ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCION DEL TÍTULO DE:

INGENIERO EN SISTEMAS E INFORMÁTICA

TEMA: "PROPUESTA METODOLÓGICA PARA REALIZAR PRUEBAS DE PENETRACION EN AMBIENTES VIRTUALES"

AUTORES: QUISPE PALACIOS, JOSÉ ADÁN

PÉREZ VINUEZA, DEBBIE ELIZABETH

DIRECTOR: ING. RON, MARIO

CODIRECTOR: ING. NINAHUALPA, GEOVANNY

SANGOLQUÍ

MARZO, 2016

CERTIFICADO DEL DIRECTOR DEL TRABAJO DE TITULACIÓN

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

CERTIFICACIÓN

Certifico que el trabajo de titulación, ***"PROPUESTA METODOLÓGICA PARA REALIZAR PRUEBAS DE PENETRACION EN AMBIENTES VIRTUALES"***, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a los señores ***QUISPE PALACIOS, JOSE ADÁN Y PÉREZ VINUEZA, DEBBIE ELIZABETH*** para que lo sustente públicamente.

Sangolquí, 03 de Marzo del 2016

ING. MARIO RON

DIRECTOR

AUTORÍA DE RESPONSABILIDAD

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORÍA DE RESPONSABILIDAD

Nosotros, ***QUISPE PALACIOS, JOSÉ ADÁN*** con cédula de identidad N° 0400876942 ***Y PÉREZ VINUEZA, DEBBIE ELIZABETH***, con cédula de identidad N° 1716965015, declaramos que este trabajo de titulación **"*PROPUESTA METODOLÓGICA PARA REALIZAR PRUEBAS DE PENETRACION EN AMBIENTES VIRTUALES*"** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaramos que este trabajo es de nuestra autoría, en virtud de ello nos declaramos responsables del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 03 de Marzo del 2016

QUISPE PALACIOS JOSÉ ADÁN

CC.0400876942

PÉREZ VINUEZA, DEBBIE ELIZABETH

CC. 1706081617

AUTORÍZACIÓN

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Nosotros, ***QUISPE PALACIOS, JOSE ADÁN Y PÉREZ VINUEZA, DEBBIE ELIZABETH***, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación ***"PROPUESTA METODOLÓGICA PARA REALIZAR PRUEBAS DE PENETRACION EN AMBIENTES VIRTUALES"*** cuyo contenido, ideas y criterios son de nuestra autoría y responsabilidad.

Sangolquí, 03 de Marzo del 2016

QUISPE PALACIOS JOSÉ ADÁN	PÉREZ VINUEZA, DEBBIE ELIZABETH
CC.0400876942	CC. 1706081617

DEDICATORIA

Dedico este trabajo a mis hijos María Ángeles, José Antonio, María José, Mateo Sebastián y Alexis Patricio quienes fueron un gran apoyo emocional durante el tiempo de ejecución del proyecto.

A mis padres quienes me aman y apoyan incondicionalmente desde mi infancia.

A mi esposa Berenice que con su amor y paciencia siempre me apoya y anima a alcanzar mis metas profesionales y personales.

A mis maestros por enseñarme e instruirme en el camino del buen estudiante.

JOSÉ ADÁN QUISPE PALACIOS

DEDICATORIA

Al ángel que la Divinidad envió a la Tierra para que guíe mi camino con su Luz, pequeño gran maestro que me eligió como su madre: mi hijo Miguel Ángel…

DEBBIE ELIZABETH PÉREZ VINUEZA

AGRADECIMEINTO

Agradezco en primer lugar a Dios por brindarme salud y bendiciones, y así haber alcanzado esta meta profesional.

Agradezco al Ing. Mario Ron e Ing. Geovanny Ninahualpa quienes con sus conocimientos y experiencia contribuyeron a que pueda terminar mis estudios con éxito.

JOSÉ ADÁN QUISPE PALACIOS

AGRADECIMIENTO

A la Divinidad por su inspiración.

A los Guerreros de Luz que han sido mis maestros en el Sendero: Barbarita Miranda, Rvda. Hna. Gilma, Shri Mataji Nirvala Devi, Ven. SCh. Gazi Baik, Omraam Mikhaël Aïvanhov, Osho, Alejandro Jodorowsky, Alessandro Di Massi por guiarme en el camino hacia la Realización Interior.

A mi madre Yolanda, por enseñarme a ser fiel a mí misma, a luchar por mis ideales y ser una persona íntegra. A mi padre Carlos, por mostrarme el camino al corazón. A mis hermanas Priscila y Marina, almas afines, de quienes aprendí la Fortaleza y Constancia.

A Julio, maestro de Luz que hizo posible traer la encarnación de mi amado hijo Miguel Ángel, gracias al amor que compartimos.

A mis profesores, de quienes aprendí lecciones de vida que atesoro en mi corazón. A mis amigos, por brindarme su amistad y apoyo incondicional, sobre todo en los momentos difíciles, en especial a Patty, mi hermana del alma: gracias por tu apoyo, ha sido un soporte fundamental en mi vida.

A todas las personas que me han permitido ser parte de su vida, que me han ayudado a ser quien soy ahora y cumplir mi Misión.

DEBBIE ELIZABETH PÉREZ VINUEZA

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

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.

PALABRAS CLAVES:
TECNOLOGÍAS DE INFORMACIÓN
PRUEBAS DE PENETRACIÓN
AMBIENTES VIRTUALES
PROPUESTA METODOLÓGICA
INVESTIGACIÓN

ABSTRACT

The growth of attacks to the infrastructure of the information and communication technology 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.

KEYWORDS:
COMMUNICATION TECHNOLOGY
PENETRATION TEST
VIRTUAL ENVIRONMENTS
PROPOSED METHODOLOGY
INVESTIGATION

CAPÍTULO 1. INTRODUCCIÓN

1.1 Tema

Propuesta metodológica para realizar Pruebas de Penetración en Ambientes Virtuales: aplicación en laboratorio de informática forense de la Universidad de las Fuerzas Armadas ESPE

1.2 Antecedentes

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.

Un Pen Test, no es tarea fácil y requiere de un conocimiento sólido y profundo de las tecnologías involucradas en los sistemas, aplicaciones y servicios, además de una óptica y experiencia amplia en el comportamiento de varios sistemas operativos. Estas técnicas utilizadas con ética por el

White Hat o Ethical Hacker, permite descubrir vulnerabilidades en el sistema estudiado para cubrir las falencias de seguridad de manera preventiva, mediante el "análisis de vulnerabilidades" que son usadas para penetrar el sistema.

Las herramientas disponibles para efectuar estas pruebas de penetración pasan por varios grados de complejidad, y el manejo de algunas de ellas puede ser todo un reto a la inteligencia y sagacidad del atacante o pen-tester.

Alejandro Reyes Plata, de la UNAM CERT México señala:

El profesional de Ethical Hacking, es aquel que explota las vulnerabilidades existentes en el sistema de interés valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc.

Entre ellas se incluyen desde scanners de puertos, complejos algoritmos para descifrar claves, sistemas de intrusión por fuerza bruta, herramientas de sniffing de redes y penetración de firewalls, así como también herramientas de escaneo de vulnerabilidades de aplicaciones web y mucho más. Todo un mundo de aplicaciones en su mayoría desarrolladas para entorno Linux con las cuales el proceso de pruebas de penetración es más sofisticado.

El artículo de Mundo Cisco (2009), “Sniffer es un programa de captura de las tramas de red, que contiene información que no está destinada al que realiza la escucha”.

Estas herramientas suelen estar agrupadas en lo que se conoce como "Toolkits" o juegos de herramientas. Algunos "toolkits" son muy famosos en

el medio por la eficiencia de sus herramientas y por haber sido utilizados en penetraciones de alto nivel a sistemas que se consideraron es su tiempo fortalezas impenetrables. Algunos además se consiguen inclusive en formato de LIVE CD o ISO, de forma que las herramientas ya están integradas e instaladas en un CD de arranque del sistema operativo de fácil distribución.

El diccionario de informática y tecnología describe:

Un LiveCD es un sistema operativo almacenado en un medio extraíble, tradicionalmente un CD o un DVD (de ahí su nombre), que puede ejecutarse desde éste sin necesidad de ser instalado en el disco duro de la computadora.

Algunas herramientas son gratuitas y de código abierto, otras de pago y propietarias, pero en ambos casos, igual de potentes.

1.3 Justificación e importancia

En el Ecuador con la masificación del uso de las computadoras y el acceso al servicio del internet, ha hecho que los usuarios cometan delitos informáticos de manera voluntaria o involuntaria, pero las autoridades se han involucrado en el tema sin dar solución por falta de infraestructura, equipamiento y de personal altamente capacitado.

Las Pruebas de Penetración permiten probar la Seguridad Informática, para evaluar el Nivel de Seguridad (*Department Of Defense*, 1985) de la Infraestructura Tecnológica (Universidad Abierta de Catalunya, 2015) y realizar los correctivos necesarios.

Desde hace varios años se ha comprobado que gracias a este tipo de pruebas, se puede descubrir falencias en la seguridad que comprometen activos críticos de las organizaciones.

A pesar de que es necesario tener experiencia y gran conocimiento para realizar pruebas de penetración, este tipo de pruebas es aplicable tanto a grandes como pequeñas organizaciones, con distinta infraestructura tecnológica.

La profundidad del estudio de penetración puede ser aplicada inclusive en equipos de uso personal; y dependerá de las necesidades requeridas, respecto de los controles de seguridad que prevengan los accesos no autorizados.

Las organizaciones frente al escalamiento de aplicaciones y servicios requeridos, se han orientado a la Virtualización (Teach Target, 2015) para optimizar recursos informáticos, y en función de precautelar la seguridad, se hace necesario se investigue respecto a pruebas de penetración orientados para ambientes virtuales, y esta inquietud busca cumplir el presente trabajo de investigación.

1.4 Objetivos

1.4.1 Objetivo General

Desarrollar una Propuesta Metodológica para realizar Pruebas de Penetración en Ambientes Virtuales.

1.4.2 Objetivos Específicos

- Analizar las Mejores Prácticas de Seguridad Informática para el Desarrollo de la Propuesta Metodológica para Pruebas de Penetración en Ambientes Virtuales
- Investigar el Estado del Arte de las Pruebas de Penetración en Ecuador.

- Evaluar las diferentes Herramientas para Realizar Pruebas de Penetración (Penetration Test) en Ambientes Virtuales.
- Identificar las Principales Vulnerabilidades en Ambientes Virtuales.
- Determinar los Niveles de Seguridad en Ambientes Virtuales que Prevengan Accesos no Autorizados sin sacrificar su rendimiento.
- Identificar Características y Métricas que permitan Evaluar los Niveles de Seguridad de Ambientes Virtuales.

1.5 Metas

- Medir el nivel de seguridad de una infraestructura tecnológica y descubrir potenciales riesgos que pueden afectar a los activos críticos de las organizaciones.
- Detectar y corregir las vulnerabilidades que podrían ser explotadas por delincuentes informáticos, afectando la infraestructura tecnológica.
- Establecer la forma adecuada de manejar el proceso de pruebas de penetración en ambientes virtuales, con el propósito de obtener resultados exitosos y confiables en una investigación de campo, fomentando su aceptación y credibilidad frente a la organización.
- Identificarán características y métricas en la propuesta metodológica.
- Documentar de manera formal cada uno de los procedimientos de esta investigación, lo cual permitirá mantener respaldos de todo el proceso de investigación.

CAPÍTULO II. MARCO TEÓRICO

2.1 Seguridad de la Información

Se dice que el término seguridad es la "Característica que indica que un sistema está libre de todo peligro, daño o riesgo." (Villalón, 2012)

Se Dice que hay que proteger la información porque tiene relevancia especial en un contexto determinado.

La Seguridad de la Información (Mifsud Elvira, 2012) también se puede definir como un conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información.

Sin los sistemas informáticos se utilizaban grandes archivadores para guardar toda la información que se encontraba impresa en papeles, como datos de clientes, proveedores, información de empleados etc., esto ocasionaba múltiples problemas para su almacenaje, transporte, acceso y procesado.

Con la aparición de los sistemas informáticos empezó la digitalización de la información, con esto se pudo reducir espacio, tiempos de análisis y procesamiento de dicha información, y mejorar en la presentación de dicha información.

Pero con estas facilidades aparecen otros problemas como:

- Fácil transportar la información, pero hay más posibilidades de que desaparezca por el camino.
- Fácil acceso a la información, pero es más fácil modificar su contenido, etc.

Desde la evolución de los grandes sistemas en los que el trabajo en red es lo habitual, los problemas relacionados con la seguridad también han ido cambiando, evolucionando, pero están ahí y las soluciones han tenido que irse adaptando a los nuevos requerimientos técnicos, es decir aumenta la sofisticación en el ataque y con ello aumenta la complejidad de la solución.

La definición de Seguridad Informática aprobada y publicada en octubre de 2005 por el estándar para la seguridad de la información ISO/IEC 27001 International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC), dice:

“La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.”

Como se puede notar, el término seguridad de la información engloba otros aspectos relacionados con la seguridad más allá de los puramente tecnológicos.

Actualmente la información es considerada como el activo más valioso, ya que permite a las organizaciones permanecer y crecer en el mercado, por ende sus activos. Por ello es primordial proteger y garantizar la protección de la información contra posibles vulnerabilidades. Constantemente las organizaciones, los sistemas y red de información enfrentan amenazas de seguridad, amenazas que podrían atentar con su normal funcionamiento.

El problema principal de la seguridad de la información tiene mucho que ver con el desarrollo de sistemas, ya que no se contempla todas las posibles vulnerabilidades, las mismas que se incrementan rápidamente y

producen mayor afectación a la continuidad de las operaciones de una organización.

Por todo esto el Haking con la ayuda de ciertas técnicas ingresa algún sistema informático sin autorización, porque cuando dispone de identificadores y passwords quiere decir que está autorizado. Entre sus medios destacan los Sniffers o escaneadores de puertos, programas que buscan claves, passwords y puertos abiertos. Actúan conjuntamente con otras aplicaciones como reventadoras de claves y nukeadores

2.2 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.

Luego debe aplicarse el plan PDCA (PLAN – DO – CHECK – ACT), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo.

La seguridad es un proceso que siempre se debe gestionar por que los riesgos siempre van a estar presentes, estos riesgos no son únicamente de naturaleza tecnológica, es por eso que no se eliminan en su totalidad.

