UNIVERSIDAD Rafael Belloso Chacín

Revista Electrónica de Estudios Telemáticos
TÉLÉMATIQUE

MODELO DE AUDITORIA PARA SERVICIOS TELEMÁTICOS DE LA UNIVERSIDAD SIMÓN BOLÍVAR.

(AUDIT MODEL FOR TELEMATIC SERVICES OF SIMÓN BOLÍVAR UNIVERSITY).

Nicolás Lagreca
Universidad Simón Bolívar
Nicolaslagreca@gmail.com

RESUMEN

El análisis de la variable auditoria a servicios telemáticos se sustentó en los criterios teóricos de Gonzales (2014), Restrepo (2015) y Muñoz (2011), entre otros. Desde el punto de vista metodológico, el estudio se desarrolló como una investigación centrada en el tipo denominado proyecto factible y de orden descriptivo de campo. La investigación está constituida por cuatro (4) fases. Se hace un diagnóstico de la situación actual de la seguridad en servicios telemáticos de la Universidad Simón Bolívar. Seguidamente se identifican los ambientes sensibles en servicios telemáticos con el fin de generar una valoración de activos y se protagonistas del modelo de auditoria. El estudio se centró en las metodologías correspondientes para la evaluación de los servicios telemáticos: OSSTMM Wireless (Open Source Security Testing Methodology Manual), OWISAM (Open Wireless Security Assessment Methodology) , OWASP (Open Web Application Security Project), NIST (National institute of standards and technology), ISSAF (Information system security assessment framework) y PETS (The penetration testing execution standard). El resultado es un modelo único unificando las diferentes metodologías, contribuyendo según su especialidad cada metodología estudiada.

Palabras Claves: Seguridad, Hacking, Auditoria, Penetración.

ABSTRACT

This research was to propose overall objective audit model for telematic services Simon Bolivar University. The analysis of the variable to telematic services audit was based on theoretical criteria Gonzales (2014), Restrepo (2015) y Muñoz (2011) among others. From the methodological standpoint, the study was developed as a research focused on the type and feasible project called descriptive field order. Research consists of four (4) phases. A diagnosis of the current situation of security in telematic services is Simon Bolivar University. Then sensitive environments are

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

identified in telematics services in order to generate a valuation of assets and audit model protagonists. The study to form the procedure focused on the corresponding free methods for the evaluation of telematic services: OSSTMM Wireless (Open Source Security Testing Methodology Manual), OWISAM (Open Wireless Security Assessment Methodology) and OWASP (Open Web Application Security Project), NIST (National institute of standards and technology), ISSAF (Information system security assessment framework) y PETS (The penetration testing execution standard). The result is a unique model unifying the different methodologies, each contributing according to their specialty studied methodology.

Keywords: Security, Hacking, Auditing, Penetration.

INTRODUCCION

Es evidente entonces, desde el surgimiento del Internet y la posibilidad que nos brinda en mantenernos siempre conectados, entender como la información y los medios por la que se transmite toman un valor critico en la sociedad actual, importancia que muchas veces pasa desapercibida permitiendo la aparición de nuevas vulnerabilidades que pueden ser explotadas en caso de no conocerse, o no solucionarse, poniendo en riesgo la integridad de unos de los bienes más valiosos que existen hoy.

Las amenazas surgen a partir de la existencia de vulnerabilidades, las cuales pueden ser explotadas por usuarios de alto nivel en conocimientos técnicos los cuales generalmente buscan aprovecharse de estos fallos en los sistemas, impulsados por razones como el espionaje industrial hasta un simple desafío personal o de la comunidad hacktivista; es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

Fijando estas ideas en las universidades, que cada día destacan más por contar con sistemas complejos, se han convertido en un objetivo cada vez más frecuente de los ciber-delincuentes, en el 2014 la Universidad de Pensilvania, ubicada en los Estados Unidos, según la página web de la propia universidad, se llevaron a cabo bloqueos de una media de 20 millones de ciberataques dirigidos a sus sistemas solo en ese año. En una nota del diario Qingxin en enero del 2016 y según las autoridades universitarias, la web oficial de la Universidad de Tsinghua, una de las más prestigiosas de China, fue atacada por piratas informáticos presuntamente ligados al Estado Islámico.

No puede tampoco olvidarse que en la universidad tiene que existir un ambiente abierto que fomente la investigación y crecimiento educativo de los alumnos, muchos de ellos disponen de cuentas de correos institucionales así como cierto

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

nivel de acceso a los servicios. Esto genera una vulnerabilidad evidente desde el punto de vista informático debido a que un estudiante en crecimiento y por la alta curiosidad que se caracteriza pudiera por ejemplo, vulnerar el sistema que almacena las notas en el claustro educativo, pudiendo modificar el registro académico de cualquier estudiante.

