UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS COMPUTACIONALES

ARTÍCULO CIENTÍFICO

TEMA:

"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)"

AUTORA:

Erika Alexandra Varela Recalde

DIRECTOR:

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. INTRODUCCIÓN

El Gobierno Autónomo Descentralizado Municipal de Antonio Ante, es una entidad pública que se encarga de promover el desarrollo integral de la comunidad Anteña, brindando servicios eficientes y de calidad, enmarcados en la participación, la equidad y la trasparencia. El Departamento de Sistemas y Tecnologías, brinda soporte técnico en el área de informática a las diferentes Unidades Administrativas, además de actualizar todos los sistemas informáticos que se utilizan en la Municipalidad a fin de mantener vigencia tecnológica.

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.

Actualmente 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 presente proyecto de grado ayudará a identificar las vulnerabilidades y riesgos a los que está expuesta la información que maneja diariamente la municipalidad de Antonio Ante, ayudando de esta manera a prevenir futuras amenazas que pueden presentarse en el desarrollo de sus actividades.

.

2. MATERIALES Y MÉTODOS

1.1 Software y Hardware empleado

1.1.1 Software

Para implementar el firewall de seguridad perimetral se aplicó la siguiente herramienta:

En la implementación del cortafuego se usa la herramienta de software libre Shoreline (Shorewall),
Sistema operativo para el servidor Centos 6.5

1.1.2 Hardware

- Implementación del firewall:
  - 1 servidor Centos
  - 1 Swtch
  - 1 router
  - 2 tarjetas de red

1.2 Metodología MAGERIT

Para elaborar un Plan de Gestión de Riesgos de Seguridad de Información es necesario aplicar una metodología se Seguridad de la Información; en este caso se aplica la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT). Esta metodología consta de cuatro etapas: Activos, Amenazas, Impacto-riesgo y Salvaguardas.

Activos.- Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Amenazas.- Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

Impacto-Riesgo.- Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza; y el riesgo es la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

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

3. RESULTADOS

Cabe resaltar que los resultados fueron favorablemente satisfactorios, logrando generar un resguardo de la información a través del firewall.

Como se mencionó anteriormente el proyecto consta de tres partes:
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.

- Plan de Seguridad de la información en base a MAGERIT: Tiene como objetivo, ayudar al Departamento de Sistemas y Tecnologías a identificar las posibles amenazas.
  - Identificar los activos sobresalientes que posee el GADM-AA.

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

Tabla 1: Identificación de Activos

  - Detallar las amenazas a los que están expuestos los activos, a través de una lista que presenta la metodología utilizada, mediante tablas que valorizan el nivel de degradación y la probabilidad de ocurrencia de las amenazas encontradas.

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

Tabla 2: Niveles de degradación

.

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

Tabla 3: Niveles de Probabilidad de Ocurrencia

- Estimación del impacto y probabilidad de riesgos que producen las amenazas encontradas.

Probabilidad de Ocurrencia Amenazas	Degradación / Probabilidad de ocurrencia	MB / Insignificante	B / Bajo	M / Medio	A/MA / Alto
		Impacto			
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

Tabla 4: Valores Matriz de Impacto

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

Tabla 5: Equivalencia numérica de la matriz de impacto

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

Tabla 6: Escala de riesgos

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

Tabla 7: Valores Matriz de Probabilidad

- Para las salvaguardas se debe tomar en cuenta la escala de riesgos Tabla 6, mediante los resultados, se debe establecer las medidas correctivas o preventivas que ayuden a disminuir los riegos encontrados.
  No se puede tener la seguridad total sobre los activos, pero se puede ir prevenir, llevando un análisis de riesgos constante, con la finalidad de ver en qué situación se encuentra el Departamento de Sistemas y Tecnologías en cuanto a Seguridad de Información.

