MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

Análisis de estrategias de gestión de seguridad informática con base en la metodología Open Source Security Testing Methodology Manual (OSSTMM) para la intranet de una Institución de Educación Superior.

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por el estudiante:
Diego Sebastián GORDÓN REVELO

Bajo la dirección de:
Rubén PACHECO VILLAMAR.

Universidad Espíritu Santo
Maestría en Auditoría de Tecnologías de la Información
Samborondón - Ecuador
Septiembre del 2017

Análisis de estrategias de gestión de seguridad informática con base en la metodología Open Source Security Testing Methodology Manual (OSSTMM) para la intranet de una Institución de Educación Superior.

Analysis of strategies of computer security management based on the Open Source Security Testing Manual Methodology (OSSTMM) for the intranet of a Higher Education Institution.

Diego Sebastián GORDÓN REVELO[1]
Rubén PACHECO VILLAMAR[2]

Resumen

El presente estudio se enfocó en tomar como referencia la metodología OSSTMM para aplicar una auditoria de seguridad informática e identificar brechas de seguridad en una Institución de Educación Superior, utilizando como tipo de prueba el Hacking ético. Mediante una investigación de campo, se estableció la situación actual de políticas de la gestión de seguridad informática de la Institución de Educación Superior objeto de estudio, en donde los principales activos de información analizados fueron: el servidor con el sistema de gestión financiera y académica, los laboratorios de informática, salas de docentes y el área administrativa. Con base en la auditoría realizada, se encontró que la institución de educación superior no lleva un control adecuado de políticas de seguridad informática y aplicación de las mismas, obteniéndose como principal hallazgo los valores de evaluación de riesgo (Rav) equivalente al 72,15% de seguridad. En el análisis de seguridad informática llevado a cabo, se concluye que la porosidad y las limitaciones permiten evaluar el nivel de impacto y criticidad de las vulnerabilidades encontradas, las cuales pueden ser mitigadas aplicando estrategias de gestión de seguridad informática y conjuntamente con el aumento de controles de seguridad se puede mejorar la valoración del Rav a una ponderación del 77,00%; de esta manera, se garantiza la confiabilidad, integridad y disponibilidad de la información.

Palabras clave: OSSTMM, seguridad informática, estrategias de seguridad

Abstract

The present study focused on taking as reference the OSSTMM methodology to apply an auditory of a computer security, and to identify security breaches in a Higher Education Institution, using as a type of test the ethical Hacking. Through a field investigation, it was established the current situation of policies of the computer security management of the Higher Education Institution which is the object of the study, where the main information assets analyzed were: the server with the financial and academic management system, computer labs, teaching rooms and the administrative area. Based on the audit that was done, it was found that the institution of higher superior doesn't carry an adequate control of information security, policies and their application, obtaining as main finding the values of risk assessment (Rav) equivalent to 72.15% of security. In the computer security analysis carried out, it is concluded that the porosity and limitations allow to evaluate the level of impact and criticality of the vulnerabilities found, which can be mitigated by applying computer security management strategies and in conjunction with increased controls the Rav's valuation can be improved to a weighting of 77.00%; in this way, the reliability, integrity and availability of the information is guaranteed.

Key words OSSTMM, Informatic security, Security strategies.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail diego.gordon @uees.edu.ec.
[2] Magíster en Seguridad Informática Aplicada. Director de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo-Ecuador.

INTRODUCCIÓN

Las tecnologías de información y comunicación (TICs) son un factor de vital importancia en la transformación de la nueva economía global y en los rápidos cambios que están tomando lugar en la sociedad (UNESCO, 2004). Esto ha provocado un crecimiento continuo del papel de la seguridad de la información, considerada, esta última, el activo más valioso de la era digital, y a que las infraestructuras tecnológicas tengan que protegerse adecuadamente contra amenazas lógicas y físicas. (Balcerek, Frankowski, Kwiecién, Smutnicki, & Teodorczyk, 2012).

Toda organización es vulnerable a los ataques informáticos y más aún las Instituciones de Educación Superior que poseen información de personal administrativo, docentes y estudiantes. Según ISACA (2015) el número de incidentes de seguridad detectados ha aumentado en un 66%, año tras año, desde el 2009, a su vez, las pérdidas suman 42,8 mil millones de dólares en todo el mundo según se desprende de encuestas y estimaciones realizadas en el año 2014. Por otra parte, Cisco (2016) en su Informe Anual de Seguridad manifiesta que el 92% de las infraestructuras tecnológicas obsoletas y sin actualizaciones, ejecutan software con vulnerabilidades conocidas; es decir, con falencias, que con una correcta disciplina de gestión pudieron haber sido subsanadas.

Así mismo, ESET (2015) menciona que la explotación de las vulnerabilidades es uno de los incidentes de mayor ocurrencia en las empresas grandes y en promedio, una de cada cinco empresas sufrió uno de estos ataques en el 2014. Respecto a este panorama, Toth & Sznek (2014) mencionan, que la necesidad de protección ha impulsado el desarrollo de estándares, métodos, procedimientos y políticas cuyo propósito es obtener información confiable sobre el estado y nivel de preparación en materia de seguridad que se tienen en las organizaciones, con el objetivo final de implementar cambios y mejoras.

