MAESTRÍA EN AUDITORIA EN TECNOLOGÍA DE INFORMACIÓN

PROPUESTA DE UNA METODOLOGÍA DE PRUEBAS DE PENETRACIÓN ORIENTADA A RIESGOS

Propuesta de artículo presentado como requisito para obtener el título de:

Magister en Auditoría en Tecnología de Información

Por la estudiante:
Vilma Karina ALVAREZ INTRIAGO

Bajo la dirección de:
Antonio Cevallos Gamboa, MSIG, MAE, PhD (c)

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de Información
Guayaquil - Ecuador
Abril del 2018

Propuesta de una Metodología de Pruebas de Penetración orientada a riesgos

Proposal of a risk-oriented Penetration Testing Methodology

Vilma Álvarez-Intriago[1]
Antonio Cevallos Gamboa[2]

Resumen

La seguridad de la información se ha convertido en la mayoría de las organizaciones un aspecto importante e indispensable para sus operaciones. Es por esto, que hoy en día existen diversas metodologías que guían a los auditores a realizar pruebas y aplicar métricas; con el fin de analizar controles y procedimientos que verifiquen mencionada seguridad. La presente investigación realiza un estudio descriptivo, con enfoque cualitativo, de las metodologías OSSTMM, OWASP, PTES, ISSAF y CVSS a fin de realizar una nueva propuesta que recopile las mejores prácticas tanto con enfoque técnico como de riesgos. Para esto se realizó una exploración de todas las características de las metodologías antes mencionadas utilizando revisión bibliográfica, entrevistas y juicios de expertos; encontrando procedimientos y estándares que guíen en la realización efectiva de pruebas de penetración. Como resultado se obtiene una propuesta de metodología orientada a riesgos, que contiene cuatro etapas: la primera, referente al acuerdo, alcance, recopilación de información; la segunda a la ejecución, la tercera que trata de la evaluación de riesgos y la última que contempla la generación de informes. La misma, se considera un aporte para los auditores tecnológicos ya que además de informar sobre aspectos técnicos, también lo hace, sobre enfoques de riesgos priorizándolos a través niveles de incidencia o de gravedad sobre los objetivos de la empresa.

Palabras clave: Seguridad de la Información, vulnerabilidad, pruebas de penetración, metodologías de auditoría, riesgos.

Abstract

The security of information has become in most organizations an important and indispensable aspect for their operations. That is why today there are several methodologies that guide auditors to perform tests and apply metrics; in order to analyze controls and procedures that verify said security. The present investigation carries out a descriptive study, with a qualitative approach, of the OSSTMM, OWASP, PTES, ISSAF and CVSS methodologies in order to make a new proposal that compiles the best practices with both a technical and risk approach. For this, an exploration of all the characteristics of the aforementioned methodologies was carried out using bibliographic review, interviews and expert judgments; finding procedures and standards that guide the effective performance of penetration tests. As a result, a risk-oriented methodology proposal is obtained, which contains four stages: the first, regarding the agreement, scope, information gathering; the second to the execution, the third that deals with the risk assessment and the last one that contemplates the generation of reports. The same, is considered a contribution for the technological auditors since in addition to informing on technical aspects, it also does it, on approaches of risks prioritizing them through levels of incidence or of gravity on the objectives of the company.

Key words Information Security, vulnerability, penetration tests, audit methodologies, risks.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail vkalvarez@uees.edu.ec.
[2] PhD (c) en Ciencias de la Dirección, MSIG, MBA, Ingeniero en Sistemas; Profesor Principal; Decano de la Facultad de Ingeniería en Sistemas, Telecomunicaciones y Electrónica en la Universidad Espíritu Santo - Ecuador; email: acevallos@uees.edu.ec

1. INTRODUCCIÓN

En la actualidad, las empresas manejan la información referente a sus procesos de negocio de forma física y digital. Dicha información, independiente de su medio de almacenamiento y transmisión, es un recurso vital para el éxito y la continuidad del servicio en cualquier organización, Díaz (2005) afirma que de ella depende la toma de decisiones y el conocimiento interno de la empresa. Con relación a esto, Voutssas (2010) expone que día a día los sistemas de información son más vulnerables a las amenazas que se presentan en el medio, convirtiéndose en un riesgo que en muchos casos ocasiona grandes pérdidas. Por esto, ISACA (2015), afirma que el número de incidentes de seguridad detectados han aumentado 66% año tras año desde el 2009; incrementando las pérdidas hasta 42,8 millones de dólares en todo el mundo según lo enuncia las encuestas del 2014. Así mismo, ESET Security Report (2015) describe que la explotación de las vulnerabilidades es uno de los incidentes de mayor ocurrencia en las empresas grandes y que en promedio 1 de cada 5 empresas sufrió uno de ellas en el 2014.

Monsalve-Pulido, Aponte-Novoa, y Chaves-Tamayo (2014) exponen que uno de los aspectos más importantes dentro de la seguridad de la información es el control de vulnerabilidades, el cual requiere un estudio, un presupuesto y una aplicación ya sea preventiva o correctiva sobre los temas de seguridad que se puedan encontrar. Es por esto, que Ramos (2013) afirma que las personas o redes de computadoras que se dedican a analizar/evaluar las debilidades o vulnerabilidades de los sistemas informáticos son llamados ethical hackers. Éstos, de acuerdo a Lakshmi & Basarkod (2015), atacan y penetran en los sistemas informáticos y redes para descubrir y señalar posibles debilidades de seguridad, de acuerdo a Salinas & Vásquez (2013) surgen las pruebas de penetración o Pent Test; Bhawana, Ankit & Shashikala (2014) explica que son metodologías y técnicas que permiten realizar una evaluación integral de las debilidades de los sistemas informáticos, las mismas que son realizadas con el consentimiento del o los propietarios de los sistemas, De acuerdo a INNOVA SECURE (2017), es obligatorio y aconsejable que esto lo realicen personas ajenas a la empresa, ya que si lo hiciera alguien de la empresa se cometería el error de ser juez y parte. Las pruebas de penetración permiten según Cuchillac (2014) verificar la seguridad o vulnerabilidad de los mecanismos actuales en las redes utilizadas, tanto en ámbitos empresariales como en el hogar. Así también, Fernandes & Junqueira (2014) afirma que la ejecución de pruebas de penetración, especifica tipos de vulnerabilidades que están expuestos los sistemas, adoptando medidas y minimizando la incidencia de ataques externos y/o internos. Por esto, Franco, Perea, & Tovar (2013) afirma que, realizar pruebas de penetración para detectar estas vulnerabilidades es importante para los evaluadores de la seguridad de la información, incluso muchos enfoques han sido propuestos recientemente para la detección de vulnerabilidades de servicios activos en equipos de red. Por esto, Hernández & Mejia (2015) describe que existen muchas herramientas que proporcionan la detección para diferentes propósitos, es decir, cubren escaneo de vulnerabilidades tanto en aplicaciones web como en dispositivos móviles utilizando variedad de plataformas.

Sin embargo, Tamayo(2016), afirma que existen desafíos que se presentan ante la problemática de establecer metodologías que se utilicen en el Ethical hacking en diferentes empresas y determinar procedimientos que se realizan para diferentes empresas en el Ecuador; para lo cual Caballero Quezada (2013), expone que se debe seguir la mejor estrategia para realizar una prueba de penetración satisfactoria con el propósito de hacer más seguros los sistemas de cómputo. Por esto, según Suresh (2014) la intensión principal de Testing & Ethical hacking se fundamenta en realizar y establecer un intento de ataque controlado sobre los sistemas de información y las redes, con el objetivo de identificar posibles vulnerabilidades a las que estos se encuentran expuestos; y donde

posteriormente, se pueda realizar una definición de planes contingentes y de acción. Sin embargo, Servicios Expertos (2017) afirma que el descubrimiento de vulnerabilidades es importante, pero ser capaz de estimar el riesgo asociado al negocio es esencial.

Por esto, al no existir una metodología de pruebas de penetración orientada al riesgo, el auditor puede estar limitado en su evaluación. De esta manera, con la nueva metodología implementada en esta investigación se dotaría a los auditores de una herramienta más ágil para evaluar los mayores riesgos y priorizarlos.

Por lo anteriormente expuesto, el objetivo de este artículo es desarrollar una propuesta de metodología para pruebas de penetración orientada a riesgos con base a las metodologías: Open Source Security Testing Methodology Manual [OSSTMM], Open Web Application Security Project [OWASP], Information Systems Security Assessment Framework [ISSAF], Penetration testing execution standard [PTES], Common Vulnerability Scoring System [CVSS] dentro del campo de la auditoría de tecnología de información

2. MARCO TEÓRICO

2.1 Seguridad Informática

Según Fuertes, Guagalango, & Moscoso (2011) seguridad informática es el área que protege la infraestructura computacional incluyendo la información contenida. Así también, Alonso (2002) afirma que la seguridad informática se encarga de identificar las vulnerabilidades del sistema y establecer las contramedidas necesarias para intentar evitarlas. Entonces, de acuerdo a lo enunciado por los autores anteriores se puede afirmar que el objetivo de la seguridad informática es proteger la información que se encuentra dentro de la infraestructura tecnológica de una empresa donde pueden existir vulnerabilidades.

2.1.1 Auditoría de Seguridad de Información

La auditoría es una actividad independiente y objetiva de aseguramiento y consulta, concebida para añadir valor y mejorar las operaciones de una organización (Mora, 2017). Así, Dávalos (2013), explica que, la auditoría de seguridad de la información se vuelve sumamente importante, ya que ayuda a detectar desviaciones de políticas y procedimientos establecidos por estándares, prácticas; permitiendo mantener la seguridad de la información. Por otro lado, Stable-Rodríguez (2012), afirma que la auditoría debe interactuar con la estrategia de la organización, realizando primeramente un levantamiento para revisar procesos, recursos y la propia estrategia dando recomendaciones, acciones correctivas, seguimiento y control. Así,
Cano (2017), afirma que la organización debe establecer lineamientos que le permitan valorar y proteger permanentemente sus activos; por lo tanto, se deben realizar auditorías de seguridad, las cuales cuando concierne en seguridad informática, se realizan, evaluaciones y pruebas de penetración que permiten identificar vulnerabilidades y amenazas que pueden a dañar la integridad, disponibilidad y confidencialidad de la información (ISACA, 2016).