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

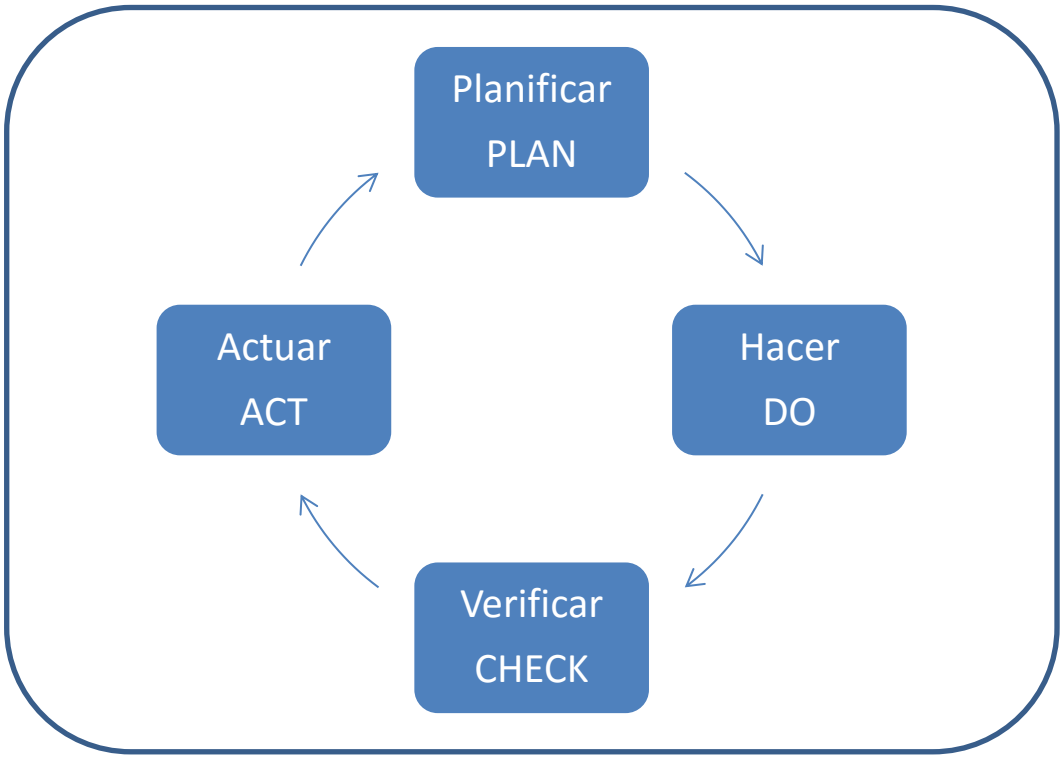

Figura 1 Modelo PDCA

2.2.1 PLANIFICAR (Plan)

Consiste en:

- Crear las políticas de seguridad.
- Realizar el análisis de riesgos.
- Seleccionar los controles y el estado de aplicabilidad.

2.2.2 HACER (Do)

Consiste en:

- Implementar el sistema de gestión de seguridad de la información.
- Implementar el plan de riesgos
- Implementar los controles.

2.2.3 VERIFICAR (Check)

Consiste en:

- Monitorear las actividades
- Hacer auditorías internas.

2.2.4 ACTUAR (Act)

Consiste en:

- Ejecutar tareas de mantenimiento
- Ejecutar propuestas de mejora, acciones preventivas y acciones correctivas (Mejoramiento Continuo).

2.3 Bases de la Seguridad Informática

2.3.1 Fiabilidad

Existe una frase que se ha hecho famosa dentro del mundo de la seguridad. Eugene Spafford, profesor de ciencias informáticas en la Universidad Purdue (Indiana, EEUU) y experto en seguridad de datos, dijo que “el único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aun así, yo no apostaría mi vida por él”.

Se define la Fiabilidad como la probabilidad de que un sistema se comporte tal y como se espera de él. Por esto un sistema será seguro o fiable si se garantizan tres aspectos:

- **Confidencialidad:** acceso a la información solo mediante autorización y de forma controlada.
- **Integridad:** modificación de la información solo mediante autorización.
- **Disponibilidad:** la información del sistema debe permanecer accesible mediante autorización.

Figura 2 Aspectos de la Seguridad de la información

La confiabilidad es otra propiedad relacionada con la calidad del servicio que se ofrece, esta se relaciona con la disponibilidad que estaría al mismo nivel que la seguridad.

2.3.1.1 Confidencialidad

En general el término confidencial hace referencia a "Que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas".

En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de prevenir la divulgación no autorizada de la información. Por eso ya sean organizaciones públicas o privadas y de

cualquier ámbito requieren que su información no sea accedida. Uno de los ejemplos más típicos es el del ejército de un país. Además, es sabido que los logros más importantes en materia de seguridad siempre van ligados a temas estratégicos militares.

Algunas empresas a menudo desarrollan o almacenan información que requiere protegerse de sus competidores, de esto depende la sostenibilidad de la empresa y su posicionamiento en el mercado, por ese motivo con mecanismos de control de acceso se procura asegurar la confidencialidad de esas informaciones.

Un ejemplo típico de mecanismo que garantice la confidencialidad es la Criptografía, cuyo objetivo es cifrar o encriptar los datos para que resulten incomprensibles a aquellos usuarios que no disponen de los permisos suficientes.

La clave de encriptación también necesita ser protegida, esta es necesaria para que el usuario pueda descifrar la información, esta clave al transportarse en la red puede ser capturada para uso indebido, esto conlleva a que toda la información queda comprometida y así se pierda la confidencialidad de la operación (sea bancaria, administrativa o de cualquier tipo).

2.3.1.2 Integridad

En general, el término integridad hace referencia a una cualidad de íntegro e indica "Que no carece de ninguna de sus partes." y relativo a personas "Recta, proba, intachable".

- En términos de seguridad de la información, la integridad se relaciona con prevenir la información de cualquier cambio impropio o desautorizado, es decir prevenir cualquier tipo de modificación no

autorizada ya sea la integridad de los datos (el volumen de la información) o la integridad del origen (la fuente de los datos, llamada autenticación). Cuando se habla de la integridad del origen, se hace referencia que la exactitud, credibilidad y confianza de la información resultó afectada.

Por ejemplo, un periódico difunde una información cuya fuente no es correcta, podemos decir que se mantiene la integridad de la información ya que se difunde por medio impreso, pero sin embargo, al ser la fuente de esa información errónea no se está manteniendo la integridad del origen, ya que la fuente no es correcta.

2.3.1.3 Disponibilidad

En general, el término disponibilidad hace referencia a una cualidad de disponible y dicho de una cosa "Que se puede disponer libremente de ella o que está lista para usarse o utilizarse."

En términos de seguridad de la información, se dice que la disponibilidad se relaciona con la accesibilidad que la información debe tener para todos los elementos autorizados. Entonces el prevenir las interrupciones no autorizadas y/o controladas de los recursos informáticos se refiere a la disponibilidad.

En términos de seguridad informática la disponibilidad de un sistema se refiere a negar deliberadamente el acceso a datos o servicios determinados. Un sistema que no está disponible no sirve, es como si no se tuviera sistema.

En resumen de todo lo comentado se puede concluir que mantener el equilibrio adecuado entre los tres factores detalladas anteriormente permite mantener un sistema seguro, confiable y disponible.

La prioridad que se pueda dar a cada uno de estos tres factores depende del entorno de trabajo y sus necesidades, por ejemplo se puede priorizar ya sea en la confidencialidad frente a la disponibilidad como en ambientes militares.

Otro ejemplo donde se puede evidenciar que la prioridad es el aspecto de la integridad de la información frente a la confidencialidad o disponibilidad son los ambientes bancarios. Se considera menos dañino que un usuario pueda leer el saldo de otro usuario a que pueda modificarlo.

2.3.2 Mecanismos básicos de la seguridad

2.3.2.1 Autenticación

Se Define la Autenticación como la verificación de la identidad del usuario, generalmente cuando este entra en el sistema o la red, o accede a una base de datos.

Generalmente el nombre de usuario y la contraseña permite el ingreso a determinado sistema. Actualmente el uso de otras técnicas que también son consideradas seguras se puede ingresar normalmente al sistema informático.

Se puede autenticarse de tres maneras:

1. Por lo que uno sabe (una contraseña)
2. Por lo que uno tiene (una tarjeta magnética)
3. Por lo que uno es (las huellas digitales)

Las empresas relacionan el valor de la información que van a proteger para validar el uso de más de un método de autenticación.

El uso de contraseñas es la técnica más usual, aunque depende de las características y la medida de está para que sea mejor o peor, esta debe ser confidencial y de uso estricto del usuario, ya que las acciones que hagan con esta contraseña es de responsabilidad del dueño.

Para que la contraseña sea segura y difícil de adivinar debe tener un conjunto de caracteres amplio y variado (con minúsculas, mayúsculas y números). El problema es que los usuarios utilizan palabras previsibles (el nombre, el apellido, el nombre de usuario, el grupo musical preferido,...), utilizan notas que colocan en lugares visibles porque difícilmente recuerdan contraseñas, esto facilita el ingreso no autorizado en el sistema.

2.3.2.2 Autorización

La Autorización se refiere al proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización.

Dependiendo lo que se va a proteger o el grado de criticidad de la información se establece el mecanismo o el grado de autorización, por ello los recursos y los datos se organizan en niveles y cada nivel debe tener una autorización.

Uno de los recursos de la autorización es la firma en un formulario o mediante una contraseña, esta debe quedar registrada para poder controlarla. Para los datos, la autorización debe asegurar la confidencialidad e integridad, ya sea dando o denegando el acceso en lectura, modificación, creación o borrado de los datos.

Por último es importante mencionar que se debe autorizar el acceso únicamente a los usuarios que lo requieran, considerando que se proveerá de autorizaciones transitorias según sean las necesidades del usuario.

2.3.2.3 Administración

La Administración establece, mantiene y elimina las autorizaciones de los usuarios del sistema.
Los administradores elaboran o modifican las políticas de la organización y las registran en un formato que pueda ser usado por el sistema.

Con el cambio continuo y evolución de las tecnologías, hace que los riesgos también cambien dentro de la organización. Normalmente todos los sistemas operativos disponen de módulos específicos de administración de seguridad. Y también existe software externo y específico que se puede utilizar en cada situación.

2.3.2.4 Auditoría y registro

Se define la Auditoría como la continua vigilancia de los servicios en producción y para ello se recaba información y se analiza.

El proceso de la auditoria permite verificar que las técnicas de autenticación y autorización utilizadas cumplen los objetivos fijados por la organización, de manera que se identifican los potenciales riesgos que puedan afectar drásticamente a la organización.

Cualquier intento de violar la seguridad queda almacenado o registrado en una base de eventos para luego analizarla, porque no tiene sentido tener toda esta información que no será analizada posteriormente, sino al contrario esta debe aportar que las seguridades sean más robustas y así no permitan ingresos mal intencionados.

La ejecución de las acciones establecidas a partir de la información recopilada se puede realizar con medios manuales o automáticos, y la periodicidad dependerá del nivel de riesgo identificado.

2.3.2.5 Mantenimiento de la integridad

Consiste en establecer procedimientos que permitan evitar o controlar que la información sufra cambios o daños, es decir garantizar que la información almacenada o enviada se encuentre sin ningún tipo de alteración.

2.4 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.

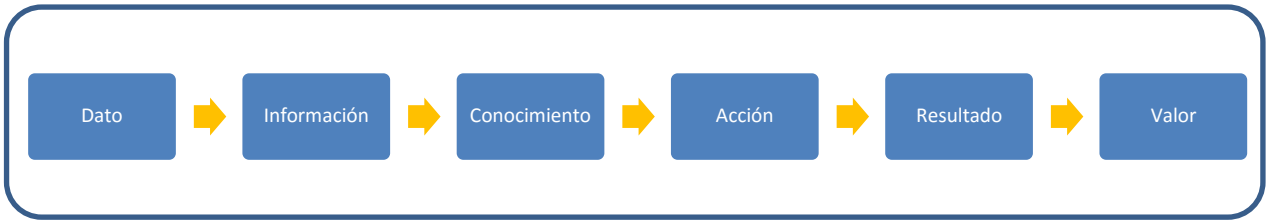

Figura 3 Recursos que forman parte del sistema

Incluso de todos ellos, el activo más crítico son los datos, ya que tanto el hardware como el software se pueden reponer, por tal motivo es importante que la organización tenga una adecuada política de seguridad que permita una pronta recuperación de la información y así evitar pérdidas de tiempo y dinero.

2.4.1 Vulnerabilidad: definición y clasificación

Se define Vulnerabilidad como debilidad de cualquier tipo que compromete la seguridad del sistema informático.

Las vulnerabilidades de los sistemas informáticos se puede agrupar en función de:

2.4.1.1 Diseño

- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficiente e inexistente.

2.4.1.2 Implementación

- Errores de programación.
- Existencia de puertas traseras en los sistemas informáticos.
- Descuido de los fabricantes.

2.4.1.3 Uso

- Mala configuración de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.

2.4.1.4 Vulnerabilidad del día cero

- Se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución conocida, pero se sabe cómo explotarla.

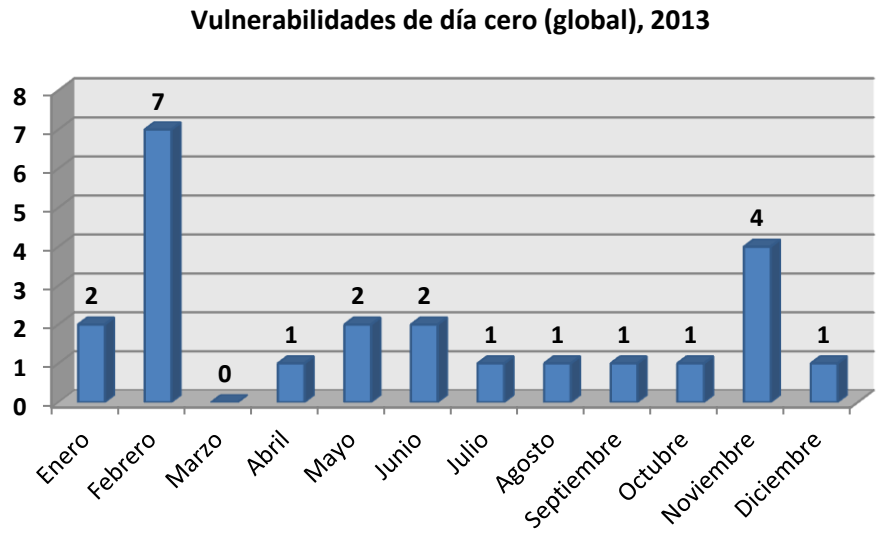

Figura 4 Vulnerabilidades de día cero

Fuente: Brian Sullivan, 2014

2.4.1.5 Vulnerabilidades conocidas

- Vulnerabilidad de desbordamiento de buffer, se refiere a que cuando existe demasiados datos en el buffer, estos pueden superar su capacidad y producto de esto hacer que los bytes que sobran se almacenen en zonas de memoria adyacentes.

- Vulnerabilidad de condición de carrera (race condition), se produce cuando varios procesos acceden al mismo tiempo a un recurso compartido, como por ejemplo una variable que cambia su estado y puede obtener de esta forma un valor no esperado.

- Vulnerabilidad de Cross Site Scripting (XSS). Está relacionada con las aplicaciones web, inyecta código VBSript o JavaScript en páginas web vistas por el usuario. El phishing es una aplicación de esta vulnerabilidad, el usuario ingresa a un sitio diferente en donde introduce sus credenciales que posteriormente le servirán al atacante para uso malintencionado.

- Vulnerabilidad de denegación del servicio. Esta vulnerabilidad hace que un servicio o recurso no esté disponible para los usuarios, está relacionada con el consumo del ancho de banda y esto provoca la sobrecarga de los recursos informáticos.

- Vulnerabilidad de ventanas engañosas (Window Spoofing). Estas generalmente te informan que eres el ganador de algún sorteo o promoción, lo cual es mentira y lo único que quieren es que el usuario de información. Hay otro tipo de ventanas que si las sigues obtienen datos del ordenador para luego realizar un ataque.