Los ataques relacionados con la seguridad informática, con el pasar del tiempo, se han ido ejecutando mediante técnicas más y más sofisticadas, para intentar explotar las vulnerabilidades presentes en cualquier arquitectura. Sobre esto, el Instituto Español de Estudios Estratégicos (2011) manifiesta que, una de las maneras más destacadas de ataques son los programas maliciosos insertados en un sistema operativo para ocultar procesos y archivos.

La mayoría de organizaciones del sector educativo no queda exenta de eventos relacionados con la seguridad informática. En la actualidad, estudiantes, docentes e investigadores requieren de las nuevas tecnologías de la información (TI) para enviar y compartir datos. Hoy en día las nuevas tecnologías evolucionan constantemente y los modelos de seguridad informática regulares que se aplican en las Instituciones de Educación Superior pueden quedar obsoletas rápidamente, por lo que es necesario realizar auditorías que permitan evaluar el estado actual de su seguridad en las redes de datos. Según ESET (2015) el sector de la educación superior a nivel mundial ocupa el tercer lugar en incidentes de seguridad informática hallándose expuestas en un 60% a contaminación por malware.

En el Manual de Políticas de Seguridad Informática de la Institución de Educación Superior objeto de este estudio, se ha definido como una de las tareas prioritarias, el realizar proyectos encaminados a reforzar la seguridad de su infraestructura tecnológica, mejorando el manejo y almacenamiento de información que se transmite a través de las redes de comunicación, o se mantiene en bases de datos; además la gran cantidad de información que se envía y recibe a través de la intranet necesita de verificaciones de los sistemas y controles de seguridad con el fin de obtener una correcta funcionalidad de la seguridad operacional (UNIANDES, 2013). Las características del escenario en el cual se desarrolló la investigación se visualizan en un diagrama de red (ver anexo 1). En el que se incluyen los diferentes lugares en cuales se desarrolló la auditoría.

Coronel (2016) realizó un trabajo, relacionado con la aplicación del hacking ético para la detección de vulnerabilidades mediante herramientas de código abierto (*open source*) en las aplicaciones web de

una institución de educación superior del Ecuador, siendo el principal resultado el fortalecimiento de todo el escenario de seguridad en cuanto a la estructura de las aplicaciones, demostrado por medio de pruebas y análisis de una serie de herramientas de distribuciones Linux, como son Kali y herramientas de plataformas Windows con licencias libres.

Otro trabajo relacionado es el de Enrique & Sánchez (2017) sobre los Riesgos de Ciberseguridad en las Empresas, siendo el principal resultado la recopilación de los riesgos de seguridad a los que se exponen las empresas en la actualidad, las amenazas digitales, la evolución del malware y las tendencias digitales de los ataques informáticos.

A diferencia de los trabajos de Coronel (2016) y del realizado por Enrique & Sánchez (2017), en el artículo se consideran los riesgos de la seguridad operacional, para lo cual se evaluó la seguridad informática lógica y física de la intranet de la institución motivo de estudio.

En este trabajo investigativo se presenta la cuantificación de los riesgos de la seguridad informática en base a la metodología Open Source Security Testing Methodology Manual (OSSTMM) para la gestión de la seguridad informática de la intranet de una Institución de Educación Superior.

MARCO TEÓRICO

Seguridad Informática

Según Costas Santos (2010) la seguridad informática consiste en asegurar que los recursos del sistema de información de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentran autorizadas. Por lo tanto la seguridad informática consiste en preparar un terreno apropiado para garantizar la integridad de los datos optando por implementar buenas prácticas de seguridad, protocolos y recursos. Por otro lado Baldeón (2012) menciona, la seguridad informática concierne a la protección de la información, almacenada en una computadora, o en una red de ellas, y también a la protección del acceso a todos los recursos del sistema. A esto Morlanes (2012) afirma que se deben evaluar y cuantificar los bienes a proteger e implantar medidas preventivas y correctivas que eliminen los riesgos asociados o que los reduzcan hasta niveles manejables. En base a estas definiciones, se establece a la seguridad informática como la disciplina que se encarga de la confidencialidad, integridad y disponibilidad de la información; por lo tanto, no se puede hablar de seguridad si no se tiene la capacidad de medir de alguna manera el estado de la misma.

Al respecto Portantier (2013) menciona que la seguridad informática está teniendo una importancia cada vez mayor, haciendo necesario establecer mejores prácticas y crear herramientas destinadas a proteger la información de las personas y de las organizaciones. Los usuarios, trabajadores y sobre todo gerentes de cualquier tipo de organización deben ser conscientes de que el funcionamiento correcto de un sistema informático depende en gran medida de la protección que estos tengan, sobre todo en infraestructuras que manejan volúmenes de datos considerables.

Metodologías Abiertas de Auditoría de Seguridad Informática

Para Maya y Jaramillo (2015) el propósito de una auditoría de seguridad no es culpar o desmerecer el diseño de una red, sino proveer elementos de juicio y acción para garantizar la eficacia, integridad y cumplimiento de políticas aplicadas. Según este criterio la auditoría de seguridad informática analiza los procesos relacionados con la seguridad física y lógica de una red de datos, garantizando la confidencialidad, integridad y disponibilidad de la información.

