# PROPUESTA METODOLÓGICA PARA REALIZAR PRUEBAS DE PENETRACION EN AMBIENTES VIRTUALES

*José Adán Quispe Palacios [1], Debbie Elizabeth Pérez Vinueza [2], Mario Ron[3], Geovanny Ninahualpa[4]*

1 Universidad de las Fuerzas Armadas - ESPE, Ecuador, jose_41998_quispe@hotmail.es
2 Universidad de las Fuerzas Armadas - ESPE, Ecuador, deblizperez@hotmail.com
3 Universidad de las Fuerzas Armadas - ESPE, Ecudor, mbron@espe.edu.ec
4 Universidad de las Fuerzas Armadas - ESPE, Ecuador, gninahualpa@espe.edu.ec

## RESUMEN

*El crecimiento de los ataques a las infraestructuras de las tecnologías de la información y comunicaciones (TIC), año tras año ha sido el motivo principal para que las organizaciones realicen periódicamente pruebas de intrusión en cada uno de los elementos importantes que componen la infraestructura tecnológica de la información y así evitar que personal malintencionado se apropie de ella sacando provecho económico o generando daño en la misma.*

*Por lo anterior, este trabajo de investigación presenta la revisión y análisis de algunas fuentes de información que describen ampliamente acerca de las pruebas de penetración y las principales metodologías existentes; cuyo propósito final es dar a conocer la importancia de estas pruebas basadas en una metodología que se acople a las necesidades de la organización y que se convierta en un apoyo para lograr sus objetivos.*

## ABSTRACT

The growth of attacks to the infrastructure of the information and communication technology (TIC) year by year. It has been the main reason for organization to conduct periodical penetration test on each important element that are part of the information technological infrastructure and thus avoid malicious personnel appropriates and bringing economic benefits or creating internal damage.

Therefore, this investigation work present the review and analyze of some information source which broadly describes about penetration test and the principal existing methodologies; whose purpose is to raise awareness of the penetration test based on a methodology that match organization needs and becomes a support to archives their goals.

## 1. INTRODUCCIÓN

Los sistemas informáticos desde sus inicios han enfrentado el reto de proteger la información con la cual trabajan, y con el desarrollo tecnológico las técnicas de Seguridad Informática se han vuelto más complejos para enfrentar los ataques. Y puesto que los intrusores también han desarrollado técnicas cada vez más sofisticadas para romper dichas seguridades, se hace necesario anticiparse a dichos eventos, simulando Pruebas de Penetración.

Las Pruebas de Penetración utilizan una variedad de herramientas especializadas para hacer pruebas mucho más rápidas y eficaces para el descubrimiento de vulnerabilidades.

Al igual que otros trabajos especializados se podría usar herramientas simples, manuales, pero las herramientas automáticas diseñadas van a lograr mucho más, mucho mejor y en mucho menos tiempo.

# 2. FUNDAMENTOS TEÓRICOS

## 2.1 Modelo PDCA

Por la importancia que la información tiene dentro de una organización, esta debe plantearse un Sistema de Gestión de la Seguridad de la Información (SGSI), cuyo principal objetivo es el de proteger la información luego de identificar que activos y en qué grado serán protegidos

Un SGSI siempre cumple cuatro niveles repetitivos que comienzan por Planificar, Hacer, Verificar y terminan en Actuar, consiguiendo así mejorar la seguridad.

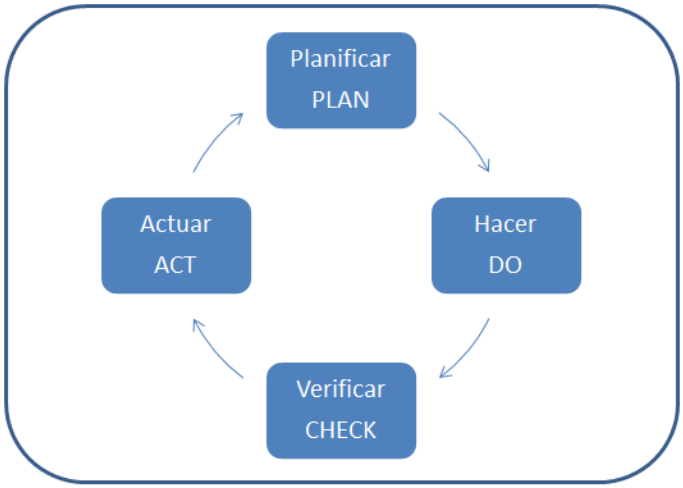



**Figura 1: Modelo PDCA**

## 2.2 Vulnerabilidades de un sistema informático

En una organización lo que se quiere proteger son sus activos, es decir, los recursos que forman parte del sistema informático, estos se agrupan en:

- Hardware: son todos los elementos físicos del sistema informático, como: procesadores, electrónica y cableado de red, medios de almacenamiento (discos, cintas, DVDs, etc.).
- Software: estos son los elementos lógicos o programas que se ejecutan sobre el hardware, como por ejemplo el mismo sistema operativo, o las aplicaciones.
- Datos: comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red.
- Otros: fungibles, personas, infraestructuras, aquellos que se usan y gastan como puede ser la tinta y papel en las impresoras, los soportes tipo DVD o incluso cintas si las copias se hacen en ese medio, etc.

Los más críticos son los datos, el hardware y el software, ya que estos datos son almacenados en el hardware y que son procesados por las aplicaciones software.


**Figura 2: Recursos que forman parte del sistema**

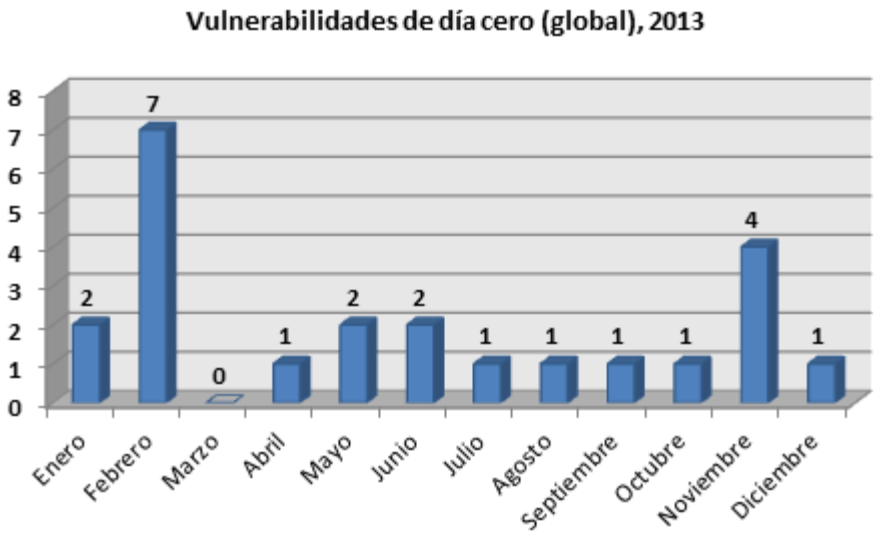



**Figura 3: Vulnerabilidades de día cero**

**Fuente: Brian Sullivan, 2014**

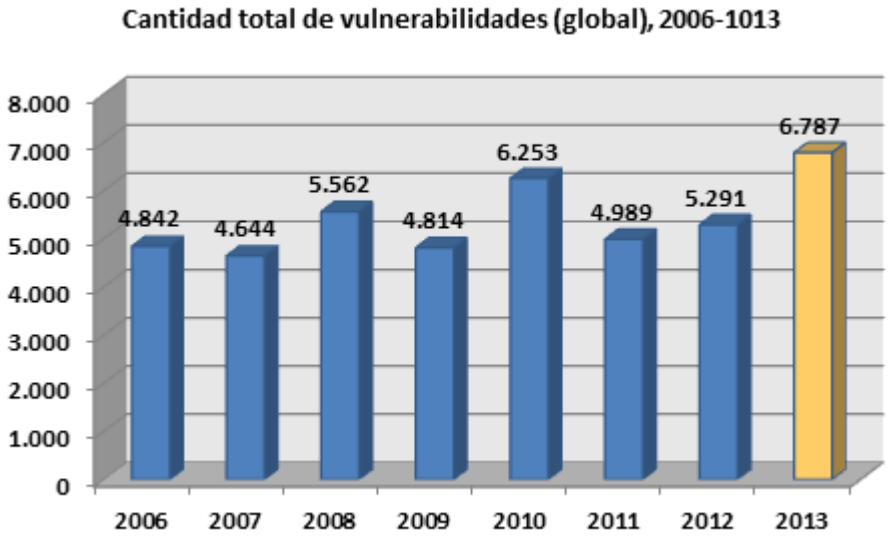



**Figura 2. 1: Cantidad total de vulnerabilidades años 2006 a 2013**

**Fuente: Brian Sullivan, 2014**

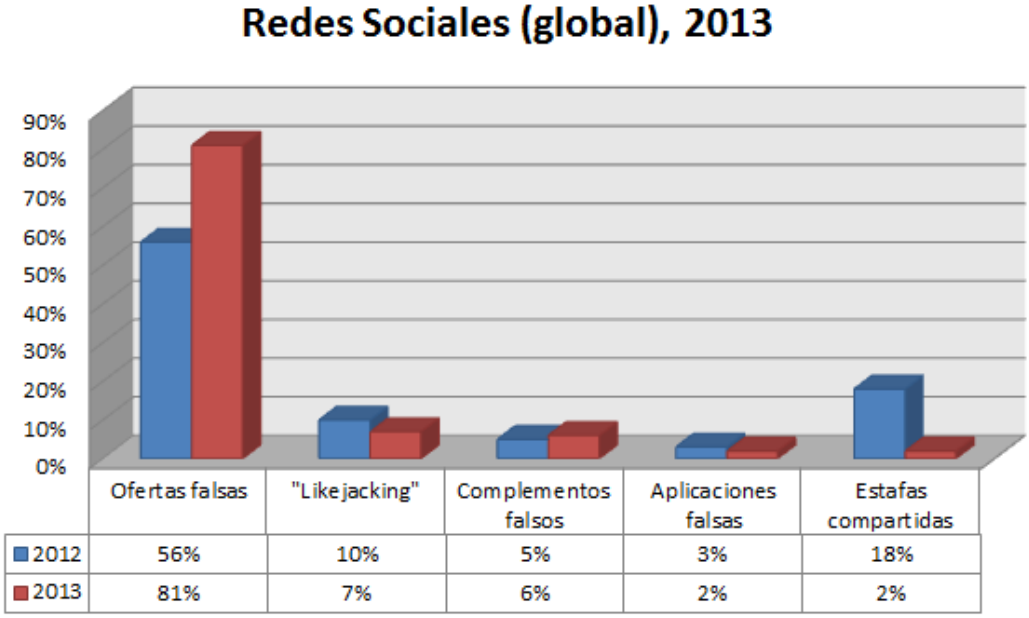



**Figura 2. 2: Robos y fraudes en Redes Sociales año 2013**

**Fuente: Brian Sullivan, 2014**

| Métrica | 1Q14 | 2Q14 | 3Q14 | 4Q14 |
|---|---|---|---|---|
| Encounter rate, Ecuador | 0,403 | 0,346 | 0,29 | 0,235 |
| Worldwide encounter rate | 0,215 | 0,192 | 0,201 | 0,159 |
| CCM, Ecuador | 33 | 41,2 | 21,6 | 13,3 |
| Worldwide CCM | 10,3 | 11,5 | 8,6 | 5,9 |