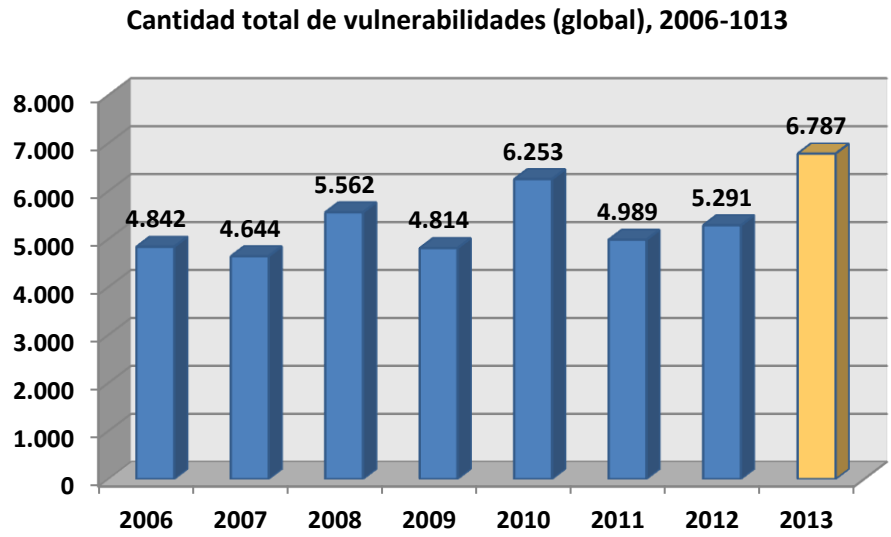

Figura 5 Cantidad total de vulnerabilidades años 2006 a 2013

Fuente: Brian Sullivan, 2014

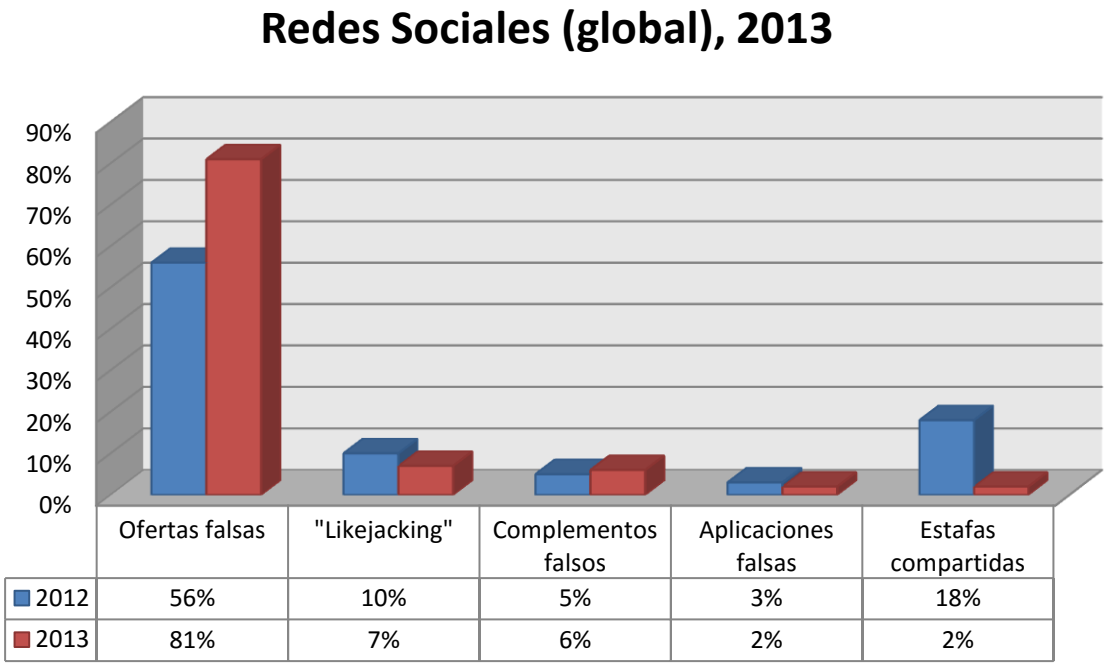

Figura 6 Robos y fraudes en Redes Sociales año 2013

Fuente: Brian Sullivan, 2014

2.4.2 Herramientas

Cuando se requiere hacer análisis de vulnerabilidades para servidores Linux/Unix generalmente se utiliza el programa Nessus.

Nessus es de arquitectura cliente-servidor OpenSource, con una base de datos de patrones de ataques que ayuda a localizar sus vulnerabilidades.

Existe software comercial que utiliza Nessus como motor para el análisis. Por ejemplo está Catbird utiliza a Nessus como motor para análisis centralizado de las vulnerabilidades, este analiza externamente e internamente la red sin descuidar los accesos inalámbricos, así como también monitorea los servicios de red como el DNS y la disponibilidad de los portales web de las organizaciones.

MBSA “Microsoft Baseline Security Analyzer” está en sistemas operativos Windows, permite verificar la seguridad en el sistema operativo y los diversos componentes instalados.

2.4.3 ¿De qué se quiere proteger el sistema informático?

Se ha analizado todos los elementos de los sistemas informáticos que son vulnerables, ahora se verá las amenazas a los que se exponen estos elementos.

Se empieza con la definición de amenaza.

Se entiende la amenaza como el escenario en el que una acción o suceso, ya sea o no deliberado, compromete la seguridad de un elemento del sistema informático.

Cuando a un sistema informático se le detecta una vulnerabilidad y existe una amenaza asociada a dicha vulnerabilidad, puede ocurrir que el suceso o evento se produzca y nuestro sistema estará en riesgo.

Si el evento se produce y el riesgo que era probable ahora es real, el sistema informático sufrirá daños que habrá que valorar cualitativa y cuantitativamente, y esto se llama impacto.

Con las definiciones anteriores se puede decir que una amenaza es un evento que pone en peligro al sistema informático y dependiendo la gravedad se define el impacto de esta. Para ello es importante establecer defensas o salvaguardas que ayudarán a proteger el sistema informático.

Algunas de las técnicas utilizadas para mantener o controlar la integridad de los datos están los antivirus, encriptación y funciones hash.

Tabla 1

Infecciones en Ecuador y el mundo

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

Fuente: Microsoft Security Intelligence Report, 2013

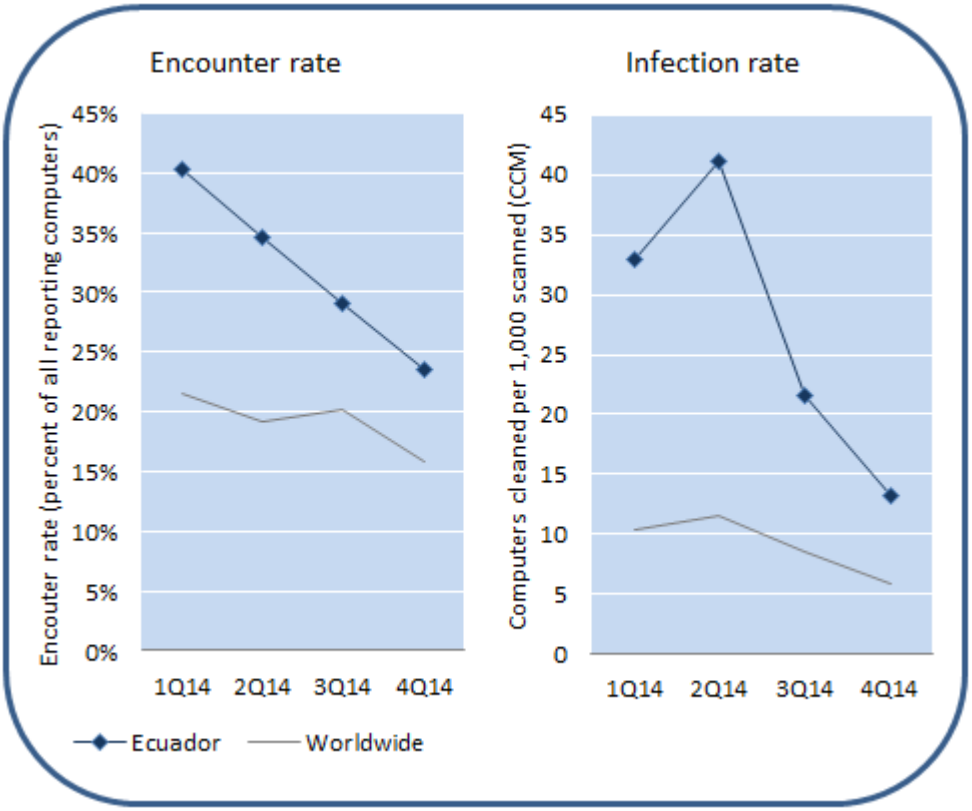

Figura 7 Estadísticas de los tipos de infecciones en Ecuador

Fuente: Microsoft Security Intelligence Report, 2015

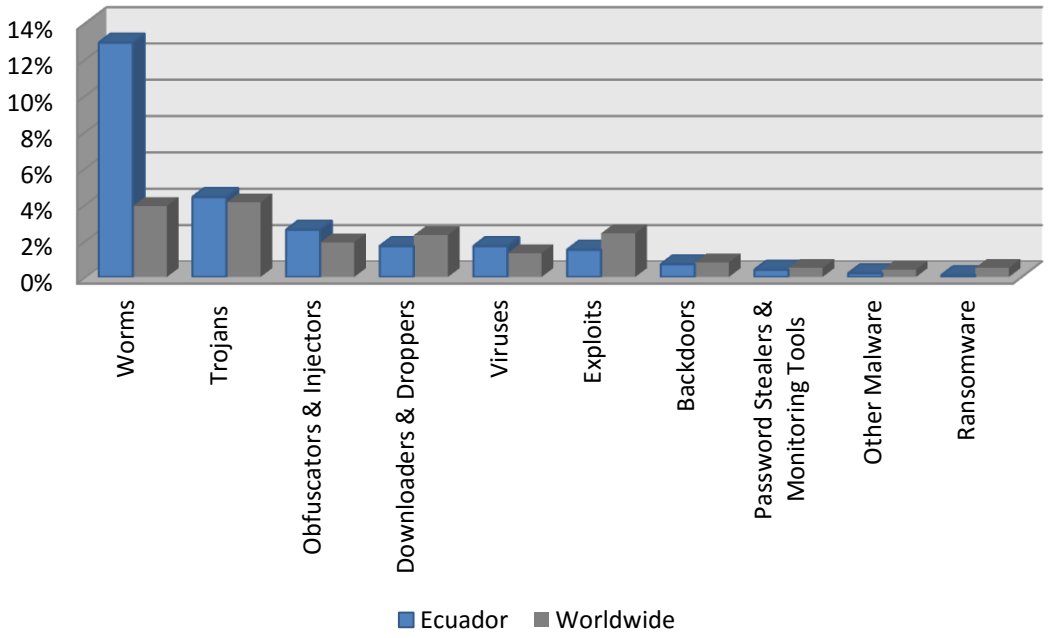

Figura 8 Malware encontrados en Ecuador en 4Q14, por categoría

Fuente: Microsoft Security Intelligence Report, 2015

La siguiente figura muestra la evolución de los ataques y el perfil de la habilidad relativa de los atacantes en los últimos años.

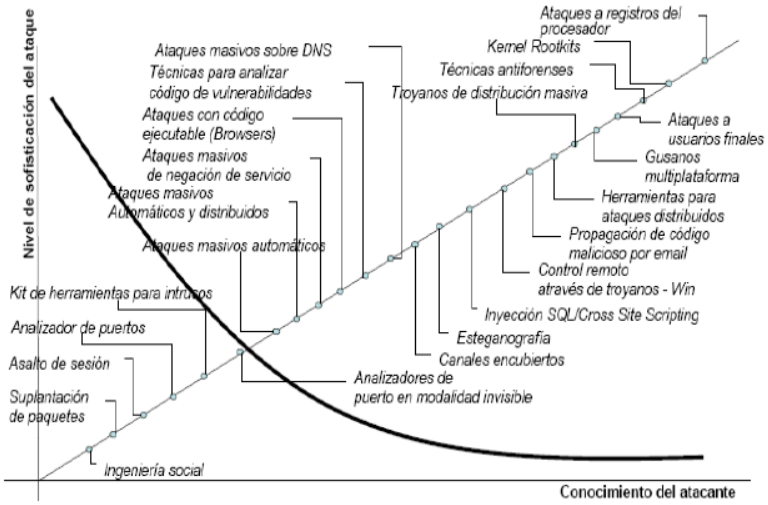

Figura 9 Curva de evolución de ataques vs habilidad

Fuente: International Council of Electronic Commerce Consultants, 2004

2.4.4 Políticas de seguridad

2.4.4.1 ¿Cómo se puede proteger el sistema informático?

Para proteger el sistema informático primero se debe analizar las posibles amenazas que tiene un sistema informático, también estimar que pérdidas podrían causar estas y la probabilidad de que ocurran.

Luego del análisis se puede diseñar la política de seguridad en la que se establecen responsabilidades y reglas que se deberá seguir para mitigar o controlar los efectos que causan las amenazas.

Se define la Política de seguridad como un “documento sencillo que define las directrices organizativas en materia de seguridad” (Villalón).

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.

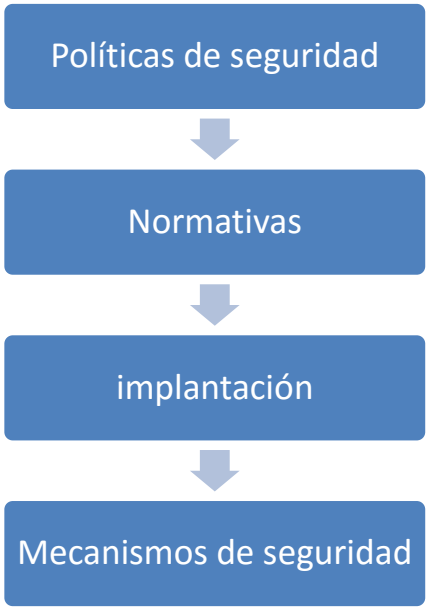

Figura 10 Mecanismos de la seguridad

Los mecanismos de seguridad se dividen en tres grupos:

2.4.4.1.1 Prevención

Evitan desviaciones respecto a la política de seguridad.

Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información en un sistema de red.

2.4.4.1.2 Detección

Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema.

Ejemplo: la herramienta Tripwire para la seguridad de los archivos.

2.4.4.1.3 Recuperación

Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento.

Ejemplo: las copias de seguridad.

2.4.4.1.4 Mecanismos de seguridad

- **Mecanismos de identificación e autenticación**

  El primero identifica de entidades del sistema, y el segundo comprueba si la entidad es quien dice ser. Cuando la entidad pasa estos filtros puede acceder a un objeto del sistema, estos mecanismos son los más utilizados por los usuarios.

- **Mecanismos de control de acceso**

  Los objetos del sistema están protegidos mediante mecanismos de control de acceso, estos establecen los tipos de acceso al objeto por parte de cualquier entidad del sistema.

- **Mecanismos de separación**

  Si el sistema dispone de diferentes niveles de seguridad se deben implementar mecanismos que permitan separar los objetos se dividen en los grupos siguientes: separación física, temporal, lógica, criptográfica y fragmentación.

- **Mecanismos de seguridad en las comunicaciones**

  Clásicamente se utilizan protocolos seguros, tipo SSH o Kerberos, que cifran el tráfico por la red.

2.4.4.1.5 Políticas de seguridad

La Política de Seguridad de Información de una organización tienen por objetivo principal mostrar el posicionamiento de la organización con relación a la seguridad, y esta es la base para desarrollar los procedimientos concretos de seguridad.

La empresa debe disponer una política formalmente elaborada y la misma debe ser divulgada entre todos los empleados. Esta no debe quedar como una declaración de intenciones, si no lograr la concienciación, entendimiento y compromiso de todos los involucrados.

La política debe especificar las prácticas que serán adoptadas por la compañía y deben ser revisadas y actualizadas periódicamente.

Las políticas deben:

- Definir qué es seguridad de la información, cuáles son sus objetivos principales y su importancia dentro de la organización
- Mostrar el compromiso de sus altos cargos con la misma
- Definir la filosofía respecto al acceso a los datos
- Establecer responsabilidades inherentes al tema
- Establecer la base para poder diseñar normas y procedimientos referidos a
    - Organización de la seguridad
    - Clasificación y control de los datos
    - Seguridad de las personas
    - Seguridad física y ambiental
    - Plan de contingencia
    - Prevención y detección de virus
    - Administración de los computadores

Una vez establecida la política se puede desarrollar las normas, y los procedimientos de seguridad que describirán en detalle las actividades.

La administración de la organización tiene la responsabilidad de definir la política de seguridad ya que afecta a todos los usuarios del sistema. Esta debe ser difundida a sus empleados (usuarios) haciendo énfasis en la concienciación.

