Recibido 2 Dic 2017
Aceptado 19 Feb 2018
ReCIBE, Año 7 No. 1, Mayo 2018

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]
dgordon@uees.edu.ec

Rubén PACHECO VILLAMAR[1]
rpachecov@uees.edu.ec

[1]Universidad de Especialidades Espíritu Santo, Guayaquil, Ecuador

Resumen: El presente estudio se enfocó en tomar como referencia la metodología OSSTMM para aplicar una auditoría 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.

Keywords: OSSTMM, Informatic security, Security strategies.

1. 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 ha obligado 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 que 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 presentan en la figura 1.

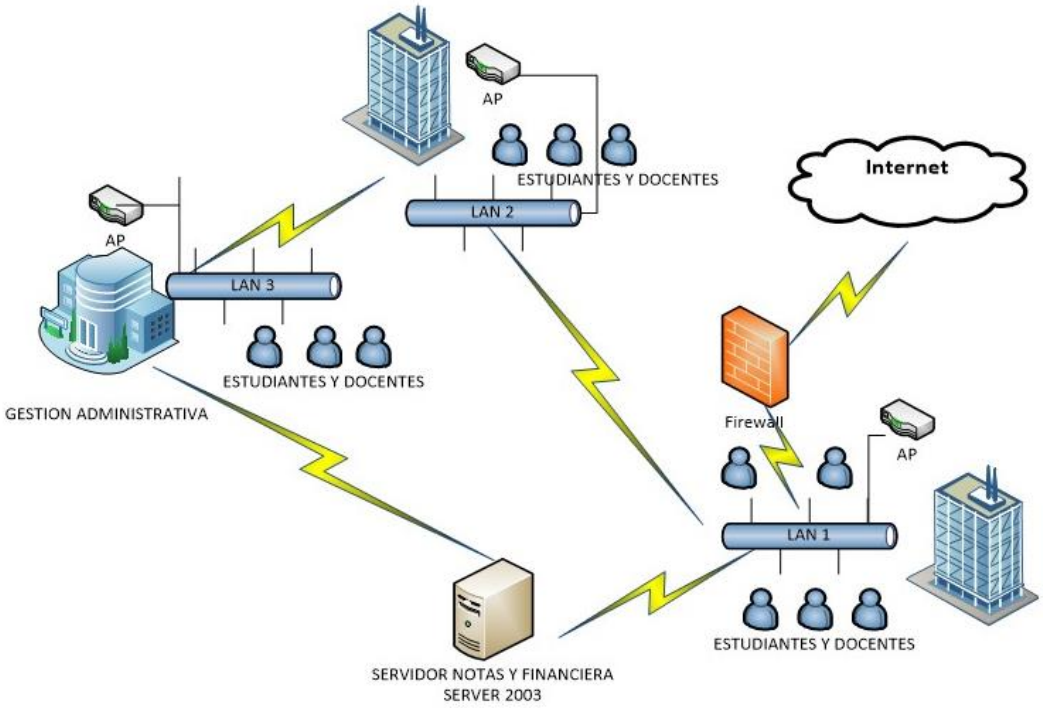

Figura 1. *Diagrama de red Intranet de la Institución de Educación Superior.*

La principal contribución de este trabajo, es la cuantificación de los riesgos y controles que presenta la intranet de la Institución de Educación Superior estudiada en base a la metodología OSSTMM v3, además se pondera el nivel de impacto y criticidad de las vulnerabilidades encontradas.

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.

2. Metodología

2.1. 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 la disciplina de 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 en la muestra se tomó datos de la gestión administrativa, docentes y estudiantes. Las técnicas de recolección de datos aplicados a este estudio fueron encuestas y entrevistas.

