Modelo para la Auditoría de la Seguridad Informática en la Red de Datos de la Universidad de Los Andes, Venezuela

Reinaldo Mayol[¶], Jacinto Dávila[º£]

Resumen

En este artículo presentamos un modelo lógico para gestionar la auditoria de seguridad informática de una Institución Universitaria. Auditar, de manera correcta, los mecanismos de seguridad utilizados en el ofrecimiento de los servicios de Tecnologías de Información (IT) es uno de los elementos fundamentales para el éxito de esta labor. El término Auditar Correctamente incluye varios elementos importantes, uno de ellos es contar con un modelo de auditoría completo, equilibrado y técnicamente correcto. Este documento propone un modelo de auditoría de la seguridad informática para aquellos servicios de IT que se ofrecen por RedULA para la Universidad de Los Andes, Venezuela y extensible a cualquier entidad de características similares.

This paper introduces a logical model to guide the processes of auditing the information services of an academic institution. Auditing is a crucial element to maintain the level of quality and confidence on the information services provided by any institution. We aimed to produce a well organized, modular set of rule to perform auditing and we actually tested this model, as we call it, for the data services of Universidad de Los Andes, in Venezuela.

¶ Reinaldo Mayol Arnao <mayol@ula.ve>, Centro de Tecnologías de Información, ULA
º £ Jacinto Dávila Alfonso <jacinto@ula.ve>, Centro de Simulación y Modelos, ULA

Introducción

En este artículo presentamos un modelo lógico para gestionar la auditoria de seguridad informática de una Institución Universitaria. La red de datos de la Universidad de Los Andes, RedULA, en Venezuela, ha venido creciendo de manera significativa en la última década. Junto con el crecimiento físico de la red, lo han hecho también los servicios que se ofrecen utilizándola como plataforma de transporte. Con una red tan extendida, tecnológicamente diversa y con una variedad significativa de actores, servicios y usuarios, es fácil que comiencen a ocurrir errores y desviaciones que pueden comprometer la propia subsistencia de la red como un entorno efectivo de trabajo. Esta realidad impone la necesidad de realizar procesos de auditoría del funcionamiento de la red que permitan detectar problemas graves , establecer patrones de comportamiento, realizar planificación de crecimiento e incluso detectar problemas incipientes que pudiesen poner en riesgo la operación futura de la red.

El uso de modelos durante el proceso de auditoría es importante, no sólo para garantizar la consecución de resultados correctos y completos, sino también para garantizar que un equipo de profesionales obtenga un resultado homogéneo, reduciendo la importancia de los niveles de pericia, instrucción, audacia, conocimiento de la organización auditada, relación con los auditados, experiencia y otros del auditor.

Descripción del Modelo Propuesto.

El modelo es una descripción general de cómo se debe proceder para realizar una auditoría de seguridad yestá constituido por grupos de reglas y pruebas agrupadas en módulos, para guiar la conducta del personal encargado de la auditoría.

Estructura detallada del modelo

La estructura del modelo propuesto ha sido establecida siguiendo la forma común de realizar un proceso de auditoría, específicamente uno de Seguridad Informática. Existen 4 módulos:

A) Definición de las condiciones para la auditoría.
B) Definición de las características técnicas
C) Pruebas de penetración
D) Revisiones de las configuraciones.

Ilustración 1: Módulos de Modelo

Como usar el modelo

Cada módulo funciona como un sistema autocontenido, permitiendo una visión general en cierto aspecto de la seguridad informática del sitio auditado. Los módulos están compuestos por secciones. Las secciones a su vez se conforman por reglas. Una regla involucra, además, un conjunto de pruebas.

El orden en que se ejecuten las secciones dentro de un módulo normalmente no es significativo. Cuando lo es, explícitamentese señalan los elementos prelatorios. El orden en que se ejecutan las pruebas y las reglas dentro de una sección suele ser significativo. Dentro de un módulo el auditor tiene libertad de ejecutar o no una sección de acuerdo a varios factores, entre ellos el objetivo de la auditoría o las características técnicas de la plataforma que se audita. La ilustración 2 muestra la estructura descrita en este párrafo.