Sin embargo, la seguridad debe ir más allá del conocimiento de los empleados y cubrir las siguientes áreas:

- Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados
- Un procedimiento para administrar las actualizaciones
- Una estrategia de realización de copias de seguridad planificada adecuadamente

- Un plan de recuperación luego de un incidente
- Un sistema documentado actualizado

2.4.5 Amenazas

2.4.5.1.1 Clasificación de las amenazas

De forma general se puede agrupar las amenazas en:

- Amenazas físicas
- Amenazas lógicas

Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por:

- Las personas
- Programas específicos
- Catástrofes naturales

Se puede tener otros criterios de agrupación de las amenazas, como son:

- Origen de las amenazas
    - Amenazas naturales: inundación, incendio, tormenta, fallo eléctrico, explosión, etc.
    - Amenazas de agentes externos: virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etc.
    - Amenazas de agentes internos: empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema, etc.

- Intencionalidad de las amenazas

    - Accidentes: averías del hardware y fallos del software, incendio, inundación, etc.
    - Errores: errores de utilización, de explotación, de ejecución de procedimientos, etc.
    - Actuaciones malintencionadas: robos, fraudes, sabotajes, intentos de intrusión, etc.

2.4.5.1.2 Naturaleza de las amenazas

La agrupación de las amenazas atendiendo al factor de seguridad que comprometen es la siguiente:

- Interceptación
- Modificación
- Interrupción
- Fabricación

2.4.5.1.3 Flujo normal de la información:

- Confidencialidad: nadie no autorizado accede a la información.
- Integridad: los datos enviados no se modifican en el camino.
- Disponibilidad: la recepción y acceso es correcto.

a. **Interceptación:** acceso a la información por parte de personas no autorizadas. Uso de privilegios no adquiridos.

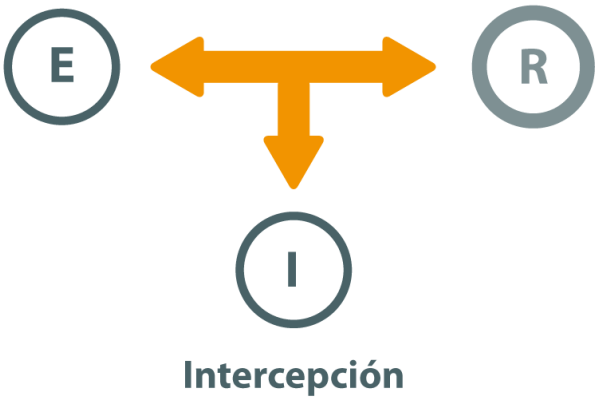

Figura 11 Intercepción

Ejemplos:

- Copias ilícitas de programas
- Escucha en línea de datos

b. **Modificación:** acceso no autorizado que cambia el entorno para su beneficio.

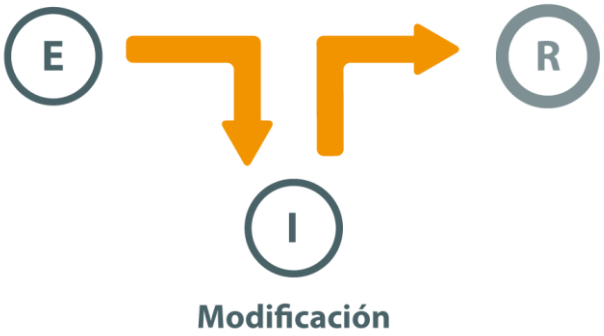

Figura 12 Modificación

Ejemplos:

- Modificación de bases de datos
- Modificación de elementos del HW

c. **Interrupción:** puede provocar que un objeto del sistema se pierda, quede no utilizable o no disponible.

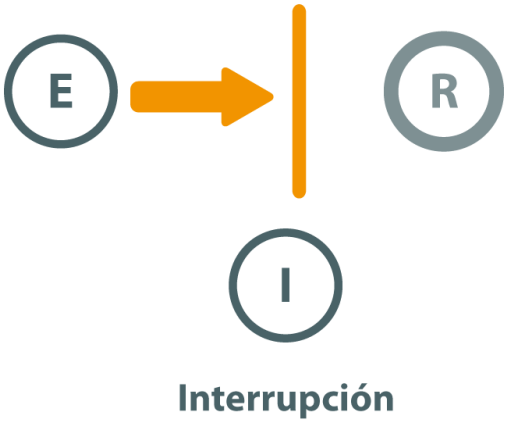

Figura 13 Interrupción

Ejemplos:

- Destrucción del hardware
- Borrado de programas, datos
- Fallos en el sistema operativo

d. **Fabricación:** puede considerarse como un caso concreto de modificación ya que se consigue un objeto similar al atacado de forma que no resulte sencillo distinguir entre objeto original y el fabricado.

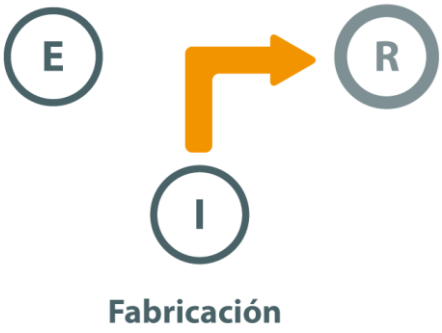

Figura 14 Fabricación

Ejemplos:

- Añadir transacciones en red
- Añadir registros en base de datos

2.4.5.1.4 Amenazas provocadas por personas

Un alto porcentaje de ataques a los sistemas informáticos son provocados por las personas.

Existen dos grupos de atacantes:

- Activos: su objetivo es hacer daño de alguna forma. Eliminar información, modificar o sustraerla para su provecho.
- Pasivos: su objetivo es curiosear en el sistema.

Las personas que pueden constituir una amenaza para el sistema informático son:

- Personal de la propia organización
- Ex-empleados
- Curiosos
- Crackers
- Terroristas
- Intrusos remunerados

2.4.5.1.5 Amenazas Físicas

Se puede mencionar como amenazas físicas cualquier error o daño en el hardware. Por ejemplo, daños en discos duros, en los procesadores, errores de funcionamiento de la memoria, etc. Todos ellos hacen que la información o no esté accesible o no sea fiable.

Las catástrofes naturales también son consideradas como amenazas físicas. Por ejemplo terremotos, huracanes, inundaciones, etc. Hay que intentar prever al máximo este tipo de situaciones para precautelar los activos de la organización.

Dentro del grupo de catástrofes poco probables se tiene los ataques nucleares, impactos de meteoritos, etc., aunque la probabilidad de que se desencadenen son muy bajas se deben considerar también.

2.4.5.1.5.1 Tipos de amenazas físicas

1. Acceso físico

A menudo se descuida este tipo de seguridad, se debe tener en cuenta que cuando el acceso físico existe, no existe la seguridad sobre él, entonces existe un gran riesgo y probablemente con un impacto muy alto.

El ejemplo típico de este tipo es el de una organización que dispone de tomas de red que no están controladas, son libres.

2. Radiaciones electromagnéticas

Las radiaciones que pueden generar ciertos aparatos eléctricos se pueden capturar y reproducir, con el equipamiento adecuado. Por ejemplo los datos que circulan por el cable telefónico. Hoy en día se puede tener este tipo de amenaza en las redes wifi abiertas.

3. Desastres naturales

Respecto a terremotos el riesgo es reducido en nuestro entorno, aunque se encuentre en una zona sísmica y por la presencia de varios volcanes, debe tenerlo en cuenta ya que sería de gran impacto para los de sistemas informáticos, y también para la sociedad en general.

Siempre hay que tener en cuenta las características de cada zona en particular. Por ejemplo las posibilidades de que ocurra una inundación son más probables en la Costa que en la Sierra.

4. Desastres del entorno

En este grupo están considerados los incendios, apagones, etc., si no se tienen medidas salvaguarda listas y operativas pueden tener un impacto muy importante para la organización.

2.4.5.1.5.2 Descripción de algunas amenazas físicas

Se describe a continuación algunas amenazas físicas y alguna sugerencia para evitar este tipo de riesgo.

- Por acciones naturales: incendio, inundación, condiciones climatológicas, señales de radar, instalaciones eléctricas, ergometría.
- Por acciones hostiles: robo, fraude, sabotaje.
- Por control de accesos: utilización de guardias, utilización de detectores de metales, utilización de sistemas biométricos, seguridad con animales, protección electrónica.

El conocer cómo se puede comprobar, evaluar y controlar permanentemente la seguridad física, permite establecer un sistema de seguridad eficaz dentro de cualquier organismo. El tener controlado el ambiente y acceso físico permite:

- Disminuir siniestros
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra accidentes

Estas decisiones pueden variar desde el conocimiento de la áreas que recorren ciertas personas hasta la extremo de evacuar el edificio en caso de accidentes.

2.4.5.1.6 Amenazas lógicas

La relación de las personas en el sistema informático es el punto más débil, ya que por su inexperiencia o falta de preparación pueden provocar accidentes intencionados, por ello también se deben prevenir.

Entre los ataques más comunes causados por estas personas, se tiene:

- Ingeniería social: consiste en manipular a las personas para que realicen actos que normalmente no harían.
- Shoulder Surfing: consiste en espiar a los usuarios para obtener donde almacenan o cuales son las claves de acceso al sistema.
- Masquerading: se refiere a la suplantación de identidad de algún usuario.
- Basureo: consiste en buscar información relacionado con el sistema informática que hayan dejado luego de la ejecución de algún trabajo.
- Actos delictivos: son actos como el chantaje, el soborno o la amenaza.
- Atacante interno: Se refiere a personas que han trabajado o trabajan con los sistemas. Estos deben privilegios mínimos, conocimiento parcial, rotación de funciones y separación de funciones, etc.
- Atacante externo: suplanta la identidad de un usuario legítimo. Si un atacante externo consigue penetrar en el sistema, ha recorrido el 80% del camino hasta conseguir un control total de un recurso.

2.4.5.1.6.1 Algunas amenazas lógicas

Los programas que pueden dañar el sistema informático son considerados amenazas lógicas, y han sido creados:

- De forma intencionada para hacer daño: software malicioso o malware (malicious software)
- Por error: bugs o agujeros.

Se detalla algunas amenazas actuales:

1. **Software incorrecto**

Son errores de programación (bugs), y con los Exploits (programas de fácil acceso) se aprovechan para atacar al sistema informático.

2. **Exploits**

Son los programas diseñados para aprovechar la vulnerabilidad del sistema. Son creados específicamente para cada sistema operativo, configuración del sistema y del tipo de red en la que se encuentren.

3. **Herramientas de seguridad**

Las herramientas de seguridad ayudan a detectar y solucionar fallos en el sistema. Herramientas como Nessus o Satan, son muy útiles y a la vez peligrosas, porque los crackers con estas herramientas son potenciales candidatos para ingresar al sistema aprovechando las vulnerabilidades de un host o de una red completa.

4. Puertas traseras

Cuando los programadores durante el desarrollo de las aplicaciones incluyen atajos, estos se llaman puertas traseras, cuyo propósito es conseguir mayor velocidad a la hora de detectar y depurar fallos. En la ejecución del [programa si estas puertas traseras no se destruyen, se está dejando abierta una puerta de entrada rápida.

5. Bombas lógicas

En desarrollo de software las bombas lógicas son partes de código que no se ejecutan hasta que se cumple una condición. Estas al activarse realizan funciones distintas al objetivo del programa.

6. Virus

Los virus son secuencias de códigos que son parte de un archivo ejecutable llamado huésped, y cuando el archivo se ejecuta, el virus también se ejecuta, propagándose a otros programas.

7. Gusanos

El Gusano es un programa que se ejecuta sólo, y también tiene la capacidad de transitar por la red por sí mismo, y llevando virus o aprovechar bugs de los sistemas a los que conecta para dañarlos.

8. Caballos de Troya

Los caballos de Troya son instrucciones incluidas en un programa, estas se ejecutan para ocultar al atacante y asegurarse la entrada en caso de ser descubierto.

9. Spyware

Son programas espía, que recopila información acerca de personas u organizaciones sin su conocimiento para ser vendida a empresas publicitarias o de la competencia.

10. Adware

Estos programas generalmente muestran publicidad de productos y servicios. El usuario descarga para su uso porque que es gratis, aunque en la mayoría de veces el usuario es consciente de que se puede tratar de alguna amenaza da su permiso.

11. Spoofing

Técnicas de suplantación de identidad con fines dudosos.

12. Phishing

Intenta conseguir información confidencial como contraseñas o códigos bancarios de forma fraudulenta, el estafador se hace pasar por una persona o empresa de la confianza del usuario mediante un correo electrónico oficial o mensajería instantánea, y de esta forma conseguir la información.

13. Spam

Generalmente se utiliza esta técnica en los correos electrónicos, mensajería instantánea y mensajes a móviles.

14. Programas conejo o bacterias

Estos programas afectan a los recursos del sistema (memoria, procesador, disco, etc.) por la velocidad de reproducción de copias.

15. Técnicas salami

Esta técnica es muy utilizada para atacar sistemas bancarios, son robos repetitivos de pequeñas de dinero de una gran cantidad origen.

2.4.6 Normas Relacionadas

La serie ISO/IEC 27000 es un conjunto de estándares desarrollados por la Organización Internacional para la Estandarización (ISO International Organization for Standardization) y la Comisión Electrotécnica Internacional (IEC International Electrotechnical Commission) que proporcionan un marco de la gestión de la seguridad de la información. Los rangos ISO van desde 27000 a 27019 y 27030 a 27044.

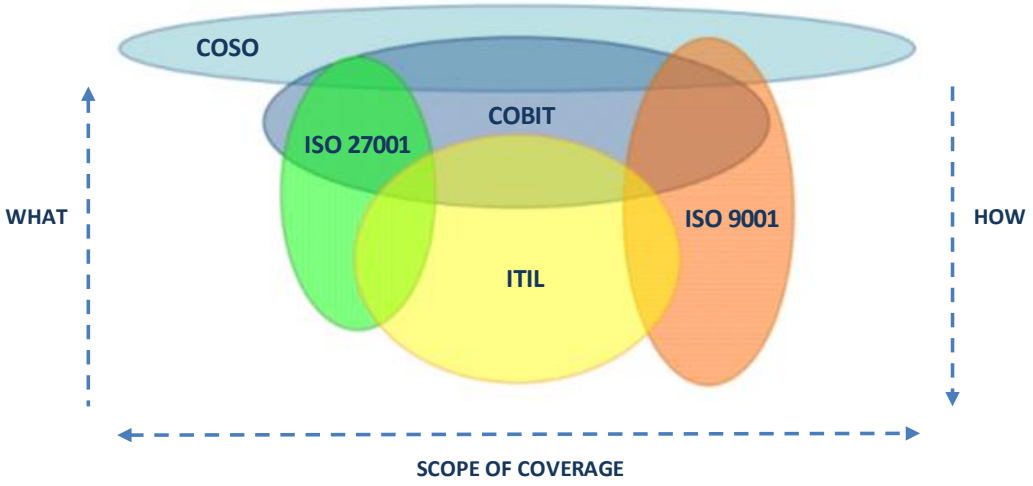

Figura 15 Relación con otras normas

Fuente: Ana Cecilia Vargas, 2014

2.4.6.1 Norma ISO/IEC 27001

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma

fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 provee los requisitos necesarios para implementar la gestión de la seguridad de la información en una organización ya sea con o sin fines de lucro, privada o pública, pequeña o grande. Si la organización lo requiere puede certificar, es decir luego del cumplimiento de esta normativa una entidad de certificación (Ejm. Bureau Veritas, SGS) confirma que la seguridad de la información ha sido implementada.