2.2. Fases de la Metodología OSSTMM

Con base en ISECOM (2012), la metodología OSSTMM, es un documento que reúne de forma estandarizada y ordenada diversas verificaciones y pruebas que se pueden realizar para una auditoría informática. Esta metodología presenta varias fases, en donde cada una de ellas se asocia con las fases del hacking ético como tipo de prueba que se aplica en este caso de estudio.

2.2.1. 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.

2.2.2. Fase de 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 verifican los accesos a aplicaciones y sistemas y los controles de seguridad establecidos para los mismos.

- Se verificó la visibilidad de los posibles objetivos propensos a ataques de seguridad.
- Se analizaron los puntos de accesos que posee la Institución de Educación Superior; es decir, escaneo de los puertos abiertos.
- Se verificaron los controles que se aplican para garantizar la confidencialidad, integridad y disponibilidad de la información.

2.2.3. 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, 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 recopila información disponible de manera abierta en buscadores utilizando técnicas como google hacking, o análisis de metadata, teniendo como objetivo la verificación de información relevante que estuviera sin ningún tipo de restricción en la red.

2.2.4. 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 conocer si la auditoria deja un rastro útil confiable.

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

- Se define las estrategias para disminuir las limitaciones y se aumenta controles.
- En esta etapa de la metodología OSSTMM, se cuantifica los resultados obtenidos.

3. 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:

3.1. Fase de Inducción – Recolección de información

3.1.1. 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 la información como en la infraestructura de suministro y protección eléctrica.
- La seguridad lógica operacional de la organización no dispone de una protección adecuada apoyada con IPS,/IDS, Antivirus bajo licencia para la detección de posibles amenazas.

CHECKLIST DE VERIFICACIÓN DE SEGURIDAD INFORMÁTICA

SEGURIDAD DE LOS DATOS						
INDICADOR	ASPECTO A EVALUAR	CUMPLE		RIESGO		
		SI	NO	Bajo	Medio	Alto
1	La organización tiene definidas políticas de seguridad informática.	/		X		
2	Las políticas de seguridad informática son revisadas periódicamente.		/		X	
3	Se dispone de un inventario de activos tecnológicos.	/		X		
4	Se monitoriza y registra la actualización, instalación de software en equipos de producción.		/			X
5	Se tiene definido perfiles de usuarios para evitar la instalación de cualquier tipo de software en los pc de usuarios finales.		/		X	
6	Dispone implementado listas de control de acceso (ACL)		/	X		
7	Se tiene software antivirus licenciado instalado de cada uno de los computadores que cuenta la organización		/		X	
8	Se tiene instalado antimalware en los equipos de la organización	/		X		
9	Se dispone de repositorios externos para salvaguardar backups y datos relevantes	/		X		
10	Se monitoriza y registra la actividad de las líneas telefónicas.	/		X		
SEGURIDAD DE LA INFRAESTRUCTURA Y SERVICIOS						
INDICADOR	ASPECTO A EVALUAR	CUMPLE		RIESGO		
		SI	NO	Bajo	Medio	Alto
11	Se dispone de Firewall	/		X		
12	Se han definido y documentado perímetros de seguridad (DMZ) en la intranet para equipos con información de alto riesgo.	/		X		
13	Se dispone, implementado, un sistema de protección anti-DDOS		/	X		X