El auditor puede utilizar el modelo desde el módulo inicial hasta completar el módulo final. Cada módulo puede tener una relación con los módulos adyacentes. Cada sección puede tener aspectos interrelacionados a otros módulos y algunas se interrelacionan con todas las otras secciones. Durante la ejecución de cada regla, o incluido de una prueba, se van produciendo las recomendaciones que conformarán el informe final de auditoría.

El auditor no debe esperar que el modelo sustituya totalmente su experiencia, su intuición y el análisis de las condiciones especiales de cada sitio auditado. Por el contrario, el modelo se basa en ellos y sólo establece un patrón a seguir para obtener resultados acordes a las necesidades de una organización como la Universidad de Los Andes.

Cada módulo debe tener valores de salida y puede tener algunos de entrada. La entrada es la información usada en el desarrollo de cada tarea. La salida es el resultado de las secciones completadas. La salida puede o no ser datos analizados para servir como entrada para otro módulo, recomendaciones que conformarán el informe final o simplemente datos que soporten las recomendaciones . Puede ocurrir que la salida de un módulo sirva como entrada para más de un módulo o sección. Ej. La definición del espectro de direcciones IP a auditar sirven de entrada para varias otras secciones correspondientes a otros módulos.

Como regla general todo módulo debe tener valores de salida[HMATS]. Un módulo sin salidas puede significar una de tres cosas:

- Las pruebas no fueron ejecutadas apropiadamente.
- Las pruebas no se aplicaban.
- Los datos resultantes de las pruebas se analizaron inapropiadamente.

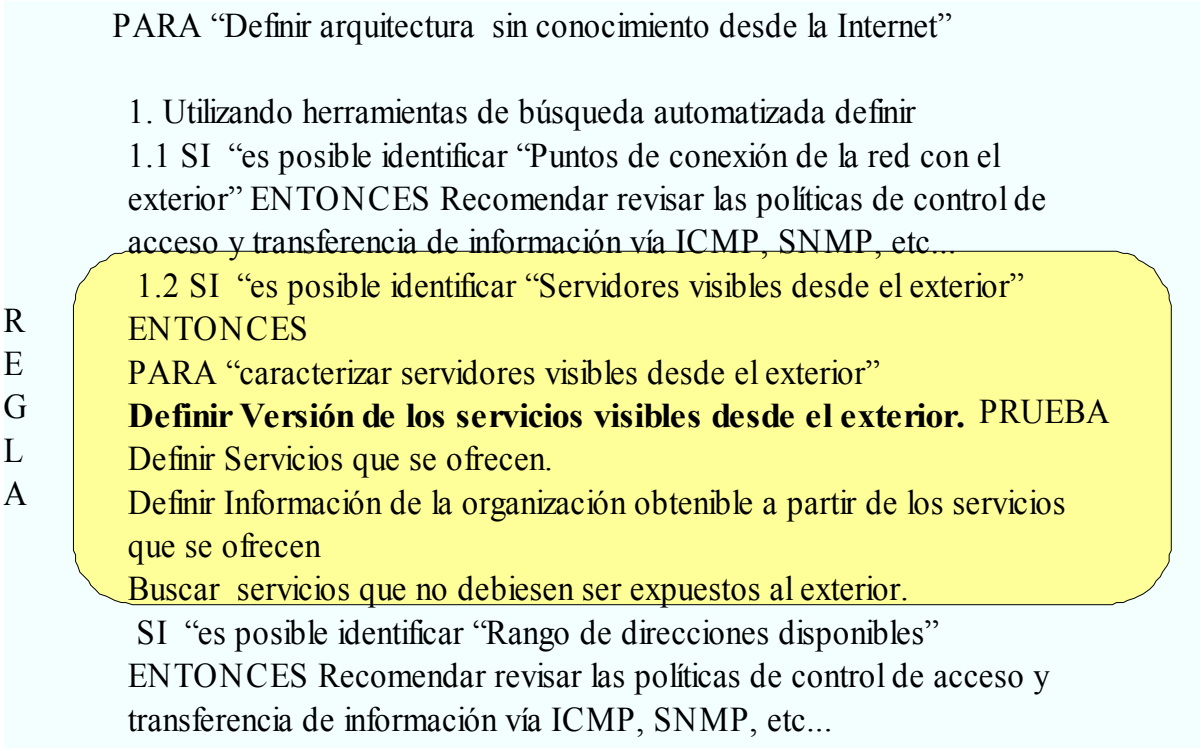

Ilustración 2: Una sección del modelo conformada por varias reglas y pruebas

En total existen aproximadamente 350 pruebas agrupadas en los 4 módulos antes señalados.