Alejandro Robayo estudiante de último semestre de ingeniera industrial de la Universidad de los Andes en Colombia, fue condenado en el 2015 por los delitos de acceso abusivo a sistema informático, violación de datos personales y uso de software malicioso, logró, a través de diferentes métodos sacar las contraseñas de algunos profesores en la plataforma de la universidad, primero violo lo sistemas modificando las notas de algunos de sus últimos examen para no ver afectado su promedio pero luego comenzó a vender sus servicios a otros estudiantes hasta que una joven recibió la propuesta y esta denuncio al estudiante frente a las autoridades de la universidad.

En este caso las universidades venezolanas, no están exentas de situaciones de riesgo que afecten su seguridad, por lo que requieren comprender el problema de inseguridad de la información, de esta manera se recomienda la creación de un modelo que permita auditar la Seguridad de la Información en las universidades, alineado con la formulación de un plan estratégico que permitan a las universidades defenderse de eventuales ataques, reduciendo las fallas y contribuyendo a proteger las vulnerabilidades encontradas.

Por consiguiente, nacen las auditorias informáticas con el objetivo fundamental de detectar, investigar y explotar vulnerabilidades en la infraestructura tecnológica de una organización, logrando prevenir la intrusión o mitigar el daño de la misma. Es importante separar los sistemas de interés, ya que si la información que contiene un sistema es menos valiosa que el tiempo que llevaría a un delincuente acceder a ella, nadie la querría.

De continuar con la situación antes planteada, se pronostica que los riesgos al que están expuestos todos los servicios telemáticos de la Universidad Simón Bolívar continuaran creciendo exponencialmente ante el avance de las tecnologías y la divulgación de las técnicas necesarias que permite a personas inexpertas en el área aprovechar las fallas y vulnerabilidades que los equipos pueden estar sufriendo, dando la oportunidad a los usuarios malintencionados degradar los servicios que presta la Universidad a sus estudiantes o inclusive imposibilitar que pueda cumplir con su objetivos principales, como es la educación de calidad.

Se trata el problema que se describe en esta investigación, como se centra en el hecho de que existen muchos casos donde las organizaciones sufren incidentes que podrían haberse evitado si los mecanismos de protección hubieran sido reforzados en su momento y no solo limitados a seguir una política de seguridad. Los incidentes comprenden sucesos tales como fuga de información, accesos no autorizados, pérdida de datos, entre muchos otros.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

OBJETIVO

Proponer un modelo de auditoría para servicios telemáticos en la Universidad Simón Bolívar.

RESULTADOS DE LA INVESTIGACION

Diagnostico de la situación actual de la seguridad en servicios telemáticos de la Universidad Simón Bolívar.

En esta primera fase, se realizó una entrevista no estructurada al personal técnico encargado de la seguridad en redes y servicios telemáticos de la Universidad Simón Bolívar, buscando el diagnóstico más detallado de la situación actual. Por medio de las técnicas e instrumentos de recolección de datos, se busca completar esta fase, de modo que resulte más confiable, específica y directa la información recolectada por parte del investigador al lector.

La entrevista, según Garcia (2014) es la recogida de información a través de un proceso de comunicación, en el transcurso del cual el entrevistado responde a cuestiones previamente diseñadas en función de las dimensiones que se pretenden estudiar planteadas por el entrevistador. Las entrevistas se dividen en estructuradas, semiestructuradas o no estructuradas o abiertas. Las primeras o entrevistas estructuradas, son aquellas en que el entrevistador se vale de una guía de preguntas específicas y se sujeta exclusivamente a estas. Por el contrario, las entrevistas semiestructuradas, se basan en una guía de asuntos o preguntas y el entrevistador tiene la libertad de introducirle preguntas adicionales para precisar conceptos u obtener mayor información sobre el tema investigado.

Dentro de este marco de ideas según Muñoz (2011) habla de la entrevista no estructurada como entrevista en profundidad. Sus objetivos son comprender más que explicar, maximizar el significado, alcanzar un respuesta subjetivamente sincera más que objetivamente verdadera y captar emociones pasando por alto la racionalidad. Es por esto que la convierte en el instrumento perfecto, que permita diagnosticar la situación actual en toda la seguridad de los servicios telemáticos de la Universidad Simón Bolívar.

En este mismo orden de ideas, se desarrolló una entrevista no estructurada al informante, experto en el área de seguridad y encargado de todos los servicios telemáticos de la Universidad Simón Bolívar, su nombre no se revela con el objetivo de no involucrar a dicha persona en ninguna situación comprometedora por la información revelada. Se le formularon una serie de preguntas que al final permitió conocer la situación actual de la seguridad en redes y servicios

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

telemáticos, siendo muchas veces reservado en sus respuestas por la confidencialidad que se maneja en la institución.

