safeguards should take into account the scale of risks Table 6 by the results, it should establish corrective or preventive measures to help reduce the risks found.
  You can not have total security on assets, but can be prevented, carrying a constant risk analysis, in order to see what situation the Department of Systems and Technologies regarding Information Security is.

➢ Performed risk analysis in the previous chapter, is continued lifting procedures of information security, in order to help employees and staff of the Department of Systems and Technologies GADM-AA to prevent risks that may arise during the development of industrial activities, while preserving the availability, integrity and confidentiality of the data.

- Advice to users on problems in information systems.
- Preventive maintenance of computer equipment.
- corrective maintenance of computer equipment.
- Data Backup by the Administrator.
- Data Backup by the user.

➢ To implement perimeter security, after Once the risk analysis information security is determined to implement a free software tool that allows set LRAs rules to allow authorized from the internal network to the outside access (internet) and in turn deny all communications that attempt to perform from the outside (Internet) to the local network whereas within the local network servers exist and information that must be protected.

.

- Shorewall (Shoreline Firewall), high-level tool that aims handling packet filtering Linux kernel, presents a series of configuration files to determine a set of rules necessary with the help of iptables, iptables-restore, ip and other services configured by Netfilter.

- Fully configurable using configuration files.
- Unlimited network interfaces.
- You can divide the networks into zones, allowing extensive control over the connections established between them.
- Multiple interfaces zones.

To get a better idea of implementing the firewall (Perimeter Security)), below a picture of the network diagram. (Figure 1).

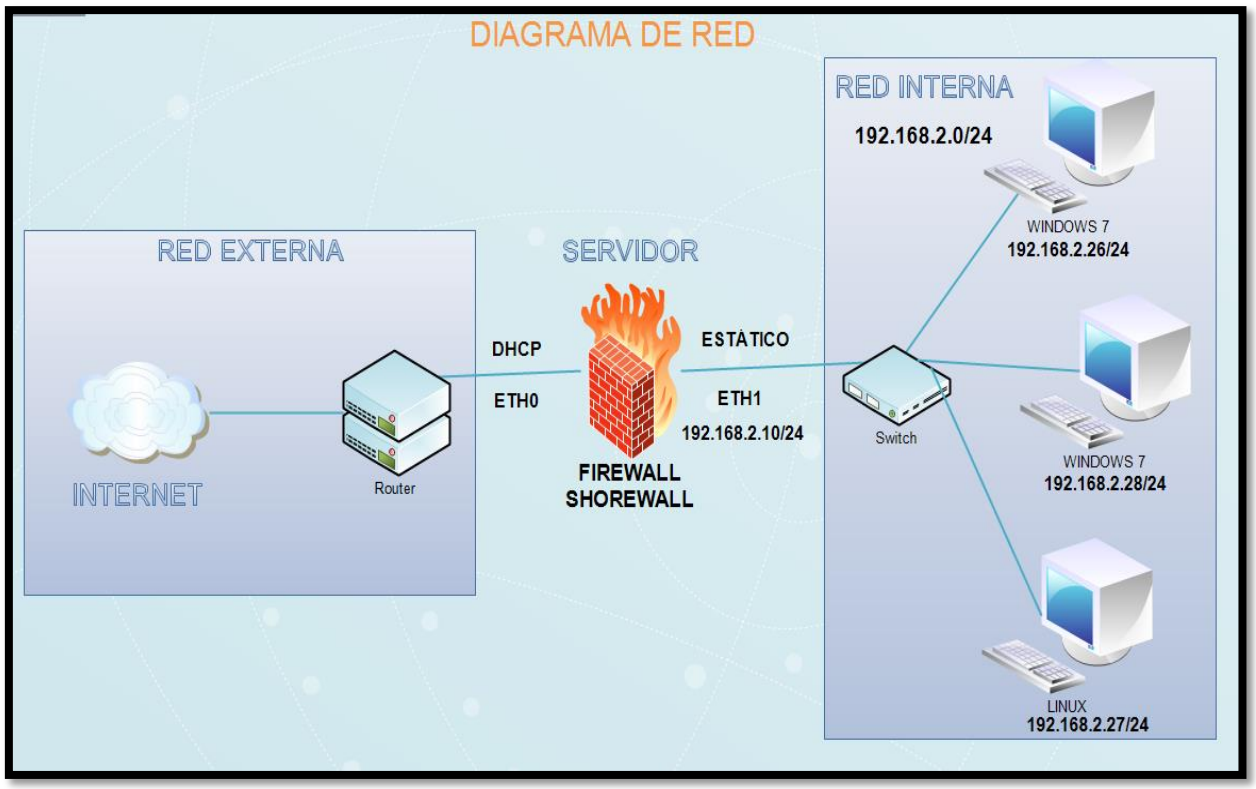


Figure 1: Network diagram

4. CONCLUSIONS

Completed this work, you can define the following conclusions:

- THE GADM-AA has an information security plan, so there is a high probability q that threats materialize.
- The Department of Systems and Technologies, is aware of the risk they have their information systems, so the municipality from this work, carried out the implementation of certain safeguards that will protect your information.
- Supported by the Department of Systems and Technologies it was essential for the preparation of the Draft Grade, as I provided the information that allowed me to assess and manage technology assets.
- Shorewall is a robust tool that facilitates access control / restriction of traffic on the network.
- Currently in our environment is not put into focus the issue of Analysis and Risk Management Information Systems, which causes an adequate knowledge of these issues can not be and will not count with specialized personnel to perform the analysis.
- Firewalls alone are not the solution to the implementation of network security. Safety is not a static concept, a network is not secure once and you will be forever, it requires constant vigilance, and for this we require tools that provide us with this task. We can say that at the moment the monitoring network is not up to what it should be, missing tools and policies.

AGRADECIMIENTOS

The Department of Systems and Technology of the Autonomous Decentralized Municipal Government of Antonio Ante, by bull support during project development grade.

The Technical University of North for giving me the opportunity to study and be a professional.

Teachers, who marked his teachings and knowledge, please prepare for a competitive future as the best professionals.

A special thanks to my supervisor, Engineer Pablo Landeta, for the trust placed in me, for their advice and ideas for the thesis will be held.

To my family, source of constant support, without their support would have been impossible to complete this work degree.

REFERENCES

.

[1] Eastep, T. M. Shorewall. (s. f.). Recuperado 17 de abril de 2015, a partir de http://shorewall.net/

[2] Escrivá Gascó, G., Romero Serrano, R. M., & Ramada, D. J. (2013). Seguridad informática. España: Macmillan Iberia, S.A.

[3] ISO27000. (2012). ISO 27000. (s. f.). Recuperado 12 de mayo de 2015, a partir de http://www.iso27000.es/

[4] Ministerio de Hacienda y Administraciones Públicas, E. (2012a). Magerit-v3 Libro I Método. (s. f.). Recuperado 20 de mayo de 2015, a partir de http://administracionelectronica.gob.es/

[5] Ministerio de Hacienda y Administraciones Públicas, E. (2012b). Magerit-v3 Libro II Catálogo de Elementos. (s. f.). Recuperado 02 de junio de 2015, a partir de http://administracionelectronica.gob.es/

[6] Escrivá Gascó, Gema; Romero Serrano, Rosa M. (2013). Seguridad Informática. London Macmillan.

[7] Díaz, Gabriel,; Alzórriz, Ignacio,; SANCRISTOBAL, Elio (2014). Procesos y herramientas para la seguridad de redes. UNED – Universidad Nacional de Educación a Distancia.

[8] Jiménez, José A. (2009). Evaluación: Seguridad de un Sistema de Información. Argentina.

[9] Martínez, Jeimy J. (2013) Inseguridad de la información: Una Visión Estratégica. México.

[10] Whitman, Michael E.; Marttord, Herbert J. (2012). Principles of Information security. Cengage Learning.

[11] Costas Santos, Jesús. (2011). Seguridad Informática. Ediciones de la U.

[12] Gómez Vieites, Alvaro. (2011). Enciclopedia de la Seguridad Informática. Alfaomega

[13] Dulaney, Emmett. (2011). Seguridad Informática: CompTIA Securiri+. ANAYA Multimedia.

[14] García Moran, Jean P; Fernández Hansen, Yago; Martínez Sánchez, Rubén. (2011). Hacking y Seguridad en Internet. Madrid Ra-Ma

[15] PAE (Portal de Administración Electrónica, Esp.).(2012). Libros de MAGERIT v3-idioma-español. (s. f.). Recuperado 12 de mayo de 2015, a partir de http://administracionelectronica.gob.es/pae_Home

[16] Gaona Vásquez, K. d. R. (2013). Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito SA en la ciudad de Machala.

[17] González, J. A., & Vanegas, C. A. (2013). LA SEGURIDAD EN LAS REDES DE COMUNICACIONES. Vínculos, 3(1), 70-91.

[18] Greiner, L. (2014). Delitos Informáticos.

.

[19] Ministerio de Hacienda y Administraciones Públicas, E. (2012c). Magerit-v3 Libro III Guía de Técnicas.
[20] Molina, U., & Andrés, J. (2014). Desarrollo de un plan de gestión de seguridad de la información para el centro de educación continua de la escuela politécnica nacional. Quito: EPN, 2015.

Sobre la Autora.



Erika Alexandra RECALDE VARELA.- I was born on May 2, 1991 in the city of Atuntaqui. My parents: Edmundo Varela and Guadalupe Recalde.
My primary instruction realized at: Santat "Luisa de Marillac" in Atuntaqui city, then I studied in the "Alberto Enriquez" Institute of the same one, where I obtained a bachelor's degree in Business and Management Science, specialization: Computing.
I began to study at the Técnica del Norte University in able to obtained the Computer Systems Engineering degree.