**Tabla 2. 1: Infecciones en Ecuador y el mundo**

**Fuente: Microsoft Security Intelligence Report, 2013**

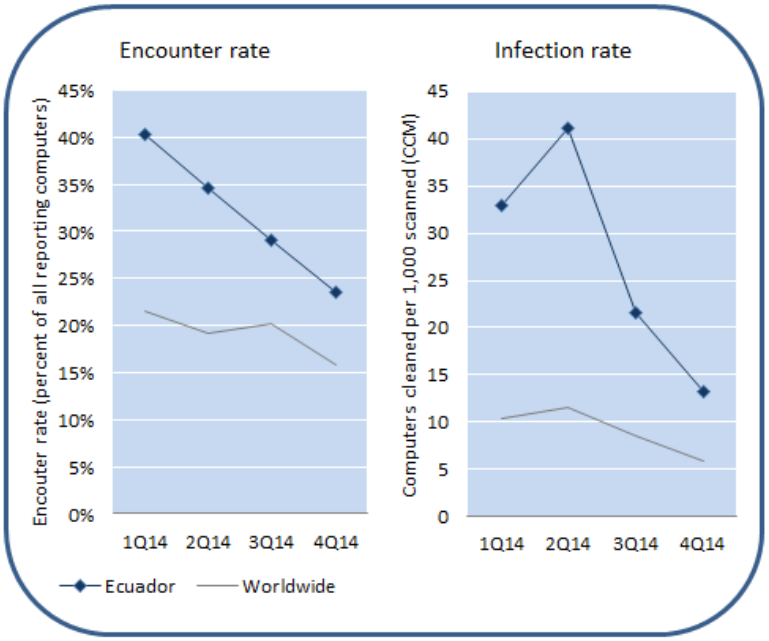



**Figura 2. 3: Estadísticas de los tipos de infecciones en Ecuador**

**Fuente: Microsoft Security Intelligence Report, 2015**

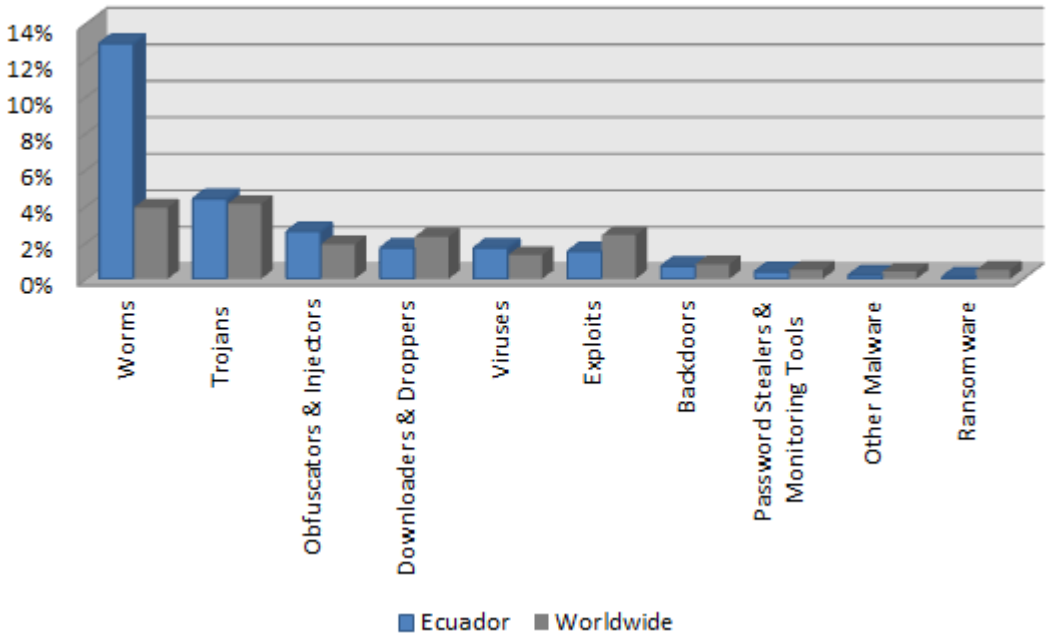



**Figura 2. 4: Malware encontrados en Ecuador en 4Q14, por categoría**

**Fuente: Microsoft Security Intelligence Report, 2015**

## 2.3 Políticas de seguridad

La política de seguridad es elaborada e implementada en base a normativas que cubren áreas más específicas y una serie de mecanismos de seguridad para la protección del sistema.

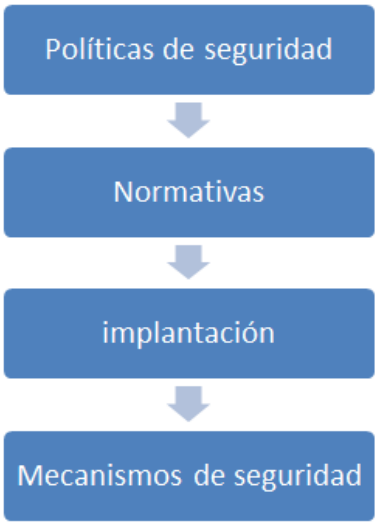


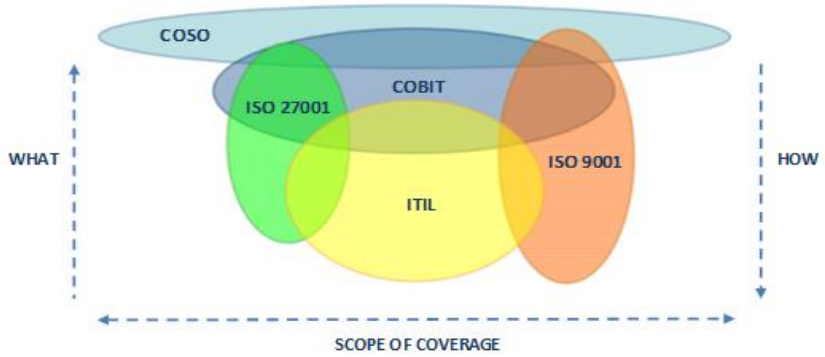

**Figura 2.9: Esquema de la política de la seguridad**

## 2.4 ISO 27000

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001.