Es importante resaltar que el uso de la entrevista no estructurada como instrumento para determinar la situación actual de la Universidad Simón Bolívar fue crucial para obtener toda la información necesaria, haciendo sentir cómodo al entrevistado a medida se fue desarrollando la entrevista fueron surgiendo nuevas y valiosas preguntas, algunas claves que requirió de una confianza entre el entrevistado y el investigador para obtener resultados.

Las preguntas más relevantes que se formularon fueron: ¿Existen políticas y normas de seguridad en la Universidad Simón Bolívar?, obteniéndose que esencialmente no existen normas y políticas de seguridad, la seguridad en la Universidad es una manera de hacer las cosas y no un procedimiento único. Siendo una institución educativa se le dificulta al personal forzar una rígida y estricta metodología de acceso a los recursos electrónicos. Están limitados todos los servicios entrantes excepto aquellos permitidos, evaluando caso por caso. La administración y correctas prácticas de seguridad son sugeridas en la mayoría de los casos. Pero no se realizan auditorías exhaustivas para ver su cumplimiento, salvo en los casos patológicos o recurrentes con problemas.

En este orden de ideas surgieron preguntas como ¿Encargados de la seguridad en la Universidad Simón Bolívar e inversión económica en el área?, obteniéndose como respuesta, que no existe un departamento como tal encargado de la seguridad informática en la institución, si no personas cuyo nombres no pueden ser revelados por asuntos de confidencialidad, las mismas ejercen funciones de administradores de redes y servicios, implantadores, son profesores y administran la seguridad. El único departamento que está separado es el de soporte técnico.

Siguiendo esta línea se le pregunto, ¿Los tipos y versiones de sistemas operativos y firmware en los diferentes equipos de la institución?, el informante manifestó sin mucho detalle, que las versiones en equipos y servicios son las últimas soportadas, en muchos casos siendo equipos viejos los cuales no cuentan ya con soporte por parte del fabricante, por falta de presupuesto y recursos que no se le asignan a la universidad, todos o casi todos los equipos y servicios se encuentran en el periodo End-of-Life.

Se desprende de la entrevista que la Universidad Simón Bolívar cuenta con dispositivos de Firewall, IDS, IPS, entre otros servicios, basado en software libre y cumpliendo con el decreto presidencial 3390, todos los equipos en laboratorios estudiantiles cuenta con Ubuntu (no su última versión), en el caso de los puestos administrativos, en general se cumple con el decreto 3390 con excepción de algunas personas que usan Windows. Se cuenta con cerca de 20 puntos de accesos inalámbricos, públicos para los estudiantes, pero de nuevo por falta de estrictas normas de seguridad, muchos usuarios administrativos tienen los suyos propios, en muchos casos con pobres configuraciones de seguridad.

Por lo demás según la información recabada del informante se pudo saber que, la Universidad Simón Bolívar, cuenta como amenazas comunes de este tipo de instituciones, sumando vulnerabilidades producidas por la falta de severidad en la

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

aplicaciones de metodologías y normas de seguridad, como puede ser una de ellas que cada computador de laboratorio estudiantil dispone de una IP publica, pudiendo acceder un atacante remotamente desde cualquier parte del mundo y luego realizar un movimiento horizontal o vertical hacia los servicios de la Universidad.

A continuación se muestra el resultado de la matriz de doble impacto donde se establecen tres referencias que facilitan la diagnosis sobre la situación actual de la Universidad Simón Bolívar. La primera referencia la define el impacto de cada eje sobre los demás. Es el perímetro del deber ser, es decir la frontera que delimita la correlación de esfuerzos entre ellos. La segunda referencia es la estimación de la situación actual, se logró mediante la estimación con el encargado de los servicios telemáticos en la Universidad Simón Bolívar. La tercera referencia la define la sensibilidad y se refiere a la facilidad que tiene un eje de ser modificado.

En este orden de ideas y con la información recabada se seleccionaron 9 ejes como las normas, infraestructura, estudiante, profesores, personal administrativo, laboratorios, redes Wifi, servidores, sitios Web. Estos ejes permitieron la construcción de una matriz de doble impacto, en la cual se ponderara el nivel de influencia de un eje sobre resto, con el fin de determinar de forma cuantitativa la valoración de la situación actual en la Universidad Simón Bolívar.