2.1.2 Vulnerabilidad

De acuerdo a Ortiz(2015), vulnerabilidad se refiere a un fallo o debilidad en un sistema informático; ISACA (2009) expresa que las vulnerabilidades son debilidades internas de un sistema de información las cuales, si son explotadas, podrían causar un daño significativo a la empresa. De acuerdo a Santiago(2009), los procesos de evaluación se detallan previo a la implementación de un sistema de gestión de seguridad de la información y apuntan a la evaluación de vulnerabilidades del sistema y en muchos casos a la realización de pruebas de penetración con el fin de determinar la posibilidad que exista sobre la plataforma, alguna vulnerabilidad existente para comprometer seriamente algún activo (Tarazona, 2006).

2.1.3 Pruebas de penetración

Según Franco, Perea & Tovar (2013), se conoce como prueba de penetración tration test o pentest) a la valoración de la seguridad de un sistema computacional en la que un evaluador lleva a cabo ataques del mundo real para identificar métodos que eluden los mecanismos de seguridad de una aplicación, sistema o red.

Así, Pérez (2012) afirma, que una prueba de penetración es un método de evaluación de seguridad de un sistema u organización simulando un ciberataque que pretende manipular la información, robarla o controlar el sistema; aprovechando fallas y vulnerabilidades conocidos por los expertos, no resueltas o mal parchadas. Así, la mayoría de las pruebas de penetración involucran la búsqueda de vulnerabilidades en uno o más sistemas computacionales que puedan ser utilizadas para ganar acceso a los mismos Vega & Hadfeg (2017).

Por eso, Broad & Brindner (2014), enuncian que en las pruebas de penetración se utilizan metodologías, procesos y procedimientos llevados a cabo por los evaluadores dentro de las pautas específicas y aprobadas para intentar eludir las protecciones de los sistemas de información. Sin embargo, OWASP Fundation (2007), expone que mientras las pruebas de penetración han demostrado ser efectivos en seguridad de redes, la técnica no se traslada de forma natural al caso de aplicaciones informáticas. Pozo Zulueta, Quintero Ríos, Hernández Aguilar, Gil Loro, & Lorenzo Álvarez, (2009) afirma en cuanto a desarrollo de sistemas, que el número de ataques aumenta cada día y no basta con garantizar la seguridad durante el

proceso de avance, sino también hay que realizar pruebas de penetración que evalúen la seguridad del software después de realizado y antes de ser entregado al cliente para su posterior uso. Por esto, Sheoran & Singh (2014) afirman que muchas personas emplean pruebas de penetración sobre aplicaciones web como su técnica de comprobación de seguridad principal; entonces de acuerdo a Serrato (2016) se debe utilizar lenguajes de programación avanzada y usar un lenguaje de bajo nivel con bibliotecas de función seguras.

Tipos de Prueba de penetración

Pérez (2012)n afirma que la elección del tipo de test no determina ni orienta la aplicación de todo el sistema de la metodología. Teniendo en cuenta el conocimiento de la aplicación que se está probando, a un alto nivel de categorización, podemos dividir las pruebas en: caja blanca, caja negra y caja gris. De acuerdo a ISACA (2016), en la técnica “black box” o caja negra, no se sabe bien qué es lo que se va a encontrar, es decir no se sabe nada del objetivo; su éxito depende de la calidad del auditor. Otro tipo de prueba es “Gray box” o caja gris, Sandulescu88 (2014) expone que, en esta prueba, el auditor tiene un conocimiento limitado de las defensas del objetivo y de sus activos, pero sabe todo acerca de sus canales. Entonces, el objetivo conoce el alcance de la auditoría, pero no las vías y vectores de ataque; es por esto, que la eficacia de este tipo de test dependerá de la calidad de la información provista al auditor. Por otro lado, Vala & Jasek, (2011) afirma que en la prueba de caja blanca, el auditor tiene un conocimiento limitado de sus defensas, activos y un completo conocimiento de sus canales, donde la auditoría forma parte del equipo de seguridad y control de los procesos.

2.2 Metodologías y Frameworks para pruebas de penetración

Junta de Andalucía (2011) afirma que existen diferentes metodologías y frameworks, que ayudan a seguir la mejor estrategia para realizar una prueba de penetración satisfactoria. Por ello, los investigadores desarrollan formas efectivas metodologías o estándares de éxito para prevenir el ataque (INFOSEC INSTITUTE,2016).

Entre las metodologías que se involucran en esta investigación están OSSTMM, OWASP, ISSAF, PTES, CVSS. A continuación, se realizará una breve descripción de cada una de ellas.

2.2.1 OSSTMM: Open Source Security Testing Methodology Manual

De acuerdo a ISECOM (2017), OSSTMM es una metodología para prueba de seguridad, diseñada para ser consistente y repetible. Permite contribuir con ideas para realizar una seguridad operacional (OpSec) más precisa, procesable y eficiente. Así también OSSTMM abarca pruebas de todos los canales: redes humanas, físicas, inalámbricas, de telecomunicaciones y de datos. Se la puede aplicar en pruebas de la computación en la nube, infraestructuras virtuales, middleware de mensajería, infraestructura móvil de comunicación, ubicaciones de alta seguridad, recursos humanos, informática confiable y cualquier proceso lógico que cubren múltiples canales y requieren un tipo diferente de prueba de seguridad. Las métricas, llamada Risk Assessment Values [RAV], proporcionan una herramienta poderosa y altamente flexible que puede proporcionar una representación gráfica de estado y mostrar cambios en el estado a lo largo del tiempo. El OSSTMM incluye información para la planificación del proyecto, la cuantificación de resultados y las reglas de compromiso para realizar auditorías de seguridad. La metodología se puede integrar fácilmente con las leyes existentes y políticas para asegurar una auditoría de seguridad completa a través de todos los canales.

Es una metodología abierta, pública y constantemente actualizada, que permite realizar la valoración de evaluación de riesgo, obteniendo una valoración cuantificable de los resultados de las pruebas realizadas. Se encuentra alineada a los estándares internacionales ISO de seguridad de la información y guías de mejores prácticas.

De acuerdo a Cotoira (2017), esta metodología es utilizada mundialmente, para pruebas de penetración sin considerar tamaño de la organización o herramientas técnicas utilizadas. Así también es flexible, ya que expresa los procesos de manera general, donde el auditor puede utilizarlos de acuerdo a su necesidad y conveniencia para el estudio.

Sin embargo, tiene limitaciones como es que no define mejores herramientas a utilizar en pruebas de penetración; ni es una metodología sencilla por lo que se necesita capacitación para entenderla. Así el acoplamiento con las otras metodologías es complicado, por lo que podría hacer más lento el proceso

La metodología está dividida en secciones, módulos y tareas. En la Figura1 se muestra la lista de módulos del mapa de seguridad, que son los elementos primarios de cada sección. Cada módulo debe incluir todas las Dimensiones de Seguridad que están integradas con tareas a ser desarrolladas.

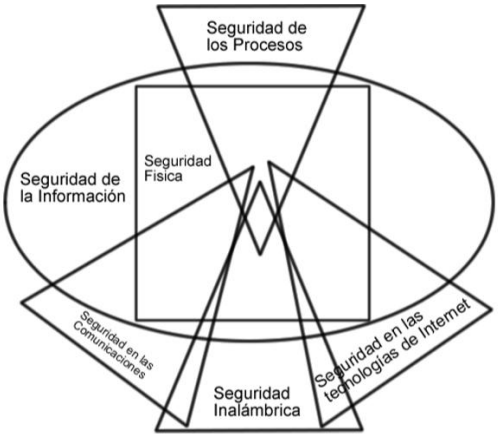

Figura 1 Mapa de seguridad OSSTMM (Herzog, 2010)

2.2.2 OWASP: Open Web Application Security Project

OWASP Fundation (2007), afirma que éste marco de trabajo, tiene por objetivo ayudar a las organizaciones a comprobar la seguridad en aplicaciones web con el propósito de construir software confiable y seguro. Esta metodología está desarrollada, centrándose en el ciclo del desarrollo de software (sus siglas en inglés SDLC). A continuación, en la Figura 2, se muestra el flujo de pruebas de esta Metodología.

De acuerdo a Pérez (2012) afirma que este método de pruebas para aplicaciones web, está basado en dos fases: pasiva y activa. En la primera se realizan pruebas hasta comprender la lógica de la aplicación y comprobar si arroja algún elemento que pueda significar una puerta abierta para su análisis detallado. Luego en la fase activa, se prueban 10 procesos: pruebas de manejo de configuración, pruebas de autenticación, pruebas de manejo de sesión, pruebas de autorización, pruebas de lógica de negocios, pruebas de validación de datos, pruebas de denegación de servicios, pruebas de JavaScript and XML (AJAX) y la última que son los reportes valorando el riesgo real.

2.2.3 ISSAF: Information Systems Security Assessment Framework

Valencia (2013) enuncia que Open Information systems security group (OISSG) desarrolló un marco metodológico en el año 2005, que permite clasificar la información de la evaluación de seguridad en diversos dominios usando diferentes criterios de prueba. Además, es una metodología libre, del tipo GNU GPL; que busca integrar herramientas de gestión y listas de control interno (OISSG, 2017); como es, la evaluación de políticas y los procesos de seguridad de la información de la organización para informar sobre su cumplimiento con los estándares de la industria de TI, y las leyes aplicables y los requisitos reglamentarios.
Así también, identifica y evalúa las dependencias comerciales en servicios de infraestructura proporcionados por TI. Luego, llevar a cabo evaluaciones de vulnerabilidad y pruebas de penetración para resaltar las vulnerabilidades del sistema que podrían generar riesgos potenciales para los activos de información. También especificar modelos de evaluación por dominios de seguridad para encontrar configuraciones erróneas y rectificarlas; identificar los riesgos relacionados con las tecnologías; identificar los riesgos dentro de las personas o los procesos comerciales y abordarlos; fortalecer procesos y tecnologías existentes; proporcionar mejores prácticas y procedimientos para respaldar las iniciativas de continuidad del negocio.
Tal como se enuncia anteriormente, ISSAF tiene como objetivo dar integridad, precisión y eficiencia a las evaluaciones de seguridad.