Del lenguaje en que se ha escrito el modelo

A sabiendas de que la base conceptual es amplia, la cantidad de reglas es extensa y muchas veces requiere conocimientos específicos de herramientas, técnicas e incluso cierto nivel de experiencia y habilidades, hemos tratado de mantener el lenguaje con la mayor sencillez posible.

El modelo está formado no por una serie de acciones que se deben seguir como una receta, sino por un conjunto de funciones individuales, casi siempre correspondientes a una sección o incluso a una regla que pueden ser utilizados libremente por el auditor, siempre y cuando cumpla los requerimientos de entrada de datos de la función.

La sintaxis utilizada es la siguiente:

***PARA* "Objetivo" "acciones"**

***SI* "Condición" *ENTONCES* "Acciones o Conclusiones" [*DE LO CONTRARIO* "Acciones o Conclusiones"]**

Se han subrayado las palabras reservadas por el lenguaje para que no sean confundidas con parte del texto descriptivo. Las acciones pueden ser reglas o llamadas a otras secciones o simplemente una prueba.

Por objetivo se entiende la meta que se busca alcanzar al realizar una determinada acción. Una condición es uno o varios elementos que deben ser evaluados previamente y que definen el ambiente de ejecución de las acciones que siguen. Una condición puede definir la pertinencia de la ejecución de una acción ulterior. Las conclusiones se refieren a las recomendaciones que el resultado de la ejecución de una acción indican y que deben ser parte del informe final. Los elementos encerrados entre corchetes son opcionales.

Una acción pueden ser grupos de subtareas o acciones individuales. Las subtareas pueden encontrarse inmediatamente en la sección o ser llamadas a otras funciones incluso fuera del módulo que se ejecuta.

Veamos nuevamente el ejemplo utilizado anteriormente identificando cada una las partes de la sintaxis descrita.

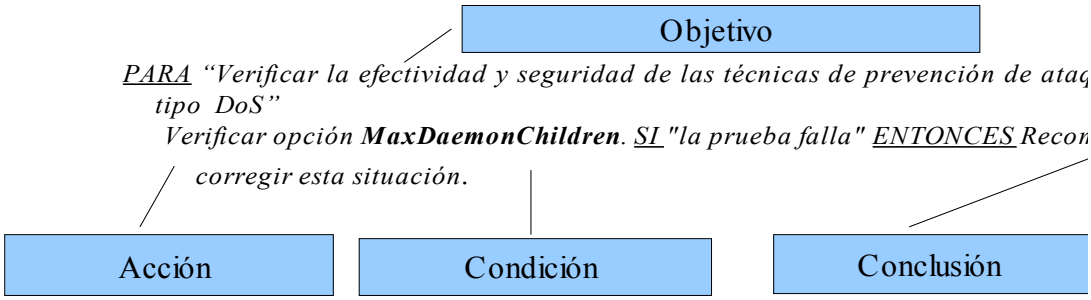

Ilustración 3: Ejemplo de la sintaxis

Como puede observarse, los criterios que se dan para definir la falla o no de una prueba son referenciales. No puede ser de otra forma. Las valores que sirven para una condición pueden ser insuficientes para otra. Por esa razón nos hemos limitado, en la mayoría de los casos, a dar los criterios para que sea el auditor quien defina, de acuerdo a múltiples factores que dependen de las condiciones en que ejecuta la auditoría.

Descripción de los módulos que conforman el modelo

En esta sección definiremos más en detalle los objetivos de cada módulo, el porqué de su selección, así como de las secciones que lo componen.