Cuadro 1
Matriz de doble impacto

	Normas	Infraestructura	Estudiante	Profesores	Personal Administrativo	Laboratorios	Wifi	Servidor	Web	Impacto
Normas		9	8	3	8	9	9	8	7	**61**
Infraestructura	4		7	2	7	10	7	9	8	**54**
Estudiante	3	10		0	3	8	9	7	10	**50**
Profesores	2	3	10		3	4	3	3	4	**32**
Personal Administrativo	5	7	4	0		2	9	10	4	**41**
Laboratorios	7	8	10	4	2		0	10	10	**51**
Wifi	10	8	9	5	10	0		4	3	**49**
Servidor	8	7	7	1	10	8	3		10	**54**
Web	10	0	10	2	6	8	0	10		**46**
Sensibilidad	**49**	**48**	**51**	**17**	**49**	**49**	**40**	**61**	**56**	

Fuente: Elaboración propia (2017)

En este orden de ideas se deja establecido que la valoración que hace la matriz en cuanto se miden los ejes en función del peso con respecto a los otros, obteniendo un valor de impacto y sensibilidad para cada uno de ellos. Luego de desarrollada la matriz de doble impacto, y logrado conseguir los valores que definen el deber ser de cada eje, se establece una línea de referencia que se

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

conoce como perímetro del deber ser, que no es más que la brecha entre el deber ser y la situación actual.

Es por eso que el tamaño de la brecha indica de forma cualitativa la magnitud de la inversión que debe hacerse para cerrarla. La inversión no solo se mide en dinero, también se deben considerar otros recursos tales como tiempo, esfuerzo, talento, disponibilidad, entre otros. En este punto, vale señalar que el cierre de la brecha está íntimamente vinculado con la mitigación de los riesgos, por lo que deben tenerse presente la necesidad de una auditoria que permita determinar las amenazas existentes.

Cuadro 2
Brecha

Eje	Deber ser	Actual	Brecha
Normas	61	16	45
Infraestructura	54	12	42
Estudiante	50	20	30
Profesores	32	25	7
Personal Administrativo	41	25	16
Laboratorios	51	12	39
Wifi	49	15	21
Servidor	54	30	34
Web	46	14	32

Fuente: Elaboración propia (2017)

En este orden de ideas y según los resultados obtenidos en la entrevista no estructurada, a juicio del investigador junto con la valoración del entrevistado se aprecia que el modelo de auditoria debe ir orientado a verificar la seguridad de los servidores, laboratorios, redes Wifi, sitio Web. De igual forma se debe resaltar que debe planificarse una campaña para la aplicación de normas de seguridad así como la concientización de los sectores más vulnerables como son los estudiantes y personal administrativo

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

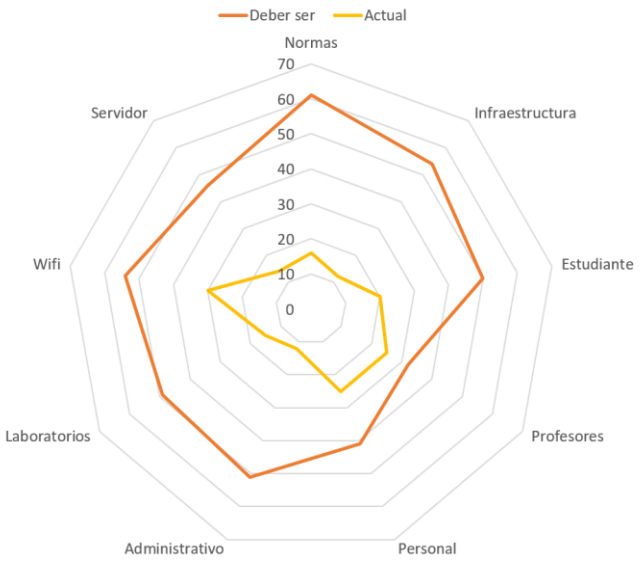

Figura 1. Deber ser vs Actual
Fuente: Elaboración propia (2017)

En atención a lo antes expuesto y lo que no se muestra en la presente investigación por motivos de seguridad, se pudo concluir que la Universidad Simón Bolívar al ser una institución educativa publica, cuenta con múltiples fallas a nivel de seguridad, abriendo esto la posibilidad de contar con un sinfín de vulnerabilidades las cuales sumadas a las amenazas intrínsecas que sufre una organización de este tipo, suben los riesgos de sufrir ataques informáticos que pueden en cualquier medida dañar la institución.

Ambientes sensibles en redes y servicios telemáticos, con el fin de elegir los recursos claves candidatos a integrar en el modelo de auditoria.

Para el cumplimiento de esta fase, de nuevo haciendo uso de la entrevista no estructurada, se buscan los activos más importantes de la institución, identificando los riesgos de cada uno de ellos, el valor o costo para la Universidad del remplazo del mismo en caso de verse afectado, el costo que representa para la institución el mantenimiento del activo y el impacto para el core de negocio en caso de verse comprometido y negar su disponibilidad.

Los activos tangibles son requisito inicial e indispensable para el desarrollo de una actividad o la prestación de un servicio, pero son claramente insuficientes si pensamos en términos de competitividad y futuro de la organización. El objetivo de

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

su gestión es la optimización en su utilización. El principal problema que presentan es que la valoración contable puede no ser significativa a efectos estratégicos (Tarasco y Tarasco, 2013).