Por otro lado, Pérez (2012) afirma que la metodología ISSAF evalúa la red, los sistemas y la aplicación de controles como IEC/ISO 27001:2005(BS7799), SarbanesOxley SOX404, CoBIT, SAS70 and COSO;

2.2.4 PTES: Penetration testing execution standard

Esta metodología se enmarca en la metodología OSSTMM, donde une esfuerzos de analistas y expertos en seguridad para hacer un estándar que pueda completar una auditoría en todos sus procesos más habituales. INFOSEC INSTITUTE (2016) afirma que la ejecución de un test se divide en 7 fases: en la primera se llega a un acuerdo con el cliente de la profundidad de las pruebas a realizar, permisividad de ataques, enfoque del test, presentación de evidencias. Luego, en la segunda, se levanta la información publicada en motores de búsqueda que nos da una idea del objetivo y de las personas que trabajan en ella. En la tercera, se realiza el modelado de amenazas, donde se definen las líneas de negocios existentes y los activos más importantes a fin de definir las pruebas de ataques siguientes. En la cuarta fase se realiza el escaneo de puertos y servicios identificando vulnerabilidades existentes; se valida las posibles opciones reales de ataque y se comprueba que pueden darse con un riesgo derivado; así como la brecha que existe entre las seguridades y vulnerabilidades.

Luego, en la quinta fase, que es la de explotación de vulnerabilidades se contempla en la forma de evasión de contramedidas existentes desde el acceso físico hasta las redes wireless, ataques web, entre otros. En la sexta fase que es la post explotación, se centra en la recopilación de evidencias y en cómo valorar el impacto real de la intrusión y hasta donde se puede llegar si el sistema está vulnerable. En la séptima fase, se entregan los reportes ejecutivo y técnico, conteniendo primeramente las razones por las cuales se hicieron las pruebas, seguido de los posibles riesgos y su valoración, luego el análisis de las vulnerabilidades encontradas y la confirmación de que las mismas han sido podido ser explotadas junto con las contramedidas propuestas y probadas. Así también las métricas utilizadas y las contramedidas propuestas para los riesgos analizados, esto es, el grado de exposición que tienen los activos de la empresa y organización.

2.2.5 CVSS: Common Vulnerability Scoring System

FIRST Improving Security Together (2017) afirma que esta metodología provee una manera de capturar las principales características de vulnerabilidad y producir una puntuación numérica que refleje su gravedad. Así se puede traducir en una representación cualitativa como crítica, baja, media, alta a fin de ayudar a las organizaciones a evaluar y a priorizar sus procesos de gestión de vulnerabilidad. Así mismo NIST (2015) expone que CVSS es adecuado para industrias, organizaciones y gobiernos ya que es un estándar de medición que brinda puntuaciones de impacto de vulnerabilidad precisas y consistentes.

El CVSS entrega dos resultados importantes, la primera es el cálculo de la gravedad de las vulnerabilidades y la segunda, la priorización de las actividades para eliminarlas. Por otro lado, base de datos nacional de vulnerabilidad [NVD] proporciona los puntajes base de CVSS que representan las características innatas de cada vulnerabilidad. Así también, proporciona una calculadora de puntaje CVSS que le permite agregar datos de puntaje ambiental y temporal.

EL NVD mantiene especificado rango de calificaciones de gravedad cualitativa para las vulnerabilidades para la metodología CVSS, tal como se muestra en la tabla1.

Tabla1.- Calificaciones de CVSS v3.0

Gravedad	Rango de puntaje base
Ninguna	0.0
Bajo	0.1 - 3.9
Medio	4.0 – 6.9
Alto	7.0 – 8.9
Crítico	9.0 – 10.0

2.3 Riesgo

De acuerdo a DELOITTE (2015), riesgo es el impacto y la probabilidad de que una amenaza pueda afectar negativamente a los objetivos de la empresa. Así también, International Organization for Standarization. International Electrotechnical Commission (2009), define al riesgo como la posibilidad de consecuencia negativa. Por otro lado, Ramírez & Ortiz (2011) afirma que el marco existente para gestión de riesgos lo conforman los estándares ISO 31000 orientado a administrador de riesgos e ISO/IEC 27005 enfocada a administración de riesgo de la seguridad de la información.

Riesgo inherente

Rodríguez, Piñeiro, & De Llano, (2013) la indeterminación intrínseca de la actividad, sin considerar la existencia de los controles existentes o que se puedan implantar para mitigarlo. Así Machado (2016), afirma que es el que sostiene una organización en ausencia de acciones para modificar su probabilidad e impacto.

Riesgo residual

Sánchez (2015), afirma que es el riesgo resultante después de aplicar los controles; así

lo confirma Sulca & Becerra (2017), al enunciar que es aquel que persiste luego de aplicar medidas de control.

3. METODOLOGÍA

El enfoque de esta investigación es de orden cualitativo con un alcance: exploratorio - descriptivo. Para el diseño investigativo, primeramente, se expondrán las características más importantes de las metodologías OSSTMM, OWASP, PTES, ISSAF y CVSS, esto es, ámbito y enfoque, alcance, profundidad, usabilidad, métricas para las vulnerabilidades encontradas, evaluación del riesgo y las distintas fases utilizadas para su aplicación: las cuales son las bases para la nueva propuesta metodológica. Luego, se realizará el diseño de la nueva metodología de prueba de penetración orientada a riesgos; esto es, partiendo de las características anteriormente recopiladas. Por último, se realizarán las conclusiones y trabajos futuros asociados a la investigación.

Para la elaboración presente investigación se tomarán en consideración metodologías utilizadas en el entorno de auditoría de sistemas como son: OSSTMM, OWASP, PTES, ISSAF, CVSS. Cabe anotar que se explicarán los aspectos y características más importantes de cada una de ellas, que servirán como base para el diseño y creación de la nueva metodología propuesta, orientada a riesgos. Entre los aspectos considerados están: 1) ámbito y enfoque; refiriéndose al tipo de organización que la utilizará, de los hackers que realizarán la prueba de penetración y de las diferentes áreas en las cuales se pueda emplear la metodología; 2) Alcance; este aspecto evidencia todas las tareas que puede abarcar la metodología incluyendo la valoración de riesgos; 3) Profundidad; se refiere al detalle con que trabaja la metodología; 4) Usabilidad; explica la facilidad con la que se puede utilizar la metodología en entorno de pruebas de penetración y riesgos. 5) Métricas; que son una forma objetiva de medir y clasificar las vulnerabilidades encontradas; 6) Evaluación del riesgo; enuncia en qué nivel de gravedad se encuentra el riesgo y como se puede mitigar el impacto de su materialización; Otro punto considerar en el análisis, son las fases que operan cada una de las metodologías para el desarrollo de pruebas; lo cual contribuirá para la elaboración de la propuesta.

Por otro lado, como técnicas de investigación se utilizarán entrevistas y revisiones documentales. Según Fernández (2001) en la investigación cualitativa, se desarrollan diversas técnicas que nos permiten un acercamiento real al campo de estudio propuesto, pero se destaca la entrevista. Según Díaz-Bravo, Torruco-García, Martínez-Hernández, & Varela-Ruiz (2013) la entrevista es una técnica de gran utilidad en la investigación cualitativa para recabar datos ya que adopta la forma de un dialogo coloquial y es muy ventajosa principalmente en los estudios descriptivos y en las fases de exploración. Así, la selección del grupo de expertos se basó en el método Delphi. De acuerdo López-Gómez (2018) permite estructurar un proceso comunicativo de diversos expertos organizados a fin de que aporten en torno a una problemática de investigación determinada. Para ello, se identifican primeramente a los expertos potenciales bajo criterios de inclusión. Para establecer los atributos de los expertos a entrevistar se debe considerar antecedentes y experiencia en el ámbito a investigar (Pill, 1971). Para este trabajo se consideró que los expertos tengan 5 años trabajando en el área de Seguridad Informática. Para la cantidad de expertos, Steurer (2011) afirma que el método Delphi no exige una muestra de expertos representativa de una población determinada, esto es no hay normas específicas respecto al número de participantes. Lo corrobora Powell (2003) enunciando que el número de expertos depende de los objetivos que se deseen alcanzar y de los recursos disponibles. Por ello, la investigación se apoya en entrevistas a expertos en el área de seguridad informática a fin de elaborar una propuesta de metodología de pruebas de penetración orientada a riesgos.

4. ANÁLISIS

La calidad del resultado de una prueba de penetración es difícil de juzgar sin una metodología estándar. Muchas variables afectan el resultado de una prueba, incluyendo el estilo personal y las predilecciones del auditor que realiza la prueba de penetración. Es por esto, que es importante definir el modo correcto de realizar la prueba, basándose en las mejores prácticas. El objetivo principal es establecer un estándar en metodologías de pruebas que al ser utilizada reúna todas las condiciones de prácticas de seguridad junto con la evaluación de riesgos.

4.1 Metodología **OSSTMM: Open Source Security Testing Methodology Manual**

Esta metodología fue diseñada por organización internacional Institute for Security and Open Methodolgy (ISECOM) en el año 2000; es considerada un manual que constantemente es actualizado. Está diseñado para ser consistente y repetible; no solo ofrece una estrategia de evaluación y medida de riesgos; sino la interpretación de los resultados. En cuanto a su *ámbito o competencia*, esta metodología abarca toda el área operativa, es utilizada por cualquier empresa que requiera evaluar su sistema de seguridad. De acuerdo a *su alcance*, OSSTMM maneja 6 secciones de seguridad y módulos que se encuentran dentro de cada una de estas secciones con sus respectivas tareas a ejecutar. Por otro lado, comentando sobre la *profundidad*, la aplicación de la estrategia es muy meticulosa y depende de la pericia del auditor, los medios y equipamiento requerido. Con respecto a la *utilización* de esta metodología requiere de capacitación y es categorizada como nivel medio en utilización.

Sin embargo, la metodología OSSTMM, utiliza las *métricas* para medir el grado de seguridad de los activos, utilizando mediciones objetivas que para la valoración de evaluación de riesgo (RAV).

En la versión 2.5 del OSSTMM se define y expone la aplicación de los RAV para poder cuantificar con precisión los niveles de riesgos (Herzog, 2003).