Piattini (2008) manifiesta que la Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De tal manera que los datos permanezcan íntegros. Además Piattini (2008) menciona que el rápido crecimiento de la

seguridad informática en los últimos años, ha hecho necesario la creación de las metodologías de seguridad informática. Una metodología persigue un conjunto de procedimientos para alcanzar un objetivo; por lo tanto, existen varias metodologías unas bajo licencia y otras open source; entre las más importantes se tienen:

Metodología OSSTMM

Según Herzog (2010) la metodología OSSTMM está alineada a la norma ISO 27001, y está conceptualiza a la seguridad como una función de separación; es decir, separar un activo de información de posibles amenazas, estableciendo controles que permitan gestionar la confidencialidad, integridad y disponibilidad de la información, además es un manual o una guía amplia, que permite la realización de pruebas de seguridad informática de una manera consistente y repetible, el objetivo de este manual es proporcionar una metodología científica en donde se busca el mejoramiento de la seguridad operacional (OpSec), la cual es adaptable a cualquier tipo de organización.

Según (Emiliani & Sierra, 2015) OpSec es una combinación de separación y controles que trabaja dentro de un entorno operativo. A esto ISECOM (2012) manifiesta que la metodología OSSTMM se centra en detalles netamente técnicos de los elementos que necesitan ser auditados, buscando el mejoramiento del aseguramiento de la información, en donde, las diferentes pruebas a aplicarse deben tratar de recoger información de todos los canales que intervienen en la operación; los canales a los que se refiere la metodología son: factores humanos, factores físicos, redes inalámbricas, servicios, aplicaciones, telecomunicaciones y redes de datos, donde se aplican diferentes actividades que componen una auditoría de seguridad asociadas a la metodología OSSTMM basados en tiempo y costo; incorporando un sistema de métricas cuantitativas, denominadas valores de evaluación de riesgo (RAV), para Fuertes (2014) estas métricas son necesarias para la evaluación de riesgos demandadas para la justificación de resultados con los que se calcula la puntuación del estado de seguridad de la organización.

Los Risk Asessment Values (RAV) se calculan teniendo en cuenta el equilibrio cuantitativo entre la porosidad, que son todos los puntos interactivos entre un activo de información y una amenaza, las limitaciones que identifica los límites de cada canal que interactúa con la seguridad y los controles que son los encargados de evitar interacciones. (Emiliani & Sierra, 2015). Por lo tanto para el cálculo final del Rav la metodología OSSTMM propone una plantilla para el ingreso de los datos cuantificados en donde su principal función es la suma de Opsec (visibilidad, acceso, confianza) + controles * 0.1 – limitaciones.

Tipos de prueba de auditoría de la metodología OSSTMM

La metodología OSSTMM, como tipos de prueba utiliza el hacking ético, caja negra, caja gris, tándem e inversión; cuyas características son:

Hacking Ético. Según Yánez (2015) el hacking ético consiste en efectuar pruebas de intrusión controladas a sistemas informáticos para encontrar vulnerabilidades, con la finalidad de protegerlos de posibles ataques. Para Jara (2012) en el hacking ético, el analista o auditor no tiene conocimiento del objetivo a auditar, solamente conoce el alcance de las pruebas a realizar, la organización auditada es consciente de las pruebas que se realizarán en donde el personal estará previamente alertado. El hacking ético comprende las siguientes etapas: recolección de información, enumeración, análisis de vulnerabilidades, explotación y post explotación.

Caja Negra. O test de intrusión, para Benchimol (2010) este tipo de prueba es similar al hacking ético, con la única diferencia de que el equipo de seguridad de la organización no está alertado, en donde se busca acceder con privilegios a un cierto objetivo, midiendo la capacidad de respuesta ante incidentes de fallos de seguridad.

Caja Gris. Según López Santoyo (2015) en este tipo de pruebas, el auditor posee algún tipo de

información de la organización y su infraestructura. El objetivo es analizar las vulnerabilidades en la infraestructura de tecnologías de la información (TI). Este tipo de prueba de Hacking generalmente es utilizado por los auditores internos de una organización, ya que conocen el entorno de la infraestructura a ser auditada.

Tándem. El objetivo de esta prueba, es evaluar, entre el auditor y administrador, los tipos de controles de seguridad que están disponibles. La verdadera naturaleza de la prueba es la minuciosidad que el analista tiene a la vista (Emiliani & Sierra, 2015). Una auditoria de este tipo, pone a prueba la protección de los controles que se encuentran establecidos en el momento de la auditoría informática.

Inversión. Se evalúa al administrador de TI para medir su respuesta ante fallos de seguridad, el analista se acopla al objetivo con pleno conocimiento de sus procesos y la seguridad operacional (Emiliani & Sierra, 2015). Este tipo de auditoria evalúa el estado de preparación ante posibles fallos de seguridad en la infraestructura tecnología a auditarse y la capacidad de respuesta ante esos fallos.

Metodología NIST 800-115

Para Guillinta & Merino (2016) es una metodología o guía técnica para evaluaciones y pruebas de seguridad de la información la cual es soportada por una amplia variedad de estándares, metodologías, lineamientos y prácticas existentes permitiendo mejorar la adaptabilidad a los encargados de promover las tecnologías de información para infraestructuras críticas de una organización. Además esta guía describe el proceso de evaluación de la seguridad de la información, la cual está establecida por tres fases:

- **Planificación.** En esta fase se recopila información sobre los activos a tomarse en cuenta para ser evaluados.

- **Ejecución**. El principal objetivo es obtener información de las vulnerabilidades que afectan a los activos de información.