Los activos intangibles son aquellos que no tienen soporte físico lo que hace muy complejas su identificación aunque son fundamentales para garantizar la innovación, flexibilidad, adaptación al cambio, la competitiva a medio y largo plazo (Rando, Chema y Aparicio, 2016). Todos los activos deberían ser justificados y tener asignado un propietario y se deberían identificar a los propietarios para todos los activos y asignarles la responsabilidad del mantenimiento de los controles adecuados.

Una vez que se identificaron los activos pertenecientes a una entidad en particular, se procedió a la tasación de dichos activos (esto con la finalidad de poder identificar posteriormente la protección apropiada a los activos, ya que es necesario tasar su valor en términos de importancia a la gestión tanto académica como administrativa de la Universidad Simón Bolívar, o dadas ciertas oportunidades determinar su valor potencial). La valoración de activos es un factor muy importante en la auditoria. La valoración de activos es la asignación apropiada en términos de la importancia que éste tenga para la empresa.

En el cuadro siguiente y según información recabada de la entrevista no estructurada al informante dentro de la Universidad Simón Bolívar, se puede observar el vaciado del análisis y evaluación de riesgo, en escala según la valoración del mismo, Alto (A), Medio (M) y Bajo (B). La gestión de riesgo permite evaluar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que sea aceptado por la dirección (Restrepo, 2015).

Los activos de información deben ser clasificados de acuerdo a la confidencialidad, integridad y disponibilidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen. Las pautas de clasificación deben contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, que ésta puede cambiar de acuerdo con una política predeterminada por la propia organización. La valoración de los activos es algo único para cada organización que va en base al objetivo general y el valor que la información representa, gracias a la información recabada por el investigador se conformó un cuadro resumen que determina los activos con su valoración.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

Cuadro 3
Valoración de los activos

Activos	Valoración				Amenazas	Probabilidad de ocurrencia	Impacto
	Confidencialidad	Integridad	Disponibilidad	Total			
Servidores de DACE	B	A	A	A	-Hackers -Virus -Seguridad Física	B A A	A
Servidores de nomina	A	A	B	A	-Hackers -Virus -Seguridad Física	B A A	A
Laboratorios	B	M	B	M	-Hackers -Virus -Seguridad Física	A A A	A
Servidores de Finanzas	M	A	A	A	-Hackers -Virus -Seguridad Física	B A B	A
Servidores DNS	A	A	A	A	-Hackers -Virus -Seguridad Física	A A B	A
Servidores de Correo	A	A	A	A	-Hackers -Virus -Seguridad Física	A B B	A
Servicios de Intranet	M	A	M	M	-Hackers -Virus -Seguridad Física	A A B	A
Servicios de Internet	M	A	A	A	-Hackers -Virus -Seguridad Física	A A B	A

Fuente: Elaboración propia (2017)

Modelo de auditoria para los servicios a ser auditados mediantes pruebas de penetración.

Cuando se hace la auditoría de seguridad a una empresa lo más probable es que siempre se acabe entregando un informe en el que se demuestra que ha sido posible entrar a zonas importantes del sistema. Además, siempre aparecen vulnerabilidades menores que ayudan a preparar ataques más importantes al sistema o fallos de configuración en el entorno que abren definitivamente la puerta. (Cárdenas, 2012)

Una auditoria informática orientada hacer un test de Penetración, es un procedimiento metodológico y sistemático en el que se simula un ataque real a una red o sistema, siendo el auditor el que se pone el traje de delincuente, tratando de pensar y actuar como uno, con el fin de descubrir vulnerabilidades y vectores de ataques y de esa manera poder reparar los problemas de seguridad que muchas veces se mantienen ocultos,

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

En esta fase final, se culminara con diseñar un modelo de auditoria para la redes y servicios telemáticos de la Universidad Simón Bolívar mediante pruebas de penetración, que cumpla con todas las exigencias que la institución requiere, siendo un modelo totalmente libre, basándose en etapas y procedimientos de las metodologías estudiadas en el capítulo II, así como también procedimientos planteados por el investigador, ajustando el modelo a las exigencias de la casa de estudio.

En este orden de ideas, se pudo comparar y determinar las características propias de las metodologías elegidas para el estudio, que según a juicio del investigador, contribuyeron según sus especialidades a formar el modelo de auditoria para redes y servicios telemáticos, que cumpla con todos los requerimientos de la institución y sea totalmente abierto, sin restricción o abuso de licencias.