ISO 27001 actualmente es la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento; aquí se puede ver la cantidad de certificados en los últimos años:

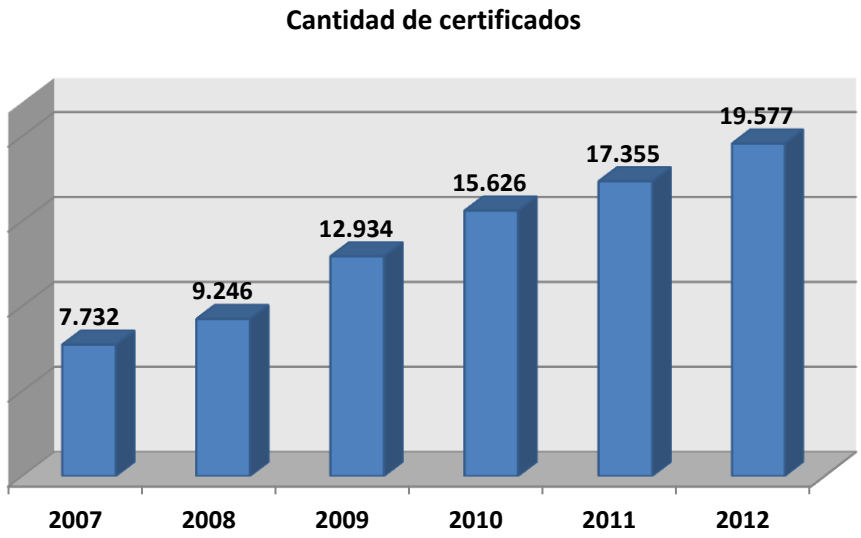

Figura 16 Certificados en los últimos años ISO 27001

Fuente: www.iso27000.es

2.4.6.2 Norma ISO/IEC 27002

Antes llamada ISO/IEC 17799, la ISO 27002 es una guía de buenas prácticas para en distintos ámbitos conocer qué se puede hacer para mejorar la seguridad de la información. Se enfoca en la Seguridad de la Información, Protección de Datos Personales y Responsabilidad Social.

2.4.6.3 Norma ISO 31000

La norma ISO es un estándar desarrollado en colaboración por ISO e IEC que provee principios y directrices genéricas sobre la gestión del riesgo. Esta norma se aplica a cualquier organización.

La norma ISO 31000 para la gestión de riesgos se estructura en tres elementos claves:

- Principios de la gestión de riesgos
- Marco de trabajo para la gestión de riesgos
- Proceso de gestión de riesgos

2.4.6.3.1 Principios de ISO 31000

Una efectiva gestión de riesgos se enfoca en satisfacer ciertos principios según el siguiente listado:

1. Crear y proteger valor para ayudar a alcanzar los objetivos de la organización y mejorar su desempeño.
2. Estar integrada en los procesos de una organización. Hacer la responsabilidad del riesgo una responsabilidad de cada gerente.
3. Ser parte de la toma de decisiones. La gestión del riesgo ayuda a la toma de decisiones evaluando la información sobre las distintas alternativas.

4. Tratar explícitamente la incertidumbre. Trata aquellos aspectos de la toma de decisiones que no son ciertos, la naturaleza de esa incertidumbre y como puede solucionarse.
5. Ser sistemática, estructurada y oportuna. Contribuye a la eficiencia y a la obtención de resultados fiables.
6. Basarse en la mejor información disponible. Los insumos del proceso de gestión del riesgo están basados en fuentes de información fiables.
7. Alinearse al contexto y al perfil de riesgos de la organización.
8. Tener en cuenta factores humanos y culturales. Las capacidades, percepciones o intenciones humanas pueden facilitar o dificultar el logro de los objetivos de la organización.
9. Ser transparente e inclusiva. Asegurar que la gestión del riesgo sea abierta, visible y accesible involucrando a las partes interesadas y responsables de la organización.
10. Ser dinámica, iterativa y sensible al cambio. La gestión de riesgos debe ser capaz de detectar y responder a los cambios de la organización y de su entorno.
11. Facilitar la mejora continua de la organización. Las organizaciones deberían desarrollar e implementar estrategias para mejorar continuamente el enfoque de la gestión del riesgo.

Esta norma se enfoca en la mejora continua, cuyo propósito principal es integrar la gestión de riesgos en la dirección, estrategia y planificación, procesos, políticas, valores y cultura de toda la organización.

Esta normativa está estructurada en base al ciclo de vida PHVA, con una etapa previa de Mandato y Compromiso. También establece una serie de mandatos que la Dirección debe cumplir para asegurar la efectividad de la gestión de riesgos así como una planificación estratégica y rigurosa.

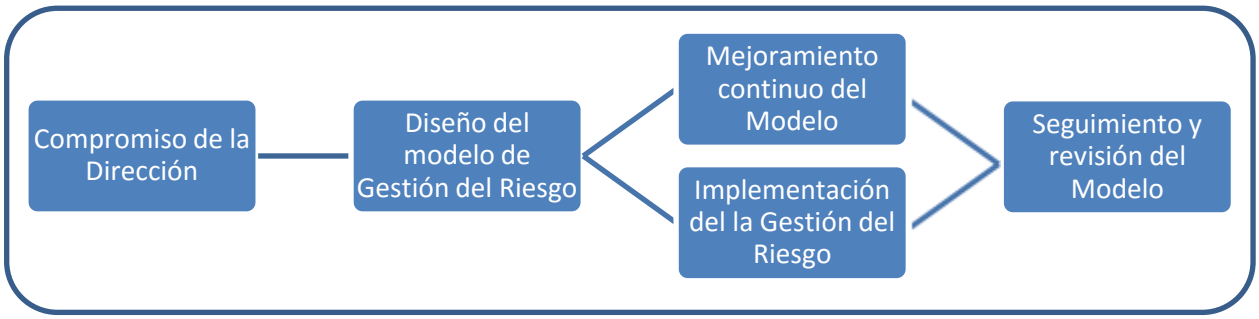

Figura 17 Marco de Trabajo para la Gestión del Riesgo

Fuente: Alejandro Reyes Plata, 2010

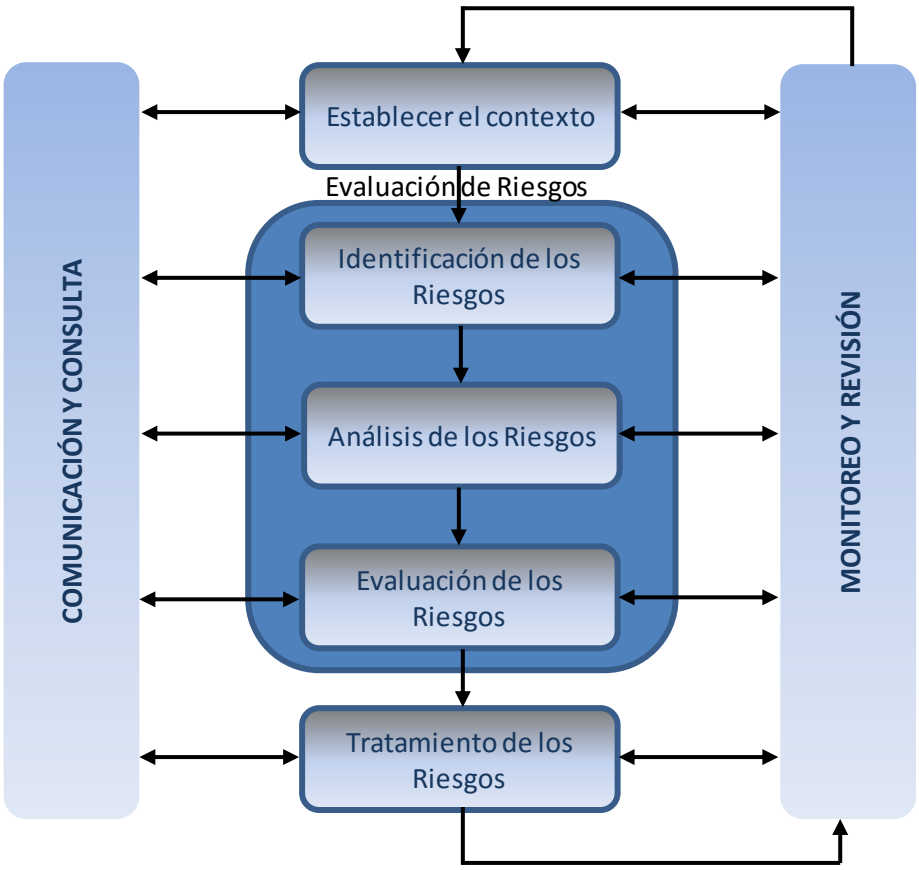

Figura 18 Proceso de Gestión del Riesgo

Fuente: Alejandro Reyes Plata, 2010

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.

Por eso es importante verificar y evaluar las seguridades físicas y lógicas de redes, aplicaciones web, bases de datos, servidores, etc., y esto se logra con el Ethical Hacking (hackeo ético), que consiste en verificar las vulnerabilidades existentes en el sistema de interés valiéndose de test de intrusión. Con toda la información recopilada las organizaciones establecen medidas preventivas y correctivas contra de posibles ataques malintencionados.

Por todo lo anterior, es importante simular los posibles escenarios donde se reproducen ataques de manera controlada, esto se logra a través del servicio de Ethical Hacking, que permite también verificar actividades de delincuentes cibernéticos, esta forma de actuar tiene su justificación en la idea de que: Para atrapar a un intruso, primero debes pensar como intruso.

Los servicios del Ethical Hacking permiten garantizar la seguridad informática mediante un conjunto de sistemas, métodos y herramientas que sirven para precautelar la información. También utilizan una variedad de métodos que incluyen tácticas de ingeniería social, uso de herramientas de hacking, uso de Metasploits que explotan vulnerabilidades conocidas. Para alcanzar el objetivo se pueden hacer uso de todas las tácticas que permitan ingresar a los sistemas informáticos e identificar las áreas críticas de las organizaciones.

2.5.1 Los Ethical Hackers

Los hackers éticos o Pen-Tester realizan pruebas de penetración, este experto en computadoras y redes de datos ataca los sistemas de seguridad en nombre de sus dueños, con el objetivo de buscar y encontrar vulnerabilidades que un hacker podría encontrar de manera maliciosa. Para probar los sistemas de seguridad utilizan las mismas tácticas, herramientas, métodos que utilizan los hakers maliciosos pero se limitan únicamente a reportarlos en lugar de sacar ventaja de ellos.

El Ethical Hacking también es conocido como penetration testing (pruebas de penetración) o intrusión testing (pruebas de intrusión). Los individuos que realizan estas actividades a veces son denominados "hackers de sombrero blanco", este término proviene de las antiguas películas del Oeste, en donde el "bueno" siempre llevaba un sombrero blanco y el "malo" un sombrero negro.

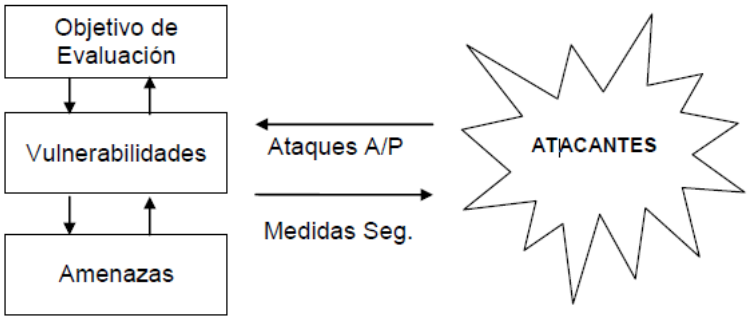

Figura 19 Flujo de un ataque

2.5.2 ¿Por qué hacer un Ethical Hacking?

A través del Ethical Hacking es posible evaluar los niveles de seguridad de una organización, se identifica que intenciones maliciosas tiene con los diferentes grados de acceso que este tiene.

Las pruebas de penetración permiten comprobar y clasificar las vulnerabilidades, en cambio el análisis de fallas de seguridad comprueba el impacto que éstas tienen sobre la organización.

Estas pruebas dejan al descubierto las vulnerabilidades que individuos maliciosos no autorizados pueden hacer uso malintencionado de los recursos informáticos de la organización, estos pueden ser: crackers, hackers, ladrones, ex-empleados, empleados actuales disgustados, competidores, etc. En base a la información propia de cada organización se determina la estructura y las herramientas de seguridad pero nunca a la inversa.

Estas pruebas de penetración permiten:

- Evaluar vulnerabilidades a través de la identificación de debilidades provocadas por una mala configuración de las aplicaciones.
- Analizar y categorizar las debilidades explotables, con base al impacto potencial y la posibilidad de que la amenaza se convierta en realidad.
- Proveer recomendaciones en base a las prioridades de la organización para mitigar y eliminar las vulnerabilidades y así reducir el riesgo de ocurrencia de un evento desfavorable.

Fases de pruebas de penetración:

1. Recopilación de información
2. Descripción de la red
3. Exploración de los sistemas

4. Extracción de información
5. Acceso no autorizado a información sensible o crítica
6. Auditoría de las aplicaciones web
7. Elaboración de informes
8. Informe final

2.5.3 Tipos de Ethical Hacking

Las pruebas de penetración se enfocan principalmente en las siguientes perspectivas:

- Pruebas de penetración con objetivo: se buscan las vulnerabilidades en partes específicas de los sistemas informáticos críticos de la organización.
- Pruebas de penetración sin objetivo: consisten en examinar la totalidad de los componentes de los sistemas informáticos pertenecientes a la organización. Este tipo de pruebas suelen ser las más laboriosas.
- Pruebas de penetración a ciegas: en estas pruebas sólo se emplea la información pública disponible sobre la organización.
- Pruebas de penetración informadas: aquí se utiliza la información privada, otorgada por la organización acerca de sus sistemas informáticos. En este tipo de pruebas se trata de simular ataques realizados por individuos internos de la organización que tienen determinado acceso a información privilegiada.
- Pruebas de penetración externas: son realizas desde lugares externos a las instalaciones de la organización. Su objetivo es evaluar los mecanismos perimetrales de seguridad informática de la organización.
- Pruebas de penetración internas: son realizadas dentro de las instalaciones de la organización con el objetivo de evaluar las políticas y mecanismos internos de seguridad de la organización.

Si el personal informático conoce o no el desarrollo de las pruebas se puede clasificar en dos modalidades:

Red Teaming: Es una prueba encubierta, sólo un grupo selecto de ejecutivos sabe de ella. Es más real y no permite hacer cambios en los niveles de seguridad de la organización.

Blue Teaming: El personal de informática conoce sobre las pruebas. Los usuarios deben estar alertados de manera que se eviten situaciones de pánico y fallas en la continuidad del negocio**.**

2.5.4 Beneficios del Ethical hacking

Al finalizar el Ethical Hacking se elabora y se entrega al cliente un reporte detallado de todos los hallazgos encontrados y verificables, así como también las recomendaciones que deben ser adoptadas y aplicadas por los responsables de la organización en tiempos determinados dependiendo de la criticidad de la vulnerabilidad detectada. Este documento se compone de un informe técnico y uno ejecutivo para que los empleados técnicos y administrativos puedan entender y apreciar los riesgos potenciales sobre el negocio.

Entre los beneficios más importantes que las organizaciones adquieren con la realización de un Ethical Hacking son :

- Ofrecer un panorama acerca de las vulnerabilidades halladas en los sistemas de información, lo cual es de gran ayuda al momento de aplicar medidas correctivas.
- Deja al descubierto configuraciones no adecuadas en las aplicaciones instaladas en los sistemas (equipos de cómputo, switches, routers, firewalls) que pudieran desencadenar problemas de seguridad en las organizaciones.

- Identificar sistemas que son vulnerables a causa de la falta de actualizaciones.
- Disminuir tiempo y esfuerzos requeridos para afrontar situaciones adversas en la organización.