El término se denomina en inglés "Information Security Management System" (ISMS).

"El concepto clave de un SGSI es para la agencia el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información".[1]




[1] López A., Ruiz J. (n.d.b). La Serie 27000. El portal de ISO 27001 en Español. España. Obtenida el 25 de Enero del 2011

**Figura 2. 15: Relación con otras normas**
**Fuente: Ana Cecilia Vargas, 2014**

## 2.5 Ethical Hacking

Los sistemas informáticos y redes de datos en todo el mundo se ven vulnerables a ser atacados por crackers o hackers, capaces de robar o borrar información valiosa para las organizaciones, por ello es imprescindible conocer si estos sistemas y redes de datos están protegidos de cualquier tipo de intrusiones.

## 2.6 Pruebas de Penetración

El término Pent Test es un procedimiento que se realiza a través de un conjunto de técnicas y métodos que simulan el ataque a un sistema, esto sirve para evaluar la seguridad de los sistemas informáticos, redes y aplicaciones.


**Figura 2. 21: Metodología**
**Fuente: Alejandro Hernández, 2007**

## 2.7 Metodologías de pruebas de penetración

### 2.7.1 OWASP (Open Web Application Security Project)

Colección de 24 tipos de vulnerabilidades centrada exclusivamente en la seguridad de aplicaciones web.
Este proyecto mantiene una metodología que consta de 2 partes, en la primera se abarcan los siguientes puntos:

- Principios del testeo
- Explicación de las técnicas de testeo.
- Explicación general acerca del framework de testeo de OWASP.

Y en la segunda parte, se planifican todas las técnicas necesarias para testear cada paso del ciclo de vida del desarrollo de software. Incorpora en su metodología de testeo, aspectos claves relacionados con el Ciclo de Vida del Desarrollo de Software o SDCL (Por sus siglas en Ingles "Software Development Life Cycle Process") a fin de que el ámbito del testeo a realizar comience mucho antes de que la aplicación web se encuentre en producción.

### 2.7.2 OSSTMM (Open Source Security Testing Methodology Manual)

Esta metodología permite realizar evaluaciones de seguridad, incluidos test de penetración.

OSSTMM representa un estándar de referencia para llevar a cabo un testeo de seguridad en forma ordenada y con calidad profesional.

Esta metodología permite identificar una serie de módulos de testeo específicos, los mismos que describen las dimensiones de seguridad y las tareas a llevar a cabo en los diferentes puntos de revisión (Seguridad de la Información, Seguridad de los Procesos, Seguridad en las Tecnologías de Internet, Seguridad en las Comunicaciones, Seguridad Inalámbrica y Seguridad Física).

#### 2.7.3 ISSAF (Information Systems Security Assessment Framework)

Framework del OISSG (Open Information Systems Security Group) que define procedimientos de aseguramiento y comprobación de la seguridad incluida pen testing.

## 3. PROPUESTA METODOLÓGICA PARA REALIZAR PRUEBAS DE PENETRACIÓN EN AMBIENTES VIRTUALES

Las fases propuestas para la ejecución de las pruebas de penetración en ambientes virtuales son:

### 3.1 Planificación y preparación de la prueba de penetración

En esta fase empieza el acercamiento inicial para el intercambio de información, planificación y preparación para la prueba, pero es importante recalcar que antes de empezar formalmente con la prueba de penetración se debe establecer y firmar un contrato entre las dos partes, este acuerdo contractual es la base al igual que la protección jurídica mutua.

### 3.2 Ejecución

En esta fase se realiza la prueba de penetración con un enfoque por capas:
- Recolección de Información
- Mapeo de la red de trabajo
- Identificación de vulnerabilidades
- Penetración
- Obtener Acceso y escalada de privilegios
- Enumeración de objetivos
- Comprometer usuarios remotos y sitios
- Mantener acceso
- Cubrir pistas

### 3.3 Informe, limpieza y destrucción de información

- Informes
- Limpieza y destrucción de la información

## 4. CONCLUSIONES Y TRABAJO FUTURO

- Una prueba de intrusión permite evaluar de manera planificada y en tiempos establecidos la protección de los sistemas de información de una organización. El uso de métricas permiten evaluar el nivel de criticidad e impacto de las vulnerabilidades detectadas, y realizar un análisis de costo/beneficio que permita concientizar a las organizaciones de su importancia como apoyo para la toma de decisiones y el cumplimiento de sus objetivos de negocio.