En este orden de ideas y para darle respuesta a este punto fue considerada la revisión documental tanto de la normativa legal que rige la materia así como, autores y antecedentes que hayan trabajado en el área de auditoria informática partiendo por cumplir el decreto 3390, donde se puede resumir principalmente que todo ente público debe estar orientado a usar tecnologías abiertas, además de la propia filosofía de la Universidad Simón Bolívar. Se estudiaron las metodologías libres que estuvieran respaldas en el campo profesional y permitieran cumplir los objetivos plateados.

En primer lugar, seis metodologías, estándares o framework fueron seleccionados para su uso potencial. Las selecciones se clasificaron en metodología, estándar o framework, respectivamente, mediante un análisis de si las características de una prueba de penetración se encontraban presentes, si se rigen por estándares de evaluación de la seguridad, si se encuentra bien documenta y así como también un apoyo de la comunidad que la haga sostenible en el tiempo. (Sanchez, 2014).

Cuadro 4
Matriz de evaluación

	Estándar	Framework	Metodología	Comunidad activa	Manual o recurso	Pruebas de penetración	Evaluación de seguridad
ISSAF		✓			✓		✓
OSSTMM			✓	✓	✓	✓	✓
PTES	✓					✓	
OWASP			✓	✓	✓	✓	✓
OWISAM			✓	✓	✓	✓	
NIST	✓						✓

Fuente: Elaboración propia (2017)

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

La evaluación de calidad de los candidatos a formar parte del modelo se determinó primero, el dominio de cobertura del candidato. El segundo criterio consistió en examinar los requisitos necesarios para el mantenimiento de dicha metodología o framework en el tiempo. Como tercer criterio se consideró la extensibilidad o flexibilidad del candidato a la hora de personalizar alguna etapa. Como cuarto criterio o métrica se consideró la facilidad de uso. Como quinto criterio, la disponibilidad del framework o metodología. La quinta métrica determino la confianza de la guía o candidato. Como ultima métrica, se consideró si posee licencia, en otras palabras es un totalmente abierto.

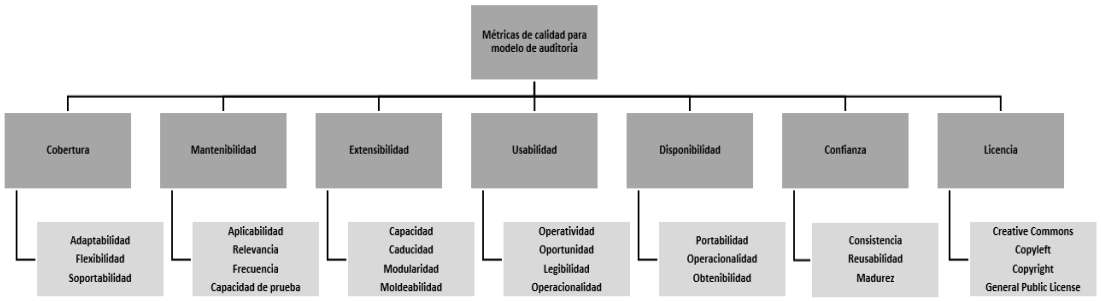

Figura 2. Modelo de calidad
Fuente: Elaboración propia (2017)

Cuadro 5
Matriz de calidad

	Cobertura	Mantenibilidad	Extensibilidad	Usabilidad	Disponibilidad	Confianza	Licencia
ISSAF	✓		✓	✓			
OSSTMM	✓	✓	✓	✓	✓	✓	✓
PTES			✓	✓			
OWASP		✓	✓	✓	✓	✓	✓
OWISAM		✓		✓	✓	✓	✓
NIST							

Fuente: Elaboración propia (2017)

En esta fase de la investigación se examinaron metodologías, estándares o frameworks de auditoria a servicios telemáticos, en especial OSSTMM, ISSAF, PTES, OWISAM, OWASP y NIST. Se encontró que muchos de estos candidatos fueron mal nombrados (es decir, no son metodologías o carecen de cobertura de dominio o una base ontológica sólida y por lo tanto se han vetado para la propuesta del modelo de auditoria. Las metodologías OSSTMM, OWASP, OWISAM fueron

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

seleccionadas para integrar la propuesta del modelo, en base a su enfoque (pruebas de penetración específicas o de seguridad general) y su capacidad para actuar como una metodología abierta.