Los beneficios no sólo se ven reflejados en la parte técnica y operacional de la organización, sino que también la relación con el cliente mejora, incremento de la reputación corporativa, que a veces la imagen es más valiosa para algunas organizaciones o empresas, como por ejemplo los bancos.

Es muy importante tener en cuenta los aspectos legales vigentes en cada país para la realización de un Ethical hacking, esto aplica tanto para las organizaciones que prestan el servicio como por quienes lo contratan.

Se deben aclarar en la parte contractual sobre los objetivos específicos de las pruebas de penetración, ya que podría existir malos entendidos una vez culminadas las pruebas, con esto se aseguraría también los aspectos relacionados con la confidencialidad sea de un adecuado manejo.

La organización que contrata el servicio debe proporcionar toda la información que requiera el Pen Tester, y esta debe ser fidedigna para que los resultados con los que se concluya sean verídicos y ayuden a que la organización tome acciones efectivas y eficaces. Sin embargo las pruebas de penetración realizadas por un Pen Tester no permiten abarcar el amplio número de técnicas y mecanismos que los crackers o hackers utilizan para vulnerar un sistema informático.

2.5.5 Aspecto Legal

Actualmente es más fácil infringir la ley a causa del progreso tecnológico, esto motiva a que se realicen los delitos tradicionales o nuevos. Esto ha permitido definir un marco legal referente a los delitos informáticos.

María de la Luz Lima indica que el delito electrónico en un sentido amplio es "cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin", y que en un sentido estricto, el delito informático, es "cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo que en la forma típica son "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y la forma atípica "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

Antes de conocer las regulaciones que se han establecido en el Ecuador y que están relacionadas con las tecnologías de la información, es importante conocer como está conformada la estructura general de dichas regulaciones, se tomará como referencia la Pirámide Kelseniana, esta permite conocer de manera ilustrativa como se conforman las normas jurídicas jerárquicamente.

Figura 20 Jerarquía de Leyes – Pirámide de Kelsen

Fuente: Julio Téllez Valdés, 1981

Desde los años ochenta, la ONU, a través de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional CNUDMI, ha promovido la unificación de legislaciones mundiales, entre los documentos aprobados está la Ley Modelo sobre Comercio Electrónico y la Ley Modelo sobre Firmas Electrónicas.

En Sudamérica, en 1999 Colombia publica la ley 527, es el primer país que regula el comercio electrónico, firmas digitales y las entidades de certificación, luego en 2000 Perú publica la ley 27269, sobre Ley de Firmas y Certificados Digitales. En el 2001 Argentina y Venezuela, Chile y Ecuador en el año 2002.

En la legislación del Ecuador bajo el contexto de que la información es un bien jurídico a proteger, se mantienen leyes y decretos que establecen apartados y especificaciones acorde con la importancia de las tecnologías, tales como:

1. Ley Orgánica de Transparencia y Acceso a la Información Pública.
2. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

3. Ley de Propiedad Intelectual.
4. Ley Especial de Telecomunicaciones.

Tabla 2

Infracciones Informáticas

INFRACCIONES INFORMÁTICAS	REPRESIÓN	MULTAS
Delitos contra la información protegida (CPP Art.202)		
1. Violentando claves o sistemas accede u obtiene información	6 meses a 1 año	$500 - $1000
2. Seguridad nacional o secretos comerciales o industriales	1 a 3 años	$1000 - $1500
3. Divulgación o utilización fraudulenta	3 a 6 años	$2000 - $10000
4. Divulgación o utilización fraudulenta por custodios	6 a 9 años	$2000 - $10000
5. Obtención y uso no autorizados	2 meses a 2 años	$1000 - $2000
Destrucción maliciosa de documentos (CCP Art.262)	3 a 6 años	……..
Falsificación electrónica (CPP Art. 353)	3 a 6 años	……..
Daños informáticos (CPP Art. 415)		
1. Daño dolosamente	6 meses a 3 años	$60 - $150
2. Servicio público o vinculado con la defensa nacional	3 a 5 años	$200 - $600
3. No delito mayor	8 meses a 4 años	$200 - $600
Apropiación ilícita (CPP Art.553)		
1. Uso fraudulento	6 meses a 5 años	$500-$1000
2. Uso de medios (claves, tarjetas magnéticas, otros instrumentos)	1 a 5 años	$1000 - $2000
Estafa 8CPP Art. 563)	5 años	$500 - $1000
Contravenciones de tercera clase (CPP Art. 606)	2 a 4 días	$7 - $14

Fuente: Código de Procedimiento Penal del Ecuador

2.6 Pruebas de Penetración

Figura 21 Metodología

Fuente: Alejandro Hernández, 2007

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.

Es muy importante realizar un pent test, con esto permitirá evaluar los sistemas informáticos así estén protegidos, ya que la posibilidad de que sufra ataques siempre va a existir, por eso la importancia de descubrir las fallas mediante el uso de las herramientas.

Entre las diferentes herramientas se incluyen desde scanners de puertos, complejos algoritmos para descifrar claves, sistemas de intrusión por fuerza bruta, herramientas de sniffing de redes y penetración de firewalls, así como también herramientas de escaneo de vulnerabilidades de aplicaciones web y mucho más. Las herramientas suelen estar agrupadas en juegos de herramientas o "Toolkits", algunos Toolkits son utilizados en

penetraciones de alto nivel, existen otros portátiles que arrancan con el sistema operativo.

2.6.1 Tipos de Pent Test

Las pruebas de penetración se enfocan principalmente en las siguientes perspectivas:

- Pruebas de penetración con objetivo: buscan vulnerabilidades en partes específicas de los sistemas informáticos críticos de la organización.

- Pruebas de penetración sin objetivo: esta busca vulnerabilidades en la totalidad del sistema informático perteneciente a la organización. Estas pruebas son generalmente extensas y laboriosas.

- Pruebas de penetración a ciegas: en estas pruebas se aplica únicamente a información pública disponible.

- Pruebas de penetración informadas: se aplica a la información privada, y se trata de simular ataques ocasionados por empleados internos que de una u otra forma tienen acceso a la información.

- Pruebas de penetración externas: se realizan fuera de la organización, de manera que se evalúan las seguridades de sistemas informáticos perimetrales.

- Pruebas de penetración internas: esta evalúa internamente las políticas y mecanismos internos de seguridad de la organización.

A su vez, cada tipo de pruebas descritas anteriormente se puede ubicar en tres modalidades:

1. Black-box: El pentester no tiene conocimiento del sistema, como por ejemplo una empresa contratada, esta realiza el trabajo simulando un atacante externo.

2. White-box: El pentester tiene conocimiento del funcionamiento del sistema, arquitectura de la red, sistemas operativos utilizados, etc. Representa a un atacante que tiene información relevante antes de atacar al sistema informático.
3. Gray-box: Este es el caso en el cual el pentester simula un empleado interno, con clave y usuario podrá encontrar vulnerabilidades que por usuarios internos.

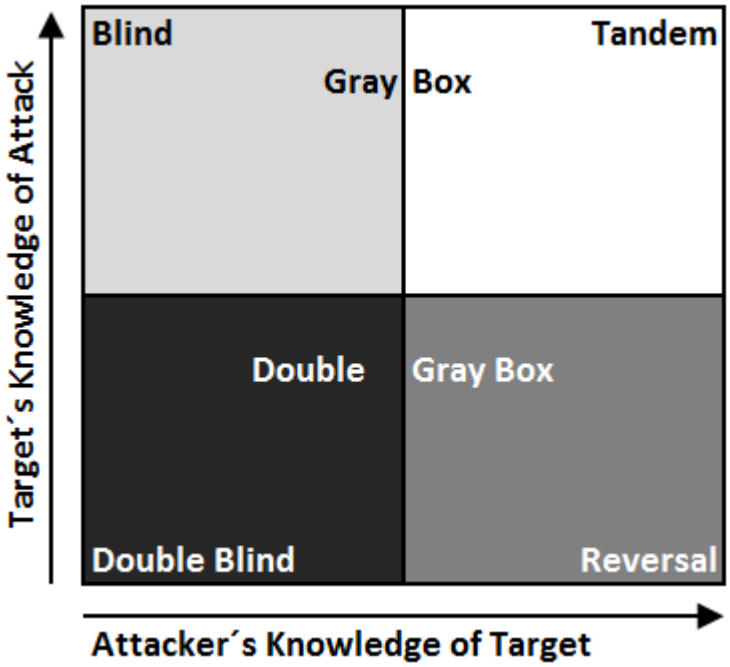

Figura 22 Conocimiento del atacante vs conocimiento del atacado

Fuente: Internet Security Auditors, 2016

2.6.2 Metodología de Evaluación

Se utiliza una metodología de evaluación de seguridad informática que incluye cuatro etapas:

2.6.2.1 Etapa de Descubrimiento

Esta etapa es la preliminar, aquí se establecerán las áreas donde se realizará la evaluación, para ello es importante conocer los riesgos del negocio asociado al uso de los activos informáticos involucrados. Es necesario realizar la recolección de información, entre la más importante están:

- Rangos de direcciones IP asignados
- Direcciones IP de servicios tercerizados
- Dirección física de la empresa
- Números telefónicos
- Nombres de personas y cuentas de correo electrónico
- Fuentes de información
- Análisis de la página WEB
- Existencia de redes inalámbricas (WiFi)

2.6.2.2 Etapa de Exploración

En esta etapa se establecen los objetivos mediante técnicas que sirven para identificar todos los blancos potenciales. Además se deberá incluir el análisis de protocolos, relevamiento de plataforma y barreras de protección, scanning telefónico, scanning de puertos TCP y UDP, detección remota de servicios y sistemas operativos, análisis de banners y búsqueda de aplicaciones web.

En esta etapa como tareas más importantes están:

- Detección de módems activos.
- Confirmación de rangos de direcciones IP.
- Detección de equipos activos e identificación de Sistemas Operativos.
- Detección de servicios activos e identificación Software y versiones.
- Detección de barreras de protección.
- Análisis de características de configuración en redes WiFi

La técnica de scanning se utiliza para detectar equipos, servicios y módems activos. Generalmente los intrusos la utilizan para poder acceder a potenciales blancos.

2.6.2.3 Etapa de Evaluación

En esta etapa se analizan los datos encontrados para la detección y determinación de vulnerabilidades de la seguridad informática que afectan a los sistemas evaluados, se analiza la seguridad de ser posible en todos los niveles, considerando las siguientes tareas:

- **Ejecución de herramientas de scanning de vulnerabilidades.**
  - Buscan automáticamente vulnerabilidades conocidas en los Sistemas Operativos y servicios que se estén ejecutando.
  - Permiten, en algunos casos, explotar las vulnerabilidades detectadas.
  - Facilitan la actualización de las bases de datos de vulnerabilidades.

- **Búsqueda manual de vulnerabilidades.**
  Para realizar esta búsqueda es necesario verificar la existencia de vulnerabilidades conocidas que puedan afectar a las versiones del software identificado en cada servicio.

2.6.2.4 Etapa de Intrusión

Esta es la etapa más compleja del pent test, aquí se debe aplicar todo el conocimiento y profesionalismo adquirido en las etapas previas, esto permite acceder a los sistemas y obtener el control de los mismos.

2.6.2.4.1 Planteamiento

Para la ejecución de un pent test se requiere una planificación previa, para ello se describe a continuación los pasos a seguir:

2.6.2.4.2 Reunión de alineamiento

Es la reunión preliminar, donde se establece el alcance del trabajo, dentro de esto se encuentra:

- ¿Qué tipo de Pentest se va a realizar?
- Horario de realización del pentest (durante las horas laborales o fuera del horario laboral).
- ¿Se permitirá DOS?
- ¿Se pueden instalar Backdoors?
- ¿Se pueden realizar Defacement de los sitios?
- ¿Se pueden borrar \ogs?
- ¿Conocerá el personal la realización del pentest?
- ¿Se puede utilizar Ingeniería Social?

Una vez concluida esta reunión quedará registrado en un documento o contrato el alcance del pent test y otorgando los permisos necesarios para la realización efectiva y eficiente de este trabajo.

2.6.2.4.3 Realización del Pentest

Para la realización del pentest se siguen los siguientes pasos:

- Reconocimiento: Que a su vez está divido en Footprint y Scanning
- Adquisición de Objetivo: Comprende Enumeración de vulnerabilidades, Acceso, estalación de privilegios y búsqueda de nuevos objetivos.
- Eliminación de Huellas: Eliminación de rastros en logs.

Luego dependiendo de lo acordado, se pueden realizar pruebas de Denegación de Servicios o dejar instalados Backdoors.

2.6.2.4.4 Reporte y Presentación de Resultados

Es necesaria la elaboración de un reporte donde se describirán detalladamente los resultados obtenidos de la evaluación del sistema informático.

2.6.2.5 Herramientas útiles en Penetration Testing para Aplicaciones Web

Existen herramientas que permiten realizar este test sobre aplicaciones web, algunas son gratuitas y de código abierto, otras de pago y propietarias. Estas son:

2.6.2.5.1 Burp Suite

Plataforma para PenTest y seguridad en sitios web, las características principales son: Intercept Proxy, detección automática de vulnerabilidades, herramienta de repetición, posibilidad de escribir plugins propios.

2.6.2.5.2 Acunetix - Scaner para vulnerabilidades web

Esta herramienta es utilizada para MS Windows, es potente y busca vulnerabilidades en formularios de subida de archivos (file upload) y otros más. Las más comunes son: Cross-Site Scripting, SQL Injection, CRLF injection. Permite generar reportes detallados porque los resultados se almacenan en una base de datos.

2.6.2.5.3 SQLmap

Herramienta Open Source, gratuita basada en línea de comandos que automatiza la detección y explotación de vulnerabilidades SQL Injection y extracción de información de bases de datos.

2.6.2.5.4 Nessus

Tiene un mayor alcance, es decir redes amplias, gran cantidad de dispositivos, etc., también es muy útil para realizar PenTesting a aplicaciones web habilitando y configurando los módulos correctos.

2.6.2.6 Consideraciones Legales

Es importante considerar las implicaciones legales que esto puede acarrear, actualmente existen legislaciones enfocadas a la intrusión a

sistemas y redes informáticas, para ello es necesario que la organización y la empresa que realiza el PenTest firmen un convenio de confidencialidad y una carta de autorización.

En el convenio de confidencialidad es un reglamento, en donde se decribe los acuerdos establecidos en relación a la información que le proveerá la empresa contratante o la organización, la misma estará a su entera disposición la realización del PenTest.

En esta carta consta la autorización debidamente firmada por el responsable de la Organización (Gerente, Oficial de Seguridad Informática, Abogado, etc.) antes de tocar un solo sistema, esta mínimo debe incluir: ¿Quién va a realizarlo?, ¿Cuándo va a ser realizado?, ¿Por qué será realizado?, ¿Qué tipo de actividad es la autorizada y cuál no?, ¿Cuál es el alcance? De contar con un departamento o área legal los tiempos para analizar los documentos cambian y seguramente introducirá modificaciones a favor de la organización.

2.6.3 Metodologías de pruebas de penetración

Existen diversas metodologías de código abierto para evaluar seguridades, algunas describen el aspecto técnico y otras se centran en criterios de gestión de las pruebas de seguridad, y unas pocas abarcan ambos puntos.

Entre las metodologías más importantes que se puede encontrar las siguientes:

2.6.3.1 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.

De este modo, y teniendo en cuenta que un programa efectivo de testeo de aplicaciones web, debe incluir como elementos a testear: Personas, Procesos y Tecnologías, OTP de línea en su primera parte conceptos claves a la vez que introduce un framework específicamente diseñado para evaluar la seguridad de aplicaciones web a lo largo de su vida.