14	Dispone de redundancia de hardware		/			X
15	Dispone de redundancia de software		/			X
16	La organización cuenta con procesos para brindar mantenimiento preventivo al software	/		X		
17	La organización cuenta con procesos para brindar mantenimiento preventivo al hardware	/		X		
18	Dispone de contratos externos de soporte	/		X		
19	Dispone de UPS en cada estación de trabajo		/		X	
20	Las instalaciones eléctricas cuentan con bajada a tierra	/		X		
CONTROLES DE ACCESO						
INDICADOR	ASPECTO A EVALUAR	CUMPLE		RIESGO		
		SI	NO	Bajo	Medio	Alto
21	Se ha definido e implementado un proceso para la creación de usuarios y contraseñas.		/			X
22	Se ha definido un proceso de altas y bajas de usuarios.		/			X
23	Se dispone de controles de acceso lógico a los servicios críticos de T.I. que dispone la organización	/		X		
24	Se monitoriza y registra la actividad de accesos lógicos en los equipos críticos que dispone.		/			X
25	En los equipos de los usuarios finales dispone de dos cuentas de inicio de sesión una como administrador y otra como usuario normal		/			X
26	Se dispone de controles de acceso físico al data center de la organización		/			X
27	Se monitoriza y registra la actividad de accesos físicos al data center de la organización.		/			X
28	Se monitorea y autentica las conexiones a la red inalámbrica de la organización	/		X		
PLANES DE RESPALDO						
INDICADOR	ASPECTO A EVALUAR	CUMPLE		RIESGO		
		SI	NO	Bajo	Medio	Alto
29	Se tiene establecido políticas de backup en caso de desastres.		/			X
30	Se ha documentado e implantado un proceso para la gestión de incidentes de seguridad informática.		/			X
31	Se ha definido planes de continuidad y de respaldos de información crítica		/			X
32	Se tiene defino planes de continuidad de negocio en la organización		/			X
33	Dispone la organización de respaldos de energía eléctrica en caso de fallas		/			X
34	Dispone de cuartos de acometidas para los servicios provistos por proveedores externos		/		X	
HABITOS SEGUROS Y PREPARACIÓN						
INDICADOR	ASPECTO A EVALUAR	CUMPLE		RIESGO		
		SI	NO	Bajo	Medio	Alto
35	Cuenta con políticas de seguridad de los equipos respecto al consumo de alimentos y bebidas	/		X		
36	Cuenta con planes de capacitación al personal sobre seguridad informática.		/			X
37	Se dispone de un plan de manejo seguro de datos críticos		/			X
38	Se destruyen discos duros catalogados como dañados	/		X		
39	El personal de la empresa se conduce y aplica hábitos seguros de manejo de la información.	/			X	
40	En general, la actitud hacia la aplicación de normas de seguridad es positiva.	/			X	

Figura 2. *Check list de verificación de seguridad informática.*

De acuerdo a la información recopilada en esta fase, como se detalla en la figura 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.

3.2. Fase Interacción – Scanning y enumeración

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**

Tabla 1. *Fase de Interacción*

En la tabla 1 se detallan todos los puntos interactivos encontrados en el momento de la evaluación de los canales: humano, físico, wireless, y redes de datos. Se encontró un total de 146 puntos interactivos de acceso y visibilidad, los cuales se evidencian en la tabla 2. Cabe indicar, que estos puntos pueden dar lugar, en algún momento, a un fallo de seguridad informática, y que solo se cuenta con 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 el 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 lógica operacional de la organización objeto de estudio.