En cuanto a evaluación al riesgo, la metodología la tiene Integrado a cada módulo de operación; a fin de ejecutarla de manera efectiva, ha desarrollo los RAV a fin de poder cuantificar con precisión los niveles de riesgo. Los RAV brindan pruebas específicas en períodos de tiempo determinados que se tornan cíclicos. Así, en la evaluación de riesgos, el OSSTMM, aplica la técnica de "Seguridad Perfecta" que se logra con las mejores prácticas, las regulaciones en la industria del cliente, las justificaciones del negocio, la política de seguridad del cliente y los asuntos legales para el cliente y las regiones donde el mismo tenga negocios.

Las acciones de la metodología OSSTMM están basadas en tiempo y costo tal como lo muestra la Figura 2. Éstas, son aplicadas a diferentes tipos de sistemas y pruebas de seguridad de redes.

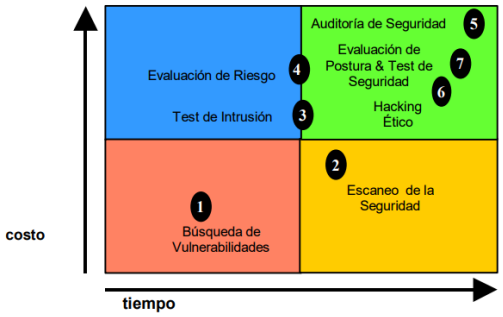

Figura 2: Acciones que se realizan en la metodología OSSTMM

Fases de esta metodología

De acuerdo a Valdez (2013), existen 4 fases para la ejecución de esta metodología; donde la primera es la *Fase de reglamentación*, comprende los requisitos, el alcance y las limitaciones de la auditoría. Luego se encuentra la *fase de definición,* donde se establece el ámbito de la aplicación en relación de los objetivos y activos. Además, se considera la visibilidad de la auditoría, la verificación de accesos, de confianza y de controles. La

tercera, es la f*ase de información,* en la cual, el auditor va descubriendo y analizando con el fin de encontrar alguna mala gestión. Además, en esta fase se considera la comprobación y configuración de procesos; una revisión en detalle. Por último, se tiene la f*ase interactiva de pruebas y controles,* donde se considera las pruebas, la auditoría de privilegios, la validación de sobrevivencia, revisión de alertas y registros. En la Figura 3 se muestran todas las fases de esta metodología.

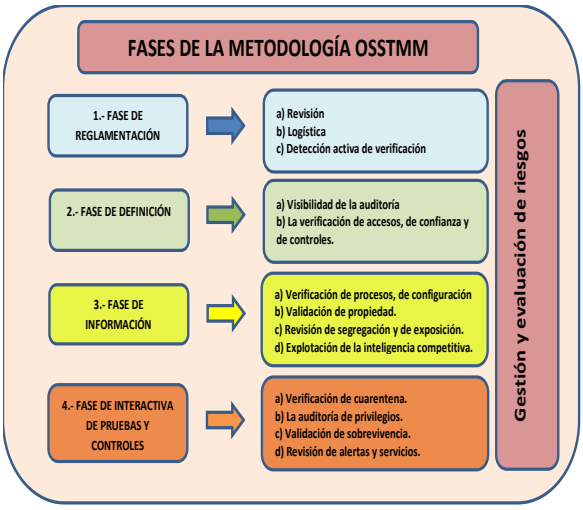

Figura 3.- Fases de la metodología OSSTMM

4.2 OWASP (Open Web Application Security Project)

OWASP Fundation (2007), afirma que es una metodología creada en el 2001 por la fundación OWASP, cuya finalidad es apoyar al proyecto que lucha contra el software inseguro, velando por mantener aplicaciones y servicios web más seguros. Las características y aspectos necesarios de esta metodología para la propuesta a realizar, se encuentra en la guía de aplicación OWASP denominada Testing Guide Versión 3.0.

El *ámbito y enfoque* de esta metodología sirve para evaluar entornos de aplicaciones web de cualquier organización y está dirigido a desarrolladores y revisores de software. Su material está disponible bajo una licencia de software. En cuanto al *alcance,* analiza la seguridad de un software especialmente en la fase de pruebas y puesta en producción utilizando buenas prácticas en el desarrollo. Por otro lado, acerca de su p*rofundidad*, OWASP emite herramientas de software y documentación basada en el conocimiento sobre la seguridad de las aplicaciones; pone a disposición todas las vulnerabilidades posibles que se han presentado y sus controles. Con respecto a *Evaluación al riesgo,* la metodología OWASP, dispone de un sistema para puntuar los riesgos, un marco de trabajo básico que se adapta a la organización. Para esto, utiliza el modelo estándar de valoración del riesgo, el cual afirma que, riesgo es igual a probabilidad de ocurrencia por el impacto. Así esta metodología considera 3 puntos importantes: factores de riesgo, personalización de factores de riesgo y ponderación factores de riesgo. En la Figura 4 se muestra el flujo de trabajo de OWASP.

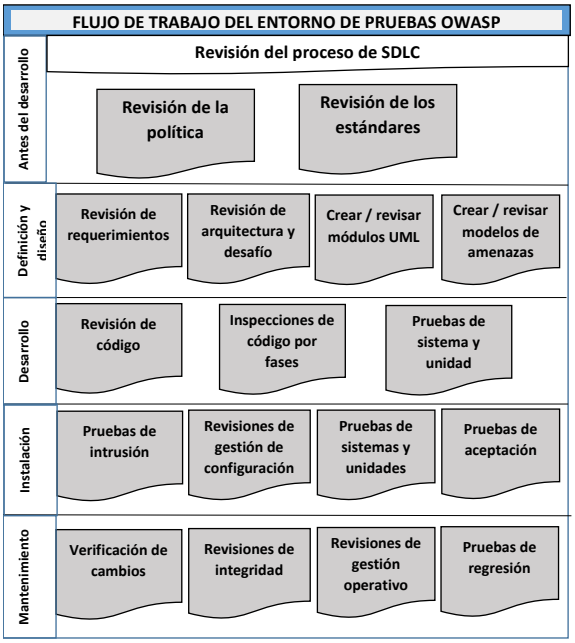

Figura 4 Flujo de trabajo del entorno de pruebas OWASP (OWASP Fundation, 2007)

Fases de la metodología

Este marco de pruebas consta de cinco fases; la f*ase 1, antes de empezar el desarrollo,* donde se tiene primero la revisión de estándares y

políticas para realizar después, el desarrollo de métricas y criterios de medición. Luego, la f*ase 2, durante el diseño y definición,* se tiene la revisión de los requisitos de seguridad, revisión de diseño y arquitectura; creación y revisión de modelos UML; así como los modelos de amenazas. Entonces viene la f*ase 3, durante el desarrollo*, donde se realiza la inspección de código por fases y revisiones de código; sigue la f*ase 4, durante la implementación,* comprende las pruebas de intrusión en aplicaciones y comprobación de gestión de comunicaciones; y por último la fase 5, *mantenimiento y operaciones*, donde se encuentra la ejecución de revisiones de la administración operativa, ejecución de revisiones de la administración operativa, ejecución de comprobaciones periódicas de mantenimiento y el aseguramiento de la verificación de cambios.

En cuanto al desarrollo de métricas y criterios de categorización de las vulnerabilidades encontradas, éstas se realizan tanto en el diseño y definición como en la ejecución del desarrollo e implementación.

4.3 PTES (Penetration testing execution standard)

Esta metodología fue realizada en base a otras de pruebas de penetración existentes a fin de hacer un standard a pesar que se enmarca en la metodología OSSTMM.

En cuanto a *Ámbito y enfoque* se adapta a cualquier ámbito de aplicación y se combina perfectamente con OWASP, dándole agilidad y cimentación a la auditoría de seguridad. Así, de acuerdo al *Alcance* PTES está orientada a niveles técnicos específicamente; por otro lado, en cuanto a la *Profundidad,* Elkan (2017) afirma que PTES son métodos básicos y guías en ciertos escenarios; pretende unir esfuerzos de analistas y expertos en seguridad para hacer un estándar que pueda completar una auditoría en todos sus procesos más habituales, cubriendo una prueba de penetración. En cuanto a *evaluación al riesgo*, esta metodología maneja niveles de riesgo dirigidos a un lenguaje para negocio y una descripción cualitativa, lo que permite una fácil comunicación con el cliente.

Sombrero blanco (2018) enuncia las 7 fases que maneja esta metodología. La primera llamada *Pre-compromiso;* en esta etapa se define el alcance de la auditoría de seguridad, la estimación del tiempo, tipo de pruebas, detalles de ingeniería social, gerentes de unidad, administradores de sistemas, denegación de servicio, calendario periódico, entregas de informe de estado y permisos para probar. Luego viene la segunda fase de *Recolección de información,* la cual busca levantar información publicada en motores de búsqueda, también se define el objetivo de la prueba. La tercera fase es el modelado de amenazas donde se identifican y clasifican los activos primarios y secundarios, realizando un mapa contra los mismos. Sigue el *análisis de vulnerabilidades*, que es la cuarta fase, aquí se realizan escáneres de aplicaciones web, ataques de fuerza bruta, monitoreo de tráfico. Luego, en la quinta fase que es *explotación* junto con las dos fases anteriores, se realiza la evasión de software o hardware que trate de impedir la auditoría, como, por ejemplo, un firewall, IDS, IPS, WAFS. En sexta fase, de post-explotación se centra la recopilación de evidencias y en cómo valorar el impacto real del ataque y hasta dónde puede llegar el sistema comprometido, incluyendo borrado de huellas y hacer persistente la intrusión mediante conexión inversa, rootkits y puertas traseras entre otros. En la última fase, involucra la realización de informes técnicos y ejecutivos como resultado de la auditoría de seguridad.

En la Figura 5 se muestra las fases de la metodología PTES.