➢ Realizado el análisis de riesgos en el capítulo anterior, se prosigue con el levantamiento de procedimientos de seguridad de la información, con la finalidad de ayudar a los empleados y personal del Departamento de Sistemas y Tecnologías del GADM-AA a prevenir riesgos que pueden presentarse durante el desarrollo de las actividades laborales, conservando siempre la disponibilidad, integridad y confidencialidad de los datos.

- Asesoría a usuarios sobre problemas en los sistemas de información.
- Mantenimiento preventivo de equipos informáticos.
- Mantenimiento correctivo de equipos informáticos.
- Respaldo de Datos por parte del Administrador.
- Respaldo de Datos por parte del Usuario.

➢ Para la implementación de Seguridad Perimetral, después de haber Una vez realizado el análisis de riesgos de seguridad de la información se ha determinado

.

implementar una herramienta de software libre que permita configura lras reglas para permitir los accesos autorizados desde la red interna hacia el exterior (internet) y a su vez denegar todas las comunicaciones que se intenten realizar desde el exterior (internet) hacia la red local considerando que dentro de la red local existirán servidores e información que debe ser protegida.

- Shorewall (Shoreline Firewall), herramienta de alto nivel que tiene como objetivo la manipulación de filtrado de paquetes del núcleo de Linux, presenta una serie de archivos de configuración para determinar un conjunto de reglas necesarias con la ayuda de iptables , iptables-restore , ip y demás servicios configurados por Netfilter .

  - Completamente configurable mediante el uso de archivos de configuración.
  - Interfaces de red ilimitadas.
  - Permite dividir las redes en zonas, permitiendo extenso control sobre las conexiones establecidas entre ellas.
  - Múltiples interfaces por zonas.

Para tener una mejor idea de la implementación del firewall (Seguridad Perimetral)), se muestra a continuación una imagen del diagrama de red. (Ilustración 1).