Paso 1: Antes de comenzado el desarrollo

a) Revisión de Políticas y Estándares
b) Desarrollo de un Criterio de Medidas y Métricas (Aseguramiento de la Trazabilidad)

Paso 2: Durante la definición y el diseño

a) Revisión de los Requerimientos de Seguridad
b) Diseño de Revisión de Arquitectura
c) Creación y Revisión de modelos UML
d) Creación y Revisión de modelos de Amenazas

Paso 3: Durante el desarrollo

a) Code Walkthroughs
b) Revisión de Código

Paso 4: Durante el deployment

a) Testeo de Penetración sobre la Aplicación
b) Testeo sobre la Administración y Configuración

Paso 5: Operación y mantenimiento

a) Revisión Operacional
b) Conducción de Chequeos Periódicos
c) Verificación del Control de Cambio

2.6.3.2 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).

OSSTMM se encarga de normar aspectos tales como: las credenciales del profesional a cargo del test, formato de reportes, normas

éticas y legales que deben ser tenidas en cuenta al momento de concretar el test, los tiempos que deberían ser tenidos en cuenta para cada una de las tareas, y por sobre todas las cosas, etc.

2.6.3.3 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.

Constituye un framework detallado respecto de las prácticas y conceptos relacionados con todas y cada una de las tareas a realizar al conducir un testeo de seguridad. La información contenida dentro de ISSAF, se encuentra organizada alrededor de lo que se ha dado en llamar "Criterios de Evaluación", cada uno de los cuales ha sido escrito y/o revisado por expertos en cada una de las áreas de aplicación. Estos criterios de evaluación a su vez, se componen de los siguientes elementos:

- Una descripción del criterio de evaluación
- Puntos y Objetivos a cubrir
- Los pre-requisitos para conducir la evaluación
- El proceso mismo de evaluación
- El informe de los resultados esperados
- Las contramedidas y recomendaciones
- Referencias y Documentación Externa.

2.7 Metodología

Para la realización de este proyecto de tesis para la obtención del título de Ingeniero en Sistemas e Informática se utilizará el Método Científico, que es el marco general de referencia que guiará toda la investigación.

Con el uso de los Métodos Teóricos Investigativos y el conocimiento empírico se podrá generar un criterio para un adecuado manejo de la investigación a realizarse en base a la recopilación, análisis y clasificación de la información relacionada con las diferentes tecnologías, métodos y herramientas involucradas en el Pentest.

Se aplica el método inductivo porque se puede observar los efectos de los ataques generados, con esto se puede llegar a la determinación de una propuesta en base a políticas de seguridad que permitan identificar las vulnerabilidades y puedan gestionarse proactivamente mediante una guía metodológica para Pruebas de Penetración en Ambientes Virtuales.

CAPÍTULO III. ANÁLISIS Y EVALUACIÓN DE HERRAMIENTAS DE PRUEBAS DE PENETRACIÓN EN AMBIENTES VIRTUALES

3.1 Descripción de las Herramientas de Pruebas de Penetración

Con el uso adecuado de herramientas para pruebas de penetración se puede evidenciar cuales son las vulnerabilidades que presentan los sistemas informáticos, esto permitirá tomar acciones correctivas y preventivas oportunas que prevengan intentos futuros de penetración mal intencionados, ya que con el paso del tiempo los sistemas informáticos se vuelven más vulnerables. Por todo aquello es importante identificar todo tipo de vulnerabilidades y aplicar métodos efectivos que aseguren el correcto funcionamiento de los sistemas informáticos.

3.2 Métricas utilizadas en la clasificación de vulnerabilidades

Una vez que son evidenciadas las vulnerabilidades, es necesario clasificarlas y cuantificarlas, para esto el Forum of Incident Response and Security Teams (FIRST), plantea un modelo tipológico basado en métricas cualitativas, temporales y de entorno según se indica en la siguiente tabla:

Tabla 3

Tipología basada en métricas para clasificar Vulnerabilidades

GRUPOS	MÉTRICAS	TIPOS
Métricas Base	Vector de acceso	Locales
Métricas Base	Vector de acceso	Red Local
Métricas Base	Vector de acceso	Remotos
Métricas Base	Complejidad de acceso	Alta o baja
Métricas Base	Autenticación	Simple
Métricas Base	Autenticación	Múltiple
Métricas Base	Autenticación	Ninguna
Métricas Base	Impacto de la confidencialidad	Alta o baja
Métricas Base	Impacto de la Integridad	Alta o baja
Métricas Base	Impacto en la Disponibilidad	Alta o baja
Métricas Temporales	Explorabilidad	Explotable
Métricas Temporales	Explorabilidad	No explotable
Métricas Temporales	Facilidad de Corrección	Corrección fácil
Métricas Temporales	Facilidad de Corrección	Corrección compleja
Métricas Temporales	Facilidad de Corrección	No existe corrección
Métricas Temporales	Fiabilidad del informe de Vulnerabilidad	Identificada y confirmada
Métricas Temporales	Fiabilidad del informe de Vulnerabilidad	Identificada sin confirmar
Métricas Temporales	Fiabilidad del informe de Vulnerabilidad	Sin fuentes
Métricas del entorno	Daños Colaterales	Alta o baja
Métricas del entorno	Distribución de los Equipos Vulnerables	Alta o baja
Métricas del entorno	Requisitos de Seguridad	Alta o baja

Fuente: Instituto Nacional de Estadística Geográfica e Informática, 2005

Las pruebas de intrusión se enfocan principalmente en las siguientes perspectivas:

a) Externas e internas, con objetivo cuando buscan vulnerabilidades en partes específicas, sin objetivo cuando examinan la totalidad de los componentes informáticos.

b) Pruebas a ciegas, aquellas que solo se emplean la información pública disponible sobre la organización.

c) Pruebas informadas, aquellas que utilizan la información privada, otorgada por la organización acerca de sus sistemas informáticos.

Es importante como buenas prácticas de seguridad ejecutar las pruebas de intrusión mínimo una vez al año, o cuando se realicen actualizaciones o modificaciones en los sistemas informáticos, con esto la organización verificará que su sistema informático se encuentre seguro y que sus políticas de respuesta a incidentes sean las adecuadas.

Para realizar las pruebas de penetración se utilizan los siguientes tipos de modelos:

a) Modelo de caja blanca: este test tiene un alcance muy amplio y simula un ataque de un usuario interno autorizado. La organización facilita toda la información requerida acerca de los sistemas informáticos, su estructura y de la red como topología, dispositivos, Sistemas Operativos, Bases de datos, etc.

b) Modelo de caja negra: en este test el atacante no posee ninguna información previa de la organización, el objetivo es que se simule un ataque externo como si fuera un hacker que desea extraer información privada de los sistemas informáticos de la organización. Un número mínimo de personas de la organización deben saber que se está llevando a cabo este ataque. Este tipo de test puede llegar a ser muy costoso tanto en tiempo como en términos económicos.
c) Modelo de caja gris: en este modelo se utilizan los métodos anteriores, la idea es simular a un atacante real interno no autorizado o un asesor externo que tiene acceso autorizado.

3.3 Metodologías del test de penetración

Una metodología define un conjunto de reglas prácticas y procedimientos que son ejecutados durante el curso de evaluación de cualquier programa de seguridad de la información y permite ordenar y estandarizar este proceso.

El atacante antes de comprometer la seguridad de cualquier sistema de información, debe conocer las cuatro etapas para realizar un test de penetración, estas son:

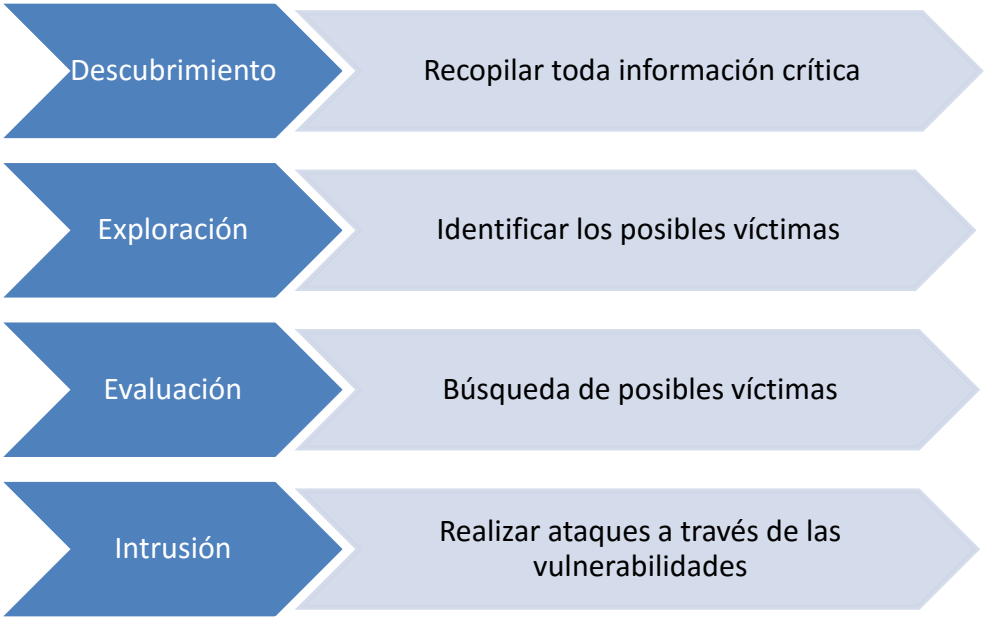

Figura 23 Etapas de un test de Penetración

Fuente: D. Monrroy, 2009

Para las pruebas de penetración, existen múltiples metodologías que pueden ser propietarias o abiertas. El eficiente uso de estas pruebas y con la ayuda de ciertas técnicas ayudará a que los sistemas de información de cualquier organización no puedan ser vulnerados fácilmente-

3.3.1.1 Según la Publicación de NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment)

- Planificación: se refiere a la aprobación de la Gerencia, identificación del alcance y los objetivos de la prueba.
- Descubrimiento: consiste en la recopilación de información y análisis de vulnerabilidades.
- Ejecución del ataque: explotación de vulnerabilidades-
- Presentación de informes: en este informe final se describe las vulnerabilidades encontradas, las recomendaciones requeridas para controlarlas o mitigarlas en base al grado de riesgo que cada una representa.

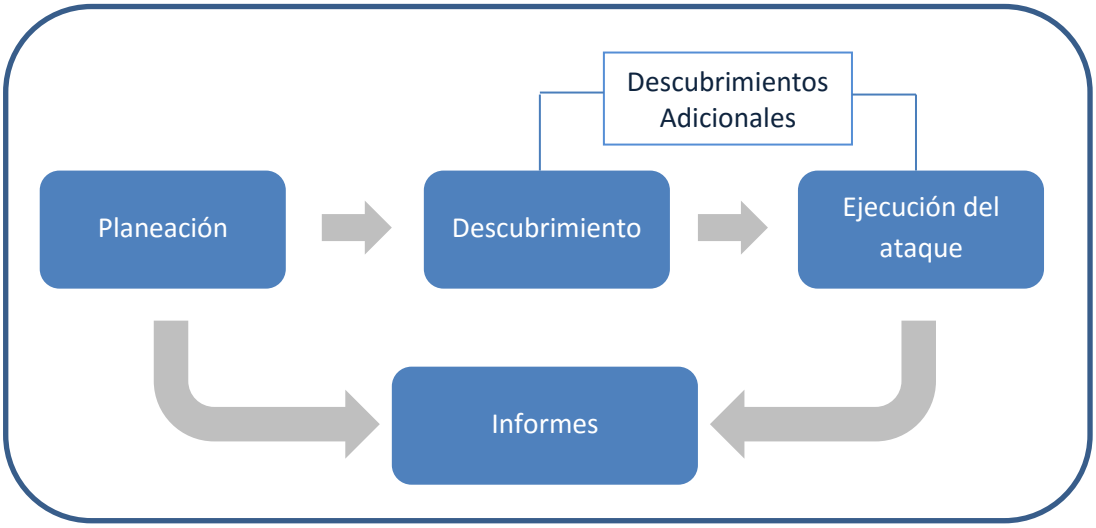

Figura 24 Metodología NIST SP 800-115

Fuente: National Institute of Standards and Technology (NIST), 2008

Otras metodologías a destacar son:

3.3.1.2 La metodología Penetration Testing Framework (PTF) - ISSAF (Information Systems Security Assessment Framework): ***incluye tres fases, cuyos pasos de ejcución son cíclicos e interativos:***

Fase I: Planificación y preparación. Previo a la ejecución de las pruebas, se debe planear los aspectos relevantes de las pruebas que se van a realizar y se debe firmar un acuerdo formal donde se detallen los mismos.

Fase II: Evaluación. Esta fase presenta un enfoque por capas, como se muestra en la figura 3.4, en el que cada una de ellas representa un mayor nivel de acceso a los activos de información.

Fase III: Informes, limpieza y destrucción de información. Una vez se han culminado todos los casos de prueba definidos en el alcance del trabajo, se debe generar un informe escrito que describe los resultados detallados y las recomendaciones pertinentes para mejorar la seguridad; no obstante, en caso de identificar un punto crítico durante la ejecución de las pruebas, se debe informar de inmediato. Adicionalmente, toda la información que se crea y/o almacena en los sistemas de prueba debe ser eliminada; si por alguna razón esto no es posible, todos los archivos (con su localización) deben ser mencionados en el informe técnico para que sean eliminados posteriormente

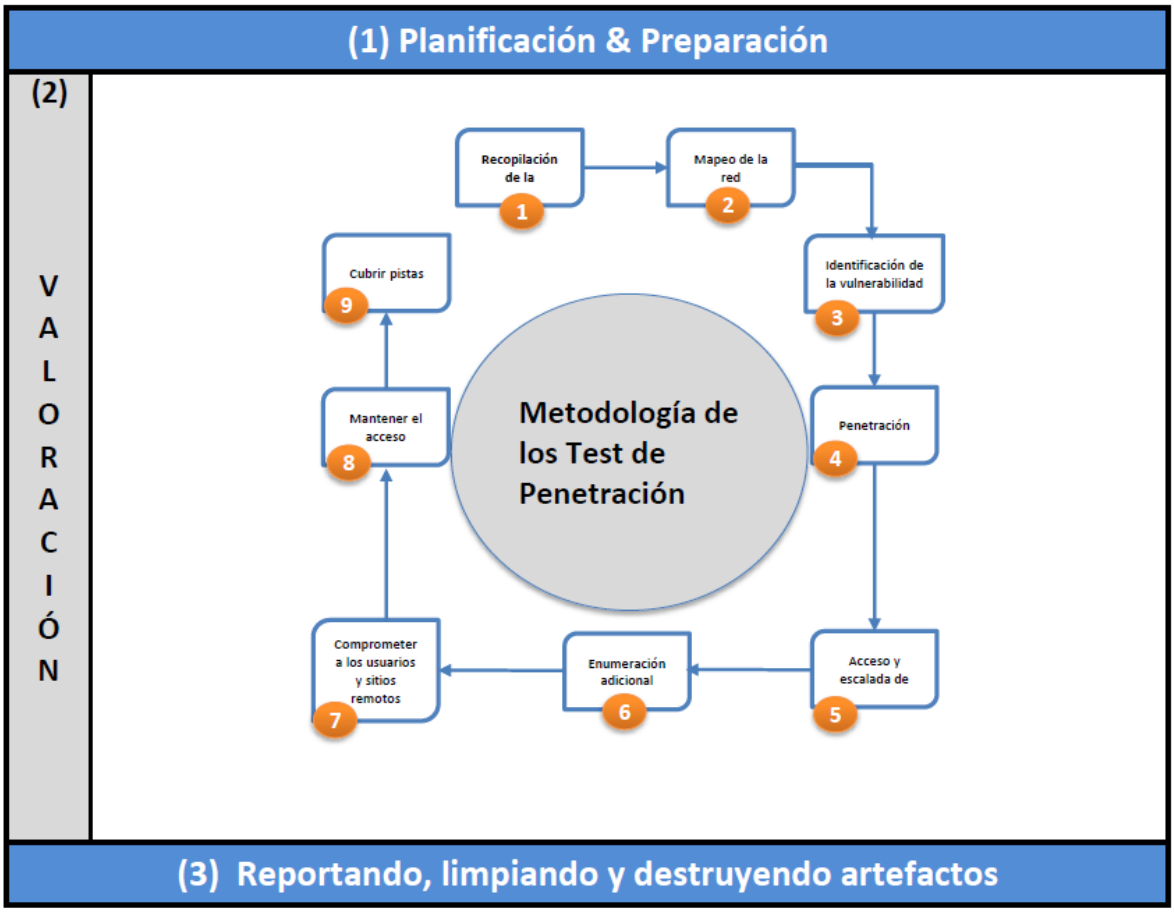

Figura 25 Fases de la metodología ISSAF (Information Systems Security Assessment Framework)