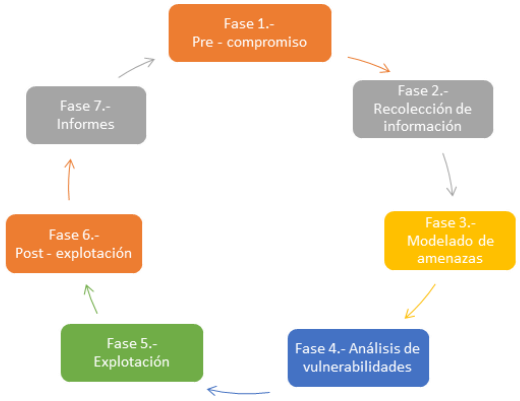

Figura 5.- Fases de la Metodología PTES

4.4 ISSAF(Information Systems Security Assessment Framework)

ISSAF se utiliza principalmente para cumplir los requisitos de evaluación de seguridad de una organización; proporciona procedimientos muy detallados para las pruebas de sistemas de información que reflejan situaciones reales. Este marco de evaluación no se enfoca en pruebas exhaustivas de penetración buscando continuidad del negocio, sino busca validar políticas de alineación del negocio con las realidades internas de TI (OISSG, 2006).

De acuerdo al *ámbito y enfoque,* esta metodología es utilizada para cumplir los requisitos de evaluación de las organizaciones y puede utilizarse además como referencia para nuevas implementaciones relacionadas con la seguridad de la información. Así, en cuanto al *alcance,* está diseñada para evaluar una red, los sistemas y la aplicación de controles que de acuerdo a web OISSG, abarcan IEC/ISO 27001:2005 (BS7799), Sarbanes Oxley SOX404, CoBIT, SAS70 y COSO. Acerca de la *profundidad*, ésta metodología se agrupa en 4 áreas de aplicación de pruebas que poseen a su vez subáreas de aplicación específicas: seguridad de redes, seguridad del host, seguridad de aplicaciones, seguridad de base de datos.

OISSG (2006), afirma en este marco referencial de seguridad con respecto a la evaluación de riesgo que se realizan primeramente la evaluación de impacto en el negocio de una amenaza contra un activo, el cual puede ser medido o estimado; posteriormente el evaluador puede elegir promediar o sumar valores de los parámetros de evaluación. Luego, se realiza la evaluación de verosimilitud, que es la probabilidad de que se presente la amenaza para la entidad de evaluación elegida, puede estimarse o medirse. Una vez obtenidos los dos resultados, se suman, obteniendo el riesgo inherente para la entidad en estudio.

Fases de la metodología

Esta metodología se compone en 3 fases: la primera f*ase es Planificación y preparación*. - En la primera fase se firma un contrato en el que queda legalizado el alcance de la evaluación, así como funciones, responsabilidades, garantía, las metodologías y herramientas a utilizarse. Además, se busca reunir una imagen completa de la infraestructura tecnológica de la información que servirá de base para la fase de evaluación. La segunda f*ase,* que es*, Evaluación*. está dividida en 2 categorías: Identificación del riesgo inherente y evaluación de controles. En la primera se identifican todos los riesgos relevantes según el impacto y la probabilidad que se produzca una amenaza independientemente de los controles realizando actividades como identificación de entidades de evaluación, que pueden ser procesos o activos, instalaciones, entre otros; luego se identifican las amenazas y vulnerabilidades utilizando herramientas de escaneo; y por último a través de pruebas de penetración se verifican las amenazas que podrían explotar una o más vulnerabilidades, las cuales son consideradas riesgos para las entidades de evaluación. En la segunda, se realiza la evaluación de controles para evaluar el riesgo residual; aquí, se evalúa el control a fin de verificar que está contribuyendo a reducir el impacto de un determinado parámetro de evaluación a nivel aceptable, dando como resultado el riesgo residual para la entidad de evaluación. En la f*ase 3, Informe-limpieza-destrucción de objetos*, los auditores preparan un informe dirigido a la alta gerencia, basado en los hallazgos encontrados y el nivel de cumplimiento que la

organización ha alcanzado. A la vez borran o limpian todas las huellas del proceso. En la Figura6 se muestran las fases de la metodología ISSAF.

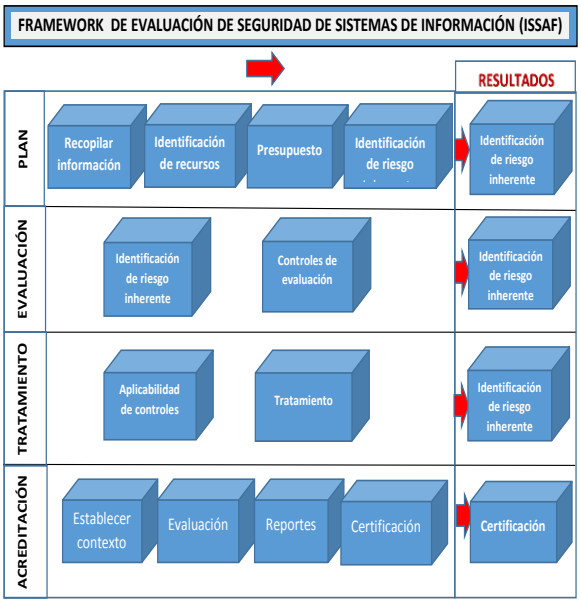

Figura 6..Fases a seguir en la metodología ISSAF
Fuente: (OISSG, 2017)

4.5 CVSS (Common Vulnerability Scoring System)

FIRST Improving Security Together (2017) afirma que esta metodología provee una manera de capturar las principales características de vulnerabilidad y producir una puntuación numérica que refleje su gravedad. Así, mantiene métricas que permite traducir en una representación cualitativa como crítica, baja, media, alta, a fin de ayudar a las organizaciones a evaluar y a priorizar sus procesos de gestión de vulnerabilidad. .En cuanto al *ámbito y enfoque,* esta metodología puede ser utilizada en cualquier empresa que necesite evaluar los riesgos de sus vulnerabilidades, ya que, de acuerdo a López (2015), proporciona un método estándar y abierto para estimar el impacto de la explotación de ellas. En cuanto a la *Profundidad,* esta metodología tiene varias métricas de evaluación, alcanza un alto nivel de detalle para su análisis y su usabilidad, ya que existen plantillas y fórmulas para aplicar las vulnerabilidades y calcular el nivel de riesgos.

De acuerdo a Sánchez (2014), CVSS mantiene *métrica*s para evaluar vulnerabilidades según el peligro que conlleva la misma. Se compone de tres grupos: base, temporal y ambiental. Las métricas base representan las características de una vulnerabilidad que son constantes en el tiempo y en los entornos del usuario; están subdivididos en métricas de explotabilidad y las métricas de impacto. Así, las primeras métricas reflejan la facilidad y los medios técnicos para explotar la vulnerabilidad. Por otro lado, las métricas de impacto reflejan la consecuencia directa de una explotación exitosa y representan la consecuencia de aquello que sufre el impacto, al que nos referimos formalmente como el componente afectado. Siguiendo con el grupo de métrica temporal refleja las características de una vulnerabilidad que puede cambiar a lo largo del tiempo, pero no a través de los entornos de usuario. Por otro lado, el grupo de métrica ambiental representa las características de vulnerabilidades que son relevantes y únicas para el entorno de un usuario en particular y se muestran en la Figura 7.

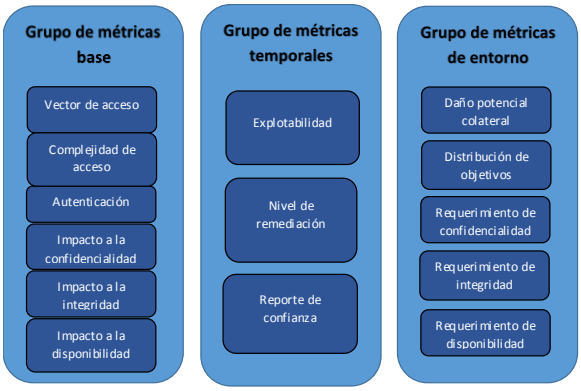

Figura 7.- Tipos de métricas para calcular el nivel de riesgos.

La puntuación de las métricas de CVSS también produce una cadena de vectores, una representación textual de los valores de métrica utilizados para calificar la vulnerabilidad. Esta metodología proporciona puntajes de vulnerabilidad estandarizados. Cuando una

organización utiliza un algoritmo común para calificar vulnerabilidades en todas las plataformas de TI, puede aprovechar una sola política de administración de vulnerabilidades que define el tiempo máximo permitido para validar y remediar una vulnerabilidad

4.6 METODOLOGÍA PROPUESTA ORIENTADA A RIESGOS

Esta nueva metodología está realizada considerando aspectos encontrados y analizados en las metodologías OSSTMM, OWASP, ISSAF, PTES, CVSS. Con respecto al enfoque y ámbito, ésta metodología podrá ser referencia para todas las empresas independientemente de su tamaño y su industria; está orientada a verificar las seguridades implantadas en la empresa y a la vez, definirá una serie de pasos a seguir a fin de realizar las pruebas necesarias de penetración a los sistemas implantados con el propósito de encontrar vulnerabilidades que pueden estar expuestos mencionados sistemas o activos de la empresa.

Tabla 1.- Tabla comparativa de características generales de metodologías de pruebas de penetración

Características	OSSTMM	OWASP	PTES	ISSAF	CVSS	Metodología propuesta
Ámbito y enfoque	Enfoque operativo, para cualquier empresa que quiera evaluar la seguridad de la información	Se enfoca en entornos de aplicaciones web de cualquier organización	Se adapta a cualquier ámbito de aplicación	Se enfoca en cumplir los requisitos de evaluación de seguridad de una organización	Enfocada a análisis y evaluación de riesgos de cualquier organización	Enfoque operativo, para cualquier empresa que quiere evaluar la seguridad de información
Alcance	Abarca equipos y sistemas asociados a la red	Auditoría en aplicaciones web, en todo el ciclo de la implementación.	Está orientado a niveles técnicos específicamente	Evalúa la red, los sistemas y la aplicación de controles ISO 27001, COBIT, SAS70 y COSO.	Abarca riesgos en vulnerabilidades de todos los equipos y software.	La evaluación y auditoría de equipos y sistemas; siguiente ISO 27001.
Profundidad	Análisis en detalle	Analiza en detalle lo concerniente a la seguridad de la aplicación	Esta metodología se enmarca en la metodología OSSTMM y se combina con OWASP	Proporciona procedimientos muy detallados para las pruebas de sistemas de información	Esta metodología tiene varias métricas de evaluación, alcanza un alto nivel de detalle para su análisis.	Proporciona procedimientos muy detallados para las pruebas de sistemas de información.
Usabilidad	Requiere de capacitación y es categorizada como nivel medio en usabilidad	Usabilidad alta en aplicaciones web	Usabilidad baja, no tiene procedimientos actualizados	Usabilidad media	Tiene una usabilidad alta, ya que existen plantillas y fórmulas para aplicarlas en pruebas de penetración	Usabilidad alta.
Métricas	Definidas para medir el grado de seguridad de los activos, utiliza mediciones objetivas llamadas RAV	Posee métricas para categorizar y evaluar los riesgos	Maneja niveles de riesgos dirigidos a un lenguaje para negocio y una descripción cualitativa para una buena comunicación con el cliente.	Puede medir o estimar la amenaza contra un activo. No hay establecidas métricas.	Posee métricas para categorizar y evaluar los riesgos	Posee métricas para categorizar y evaluar los riesgos.
Evaluación del riesgo	Aplica los RAV para cuantificar con precisión, los niveles de riesgos; los mismos que están integrados en cada módulo de operación.	Aplica métricas para evaluar y valorar los riesgos.	No maneja evaluación del riesgo propio, se enmarca en lo establecido en la metodología OSSTMM	Se realiza la evaluación de verosimilitud, que es la probabilidad de que se presente la amenaza para la entidad de evaluación elegida. Puede estimarse o calcularse.	Aplica calculadora y fórmulas establecidas para la valoración	Aplica métricas para evaluar y valorar los riesgos.