Cuadro 6
Análisis final ISSAF

ITEMS	ISSAF
Rigor	Alta. Desactualizada. Año2006.
Nivel de detalle	Muy detallada, pero sencilla. No se abarca la seguridad en la nube y la verificación de cómo se protegen los datos
Facilidad de uso	Muy Alta. Se puede usar con conocimientos medios.
Ámbitos de aplicación	PYMES, organizaciones e instituciones varias
Entornos de aplicabilidad	Todos. Genérico para auditorías de todo tipo.
Uso por los auditores	Cubre las etapas más usuales de una auditoria de penetración, siguiendo una serie de pasos muy líneas, no muy usada por su desactualización
Ventajas	Fase de evaluación conocida. Uso frecuente del método. Largo recorrido en el campo de la auditoria. Facilita el informe en función de los pasos seguidos y los resultados obtenidos. Recomienda herramientas para la evaluación
Inconvenientes	No establece claramente los límites en las pruebas de penetración, siendo mucho menos rigurosa que el resto. Si no se tiene el control en todo momento es muy fácil que las pruebas se salgan de control. Estancada y falta de actualización

Fuente: Elaboración propia (2017)

El análisis final determino que la metodología ISSAF cuenta con un alto nivel de exigencia, por el nivel de detalle que abarca en sus controles y es muy fácil de usar, pero carece de evaluaciones referente a la seguridad en la sube, esto siendo de vital importancia para auditorias futuras, además que no tiene un exigente examen para establecer el nivel de eficiencia en cuanto la protección de los datos se refiere, es una metodología que actualmente se encuentra desactualizada y no posee un comunidad activa.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

Cuadro 7
Análisis final PTES

ITEMS	PTES
Rigor	Alta. Desactualizada. Año2008.
Nivel de detalle	Es una marco de pruebas altamente detallada, los procesos están perfectamente definidos aunque no suelen actualizarse los procesos
Facilidad de uso	Media. Al principio puede parecer de fácil uso, pero es altamente recomendable entrenamiento previo.
Ámbitos de aplicación	Organizaciones complejas .PYMES
Entornos de aplicabilidad	Todos. En combinación con otra metodología.
Uso por los auditores	No se usa con mucho auge en la actualidad, aunque todavía hay ciertas empresas tradicionalistas que la mantienen
Ventajas	Muy bien definido los controles de las pruebas de penetración, tiene muchas similitudes con la OSSTMM. Ofrece una excelente guía de cómo deben ser conducidas las pruebas.
Inconvenientes	A pesar de contar con buenas perspectivas está todavía muy incompleto. Se han hecho diferentes llamados a la comunidad para su colaboración pero sin éxito. Altamente desactualizada.

Fuente: Elaboración propia (2017)

Para el análisis final de la metodología PTES se concluyó que cuenta con un alto nivel de exigencia, ya que sus procesos están perfectamente definidos, pero carece de una comunidad activa, pese a contar con procesos bien definidos los mimos, individualmente, están todavía incompletos, es una metodología que actualmente se encuentra desactualizada y no posee un comunidad activa, es por esto y más que no cumple con lo necesario para formar parte del modelo a proponer.

Cuadro 8
Análisis final OWASP

ITEMS	OWASP
Rigor	Muy Alta. Solo centrada en la web, pero muy didáctica e instructiva
Nivel de detalle	Enfocada al ambiente WEB, sigue con perfecta meticulosidad las pruebas y métricas necesarias para evaluar cualquier aplicación
Facilidad de uso	Media, es una metodología que ofrece todo lo necesario, pero se debe tener conocimiento previo para poder usar
Ámbitos de aplicación	Toda organización que ofrezca algún servicio WEB
Entornos de aplicabilidad	Cualquier servicio WEB
Uso por los auditores	La metodología más usada en actualizada para auditorias y pruebas de penetración a nivel WEB, por su amplio repertorio de controles
Ventajas	Establece un TOP 10 de las vulnerabilidades más comunes en sitios WEB, perfectamente estructurado y definido por muchos expertos en la materia. Ofrece las pruebas necesarias para comprobar si un sitio o aplicación WEB es vulnerable al TOP 10
Inconvenientes	Presta atención solamente a la parte WEB, lo que hace necesario combinarla con otras metodologías para que la auditoria sea más completa.

Fuente: Elaboración propia (2017)

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

Para el análisis final de la metodología OWASP se pudo establecer como una metodología especializada en el auditoria web, con un muy alto nivel de exigencia, ya que todos sus procesos y controles permiten establecer con gran precisión el nivel de seguridad de la plataforma, esto debido a que es altamente mantenida por diferentes cluster de personas a nivel mundial, siendo referente en su área, es un metodología también totalmente abierta, de uso y modificación, tiene como defecto a que necesita de otras metodologías para conseguir una auditoria completa a una infraestructura telemática, a pesar de esto cumple con lo necesario para formar parte del diseño.