	IP	Tipo	Número	Servicio	Observación	Herramienta	
1	10.10.2.2	TCP	2082	Cpanel	Servicio desactualizado	nessus	GESTIÓN ADMINISTRATIVA
2		TCP	445	microsoft-ds	Puerto abierto	nmap	
3		TCP	135	msrcp	Puerto abierto	nmap	
4	10.10.2.8	TCP	137	netbios-ns	Puerto abierto	nmap	
5		TCP	139	netbios-ssn	Puerto abierto	nmap	
		TCP	1736	desconocido	Puerto abierto	nessus	
6		UDP	5535	DNS-LLMNR	Puerto abierto	nessus	
7	10.10.2.4	TCP	21	ftp	puerto abierto	nmap	
8		TCP	443	ssl	pueto abuerto	nmap	
9		TCP	3306	mysql	Puerto abierto	nessus	
10		TCP	80	http	puero abiero	nmap	
11	10.10.5.1	TCP	135	msrpc	puero abiero	nmap	
12		TCP	139	netbios.ssn	puero abiero	nmap	
13		TCP	445	microsoft-ds	puero abiero	nmap	
14		TCP	1433	ms-sql-s	puero abiero	nmap	
15		TCP	3389	ms-wbt-server	puero abiero	nmap	
16		TCP	49152	desconocido	puero abiero	nmap	
17		TCP	49153	desconocido	puero abiero	nmap	
18		TCP	49154	desconocido	puero abiero	nmap	
19		TCP	49155	desconocido	puero abiero	nmap	
20		TCP	49156	desconocido	puero abiero	nmap	
21		TCP	49157	desconocido	puero abiero	nmap	
22		TCP	135	nsrpc	puero abiero	nmap	
23	10.10.5.24	TCP	139	netbios-ssn	puero abiero	nmap	
24		TCP	445	microsoft-ds	puero abiero	nmap	
25		TCP	2968	empp	puero abiero	nmap	
26		TCP	49155	desconocido	puero abiero	nmap	
27	10.10.5.67	TCP	135	msrpc	puero abiero	nmap	
28		TCP	139	netbios-ssn	puero abiero	nmap	
29		TCP	445	microsoft-ds	puero abiero	nmap	
30		TCP	2968	empp	puero abiero	nmap	
31		TCP	49163	desconocido	puero abiero	nmap	
32	10.10.5.92	TCP	445	microsoft-ds	puero abiero	nmap	
33		TCP	2869	icslap	puero abiero	nmap	
34		TCP	2868	empp	puero abiero	nmap	
35	10.10.5.95	TCP	135	msrpc	puero abiero	nmap	
36		TCP	445	microsoft-ds	puero abiero	nmap	
37		TCP	5000	vnc-http	puero abiero	nmap	
38		TCP	5900	vnc	puero abiero	nmap	
39	10.10.5.120	TCP	80	http	puero abiero	nmap	
40		TCP	443	https	puero abiero	nmap	
41		TCP	902	iss-realsecure	puero abiero	nmap	
42		TCP	912	apex-mesh	puero abiero	nmap	
43	192.168.120.12	TCP	139	netbios-ssn	puerto abierto	nmap	DOCENTES Y ESTUDIANTES
44		TCP	445	microsoft-ds	puerto abierto	nmap	
45		TCP	2869	icslap	puerto abierto	nmap	
46		TCP	2868	empp	puerto abierto	nmap	
47	192.168.120.14	TCP	135	msrpc	puerto abierto	nmap	
48		TCP	139	netbios-ssn	puerto abierto	nmap	
49		TCP	445	microsoft-ds	puerto abierto	nmap	
50	192.168.120.24	TCP	135	msrpc	puerto abierto	nmap	
51		TCP	445	microsoft-ds	puerto abierto	nmap	
52		TCP	2968	empp	puerto abierto	nmap	
53		TCP	49155	desconocido	puerto abierto	nmap	
54	192.168.120.39	TCP	135	msrpc	puerto abierto	nmap	
55		TCP	445	microsoft-ds	puerto abierto	nmap	
56		TCP	2968	empp	puerto abierto	nmap	
57		TCP	49163	desconocido	puerto abierto	nmap	
58	192.168.120.89	TCP	135	msrpc	puerto abierto	nmap	
59		TCP	139	netbios-ssn	puerto abierto	nmap	
60		TCP	445	microsoft-ds	puerto abierto	nmap	
61		TCP	554	rtsp	puerto abierto	nmap	
62		TCP	2869	icslap	puerto abierto	nmap	
63		TCP	5357	wsdapi	puerto abierto	nmap	
64		TCP	10243	desconocido	puerto abierto	nmap	
65	192.168.120.8	TCP	135	msrpc	puerto abierto	nmap	
66		TCP	139	netbios-ssn	puerto abierto	nmap	
67		TCP	445	microsoft-ds	puerto abierto	nmap	
68		TCP	49152	desconocido	puerto abierto	nmap	
69		TCP	49153	desconocido	puerto abierto	nmap	
70		TCP	49154	desconocido	puerto abierto	nmap	
71		TCP	49155	desconocido	puerto abierto	nmap	
72		TCP	49163	desconocido	puerto abierto	nmap	