- **Post ejecución**. Permite establecer recomendaciones para mitigar las vulnerabilidades encontradas en la fase de ejecución. En esta fase propone un plan de contingencia que permite salva guardar de mejor manera los activos de información.

Metodología OWASP

OWASP (2013) menciona que esta metodología es un proyecto abierto de seguridad en aplicaciones web, dedicado a facultar a las organizaciones a desarrollar, adquirir y mantener aplicaciones confiables, identificando los riesgos críticos que enfrentan las organizaciones. El marco de trabajo de esta metodología pretende promover a personas a evaluar y tomar medidas de seguridad, haciendo necesario acudir a procesos involucrados en el testeo de aplicaciones web, tomando en cuenta el alcance, los principios del test, explicar las técnicas a aplicar y el marco de pruebas.

Análisis comparativo de las metodologías OSSTMM, NIST 800-115 y OWASP.

Con base al juicio de expertos, las metodologías descritas anteriormente se comparan en función de los factores de su aplicabilidad, siendo estos:

- **Factor digital.** Se evalúa el ámbito digital de la seguridad informática y seguridad de la información.

- **Factor físico.** Permite la evaluación de la seguridad física de las instalaciones de la organización a auditarse.

- **Factor social.** Evalúa el ámbito de ingeniera social.

- **Métricas.** Evalúa mediante métricas la seguridad informática actual que presenta una organización.

- **Informes.** Al finalizar la auditoría es necesario la realización de un informe estructurado y parametrizado.

- **Guía técnica.** Permite seguir sistemáticamente los pasos necesarios para realizar la auditoría en una organización.

Tabla 1. Análisis comparativo de las metodologías de seguridad informática.

FACTORES	METODOLOGÍAS		
	OSSTMM	NIST 800-115	OWASP
Factor Digital	X	X	X
Factor Físico	X		
Factor Social	X	X	
Métricas	X		
Informes	X	X	
Guía Técnica			X

Fuente: (López Santoyo, 2015).

Con base a lo expuesto por López Santoyo (2015) se establecen las siguientes diferencias entre las metodologías analizadas:

- Todas las metodologías abarcan el factor digital de la seguridad, pero solo la metodología OSSTMM abarca el factor físico.

- El factor social lo incluyen OSSTMM Y NIST 800-115; es decir, estas metodologías permiten realizar pruebas de seguridad al canal humano.

- Las métricas son propias de la metodología OSSTMM; es decir, permite la cuantificación de los resultados expresados en Rav.

- Una vez finalizada la auditoría es importante la presentación mediante un informe que transmita la información al cliente. Solo la metodología OWASP no habla como deberían ser los informes.

- Uno de los factores importantes por los que se puede comparar una metodología, es si cuenta con una guía técnica que explique cómo hay que realizar las pruebas que indica la metodología, en la tabla 1 se puede observar que solo OWASP cuenta con la guía técnica.

OSSTMM como metodología de gestión de seguridad informática.

Teniendo como referencia el análisis comparativo de las metodologías realizado en la tabla 1, la OSSTMM, es la única que abarca los factores esenciales para cumplir con el objetivo que se propone en este trabajo, esta metodología se enfoca en el análisis completo de la seguridad, en donde actúa en cinco ámbitos: humano, físico, medios inalámbricos, telecomunicaciones, redes de datos; tomando en cuenta que la metodología OSSTMM aún no es estandarizada, por lo tanto, no incluye aplicaciones.

Además la metodología OSSTMM posee un valor añadido a favor, como lo son las métricas cuantitativas de seguridad Risk Asessment Value (RAV), las mismas que son imprescindibles para gestionar la seguridad informática y de la información dentro de cualquier tipo de organización, sin estas no se podría cuantificar de forma global el estado actual de seguridad operacional.

Tabla 2: Ámbitos de la metodología OSSTMM

Clase	Canal	Descripción
PHYSSEC Seguridad física	Humano	Involucra la interacción entre personas.
	Físico	Hace referencia a los elementos tangibles tales como el hardware, maquinaria, puertas, ventanas, pizarras, escritos, etc.
SPECSEC Seguridad inalámbrica	Medios inalámbricos	Son las comunicaciones, señales y emanaciones que tienen lugar dentro del espectro electromagnético.
COMSEC Seguridad en las comunicaciones	Telecomunicaciones	Redes de comunicación donde la interacción se produce sobre líneas del tipo telefónico.
	Redes de datos	Establecidas sobre redes de datos cableadas.

Fuente: (Toth & Szneck, 2014).

METODOLOGÍA

Tipo y Alcance de la Investigación

El tipo de investigación empleada en este artículo es de carácter cuantitativo, puesto que la metodología OSSTMM, presenta los resultados representados en métricas o RAV; además con esta metodología, se pretende cubrir la mayoría de

los entornos que posee la Institución de Educación Superior objeto de estudio.

El alcance de la investigación es de tipo descriptivo, puesto que su propósito es especificar propiedades, características y rasgos importantes de la auditoría de seguridad informática realizada en una Institución de Educación Superior (Hernández Sampieri, Fernández & Baptista, 2010). En esta investigación se recopiló información para la cuantificación de los riesgos de la seguridad informática tomando en cuenta la metodología OSSTMM y el hacking ético, con lo que se pretende conocer los riesgos de seguridad informática de la organización motivo de estudio. La población es una Institución de Educación Superior, y la muestra se tomó datos de la gestión administrativa, docentes, estudiantes. Las técnicas de recolección de datos aplicados a este estudio fueron las encuestas y entrevistas.