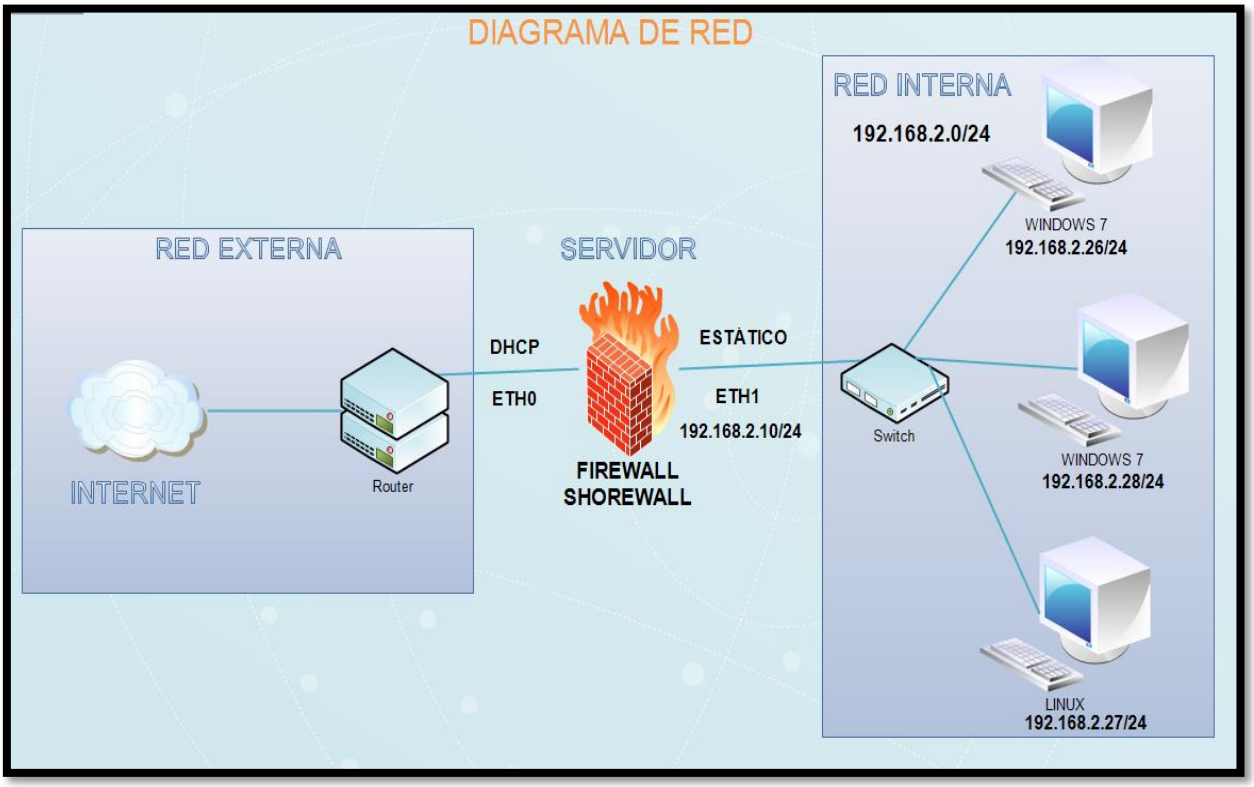

Ilustración 1: Diagrama de red

4. CONCLUSIONES

Culminado este trabajo, se pueden definir las siguientes conclusiones:

- EL GADM-AA cuenta con un plan de seguridad de información, por lo q existe una alta probabilidad de que las amenazas se materialicen.
- EL Departamento de Sistemas y Tecnologías, está consciente del riesgo que poseen sus sistemas de información, por lo que la municipalidad a partir de este trabajo, realizó la implementación de ciertas salvaguardas que permitirá proteger su información.
- El apoyo del Departamento de Sistemas y Tecnologías fue indispensable para la elaboración del Proyecto de Grado, ya que me facilitaron la información que me permitió evaluar y gestionar los activos tecnológicos.
- Shorewall es una herramienta robusta que facilita controlar el acceso/restricción de tráfico en la red.
- Actualmente en nuestro medio no se pone en énfasis el tema de Análisis y Gestión de Riesgos de los Sistemas de Información, lo que ocasiona que no se tenga un conocimiento adecuado de dichos temas y no se cuente con el personal especializado para realizar el análisis.
- Los firewalls por sí mismos no son la solución a la implementación de seguridad en una red. La seguridad no es un concepto estático, una red no es segura una vez y ya lo será para siempre, se requiere de una vigilancia continua, y para ello requerimos de herramientas que nos faciliten ésta tarea. Podemos afirmar que en estos momentos el monitoreo de la red no está al nivel de cómo debería estar, faltan herramientas y políticas.

AGRADECIMIENTOS

Al Departamento de Sistemas y Tecnologías del Gobierno Autónomo Descentralizado Municipal de Antonio Ante, por toro el apoyo brindado durante el desarrollo del proyecto de grado.

A la Universidad Técnica del Norte por darme la oportunidad de estudiar y ser una profesional.

A los Docentes, que marcaron sus enseñanzas y conocimientos, gracias por prepararnos para un futuro competitivo como los mejores profesionales.

Un agradecimiento especial a mi director de tesis, el Ingeniero Pablo Landeta, por la confianza depositada en mi persona, por sus consejos e ideas para que la tesis se llevara a cabo.

A mi familia, fuente de apoyo constante, sin su apoyo habría sido imposible culminar este trabajo de grado.

REFERENCIAS

.

[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 VARELA RECALDE.- Nací el 02 de mayo de 1991 en la ciudad de Atuntaqui. Mis padres: Edmundo Varela y Guadalupe Recalde.
Mi instrucción primaria la realicé en la escuela: Santa “Luisa de Marillac” del cantón Antonio Ante, posteriormente ingresé al Instituto Tecnológico Superior “Alberto Enríquez”, donde obtuve el título de bachiller en Ciencias de Comercio y Administración, especialización: Informática.
Ingresé a la Universidad Técnica del Norte con el objetivo de obtener el título de Ingeniería en Sistemas Computacionales.