- ***Módulo: Definición de las condiciones***

El objetivo principal de este módulo es definir los detalles del proceso de auditoría a realizar. Este módulo debe siempre realizarse antes del inicio del proceso de auditoría. Cualquier proceso de auditoría debe comenzar definiendo los detalles que constituyen la salida de este módulo. Al ejecutarlo los responsables de auditoría deben ser capaces de definir:

- Objetivos Generales.
- Alcance.
- Necesidades de información para el inicio de la auditoría.
- Conformación del equipo auditor.
- Requerimientos técnicos del equipo auditor.

- Conformación de la contraparte.
- Cronograma de entregas.
- Requisitos de confidencialidad y retorno de información.
- Condiciones de garantía de los resultados.

Esta etapa del proceso de auditoría es posiblemente más gerencial que técnica, y es una de las más importantes. Una auditoría de calidad debe enfocarse en criterios claramente definidos y documentados.

Para asegurar la objetividad del proceso de auditoría, sus resultados y cualquier conclusión, los miembros del equipo auditor deben ser independientes de las actividades que auditan, deben ser objetivos, y libres de tendencia o conflicto de intereses durante el proceso. [KLHCA]

Además de la definición de metas, objetivos y el alcance uno de los elementos fundamentales que debe salir de este módulo es la conformación del equipo auditor. Dicho equipo debe ser una combinación adecuada de conocimientos técnicos y experiencia como auditor.

- ***Módulo definición de las características técnicas***

El objetivo fundamental de este módulo es definir los detalles de la red que será auditada. El mismo debe realizarse ANTES del inicio de las pruebas y revisiones y DESPUÉS de haber definido las características del proceso de auditoría.

Como resultado de la ejecución del módulo, el equipo auditor debe obtener el inventario completo de la arquitectura que deberá ser auditada, incluyendo:

- Espacio de direcciones
- Mecanismos de distribución de direcciones
- Descripción de conexiones
- Dispositivos de red
- Servidores
- Estaciones clientes
- Dispositivos de Seguridad

Este módulo está compuesto por las siguientes secciones:

A) Caracterizar el rango de IP que utiliza la organización
B) Definir la forma en que se asignan las direcciones IP de la organización
C) Definir los dispositivos de red
D) Definir estructura de dominios
E) Caracterizar los enlaces de comunicaciones existentes
F) Caracterizar cada equipo servidor
G) Caracterizar equipos clientes

Cada sección de las mencionadas anteriormente está constituida por varias pruebas. Luego de ejecutar el módulo, el equipo auditor debería tener una visión muy completa, desde el punto de vista técnico, del sitio a auditar. Muchas veces este conocimiento permite validar o incluso desechar información ofrecida por el auditado en el primer módulo. Tal fue el caso del escenario en que se probó el modelo y que será descrito más adelante en este documento.

La participación del auditor en este módulo es activa. Los resultados se obtienen realizando pruebas, algunas de ellas incluso intrusivas, en la red del auditado.

- ***Módulo Pruebas de Penetración***

Este módulo define las acciones a llevar a cabo para realizar pruebas de penetración externas e internas sobre la arquitectura bajo estudio.

Para la ejecución de las pruebas de penetración deben seguirse las siguientes reglas [MSSPT]:

- La prueba de penetración de seguridad se inicia recopilando toda la posible información relativa a la infraestructura y las aplicaciones involucradas. Este paso es fundamental, ya que sin un conocimiento sólido de la tecnología subyacente, podrían omitirse algunas pruebas durante la fase de pruebas.
- Los auditores deberían intentar explotar todas las vulnerabilidades descubiertas. Aún cuando la explotación falle, el auditor obtendría un mayor conocimiento del riesgo de la vulnerabilidad.
- Cualquier información obtenida verificando las vulnerabilidades (por ejemplo, errores de programación, obtención de código fuente, u otro descubrimiento de información interna) debería utilizarse para volver a evaluar el conocimiento general de la aplicación y como se ejecuta ésta.
- Si, en cualquier punto durante la prueba, se detecta una vulnerabilidad que pueda llevar al compromiso del objetivo o pueda mostrar información crítica para la organización auditada, debe ponerse en contacto inmediatamente con la contraparte auditada y hacer que tome conciencia del riesgo involucrado.