Fases de la Metodología OSSTMM

Cada una de las fases de la metodología OSSTMM, se asocia con las fases del hacking ético como tipo de prueba que se aplica en este caso de estudio, esta metodología tiene como fases:

Fase de Inducción

El propósito de esta fase es la recolección de datos, tales como: cultura organizacional, reglas, normas y políticas, además permite establecer las limitaciones de la auditoría, esta fase de la metodología OSSTMM se la aplica conjuntamente con la etapa de recolección de información del hacking ético, para lo cual:

- Se revisó el entorno de la Institución de Educación de Educación Superior objeto de estudio, conociendo la cultura organizacional y políticas de seguridad informática implantadas.

- Se analizaron detalles del canal humano, determinando los horarios en los que laboran o están activos el personal administrativo y los estudiantes.

- Se realizó un *check list* de verificación, en donde se averiguó la existencia de controles establecidos para mitigar ataques en contra de la seguridad informática.

Fase Interacción

Esta fase es el núcleo de las pruebas de seguridad informática, en donde se determina el alcance de las interacciones de los activos de información y posibles brechas de seguridad, en esta fase se verifica los accesos a aplicaciones y sistemas y los controles establecidos para los mismos.

- Se verificó la visibilidad de los posibles objetivos propensos a ataques de seguridad.

- Se analizó los puntos de accesos que posee la Institución de Educación Superior; es decir, escaneo de los puertos abiertos.

- Se realizó la verificación de los controles que se aplican para garantizar la confidencialidad, integridad y disponibilidad de la información.

Fase de Investigación

En esta etapa se realizan diferentes actividades, tales como la verificación de procesos y exposiciones que puedan provocar algún tipo de interacción, además se analiza la información que se descubre; es decir, se ponen a la luz los activos de información que se encuentran mal situados o mal administrados. Además se buscó información disponible de manera abierta en buscadores utilizando técnicas de google hacking, teniendo como objetivo la verificación de información relevante que estuviera sin ningún tipo de restricción en la red.

Fase de Intervención

En esta fase se determina la efectividad de los controles, el mapeo del impacto del mal uso de los mismos y se realiza una revisión de la auditoría realizada donde se pretende saber si la auditoria deja un rastro útil confiable.

- Se expone la seguridad operacional actual de la Institución con el cálculo de RAVs.

- Se define estrategias para disminuir las limitaciones y se aumenta controles.

- En esta etapa de la metodología OSSTMM, se cuantifica los resultados obtenidos.

ANÁLISIS DE RESULTADOS

Una vez ejecutada la auditoría de seguridad informática, con base en la metodología OSSTMM en la intranet de una Institución de Educación Superior, se destacan los siguientes resultados:

Fase de Inducción – Recolección de información

Entorno Organizacional

- En el área de Tecnologías de la Información de la Institución de Educación Superior estudiada, se establecen y aplican políticas de seguridad informática y de la información de carácter básico, tales como: listas de filtros de contenido en la intranet, firewall perimetral, repositorios externos y controles de acceso lógico.

- Los planes de continuidad no son definidos de manera eficiente puesto que no se disponen de políticas de respaldos tanto de información como de energía eléctrica.

- La seguridad operacional de la organización no dispone de una protección adecuada apoyada con IPS, IDS, antivirus bajo licencia para la detección de posibles amenazas.

De acuerdo a la información recopilada en esta fase (ver anexo 2), la Institución objeto de estudio aplica políticas básicas de seguridad informática; encontrando similitudes de resultados con un estudio reciente realizado por ESET (2017) en donde indica un 74% de las organizaciones en Latinoamérica, incluyendo el Ecuador, ha implementado la creación de políticas de seguridad aplicando controles como antivirus, firewall, controles de acceso entre otros. Con lo indicado anteriormente se hace evidente la necesidad de mejoramiento de los controles de seguridad informática que permitan gestionar de una mejor manera la seguridad de la Institución de Educación Superior estudiada.

Fase Interacción – Scanning y enumeración

Tabla 3. Fase de Interacción

RIESGO	Seguridad Física		Seguridad en el Espectro	Seguridad en las Comunicaciones	Total
	Humano	Físico	Wireless	Redes de datos	
POROSIDAD					
Visibilidad	2	4	3	15	**24**
Acceso	8	10	12	87	**117**
Confianza	1	0	0	4	**5**
Total Porosidad	**11**	**14**	**15**	**106**	**146**

Fuente: Check list de verificación de seguridad informática y Nmap.

En la tabla 3 se detallan todos los puntos interactivos encontrados en el momento de la evaluación de los canales humano, físico, Wireless, y redes de datos (ver anexo 3). Encontrándose un total de 146 puntos interactivos de acceso y visibilidad que pueden dar lugar, en algún momento, a un fallo de seguridad informática y tan solo 5 puntos interactivos de confianza.
Los resultados anteriores pueden desbordar en una posible red botnet de la Institución de Educación Superior estudiada ya que según ESET (2017), en el Ecuador existe 46,6% de las

organizaciones que en algún momento fueron parte de una de estas redes maliciosas a causa de no implementar buenas prácticas de seguridad informática.

Por lo expuesto anteriormente se hace necesario analizar estrategias que permitan regularizar la seguridad operacional de la organización objeto de estudio.