Así también se analizarán las vulnerabilidades encontradas a fin de establecer si pueden ser realmente explotadas mediante herramientas informáticas que se encuentran el en mercado. Posteriormente, se realiza la matriz de riesgo, donde se asignarán riesgos que conllevan la materialización de las amenazas con la explotación de las vulnerabilidades; impactando a la organización en diferentes niveles. Es por esto, que se evalúa y se valoriza el riesgo en base a un análisis de costo / beneficio utilizando métricas; dando como resultado la aplicación de la gestión del riesgo por medio de acciones de políticas, controles y procedimientos.

Refiriéndose al *alcance*, la metodología aplicada en la auditoría, abarcará todos los aspectos técnicos físicos y lógicos que inciden en la seguridad de la información de los activos de valor de la empresa. De acuerdo a la *profundidad*, esta metodología persigue analizar las vulnerabilidades existentes en toda la infraestructura de Tecnología de Información; esto es enfocado en el hardware, software y servicios; esto son equipos de red, aplicaciones web y locales; así también servicios TI que dan dentro y fuera de la empresa. Todo esto, utilizando las mejores prácticas en aplicación de herramientas; entonces, utilizando métricas adecuadas y buenas prácticas basadas en estándares internacionales se logran valorar los riesgos y clasificarlos con el fin de gestionarlos para mantener la seguridad de la información.

4.6.1 Fases de la propuesta de metodología

La nueva metodología divide en 4 fases que abarcarán todo el ciclo de auditoría en tecnología, incluyendo evaluación de riesgos:

4.6.1.1 Fase 1.- Acuerdo, alcance y recopilación de información.

En esta fase se definirán acuerdos y alcance de la auditoría con el comité gerencial de la empresa, para lograrlo de manera exitosa, se utilizan formatos, plantillas que se exponen en el capítulo 2 del manual OSSTMM versión 3.0 y al capítulo 4 del marco de seguridad ISSAF versión 0.2.1. Luego, se levanta la información de todos los activos de la empresa basándose en un análisis de impacto o riesgo con respecto a los objetivos de la empresa; obteniendo los que intervendrán en las pruebas de penetración.

Con esta información se procede a realizar la programación de las siguientes fases de la metodología.

4.6.1.2 *Fase 2. Ejecución.*

Esta es la fase que se lleva a cabo el escaneo de vulnerabilidades, evaluación de seguridad y pruebas de penetración. Para ello se definen primeramente las líneas tecnológicas a aplicar las pruebas.

Líneas tecnológicas a aplicar las pruebas de penetración.

Las líneas de aplicación donde se aplicarán las pruebas de penetración, serán: Infraestructura de red (ethernet, inalámbrica, elemento de seguridad, accesos remotos), sistemas operativos (plataformas, versiones), servicios (firewall, IDS, IPS, honey pots) y aplicaciones (locales y ámbito web).

Escaneo o recopilación de información

Este paso es fundamental para el éxito de las pruebas de penetración. Por esto, se debe recopilar todos los datos posibles, categorizados en 2 aspectos: información pública del sistema (footprinting) e información concreta como sistemas, elementos de red, mecanismos de seguridad, versiones de los sistemas (fingerprinting).

Footprinting

La información pública o footprinting se puede obtener por medio de técnicas avanzadas en buscadores como google o bing, páginas web especializada como www.netcraft.com ó www.goolag.org, herramientas especializadas para búsqueda como maltego, netblug, herramientas para obtener datos de servidores web y herramientas para extracción de los metadatos de los documentos de los sitios web como Foca, anubis.

Fingerprinting

A fin de obtener información concreta, se realiza la fase de sondeo y fase de enumeración. El primero es una actividad que intenta una conexión a cada uno de los sistemas para provocar una respuesta y extraer información; aquí se utilizan herramientas de escaneo como nmap, netcat, traceroute. Por otro lado, la enumeración se utiliza para obtener información detallada y precisa de un objetivo.

Evaluación de seguridad

A continuación, se determina el nivel de seguridad que se aplicará a la organización dependiendo de la madurez en que se encuentre, con el fin de determinar el tipo pruebas de penetración a ejecutarse. Para ello, se utiliza el modelo de madurez expuesto en la

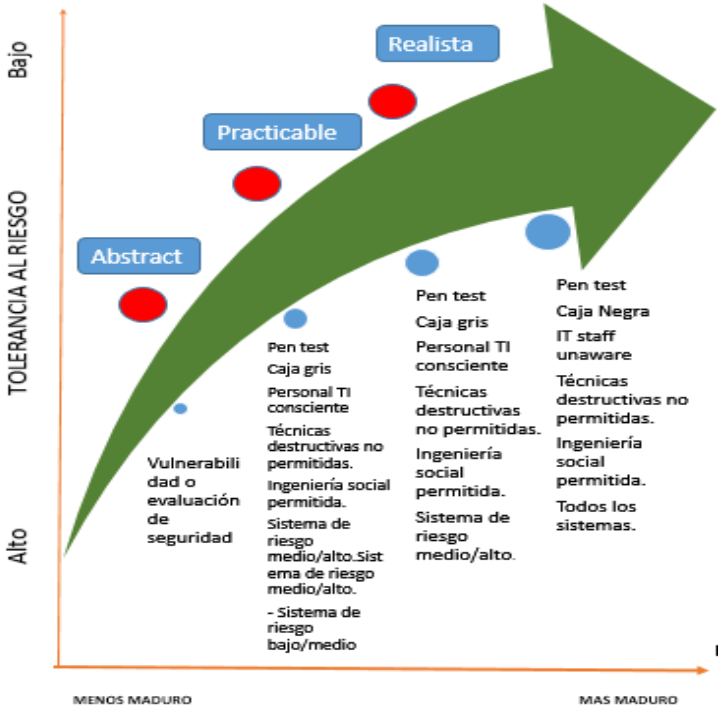

Figura 5.

Figura 5.- Modelo de madurez para pruebas de seguridad de la información. ISACA (2016)

Pruebas de penetración

Haciendo referencia a las metodologías estudiadas, se debe considerar para las pruebas de las líneas de aplicación antes mencionadas, la información expuesta en el manual OSSTMM versión 3.0, el capítulo 9 – Wireless security testing y capítulo 11 – Data network security testing. Así mismo, del marco de seguridad ISSAF version 0.2.1, se consideraran los capítulos: "E"- password security testing, "F"-switch security assessment, "H"-Firewall security assessment, "I"-Intrusion detection system security assessment, "J"-VPN security asseessment, "M"- WLAN security assessment, "Q"-Unix-linux system security assessment, "R"-Windows system security assessment, "T"-web server security assessment , U-web application security assessment, V-Web application security assessment, Z-database security assessment. Además, se referencia a la metodología OWASP versión 3.0, capítulo 4 – pruebas de intrusión de aplicación web.

Tipo de prueba de penetración

Luego, se establece tipo de pruebas de penetración en función del conocimiento del auditor y las áreas, así puede ser, caja negra, caja blanca, caja gris.

Una vez establecido el tipo de prueba de penetración, se procede a ejecutarlas mediante el análisis y explotación de vulnerabilidades

Análisis de Vulnerabilidades

Una vez obtenida la información se procede a realizar el análisis de vulnerabilidades. Para esto, se utilizará herramientas automáticas como OpenVas, Nessus, las cuales sondean posibles vulnerabilidades a partir de datos que se recopilan sobre sistemas operativos, servicios, aplicaciones con ámbito local como web, realizando un diseño de infraestructura de red donde se visualiza la ubicación, funcionalidad, de elementos de software y hardware instalados en la misma, donde se realiza el análisis de las vulnerabilidades o debilidades que puedan presentar los mismos.

Explotación de vulnerabilidades e intrusión

Luego del análisis de vulnerabilidades se procede a explotar las mismas, esto es, materializar la amenaza en las aplicaciones o elementos de red que se encontraron mencionadas vulnerabilidades. Para ello, se utiliza un conjunto de técnicas y herramientas de hacking ético que pueden ser ejecutadas de forma manual o automática. Una vez explotadas se tratan de escalar los privilegios a fin de aumentar los permisos para acceder a otros servicios, utilizando técnicas hacking como sniffer, keylogger, rootkit. Como opcional se realizará la eliminación de huellas, borrando la información de los registros de cada una de las intrusiones.

4.6.1.3 Fase 3.- Evaluación de riesgo. - En esta fase se genera una matriz de riesgos con respecto a cada activo definido en la primera fase y en base al análisis de vulnerabilidades, pruebas de penetración realizadas en la fase 2. A continuación, se aplican métricas que categoricen los riesgos, para finalmente evaluarlos dependiendo del impacto a los objetivos de la empresa. En esta fase, también se puede definir los controles y procedimientos que se deberían utilizar para mitigar los riesgos encontrados.