Es importante entender la posición del auditor durante la ejecución de las pruebas de penetración. El auditor debe comportarse como un atacante que busca encontrar sitios por donde penetrar y luego comprometer la infraestructura de IT de la organización auditada. En ese proceso obtener la mayor cantidad posible de información de la organización no es un proceso repetitivo (tomando en cuenta los módulos anteriormente ejecutados del modelo). Aquí el objetivo y los métodos son diferentes. Se busca encontrar aquello que un intruso pudiese llegar a conocer de la organización. No debe olvidarse que el conocimiento detallado de la organización es uno de los primeros elementos que procurará un atacante. Veamos un ejemplo. El atacante sabe que la organización a la que desea atacar tiene un servidor WEB pero, ¿Que versión posee del demonio web? ¿Se permite que los usuarios coloquen sus propias páginas? ¿ Qué sistema operativo está corriendo el servidor? [SILHTCP][SHENS][MSSPT][FORUG].

Estos son algunos de los elementos que el atacante desearía conocer antes de comenzar su ataque. Otro ejemplo fue obtenido de la ejecución de las pruebas del modelo: durante el proceso de auditoría se descubrió el rango de direcciones privadas del sitio auditado, como consecuencias de errores en la configuración de servicio DNS. Esta información no había sido suministrada al iniciar el proceso de auditoría y permitió acceder de manera más sencilla a información confidencial del sitio auditado.

Una vez conocida, siguiendo los métodos de un atacante, la mayor cantidad de información de la empresa auditada el siguiente paso será verificar las vulnerabilidades y errores de las aplicaciones que se identifiquen. En este proceso es muy importante descartar falsos positivos y negativos[1].

La salida del módulo debe ser un inventario completo de las vulnerabilidades (incluyendo el acceso a información de la organización, los sistemas, etc...) y errores encontrados con sus correspondientes niveles de ponderación y un glosario de las evidencias que soporten los hallazgos realizados.

1 Situaciones que parecen errores pero no lo son y viceversa, situaciones que parecen normales y que en realidad esconden errores o vulnerabilidades serias.

Este módulo está compuesto por las siguientes secciones:

A) Definir arquitectura de IT sin conocimiento
B) Generar condiciones de DoS[2]
C) Ejecutar Pruebas contra Firewalls
D) Identificar vulnerabilidades en Servidores WEB
E) Identificar errores básicos de configuración en servidores SMTP
F) Identificar errores básicos de configuración en ambientes inalámbricos
G) Identificar errores de la configuración básica de servidores Unix ó GNU/Linux
H) Fisgonear información sensible en la red
I) Identificar errores básicos de la configuración de servidores Windows

Dependiendo de las características técnicas pudiese no aplicar todas las secciones. La selección de los objetivos ha sido realizada tomando en cuenta los servicios de RedULA y pudiesen servir para la mayoría de las organizaciones.

2 Negación de Servicios

- ***Módulo Revisiones de las Configuraciones***

Aunque la realización de las pruebas de penetración es un elemento muy importante y da una visión de lo que un intruso pudiese hacer, no es suficiente. Existen otras muchas condiciones de riesgo que no serán encontradas durante un proceso de intrusión y que sin embargo pudiesen acarrear problemas de seguridad. Pongamos un ejemplo: una partición de disco de un servidor con poco espacio, consecuencia de una mala planificación de capacidades, pudiese significar la paralización de un servicio pero difícilmente será encontrada por un intruso. Supongamos que un intruso desea probar el sistema de correo de una organización. Para hacerlo genera correos con direcciones falsas (falso el nombre de usuario, no el dominio). En condiciones normales el sistema reenviará al dominio de destino el mensaje y recibirá un mensaje de que el usuario no existe. Este proceso llevará a aumentar el tamaño de las colas de correo y eventualmente hará colapsar a un sistema mal dimensionado. El atacante posiblemente buscaba otro objetivo pero consiguió la paralización del sistema de correo[ZWBIF] . Ejemplos de este tipo existen muchos.

Por la razón antes expuesta se hace necesario un tipo de auditoría sistemática, en la que el auditor revisa un grupo de elementos adicionales que están relacionados. Encontrar este tipo de relaciones es el objetivo del módulo más extenso y complejo que incluye el modelo: Las Revisiones.