Tabla 4. Controles de seguridad cuantificados por canal humano, físico, Wireless, redes de datos.

RIESGO	Seguridad Física		Seguridad en el Espectro	Seguridad en las Comunicaciones	Total
	Humano	Físico	Wireless	Redes de datos	
CONTROLES					
Clase A (Interacción)					
Autenticación	14	0	3	14	31
Indemnización	1	3	0	1	5
Resistencia	1	0	1	0	2
Subyugación	0	0	0	2	2
Continuidad	0	15	0	8	23
Total Clase A	**16**	**18**	**4**	**25**	**63**
Clase B (Proceso)					
No repudio	0	0	1	1	2
Confidencialidad	1	0	0	3	4
Privacidad	3	0	1	1	5
Integridad	0	0	3	1	4
Alarma	2	1	3	1	7
Total Clase B	**6**	**1**	**8**	**7**	**22**
Total Controles	**22**	**19**	**12**	**32**	**85**

Fuente: Fuente: Check list de verificación de seguridad informática y Nmap.

Al analizar los datos de la tabla 4, en donde se cuantifican los controles encontrados durante la auditoria de tipo hacking ético, se puede observar que los controles de interacción o tipo A son un total de 63 que afectan directamente a la visibilidad, acceso y confianza (porosidad); en cambio, los controles de proceso o tipo B se cuantifican un total de 22 los cuales proporcionan seguridad ante amenazas (ver anexo 4).

Fase de Investigación – Análisis de Vulnerabilidades.

Tabla 5. Fase Investigación – Limitaciones

RIESGO	Seguridad Física		Seguridad en el Espectro	Seguridad en las Comunicaciones	Total
	Humano	Físico	Wireless	Redes de datos	
LIMITACIONES					
Exposición	3	1	**0**	3	7
Vulnerabilidad	0	1	**3**	14	18
Debilidad	2	2	**0**	2	6
Preocupación	0	2	**0**	1	3
Anomalías	0	0	**0**	0	0
Total Limitaciones	5	6	**3**	20	34

Fuente: Fuente: Check list de verificación de seguridad informática, Nessus y armitage.

.

En la tabla anterior se expone la cuantificación de las limitaciones, obteniéndose un total de 34, de las cuales 18 son vulnerabilidades que afectan directamente a la confiabilidad, integridad y disponibilidad de la información (ver anexo 5); en torno a esto ESET (2017) reporta que en Latinoamérica existe un crecimiento en cuanto a infecciones por malware, siendo Nicaragua el país que soporta más ataques de este tipo y apenas un 38% de las organizaciones en Latinoamérica realizan auditorías internas o externas enfocadas

a cuantificar los riesgos en cuanto a seguridad informática.

Fase de Intervención

En esta fase se da a conocer el estado actual de la seguridad operacional de la Institución de Educación Superior objeto de estudio (ver anexos 6 y 7), una vez concluida la cuantificación de la porosidad los controles y las limitaciones que se establecen en dicha Institución, los datos obtenidos son ingresados a la matriz de cálculo de RAV, propia de la metodología OSSTMM, obteniendo como resultado el 72,15% de seguridad actual y un 28,04% de brechas de seguridad informática.

Estrategias de gestión de seguridad informática en base a la metodología OSSTMM

La metodología OSSTMM propone para la optimización de la seguridad de los activos de información, que se disminuyan las limitaciones entre activos de información a proteger y posibles brechas de seguridad, así como también, la no separación de activos de información y brechas de seguridad informática, dando como resultado la porosidad. Según Herzog (2010) existen cuatro formas para crear separación de activos de información, siendo tres las recomendadas, estas son:

- **Mover el activo y crear una barrera entre él y las amenazas**.

Los controles establecidos en la Institución de Educación Superior estudiada son pocos para toda la seguridad operacional, por lo que es considerable aumentar controles de proceso que permitan gestionar de una mejor manera la intranet con el fin de que los puntos interactivos y las limitaciones encontradas sean minimizados.

- **Cambiar la amenaza a un estado inofensivo**

Viable para este estudio, puesto que existen una cantidad considerable de puntos interactivos los cuales deben ser reducidos mediante el aumento de controles de confidencialidad, privacidad e integridad que permitan reducir amenazas y vulnerabilidades aumentando la seguridad operacional de la intranet en la Institución de Educación Superior objeto de estudio.

- **Destruir la amenaza**

Las amenazas de carácter crítico que fueron halladas, deben ser destruidas para salvaguardar los activos de información precautelando la confidencialidad, integridad y disponibilidad de la información. Se cataloga como amenazas potenciales a los sistemas operativos, servicios y aplicaciones obsoletas.

Mejoramiento del Risk Asessment Values (RAV)

Como se lo ha mencionado anteriormente, el valor agregado de la metodología OSSTMM es la cuantificación de los riesgos que se obtienen al realizar una auditoría informática, para este caso de estudio el resultado de protección en la intranet es de 72,15% de seguridad y de inseguridad es el 28,04%; para mejorar los resultados obtenidos se aplican las tres estrategias antes citadas en los puntos que se detallan en la tabla 6.