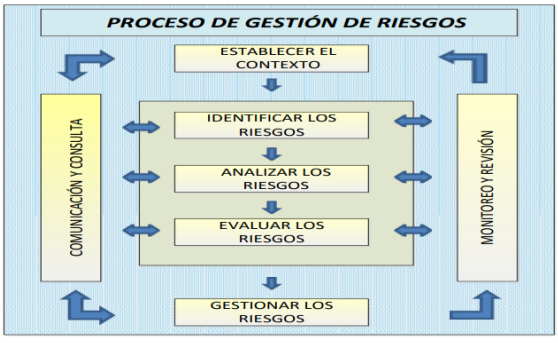

Figura 6. Proceso de Gestión de Riesgos

Analisis de riesgos

Una vez identificadas las vulnerabilidades y las amenazas, se determinan los riesgos inherentes y se procede a realizar el análisis de cada riesgo; el mismo que consiste en determinar la probabilidad de ocurrencia de los mismos, así como su impacto. Para ello se considera tres variables: probabilidad, impacto e importancia. Para la primera variable se utilizará la tabla No. 1.

Tabla 1.- Escala de probabilidad de ocurrencia de una menaza.

Valor	Escala	Concepto
3	Muy probable	Puede suceder 1 vez al año y ha sucedido otras veces
2	Probable	Puede ocurrir alguna vez/ha ocurrido una sola vez
1	Improbable	No ha ocurrido antes pero puede ocurrir en circunstancias excepcionales.

Por otro lado, para determinar la segunda variable que es el impacto, se utilizará la tabla No. 2

Tabla No. 2.- Escala del impacto de materialización de un riesgo

Valor	Escala	Concepto
3	Alto	Las consecuencias amenazarán los objetivos y la supervivencia de la organización
2	Medio	Las consecuencias harán realizar cambios significativos en la organización o sus operaciones.
1	Bajo	Las consecuencias pueden solucionarse con cambios y aplicación de políticas.

Finalmente, para determinar la tercera variable, que es la relevancia e importancia del riesgo, el cual se muestra en la tabla No. 3.

Tabla No. 3.- Escala de relevancia de un riesgo

Valor	Escala	Concepto
10	Alta	Factor de riesgo relevante o muy importante para la organización o entidad.
5	Media	Factor de riesgo de relevancia media para la organización o entidad.
1	Baja	Factor de riesgo no relevante para la organización

Evaluación del riesgo

A fin de evaluar el riesgo, se lo clasifica de acuerdo a los resultados obtenidos en las variables definidas en la sección anterior, análisis de riesgo. Para ello se utiliza la escala de clasificación del riesgo, que se muestra en la tabla No. 4.

Tabla No. 4 Escala de evaluación del riesgo.

Calificación Final	Riesgo	Color
De 1 a 10	Bajo	Verde
De 11 a 30	Aceptable	Naranja
De 31 a 90	Alto	Rojo

Una vez definidas los parámetros o escalas para la revaluación del riesgo, se procederá a calificarlos en la matriz de riesgos; obteniendo de manera automática el resultado de acuerdo con el color establecido.

Para realizar la evaluación, se debe considerar las calificaciones obtenidas. Si el riesgo es bajo, permite a la organización asumirlo, esto es, que no es necesario establecer controles ya que su ocurrencia es mínima, su impacto es bajo y su grado de importancia baja.
Sin embargo, si el riesgo es aceptable o alto, significa que la posibilidad de ocurrencia puede ser muy probable, por lo que es necesario implementar medidas de control que permitan disminuir el grado de impacto.

Valoración de riesgos

En la valoración de los riesgos es donde se establecen las prioridades y revisión de controles; los cuales pueden ser preventivos o correctivos. El tipo de control preventivo es aquel que elimina la causa del riesgo y prevenir su ocurrencia o materialización; y correctivos, aquel que reestablecen la actividad luego que se materializa la amenaza. Además se debe determinar si el control está documentado, si se está aplicando en la actualidad y si es efectivo para minimizar el riesgo.
Por lo que se realiza la valoración de riesgos en función de la evaluación de controles, tal como lo muestra la tabla No. 5.

Tabla No. 5 Criterios para la valoración del riesgo

Criterios	Valoración del riesgo
No existen controles	Se mantiene el resultado de la evaluación
Existen controles pero no son efectivos	Se mantiene el resultado de la evaluación
Si existen controles pero no están documentados	Cambia el resultado a un valor inferior, se debe documentar
Si existen controles y están documentados	Cambia el resultado a un valor inferior.

Gestión o tratamiento de los riesgos

En esta gestión o tratamiento se identifican las opciones para mitigarlos, esto es, realización de acciones dentro de un plan de mejoras; Sin embargo, es pertinente analizar el costo beneficio de la gestión de riesgo para tomar la mejor decisión.

Fase 4. Generación de informes. - En esta fase se elaboran los informes técnicos y ejecutivos. En el informe técnico se mostrarán las vulnerabilidades encontradas en los activos físicos y lógicos, además de las herramientas utilizadas para ello. El informe ejecutivo consta primeramente de los riesgos en que puede incurrir la empresa y los controles o procedimientos adecuados que se deberían implementar en base a un análisis costo/beneficio. Haciendo referencia a las metodologías estudiadas, se pueden utilizar lo enunciado en el manual OSSTMM versión 3.0 – capítulo 13 – Reporting with the STAR. Así también en el marco ISSAF versión 0.2.1 – capítulo 5 – Phase III – Post Assessment. Por último, en la guía de pruebas de OWASP versión 3.0 – capítulo 5.2, “como escribir el informe de pruebas”.

A continuación, en la figura 7, se muestra el diagrama de la nueva propuesta metodológica para pruebas de penetración.

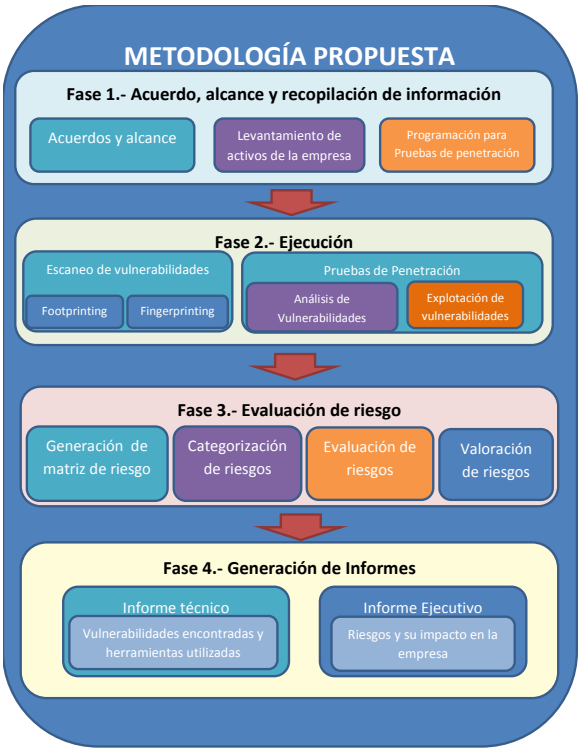

Figura 7.- Diagrama de la metodología propuesta para pruebas de penetración

CONCLUSIONES, LIMITACIONES Y TRABAJOS FUTUROS.

La aplicación de la nueva metodología permitirá que los auditores tengan una forma de abarcar además de la parte técnica, la parte de evaluación de riesgos, aplicando métricas y categorizando de acuerdo a su impacto. Así también, se pretende establecer controles y procedimientos de seguridad para proteger los activos de valor de la empresa.

La revisión de literatura exhaustiva permitió conocer al detalle cada una de las bondades de las metodologías utilizadas actualmente como son la OSSTMM, ISSAF, PTES, CVSS, con lo cual se establecieron características y mejores prácticas para la nueva metodología propuesta.

La metodología CVSS si bien es cierto no es una metodología enfocada en el análisis de vulnerabilidades y explotación; se acopla de muy buena manera a las metodologías que dan el resultado de vulnerabilidad como OSSTMM, OWASP, PTES, ISSAF, a fin de establecer un estándar de métricas para el análisis y evaluación de riesgos, estableciendo categorización de impactos a la empresa.

Como limitación de la investigación se obtuvo que, en todas las metodologías estudiadas, no intervenían el aspecto de riesgos por lo que las métricas de riesgo, así como aspecto de evaluación del mismo lo determinaron las metodologías OSSTMM, ISSAF y CVSS.

Con la implementación de la fase de evaluación del riesgo en la nueva propuesta metodológica, permite determinar los factores de riesgo que, al no determinarlo y combatirlo, pueden disminuir la capacidad de la organización para cumplir sus objetivos. Así también determinar los factores internos o externos de riesgo de mayor incidencia y sus consecuencias sobre las personas, recursos o procesos, permite coordinar las acciones necesarias y alcanzar los objetivos institucionales.

El propósito de la propuesta metodológica es identificar métodos de acción que se podrían utilizar para afectar de alguna manera un determinado sistema, obteniendo evidencias concretas y certeras que sean funcionales y que sirvan como insumos para proteger los sistemas a ser analizados. Adicionalmente, es necesario tomar en cuenta que es indispensable realizar pruebas periódicas de funcionamiento, mantenimiento y privacidad del sistema, puesto que a pesar de las precauciones que se tomen para evitar los ataques, no siempre todas las metodologías empleadas serán suficientes para mitigar las posibles y futuras amenazas.

Es fundamental que la metodología a utilizarse en la auditoría y en las pruebas de penetración debe ser integral a fin de revisar todos los procesos y así poder entregar informes que contemplen tanto la sección técnica como la sección estratégica incluyendo valoración de riesgos dependiendo de las vulnerabilidades de alto impacto para los objetivos de la empresa.

Se concluye que tener establecidos controles en todos los procesos relacionados con la seguridad de la información es imprescindible para que las empresas puedan sobrevivir en esta era donde nuevas amenazas surgen periódicamente y con ella riesgos que atentan a los objetivos de la organización.

Como investigación futura, se puede abordar el análisis de aplicación de las metodologías de pruebas de penetración en las empresas del Ecuador, así como las medidas y controles gestionados a partir de los resultados obtenidos; de manera que se pueda establecer cuáles son las herramientas técnicas mayormente utilizadas y a la vez cuales son los controles y procedimientos que han sido eficientes en la gestión de riesgos identificados.