Este módulo está compuesto por las siguientes secciones:

A) Revisión de la Seguridad Física
B) Revisión de Servidores UNIX
C) Revisión de Servidores y Estaciones Windows
D) Revisión de Servidores Sendmail
E) Revisión de Servidores Apache
F) Revisión de la infraestructura inalámbrica
G) Revisión del Sistema de Detección de Intrusos
H) Revisión de Dispositivos Firewalls
I) Revisión de las Políticas de Seguridad

Este es el módulo mas extenso y complejo del modelo y reune aproximadamente el 60 % de las reglas y acciones presentes en el mismo. La salida del módulo es un inventario completo de las vulnerabilidades detectadas durante el proceso de revisión sistémica así como de las recomendaciones para superar las condiciones encontradas. Tal como con los otros módulos, cada regla o prueba tiene asociado un nivel de ponderación que permitirá al auditor dar un valor cuantitativo final del nivel de seguridad del auditado. A continuación describiremos con más detalles cada una de las secciones que conforman este módulo del modelo.

Ponderación de los Resultados

Una entidad auditada estará muy interesada en obtener, como resultado del proceso de auditoría, un listado completo de las condiciones de riesgo a las que está sometida su infraestructura de información. Sin embargo, es también muy importante definir cuantitativamente el peso específico de cada condición hallada. Como es de suponer no todos las vulnerabilidades, errores y otras condiciones significan igual nivel de riesgo para la integridad, disponibilidad y confidencialidad de la información y los medios que la soportan [CRISPMS] .

Esta ponderación es de suma importancia para la definición del necesario proceso ulterior de correcciones, toda vez que siempre debe comenzarse por aquellas condiciones que impliquen mayor nivel de riesgo. La ilustración no. 4 muestra la relación entre el orden en que deben ejecutarse las correcciones y el nivel de riesgo que las vulnerabilidades encontradas tienen. Como se muestra en la ilustración las vulnerabilidades (marcadas como puntos blancos) que se encuentran dentro del rectángulo rojo deben ser las primeras a ser corregidas toda vez constituyen los mayores riesgos.

Establecer niveles de ponderación para cada prueba suele ser un proceso mas complejo de lo que parece a primera vista, debido al nivel de subjetividad que puede acarrear y la los múltiples factores que deben tomarse en cuenta (por ejemplo lo que es muy crítico para una organización puede no serlo para otra). Para hacerlo nos hemos basado en dos fuentes y tratado de conjugar sus resultados. La primera ha sido la categorización de los resultados que comúnmente hacen las herramientas de búsqueda de vulnerabilidades automatizadas (alto , medio y bajo). La segunda fuente fue la Metodología Abierta para Pruebas de Seguridad[HMAST].

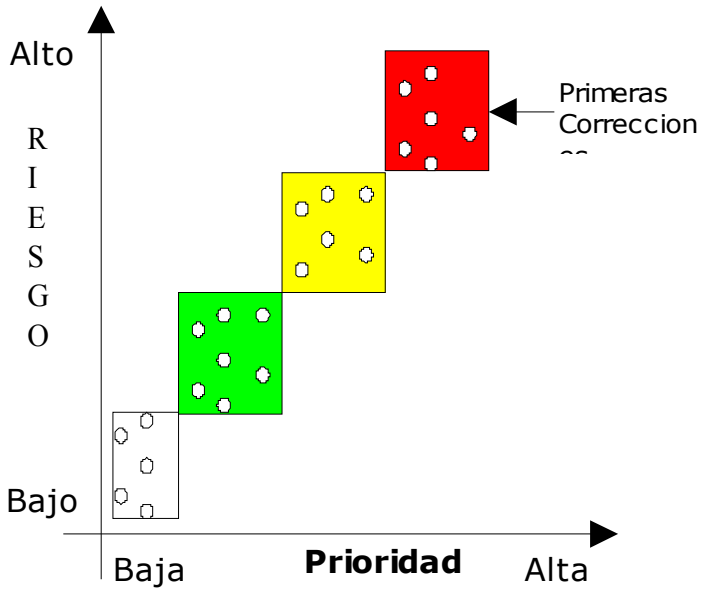

Ilustración 4: Ponderación de los resultados y su relación con el orden de las correcciones