Tabla 6. Riesgos y Controles a mejorar

RIESGO	Seguridad Física		Seguridad en el Espectro	Seguridad en las Comunicaciones	Total
	Humano	Físico	Wireless	Redes de datos	
POROSIDAD					
Acceso	8	10	12	87	**117**
CONTROLES					
Confidencialidad	1	0	0	3	**4**
Privacidad	3	0	1	1	**5**
Integridad	0	0	3	1	**4**
Alarma	2	1	3	1	**7**
LIMITACIONES					
Vulnerabilidad	0	1	3	14	**18**
Exposición	3	1	0	3	**7**
Debilidad	2	2	0	2	**6**

Fuente: Propuesta por el autor.

Los resultados obtenidos de la porosidad en accesos sobrepasan los controles establecidos, para cambiar este estado, es necesario aplicar más controles de confidencialidad y privacidad en cada uno de los canales auditados, sobre todo en el canal redes de datos, puesto que existen puertos abiertos, algunos de manera innecesaria, los cuales se los puede cambiar a un estado inofensivo cerrándolos o controlando de mejor manera para evitar que afecte a la integridad, disponibilidad y confidencialidad de la información.

Así mismo existen algunas vulnerabilidades, exposiciones y debilidades encontradas en la auditoría realizada, que en su mayoría son sistemas operativos, aplicaciones y servicios obsoletos, antivirus sin actualizaciones, entre otros; los cuales se los puede controlar aumentando controles de alarma y de integridad o a su vez actualizar servicios, aplicaciones y sistemas operativos, para cual se debe cambiar las vulnerabilidades a un estado inofensivo.

Tabla 7. Mejoramiento de riesgos y controles

RIESGO	Seguridad Física		Seguridad en el Espectro	Seguridad en las Comunicaciones	Total
	Humano	Físico	Wireless	Redes de datos	
POROSIDAD					
Acceso	4	5	12	40	**61**
CONTROLES					
Confidencialidad	2	2	3	4	**11**
Privacidad	5	3	6	12	**26**
Integridad	3	3	5	10	**21**
Alarma	4	3	6	10	**23**
LIMITACIONES					
Vulnerabilidad	0	1	3	5	**9**
Exposición	1	1	0	2	**4**
Debilidad	2	2	0	2	**3**

Fuente: Propuesta por el autor.

En la tabla anterior se propone la cuantificación para el mejoramiento de la seguridad informática en la Institución de Educación Superior estudiada, obteniéndose como resultado de los cambios realizados un 77,00% de seguridad (ver anexos 8 y 9), lo cual disminuye el riesgo de inseguridad, teniendo en claro que no existe una seguridad perfecta, ya que el exceso de controles podría desencadenar otro tipo de fallos que pueden estar ocultos pero actuando activamente sin que el administrador de la intranet se dé cuenta.

CONCLUSIONES

En este trabajo se realizó una auditoría de seguridad informática a una institución de educación superior, mediante la aplicación de la metodología OSSTMM y pruebas de hacking ético, estableciendo métricas para evaluar el nivel de impacto y criticidad de las vulnerabilidades encontradas en donde el principal hallazgo encontrado fue 72,15% de seguridad, equivalente

a una seguridad informática media. Por lo tanto, se propone el mejoramiento de los valores de evaluación de riesgo (RAV) mediante la aplicación de estrategias, tales como: la creación de barreras entre el activo de información y la amenaza, cambiar la amenaza a un estado inofensivo y destruir las amenazas que pueden vulnerar a la seguridad informática de la intranet, en donde punto de equilibrio estratégico es la disminución de la porosidad y de las limitaciones, obteniéndose un aumento del RAV de 77,00%. Adicionalmente, la disminución de las brechas de seguridad debe ser tratada de manera especial para cada activo de información, garantizando la confiabilidad, integridad y disponibilidad de la información.

Además, como parte de la investigación se cuantificaron los riesgos de la seguridad informática en los canales de información mediante la aplicación de la metodología OSSTMM y herramientas adecuadas para la evaluación de cada aspecto de la seguridad operacional, tales como: factores humanos, factores físicos, redes inalámbricas, servicios, aplicaciones, y redes de datos; encontrándose como resultados, que la mayoría de los elementos de la intranet evaluada, tienen riesgos altos de ser vulnerados y de sufrir ataques de seguridad informática.

El presente paper tuvo como limitaciones el estudio a dos extensiones de una Institución de Educación Superior; estas limitaciones se deben al lugar geográfico de ubicación de las demás extensiones, recursos económicos personales y permisos para establecer la investigación por parte de los Directivos. Además por razones de tiempo no se evaluaron todos los canales propuestos por la metodología OSSTMM, puesto que el canal de telecomunicaciones hace que sea más extensa la investigación debido a los elementos que poseen estos canales, por lo tanto el cálculo general del RAV no está evaluado al 100%.

Como trabajo futuro, se puede expandir este estudio a más Universidades y así entender globalmente todos los aspectos que se pueden mejorar en materia de seguridad informática dentro de las intranets de las instituciones educativas de nivel superior, ya sean de carácter público o privado del país y contribuir a la asignación presupuestaria de recursos orientados a la seguridad informática. Según el criterio de expertos, otro trabajo futuro, a tener en cuenta, es la realización de un estudio con la metodología OSSTMM que permita establecer una métrica de seguridad estandarizada para las Instituciones de Educación Superior con un enfoque a realizar un plan de mejora continua. Además en futuras evaluaciones de seguridad informática, también se debe tomar en cuenta al canal de telecomunicaciones y sus elementos, para así tener resultados más globalizados.