- Las metodologías estudiadas se complementan entre sí y aportan para verificar el nivel de resistencia que tienen los ataques informáticos, así como también contribuye a que el proceso de evaluación sea organizado y estandarizado para que se observe el grado de seguridad que la empresa tiene a través del tiempo.

- La metodología del NIST, indica el proceso general de cómo llevar a cabo una prueba de intrusión y trata de cubrir todos los aspectos informáticos y humanos que tienen contacto con la información de las organizaciones, pero se puede complementar en forma práctica.

- La metodología OSSTMM se enfoca en base a las políticas de seguridad, cuyas características no cubren otras metodologías como la existencia de los controles de seguridad y la indemnización de los activos de información.

- La metodología ISSAF, está orientada principalmente a cubrir los procesos de seguridad y la evaluación de los mismos para así obtener un panorama completo de las vulnerabilidades existentes.

- Al analizar el costo/beneficio de una herramienta, se puede determinar que una gratuita proporciona la misma funcionalidad que una privada.

## 5. AGRADECIMIENTOS

Agradecemos al Director de Tesis Ing. Mario Ron y Codirector de Tesis Geovanny Ninahualpa quienes con sus conocimientos y experiencia contribuyeron a que este proyecto pueda alcanzar su ejecución, y así obtener nuestro título profesional.

## 6. REFERENCIAS BIBLIOGRÁFICAS


- (NSA), N. S. (s.f.). Information Assessment Methodology (IAM). Obtenido de http://www.nsa.gov/ia/industry/education/iam.cfm?MenuID=10.2.4.2
- 800-53A, N. S. (2015). Guide for Assessing the Security Controls in Federal Information Systems. Obtenido de http://csrc.nist.gov/publications/PubsSPs.html
- Álvarez, A. (2013). Detección de Intrusiones con SNORT.
- Catalunya, U. A. (s.f.). Infraestructura Tecnológica. Obtenido de http://www.uoc.edu/portal/es/tecnologia_uoc/infraestructures/index.html
- Cisco, M. (2009). Obtenido de http://www.mundocisco.com/2009/08/que-es-un-sniffer.html
- Ezequiel Sallins, C. C. (2010). Ethical Hacking un enfoque metodológico para profesionales.
- G. Tóth, G. K. (2008). Case study: automated security testing on the trusted computing platform. 1st European workshop on system security. ACM New York, USA.
- Group, O. I. (2005). Information Systems Security Assessment Framework (ISSAF) draft 0.2 . OISSG.
- Informática, D. d. (2015). Obtenido de http://www.alegsa.com.ar/Dic/livecd.php
- Liliana Carolina Pinzón G., E. M. (2013). INTRUSION TEST AND OPEN SOURCE.
- McGraw, G. (2004). Software security. Security & Privacy Magazine, IEEE, 2(2).
- Microsoft. (2014). Microsoft Security Intelligence Report. Ecuador.

- Mifsud, E. (2012). Seguridad de la Información. Obtenido de Mifsud, Elvira. (2012). Introducción a la seguridad informática. Seguridad de la información e informática. http://recursostic.educacion.es/observatorio/web/ca/software/software-general
- Orange, T. (1895). Obtenido de http://csrc.nist.gov/publications/history/dod85.pdf
- Repositorio de información de WackoPicko. (2012). Obtenido de https://github.com/adamdoupe/WackoPicko/
- Soriano, A. (25 de septiembre de 2014). El hacking ético y la seguridad de la información de empresas en México - Parte II. Obtenido de http://revista.seguridad.unam.mx/numero-13/el-hacking-%C3%A9tico-y-la-seguridad-de-la-informaci%C3%B3n-de-empresas-en-m%C3%A9xico-parte-ii
- Target, T. (2015). Virtualización. Obtenido de http://searchdatacenter.techtarget.com/es/definicion/Virtualizacion
- Technology, N. I. (2008). Technical Guide to Information Security Testing and Assessment. Gaithersburg.
- Una Guía para Construir para Construir Aplicaciones y Servicios Web seguros. (2005). New York: Edición 2.0 Black Hat.
- Verde, C. (2015). Pruebas de penetración. Obtenido de http://codigoverde.com/consultoria-especializada/prueba-de-penetracion-pentest/
- w3af, R. d. (2014). Obtenido de https://github.com/andresriancho/w3af/