Referencias Bibliográficas

Alonso Romero, L. (2002). *Seguridad Informática. Conceptos generales*. Obtenido de http://campus.usal.es/~derinfo/Activ/Jorn02/Pon2002/LARyALSL.pdf

Bhawana, S., Ankit, N., & Shashikala, K. (2014). Study Of Ethical Hacking. *International Journal of Computer Science Trends and Technology (IJCST), 2*(4), 6-10.

Broad, J., & Brindner, A. (2014). *Hacking with Kali: Practical Penetration Testing Techniques.* Waltham: Elsevier.

Caballero Quezada, A. E. (30 de 12 de 2013). *Metodologías y frameworks para pruebas de penetración.* Obtenido de http://www.reydes.com/d/?q=Metodologias_y_Frameworks_para_Pruebas_de_Penetracion

Cano, J. (31 de 03 de 2017). *Auditoría de seguridad, evaluación de seguridad y pruebas de penetración: tres paradigmas en la seguridad informática.* Obtenido de https://www.helasconsultores.com/data/documentos/Microsoft%20Word%20-%2058_auditoria_seguridad.pdf

Cotoira, F. (2017). Pruebas de penetración para principiantes: explotando una vulnerabilidad con Metasploit framework. .*Seguridad*.

Dávalos Suñagua, A. F. (2013). Auditoría de seguridad de información. *Fides ET Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*, 19-30.

DELOITTE. (Noviembre de 2015). *COSO Evaluación de Riesgos.* Obtenido de https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/Evaluacion-Riesgos-COSO.pdf

Díaz Duarte, D. (2005). Toma de decisiones: el imperativo diario de la vida en la organización moderna. *ACIMED*.

Díaz-Bravo, L., Torruco-García, U., Martínez-Hernández, M., & Varela-Ruiz, M. (2013). La entrevista, recurso flexible y dinámico. *Elsevier*, 162-167.

Elkan, M. (08 de 08 de 2017). *Auditoría de seguridad, hacking ético y prueba de penetración.* Obtenido de http://blogdeauditoriadeseguridad.blogspot.com/2017/09/metodologia-ptes-penetration-testing.html

ESET Latinoamérica. (21 de Abril de 2016). *WELIVESECURITY.* Recuperado el 22 de 06 de 2016, de ESET Security Report Latinoamérica 2016: http://www.welivesecurity.com/wp-

content/uploads/2016/04/eset-security-report-latam-2016.pdf

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

Fernandes Belarmino, V., & Junqueira Araújo, W. (2014). Análisis De Vulnerabilidades Computacionales En Repositórios Digitales. *Biblios*, 1-17.

Fernández Carballo, R. (2001). La entrevista en la investigación cualitativa. *Revista Pensamiento Actual*, 14-19.

FIRST Improving Security Together. (2017). *Sistema común de puntuación de vulnerabilidad v3.0.* Obtenido de https://www.first.org/cvss/specification-document

Franco, D., Perea, J., & Tovar, L. (2013). Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. *Información Tecnológica*, 13-22.

Fuertes, W., Guagalango Vega, R. N., & Moscoso Montalvo, P. E. (Agosto de 2011). Evaluación técnica de la seguridad informática del Data Center de la Escuela Politécnica del Ejército. Sangolquí, Quito, Ecuador.

Hernández Saucedo, A. L., & Mejia Miranda, J. (2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones Web. *Recibe*, 1-17.

Herzog, P. (23 de Agosto de 2003). *Manual de la metodología abierta de testeo de seguridad OSSTMM*. Obtenido de http://fcbi.unillanos.edu.co/segurinfo.unillanos/archivos/materialApoyo/OSSTMM.es.2.1.pdf

Herzog, P. (2010). *OSSTMM-3: Open Source Security Testing Methodology Manual.* ISECOM.

INNOVA SECURE. (15 de 08 de 2017). *Mitos sobre pruebas de penetración.* Obtenido de http://innovasecure.com/mitos-sobre-las-pruebas-de-penetracion/

International Organization for Standarization. International Electrotechnical Commission. (2009). *Guia ISO-CEI 73.* Obtenido de https://mybmt.org/wp-content/uploads/2017/10/Cap-1-8-2-a-6-Guia_ISO-IEC-73.pdf

ISACA. (2009). Virtualization Security. *ISACA JOURNAL VOLUME 1* .

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

ISACA. (2016). *Planificación de pruebas de seguridad de la información - Un enfoque práctico.* Obtenido de https://www.isaca.org/Journal/archives/2016/volume-5/Pages/planning-for-information-security-testing-spanish.aspx

ISECOM. (2017). *Open Source Security Testing Methodology Manual (OSSTMM).* Obtenido de http://www.isecom.org/research/osstmm.html

Junta de Andalucía. (2011). *Metodología y frameworks de testeo de la seguridad de las aplicaciones.* Obtenido de http://www.juntadeandalucia.es/servici

os/madeja/sites/default/files/historico/1.3.0/contenido-recurso-216.html

Lakshmi S, C., & Basarkod, P. (2015). Basics of ethical hacking. *International journal of enigineering sciencies & emerging technologies* , 715-720.

López, A. (21 de 07 de 2015). *Métricas de evaluación de vulnerabilidades: CVSS 3.0*. Obtenido de https://www.certsi.es/blog/cvss3-0

López, P. A. (2010). *Seguridad informática.* Editex.

López-Gómez , E. (2018). El método Dephi en la investigación actual en educación: una revisión teórica y metodológica. *Educación XX1*, 17-40.

Machado Bello, X. A., & Castillo Orozco, Y. M. (2016). Gestión de riesgos en las IES. *Revista estratégica y gestión universitaria*, 118-129.

Monsalve-Pulido, J., Aponte-Novoa, F. A., & Chaves-Tamayo, D. F. (2014). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia) . *Revista Facultad de Ingeniería* , 65-72.

Mora Quirós, E. (2017). Auditoría Informática. *Instituto de auditores internos*, 1-12.

OISSG. (30 de Abril de 2006). *Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1.* Obtenido de http://www.oissg.org/files/issaf0.2.1.pdf

OISSG. (2017). *INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK (ISSAF).* Obtenido de http://www.oissg.org/issaf.html

OWASP Fundation. (2007). Guíade pruebas OWASP. *Attribution-ShareAlike 2.5*, 1-309.

Pérez Fernández, M. (02 de 2012). *Metodologias más usadas en pentesting. Estudio comparativo.* Obtenido de https://es.scribd.com/doc/98081446/Metodologias-mas-usadas-en-pentesting-Estudio-comparativo

Pill, J. (1971). The Delphi method: Substance, context, a critique and an annotated bibliography. *Socio-Economic Planning Sciences*, 57-71.

Powell, C. (2003). The Delphi technique:myths and realities. *Journal of advanced nursing*, 376-382.

Pozo Zulueta, D., Quintero Ríos, M., Hernández Aguilar, V., Gil Loro, L., & Lorenzo Álvarez, M. (2009). Procedimiento para pruebas de intrusión en aplicaciones Web. *Revista Española de Innovación, Calidad e Ingeniería del Software*, 70-76.

Ramirez Castro, A., & Ortiz Bayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería*, 56-66.

Ramos Ramos, J. L. (2013). Pruebas de Penetración. *Revista de Información, Tecnología y Sociedad*, 31-33.

Rodríguez López, M., Piñeiro Sánchez, C., & De Llano Monelos, P. (2013). Mapa de Riesgos: Identificación y Gestión de Riesgos. *Atlantic Review of Economics - 2nd Volume*, 1-29.

Salinas Galindo, L. M., & Vásquez Ortiz, J. (2013). *Implementación de pruebas de penetración a los sistemas informáticos de una entidad gubernamental.* Obtenido de http://polux.unipiloto.edu.co:8080/00000759.pdf

Sánchez Sánchez, L. R. (2015). COSO ERM y la Gestión de Riesgos. *QUIPUKAMAYOC*, 1-8.

Sánchez, E. (14 de Octubre de 2014). *Análisis del CVSS de ShellShock*. Obtenido de https://hacking-etico.com/2014/10/14/analisis-del-cvss-de-shellshock/

Santiago Chinchilla, E. (2009). Test de penetración como apoyo a la evaluación de riesgos en seguridad de la información. *Prospectiva*, 41-45.

Serrato Polanía, G. (2016). Metodología para el análisis de vulnerabilidades. *TIA*, 20-27.

Servicios Expertos. (12 de 02 de 2017). *Gestión de Vulnerabilidades.* Obtenido de https://www.ransecurity.com/wp-content/uploads/2015/05/S.E._Gestion_de_Vulnerabilidades.pdf

Sheoran, P., & Singh, S. (2014). Applications of Ethical Hacking. *International Journal of Enhanced Research in Science Technology & Engineering*, 112-114.

Sombrero blanco, Hacking ético. (19 de 03 de 2018). *Hacking ético.* Obtenido de http://hackingetico.somee.com/Logotipoes/PTES

Stable-Rodríguez, Y. (2012). Auditoría de información y conocimiento de la organización. *Ingeniería Industrial*, 260-271.

Steurer, J. (2011). The delphi method: an efficient procedure to generate knowledge. *Skeletal Radiol*, 959-961.

Sulca Córdova, G. C., & Becerra Paguay, E. (2017). Control interno. Matriz de riesgo: Aplicación metodología COSO II. *Revista Publicando 4 No. 12*, 106-125.

Suresh Kumar, V. (2014). Ethical Hacking and Penetration Testing Strategies. *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)*, 21-23.

Tamayo Veintimilla, O. (Junio de 2016). *Desarrollo de una guía técnica estándar para aplicar herramientas de ethical hacking en Redes de Datos, dirigido a Pymes.* Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/12612/disertaci%C3%B3ndegrado%20OswaldoTamayo.pdf?sequence=1

Tarazona, C. (2006). *Amenazas informáticas y seguridad de la información.* Obtenido de www.laccei.org/LACCEI2007-Mexico/p119.doc

Valdez Alvarado, A. (2013). OSSTMM 3. *Revista de Información, Tecnología y Sociedad*, 29-30.

Valencia, B. L. (2013). Metodologías Ethical Hacking. *Revistas Bolivianas*, 27-28.

Voutssas, J. (2010). Preservación documental digital y seguridad informática. *Investigación Bibliotecológica*, 127-155.