Referencias Bibliográficas

Benchimol. D. (2010). *Redes Cisco*. Banfield. Argentina: Gradi.

Baldeón, M. & Coronel, C. (2012). *Plan maestro de Seguridad Informática para la UTIC de la ESPE con lineamiento en la norma ISO 27002*.

Balcerek, B., Frankowski, G., Kwiecién, A. Smutnicki, A., & Teodorczyk, M. (2012). Security best practices: applying defense-in-depth strategy to protect the NGI_PL. Springer Berlin Heidelberg.128-141.

Costas Santos, J. (2010). *Seguridad Informática*. España: Service Ponit S.A.

Coronel, I. (2016). *Aplicar Hackeo Ético para Detección de Vulnerabilidades Mediante Herramientas Open Sourse en las Aplicaciones Web de una Institución de Educación Superior*. Disponible en: https://www.dspace.espol.edu.ec/retrieve/97627/D-103391.pdf. (Consultado 05/05/2017).

CISCO. (2016*). Informe anual de seguridad de Cisco 2016*. San José.

Emiliani, R. Sierra, Y. (2015). *Manual Metodológico para pruebas de seguridad OSSTMM 3 y Guía de Pruebas OWASP 4.*

Disponible en: https://es.scribd.com/document/265102425/Resumen-de-Guias-OSSTMM-OTGv4. (Consultado 25-04-2017).

Enrique, J, & Sánchez, J. (2017). *Riesgos de Ciberseguridad en las Empresas*. Madrid

ESET Security Report. (2015). *ESET Security Repor*t, Latinoamérica 2015.

ESET Security Report. (2017). ESET Security Report, Latinoamérica 2017.

Fuertes, A. (2014). *Elaboración de una Metodología de test de intrusión dentro de la Auditoría de Seguridad*. Disponible en: http://reunir.unir.net/bitstream/handle/123456789/2331/AntonioFuertesMaestroTFM.pdf?sequence=3&isAllowed=y. (Consultado 25-06-2017).

Guillinta, O. Merino, J (2016). *Modelo de Prevención y Defensa contra Ataques Cibernéticos basado en estándares de seguridad internacionales para IT-Expert.* Disponible en: repositorioacademico.upc.edu.pe/upc/bitstream/10757/620848/1/MERINO_R_J.pdf. (Consultado 25-05-2017)

Hernández Sampieri, R., Fernández, C., & Baptista, M. (2010). *Metodología de la Investigación.* Quinta edición. México: McGraw-Hill.

Herzog P, et al. (2001). *Open Source Security Testing Methodology*. Manual v2.1. Agregar País: Editorial

Herzog P, et al. (2010). *Open Source Security Testing Methodology*. Manual v3. United Estates: Creative Commons

ISACA. (2015). *State of Cybersecurity: Implications for 2015*. Usa: Creative Commons

ISECOM. (2012). *Hacker Highschool Security Awareness for teens*, lección 1. United Estates: Creative Commons.

ISO/IEC 27001. (2013). ISO 27001:2013 Information technology – Security.

Instituto español de estudios estratégicos. *(2011) Ciberseguridad, restos y amenazas a la seguridad nacional en el ciberespacio.* Barcelona: Ministerio de Defensa.

Jara. H. (2012). Ethical Hacking 2.0. Buenos Aires. Argentina: Fox Andina.

López Santoyo, R. (2015). *Propuesta de Implementación de metodología de auditoría de seguridad informática*. Madrid: Universidad Autónoma de Madrid.

Maya, E. Jaramillo, D. (2015). *Auditoría de Seguridad Informática para el Gobierno Autónomo Descentralizado de Santa Ana de Cotacachi, basada en la norma NTP-ISO/IEC 17799:2007 y la metodología OSSTMM V2*. Disponible en: http://repositorio.utn.edu.ec/bitstream/123456789/3774/2/04%20RED%20034%20Art%C3%ADculo%20Cient%C3%ADfico%20Espa%C3%B1ol.pdf. (Consultado 05-04-2017).

Morlanes, G. (2012). *Seguridad informática, Matanzas. CU. Revista de arquitectura e ingeniería*. Vol 6. N° 2. P 1-14.

OWASP. (2013). *Owasp Top 10 – 2013. Los 10 Riesgos más Críticos en Aplicaciones Web.* Disponible en https://www.owasp.org

Piattini, M. Peso Navarro, E. y Peso Ruiz. M. (2008). *Auditoría de tecnologías y sistemas de información*. Madrid: RA-MA Editorial.

Portantier, F. (2013). *Gestión de la Seguridad Informática.* Buenos Aires. Argentina: Fox Andina.

Toth, G. Sznek, J. (2014). *Implementación de la guía NIST SP 800-30 mediante la utilización de OSSTMM*. Disponible en: https://es.scribd.com/document/323455632/Tesis-Toth-pdf. (Consultado 30-06-2016).

UNESCO. (2004). Las Tecnologías de la Información y la Comunicación en la Formación Docente. Montevideo. Uruguay: Gráfica Futura.

Uniandes. (2013). Manual de Políticas de Seguridad Informática. Ambato.

Yánez, E. (2015). *Análisis de las Herramientas para el Proceso de Auditoría de Seguridad Informática Utilizando Kali Linux*. Disponible en: http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Ericka_Yanez_Cedeno_2015.pdf. (Consultado 04-27-2017).
.