Tabla 2. *Evidencia de puntos interactivos. Fuente: Nmap, nessus*

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**

Tabla 3. *Cuantificación de los controles de seguridad en los canales: humano, físico, wireless, redes de datos.*

Al analizar los datos de la tabla 3, en donde se cuantifican los controles encontrados durante la auditoria del 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, de los controles de proceso o Tipo B, se cuantifica un total de 22, los cuales proporcionan seguridad ante amenazas. En la tabla 4 se evidencian los controles encontrados durante el estudio realizado.

Control / Factor	Humano	Físico	Wifi	Redes de Datos
Autenticación	Cada usuario establece contraseña de acceso al PC	No aplica	Validación de contraseña en cada acceso wifi y dirección mac	Autenticaciones puntos wifi
				Autenticaciones sistemas académico y financiero
				Administrador establece contraseña en pc de gestión administrativa
Indemnización	Soporte técnico externo	Posee Seguro de robos	No aplica	Contratos externos de soporte
		Posse seguro de catastros		
		Posee invetarios de activos		
Resistencia	Guardia de seguridad	No aplica	Permite acceso solo a usuarios registrados	No aplica
Subyugación	No aplica	No aplica	No aplica	Intercambio de informacion entre servidor de sistema financiero y académico y host clientes
Continuidad	No aplica	Conectividad a tierra	No aplica	Redundancia de hardware y software
		UPS en estaciones de trabajo administrativo		UPS para servidor de sistema financiero y académico
				UPS rack de redes de datos
No repudio	No aplica	No aplica	Solo se permiten usuarios registrados	Firma electrónica director
Confidencialidad	Firma electrónica dirección	No aplica	No aplica	Se destruyen discos catalogados como dañados
				Personal conoce habitos seguros de manejo de información relevante
				Repositorio externo para respaldos
Privacidad	Politicas de privacidad gestión financiera	No aplica	No aplica	Red de datos con 2 proveedores ISP
Integridad	No aplica	No aplica	Se autentica cada punto wifi	Firma electrónica director
Alarma	Si existen hurtos actuan los guardias de seguridad	Alarma contra incendios	Registro de eventos en puntos wifi	Firewall activo

Tabla 4. *Evidencia de controles encontrados. Fuente: Check list de verificación, nessus, nmap*

3.3. Fase de Investigación – Análisis de Vulnerabilidades.

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

Tabla 5. *Fase Investigación – Limitaciones*

En la tabla 5 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; 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. En torno a esto en la tabla 6 se evidencian vulnerabilidades más relevantes encontradas en la intranet de la Institución de Educación Superior objeto de estudio.

	IP	Descripción	Observación	Herramienta	Riesgo
Gestión Administrativa	10.10.2.1	Host vulnerable a un buffer overrun en el servicio de acceso remoto	Servidor sistema académico y financiero	nessus	ALTO
		Sistema Operativo Obsoleto - Windows 2003 server		nessus	
	10.10.2.20	Sistema Operativo Obsoleto - Windows XP	Pc posee modulo del sistema financiero	nessus	ALTO
	10.10.2.8	Sistema Operativo con falla en el DNS - S.O Windows 7	S.O sin actualizar	nessus	MEDIO
	10.10.2.4	Servicio OpenSSL obsoleto	version desactualizada Pc posee modulo académico	nessus	ALTO
		XAMPP Obsoleto		nessus	
		Servicio de Apache obsoleto.		nessus	
	10.10.5.1	Autenticacion SMB obsoleta	Actualizar SMB Windows 7	nessus	MEDIO
		Windows afectado por vulnerbilidad de privilegios en protocolos SAM		nessus	
Gestión Docente y estudiantes	192.168.120.23	Pc con sistema Windows XP	S.O obsoleto	nessus	ALTO
		Autenticacion SMB obsoleta		nessus	
	192.168.120.12	Autenticacion SMB obsoleta	Actualizar SMB Windows 7	nessus	MEDIO
	192.168.120.14	PHP V.4	Actualizar PHP v5	nessus	MEDIO
	182.168.120.24	XAMPP Obsoleto	Actualizar aplicativo de xampp server a la versión mas reciente	nessus	MEDIO