Las ponderaciones que se ofrecen en el modelo son puramente referenciales. El auditor tiene capacidad de variar la ponderación sugerida para una prueba debido a condiciones específicas del sitio a auditar o de las propias condiciones en que se ejecuta la prueba. Por ejemplo, transmitir datos críticos sin cifrar a través de la red puede considerarse como una condición de alto impacto debido a la posibilidad de que alguien acceda físicamente al medio y "escuche", cambie o destruya la información mientras viaja por la red. Sin embargo, esta ponderación pudiese variar si acceder a los medios de transmisión, los extremos de comunicación o cualquiera de las partes por donde viaja la información es físicamente prohibitivo. La ponderación de los niveles se riesgo ha sido establecida por cada prueba, entendiendo que la ponderación del resto de las unidades superiores en que ha sido dividido el modelo (módulos, secciones y reglas) puede obtenerse a partir de estas sistemáticamente.

Conclusiones y Recomendaciones

En el trabajo presentado se ha producido un extenso modelo lógico (aproximadamente 250 reglas) para gestionar la auditoria de seguridad informática de una institución, que cubre las áreas más importantes para el desarrollo seguro de la Red de Datos de la Universidad de los Andes y establece los procedimientos y los mecanismos genéricos para auditarla.

El modelo fue sometido a una va.lidación. La arquitectura de TI y de seguridad de la dependencia que se utilizó para realizar la prueba del modelo fueron modificadas para atender las recomendaciones emanadas de la utilización que se propone en este trabajo. La utilización del modelo no sólo permitió detectar condiciones de riesgo en la plataforma ya existente, sino también detectar insuficiencias importantes en el dimensionamiento del equipamiento y carencias en temas vitales como las Políticas de Seguridad Informática.

Al utilizar un modelo que ofrece procedimientos y salidas normalizados los auditores pueden volver a auditar, una vez realizadas las correcciones, y verificar con mayor facilidad que las condiciones de riesgo detectadas han sido corregidas.

El modelo ha sido desarrollado con un enfoque intermedio entre una visión de alto nivel, muy separada de la arquitectura que soporta los servicios y una posición de muy bajo nivel que haga el modelo muy dependiente de la arquitectura. La razón de hacerlo de esta forma es obtener una herramienta útil para el encargado de auditoría pero que a su vez pueda trascender cambios simples de la arquitectura.

El modelo puede ser utilizado no sólo para auditar, puede ser visto también como una guía de mandatos básicos para asegurar un sitio. En este momento también está siendo utilizado de esa forma por el equipo de Seguridad Informática de RedULA.

Al crear un modelo que incluye una serie de reglas que pueden ser utilizadas como criterios de buenas prácticas de seguridad el modelo igualmente puede ser utilizado para la instrucción del personal técnico en los elementos básicos de seguridad informática.

Por todos los elementos antes expuestos que se han cumplido con los objetivos planteados y hemos creado una herramienta útil y versátil para la auditoría y otras funciones necesarias para la seguridad informática de la Red de Datos de La Universidad de Los Andes.

Referencias Bibliográficas

[HMATS]Herzog P. , Metodología Abierta de Testeo de Seguridad 2.1 (2003), Institute for Security and Open Methodologies.

[MSSPT] Mainstream Security INC, Security Penetration Testing, URL: http://www.mainstream.net/security_howto/security_penetration_testing.shtml

[SHENS] Stuart Mc. ,Hacking Exposed: Network Security, 4th edition, (2003), McGraw-Hill

[SILHTCP] Siles R. Hacking TCP/IP, (2003) EE.UU, GNU Free Software Foundation

[ZWBIF] Zwicky T. Building Internet Firewalls, (2003), EE.UU: O'Relly Media Inc.

[KLHCA] Klarp J., How to Conduct a Security Audit. (2000) ,PC Network Advisor URL: http//www.itp-journal.com

[CRISPMS] Cresson Ch., Information Security Police Made Easy, (2002) EE.UU, Pentasafe