Cuadro 9
Análisis final OSSTMM

ITEMS	OSSTMM
Rigor	Muy Alta. Actualizada y en constante revisión
Nivel de detalle	Se ha ido actualizando con los años, hasta volverse una metodología referente para las pruebas de penetración, pero necesita conocimiento para realizar alguna de sus fases
Facilidad de uso	Media. Muy técnico. Requiere entrenamiento y práctica. Certificaciones
Ámbitos de aplicación	General. Todo tipo de organizaciones y pymes. instituciones educativas
Entornos de aplicabilidad	Todos. Incluso los que todavía no se han implementado.
Uso por los auditores	Es la metodología de más amplio uso en el mundo de PYMES y la comunidad en general, al ser un proyecto permite que las personas contribuyan y de esta manera ir creciendo
Ventajas	Tiene una de las comunidades más grande, lo que le permite estar altamente documentada, poniendo a punto el uso de plantillas y medidas en las pruebas realizadas. Tiene en cuenta todos los estándares de seguridad de la información y su nivel de detalle es tal que está a punto de ser reconocida por la ISO
Inconvenientes	No hace referencia clara los objetivos que se deben cumplir para cada tipo de prueba. El cambio entre cada versión es intenso, lo que requiere una lectura prácticamente de cero, no recomienda ninguna herramienta y deja mucho a la creatividad del auditor

Fuente: Elaboración propia (2017)

Para el análisis final de la metodología OSSTMM se pudo establecer como una metodología una metodología referente para las pruebas de penetración , siendo la de más amplio uso en el mundo de PYMES y la comunidad en general, al ser un proyecto permite que las personas contribuyan y de esta manera ir creciendo, con un muy alto nivel de exigencia, ya que todos sus procesos y controles permiten establecer con gran precisión el nivel de seguridad de la plataforma, pero requiere de un conocimiento medio para realizar alguna de sus fases. Tiene en cuenta todos los estándares de seguridad de la información. Es por esto y mucho más, que pese hacer requerir ciertas habilidades, es una metodología perfecta para formar parte del modelo.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

Cuadro 10
Análisis final NIST

ITEMS	NIST
Rigor	Alta. Última actualización 2016
Nivel de detalle	Muy detallada, ya que recoge ideas del gobierno de EE.UU y la industria. Protección datos
Facilidad de uso	Alta. Serie de documentos que recogen las pruebas a nivel de seguridad pero muy disperso
Ámbitos de aplicación	Pymes, organizaciones e instituciones varias
Entornos de aplicabilidad	Todos. Genérico para auditorías de todo tipo
Uso por los auditores	Ampliamente usado ya que respeta los modelos requeridos por el gobierno de EE.UU
Ventajas	Por estar públicamente soportada y mantenida por el gobierno de EE.UU la hace una guía de alta confianza respecto a las pruebas a realizar
Inconvenientes	No se concentra en una serie de pasos, esto dificulta al auditor sin experiencia, al ser muchos documentos, es poco usual conocer todas las recomendaciones y pruebas

Fuente: Elaboración propia (2017)

Siguiendo con el orden y para finalizar el análisis de la metodología NIST demostró que es una metodología con un alto nivel de detalle ya recoge ideas del gobierno de los Estados Unidos , está formada por una serie de documentos en los que recoge las pruebas que se deben hacer a nivel de seguridad, el problema de esto es que es muy disperso y no hay un orden definido de como buscar, a pesar de ello es altamente usado en ese país ya que cumple con todas las exigencias que por ley el gobierno exige. No está orientada a instituciones que deseen auditar sin depender de un agente externo ya que no permite conocer todas sus pruebas y recomendaciones.

Así se ha calificado entonces la OSSTMM, OWASP, OWISAM, como las indicadas a integrar la propuesta, cada una especialista en su área según el anterior análisis, cubriendo con los cuatro puntos que fueron determinados como de vital importancia en el funcionamiento de la universidad: laboratorios y servidores, servicios web, redes inalámbricas e infraestructura física.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017

REFERENCIAS BIBLIOGRÁFICAS

Sanchez. R., Alberto y Behrens L. Morella. (2014) Carta de navegación para una organización segura MAP3S

García, R. Juan, L (2014) Ataques a redes de datos IPV4 e IPV6

Rando, Alonso y Aparicio (2016) Hacking Web Technologies. SQL Injection.

Gonzales (2014) Metodología para análisis de seguridad en aplicaciones.http://www.seguridadparatodos.es/2013/02/OWASP-Parte1MetodologiaAppMobile.html

Restrepo, Jaime (2015) OSSTMM cerca de ser oficialmente aceptada por la ISO. http://www.dragonjar.org/osstmm-cerca-oficialmente-aceptada-iso.xhtml

Tarasco Andres y Tarasco Miguel (RootedCON 2013), OWISAM Open Wireless Security Assessment Methodology.

Muñoz, Jesus (2011) Metodología de auditoria OSSTMM. http://www.jesusdml.es/2011/06/16/metodologia-de-auditoria-de-seguridad-osstmm/

Cardenas, Elvis (2012) Metodologías para el análisis de riesgos en Seguridad Informática.http://msnseguridad.blogspot.com/2012/08/seguridad-informatica-la-seguridad.html

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 16 Edición No 2 – Año 2017