Tabla 6. *Vulnerabilidades. Fuente: Nessus*

3.4. 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, 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.

4. Estrategias de gestión de seguridad informática con base en 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 existe 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.

5. 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 7.

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**

Tabla 7. *Riesgos y Controles a mejorar*

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.

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**

Tabla 8. *Mejoramiento de riesgos y controles*

En la tabla 8 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, lo cual disminuye el riesgo de inseguridad, teniendo en claro que no existe una seguridad perfecta, ya que el exceso de controles podría desencadenar en otro tipo de fallos que pueden estar ocultos pero actuando activamente sin que el administrador de la intranet se dé cuenta.

6. 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 el valor de 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, el 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.

Referencias

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 Report, 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%2

0Art%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).

Notas Biográficas:

Ing. Diego Sebastián Gordón Revelo Mgs. Ecuatoriano, nacido en la ciudad de Quito, el 18 de Octubre de 1990. Inició sus estudios universitarios en la Universidad Regional Autónoma de los Andes UNIANDES, obteniendo el título de Ingeniero en Sistemas e Informática y posteriormente continuó sus estudios en la Universidad de Especialidades Espíritu Santo donde obtuvo el título de Magister en Auditoría de Tecnologías de Información. En su vida profesional se ha desempeñado como Asistente de Tics y Analista de Soporte de TI en instituciones gubernamentales. Sus áreas de interés se centran en el estudio y aplicación de seguridad informática y soporte en tecnologías de información

M. Sc. Ing. Rubén Pacheco Villamar. Ecuatoriano, nacido en la ciudad de Guayaquil, el 22 de septiembre de 1965. Inició sus estudios universitarios en la Escuela Superior Politécnica del Litoral (ESPOL) de Guayaquil, y luego, en goce de una beca, continuó en Rusia, en la ciudad de San Petersburgo (entonces Leningrado), en la Universidad de Telecomunicaciones “Bonch Briyevich”. En esta universidad se graduó de Ingeniero en Telecomunicaciones en Transmisión de Datos, y posterior recibió el título de Master of Science en Telecomunicaciones. En su vida profesional se ha desempeñado como: Ingeniero de Soporte en Telecomunicaciones, Ingeniero de Diseño y Gerente de Proyectos para Enlaces de Telecomunicaciones, Redes de Computadoras, e Instalación y Operación de Centros de Datos, como Consultor en Gestión de Proyectos de TI, en Gestión de Procesos y Servicios de TI, y en Seguridad de Redes, y actualmente como Coordinador Nacional de Infraestructura y Producción de TICs en una institución gubernamental. Paralelamente, ha sido docente universitario y de investigación en Protel-ESPOL, en la Universidad San Francisco de Quito y en la Universidad de Especialidades Espíritu Santo; en esta última imparte clases en el pregrado de Ingeniería en Sistemas y Telecomunicaciones, y en posgrado, en la Maestría de Auditoría de Tecnologías de Información. Esporádicamente, realizo traducciones al español de textos en ruso y en inglés, y también se desempeña como Gerente General de una pequeña empresa de servicios de TI, fundada con un par de socios. A sus estudiantes siempre les menciona que “el solo hecho del conocimiento justifica el sacrificio”, pero que si, además, logran generar un cambio positivo en su entorno, se den por muy bien recompensados.