Fuente: Information System Security Assessment Framework (ISSAF), 2006

3.3.1.3 OSSTMM 3: Manual de metodología abierta para pruebas de seguridad

Esta metodología divide la totalidad de una infraestructura en cinco canales: humano, físico, redes inalámbricas, telecomunicaciones y redes de datos para su estudio. Como se observa en la tabla 3.1, está constituida por cuatro fases:

Tabla 4

Fases y Módulos de la Metodología OSSTMM

Fases	Módulos	Descripción
Introducción	Revisión de Postura	La revisión de la cultura, reglas, normas, reglamentos, leyes y políticas aplicables al objetivo. Define el alcance y qué pruebas deben hacerse. Requerido para realizar de manera correcta la Fase C.
Introducción	Logística	La medición de las limitaciones de interacciones tales como: la distancia, velocidad, y la falibilidad de determinar los márgenes de exactitud en los resultados.
Introducción	Verificación de la Detección	La verificación de la práctica y la amplitud de detección de interacciones, y la previsibilidad de respuesta.
Introducción	Activa	Para conocer las restricciones impuestas a las pruebas interactivas y llevar adecuadamente las Fases B y D.
Fase de Interacción	Auditoría de la Visibilidad	La determinación de los objetivos que van a ser probados dentro del ámbito. La visibilidad es considerada como “presencia” y no se limita a la vista humana.
Fase de Interacción	Verificación de Acceso	La medición de la amplitud y profundidad de los puntos de acceso interactivos dentro del objetivo y la autenticación necesaria.
Fase de Interacción	Verificación de la Confianza	La determinación de las relaciones de confianza de y entre los objetivos. Una relación de confianza existe donde quiera que el objetivo acepta la interacción entre los objetivos en el ámbito de aplicación.
Fase de Interacción	Verificación de los Controles	La medición de la utilización y eficacia de los controles de pérdida basados en procesos: el no repudio, confidencialidad, privacidad e integridad. El control de alarma se verifica al final de la metodología.
Fase de Investigación	Verificación de los Procesos	La determinación de la existencia y eficacia del registro y mantenimiento de los actuales niveles de seguridad se define por la revisión de la postura y los controles de indemnización. La mayoría de los procesos tienen definidos un conjunto de reglas; sin embargo, las operaciones reales no reflejan ninguna eficiencia, por lo tanto, es necesario redefinir las reglas establecidas.

Fase de Investigación	Verificación de Configuración/Verificación de la Capacitación	La investigación del estado estable (funcionamiento normal) de los objetivos tal como han sido diseñados para funcionar en condiciones normales para determinar problemas de fondo fuera de la aplicación de pruebas de stress de seguridad.
Fase de Investigación	Validación de Propiedad	La medición de la amplitud y profundidad en el uso de la propiedad intelectual ilegales o sin licencia o aplicaciones dentro del objetivo.
Fase de Investigación	Revisión de la Segregación	La determinación de los niveles de identificación de información personal definido por la revisión de la postura. Se sabe cuáles son los derechos de privacidad que se aplican y en qué medida la información detectada como personal puede ser clasificados con base en estos requisitos.
Fase de Investigación	Verificación de la Exposición	La búsqueda de información libremente disponible que describe la visibilidad indirecta de los objetivos o los activos en el canal elegido por el alcance.
Fase de Investigación	Exploración de Inteligencia Competitiva	La búsqueda de información libremente disponible, directa o indirectamente, que podría perjudicar o afectar negativamente al propietario del objetivo a través de medios externos. Descubrir información que por sí sola o en conjunto puede influir en las decisiones de negocios.
Fase de Intervención	Verificación de la Cuarentena	La determinación y la medición del uso eficaz de la cuarentena para todos los accesos hacia y dentro del objetivo. Determinar la efectividad de los controles de autenticación y el sometimiento en términos de cuarentena de listas blancas y negras.
Fase de Intervención	Auditoría de Privilegios	El mapeo y la medición del impacto del mal uso de los controles de sometimiento, las credenciales y los privilegios o la escalada no autorizada de privilegios. Determinar la eficacia de la autorización en los controles de autenticación, la indemnización, y el sometimiento en términos de profundidad y roles.
Fase de Intervención	Validación de la Supervivencia/ Continuidad del Servicio	La determinación y la medición de la resistencia del objetivo a los cambios excesivos o adversos (Denegación de Servicios) en los controles de continuidad y la capacidad de recuperación que se verían afectados.

Fuente: Carolina Pinzón, 2013

Tabla 5

Comparación de Metodologías

ASPECTOS	ISSAF	OSSTMM
Permite realizar pruebas y análisis de seguridad	Si	Si
Establece requisitos previos para la evaluación	Si	No
La metodología define un proceso detallado para la realización de pruebas	Si	Si
Define áreas de alcance	Si	No
Contiene plantillas para realizar las pruebas	Si	Si
Detalla técnicas para cada prueba	Si	No
Contiene ejemplos de pruebas y resultados	Si	No
Recomienda herramientas para cada prueba	Si	No
Presenta procesos de análisis y evaluación de riesgos	Si	Si
Define dimensiones de seguridad a evaluar	No	Si
Establece valores o niveles de evaluación de riesgos	Si	Si
Enumera y clasifica las vulnerabilidades encontradas	Si	No
Realiza estimación de impacto	Si	Si
Genera reportes e informes	Si	No
Presenta contramedidas y recomendaciones	Si	No
Contiene referencias a documentos y enlaces externos	Si	No

En la Tabla 3.2 se consideran aspectos fundamentales de las metodologías OSSTMM e ISSAFT, la misma ayudará en la determinación de la metodología a plantearse durante este trabajo investigativo. De la comparación realizada se determina que ISSAF, es una metodología que contempla aspectos importantes para identificar riesgos, analizarlos, evaluarlos y establece las medidas apropiadas para reducir su impacto.

3.4 Descripción de herramientas para pruebas de penetración

En la publicación especial 800-115 de NIST, presenta una Guía Técnica de Pruebas de Seguridad y evaluación de la información, en esta se describe las 100 mejores herramientas para pruebas de penetración, la principal diferencia entre ellas es que pueden ser de código libres o comerciales. Para realizar esta clasificación se consideraron varios criterios importantes como precisión, cobertura, versatilidad, adaptabilidad. A continuación se describen brevemente algunas de ellas:

- **Nessus:** Herramienta de seguridad "Open Source", es un escáner de seguridad remoto para Linux, BSD, Solaris y Otros Unix. Está basado en plug-in(s), tiene una interfaz basada en GTK, y realiza más de 1200 pruebas de seguridad remotas.

- **Ethereal**: herramienta de libre uso, analizador de protocolos de red para Unix y Windows en una red viva o de un archivo de captura en algún disco.
- **Snort:** es una herramienta que permite detectar intrusiones en una red de poco peso para el sistema, realiza análisis de tráfico en tiempo real y registro de paquetes en redes con IP. Puede realizar análisis de protocolos, búsqueda/identificación de contenido y puede ser utilizado para detectar una gran variedad de ataques y pruebas, como por ej. buffer overflows, escaneos indetectables de puertos "stealth port scans", ataques a CGI,

pruebas de SMB "SMB Probes", intentos de reconocimientos de sistema operativos "OS fingerprinting" y mucho más.

- **TCPDump / WinDump:** Tcpdump es un analizador de paquetes de red basado en texto. También se puede utilizar esta herramienta para rastrear problemas y actividades en una red. Existe una versión para Windows llamada WinDump.

- **nHping2:** esta herramienta analiza hosts detrás de un firewall que bloquea los intentos que utilizan las herramientas estándar.

- **bDSniff:** se refiere a un conjunto de herramientas (dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, y webspy) que monitorean pasivamente una red en busca de datos como passwords, e-mail, archivos, etc.
- **GFI LANguard:** este es un escáner de red comercial para Windows. Esta herramienta escanea redes y reporta información como el nivel de "service pack" de cada máquina, faltas de parches de seguridad, recursos compartidos, puertos abiertos, servicios/aplicaciones activas en la computadora, datos del registro "key registy entries", passwords débiles, usuarios y grupos; y más. Los resultados del escaneo se muestran en un reporte en formato HTML.

- **aircrack-ng:** software de seguridad y auditoría inalámbrica que entre otros permite crakear redes con seguridad WEP y WPA.

- **brupsuite:** herramienta para la realización de test de intrusión en aplicaciones web permitiendo una completa metodología hasta la explotación de la aplicación.

- **john:** herramienta que permite a los administradores de sistemas comprobar la seguridad de las contraseñas.

- **maltego:** es una herramienta que obtiene información de diferentes fuentes, con ella se logra investigar empresas, personas, sitios así como IP, zona o zonas geografías del objetivo, alias de redes sociales, etc.

- **owasp-zap / zapproxy:** herramienta para encontrar vulnerabilidades en aplicaciones web.
- **metasploit framework:** esta herramienta contiene muchas funciones para test de penetración, ayuda a la creación y ejecución de ecploits contra equipos remotos.

En la Tabla 3.3 la normativa ISO 27000 considerando los objetivos y actividades de control clasifica varias herramientas de análisis, esto permitirá determinar según los requerimientos de pent test que herramienta se ajusta a la metodología propuesta, aquí algunos ejemplos:

Tabla 6

Clasificación herramientas en base la normativa ISO 27000

Objetivos Control	Actividades Control	Herramientas
Garantizar la integridad de los siste	• Instalación del software en sistemas en producción	Genos Open Source: GMF es una implementación de las recomendaciones ITIL (IT Infrastructure Library) para la gestión de servicios de TI (IT Service Management o ITSM). GMF es un producto de software libre distribuido bajo licencia GPL e incluye módulos de gestión de incidencias (Trouble Ticketing), gestión de inventario, gestión del cambio (Change Management), SLA y reporting.
Evitar la explotación de vulnerabili	• Gestión de las vulnerabilidades técnicas • Restricciones en la instalación de software	Belarc: Belarc Advisor construye un perfil detallado del software y hardware instalado, el inventario de la red, la falta de revisiones en productos de Microsoft, el estado de anti-virus, puntos de referencia de seguridad, y muestra los resultados en el explorador Web. Toda la información del perfil del PC se mantiene privada y no se envía a servidores de la web.
Minimizar el impacto de actividade	• Controles de auditoría de los sistemas de información	SANS: SIFT Workstation es un Appliance de VMware pre-configurado con todas las herramientas necesarias para llevar a cabo un examen forense detallado digital. Es compatible con el formato Expert Witness Format (E01), Advanced Forensic Format (AFF), y formatos raw (dd) de evidencias.

Fuente: ISO 27001. Es

3.4.1 Análisis y evaluación de herramientas para Pruebas de Penetración en Ambientes Virtuales.

En la actualidad existen diferentes mecanismos de evaluación de las medidas de protección de una organización y de sus servicios expuestos a internet, por esto es importante analizar la efectividad de los controles de seguridad implantados realizándose una batería de acciones planificadas que simulan el comportamiento de un intruso.

Un test de penetración tiene el propósito de generar un informe técnico en el que se ponga de manifiesto la identificación del riesgo, la probabilidad de su ocurrencia, el impacto en la organización y la estimación de su gravedad así como las correspondientes recomendaciones.

A continuación se describen dos herramientas a utilizar para el desarrollo de este trabajo de investigación, se ampliará la importancia de la conectividad en una red, ya que si no se conectan adecuadamente los sistemas informáticos no funcionan. Luego se describirán algunos escenarios compatibles para la instalación del IDS (Intrusion Detection Systems). Por último se analizarán los programas escogidos para simular ataques.

A los IDS se los clasifican en tres tipos:

- **En cuanto a tipos de ataques y utilización de recursos:** En la figura 3.5 se detallan 4 tipos diferentes de IDS, que detectan ataques conocidos y también nuevos ataques.

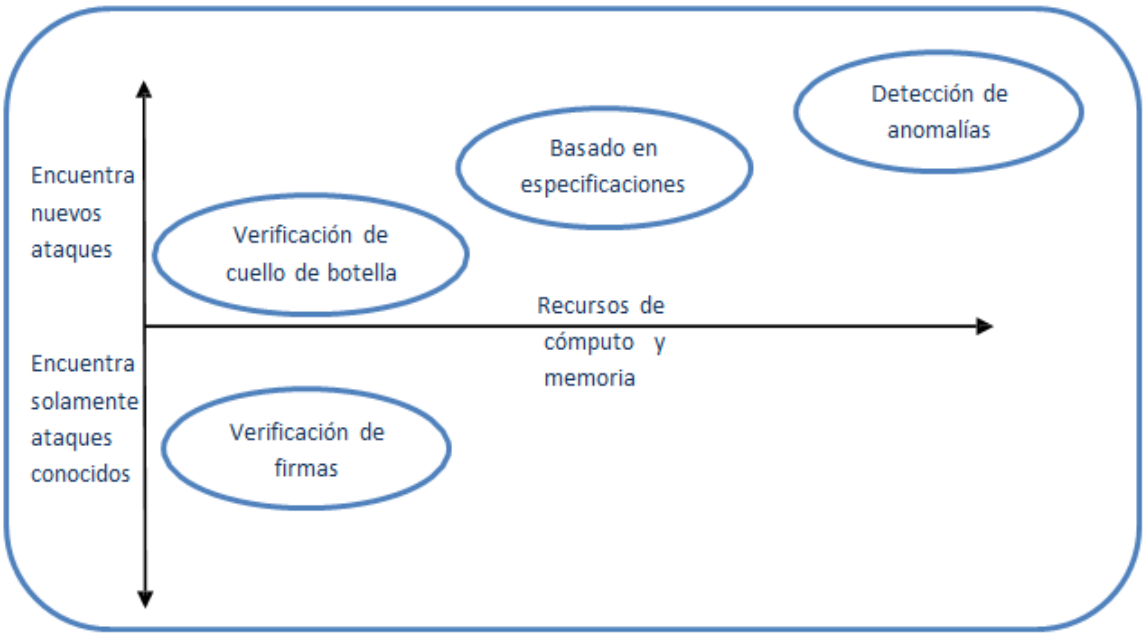

Figura 26 Modelos IDS

Fuente: www.tripwire.org, 2015

- **En cuanto a la metodología de detección de intrusos:** se clasifica en base a los algoritmos que utilizan, estos son:
    - Basados en patrones/firmas simples: en base a secuencias fijas comparan si el paquete coincide con la

firma que se almacena en una base de datos y la trata como potencial ataque.

- Basados en la coincidencia de los patrones de estado: En este caso verifica el paquete de modo aislado y también el flujo al que pertenece el paquete.
- Firmas basadas en decodificación de protocolos: Es una extensión de la anterior. Estas firmas se implementan decodificando los elementos que componen el flujo de información de la misma manera tanto como cliente como servidor en el proceso de comunicación.
- Firmas basadas en algoritmos heurísticos: Están basados en logaritmos que evalúan el tráfico que pasa por la red desde un punto de vista estadístico y trazan líneas base de comportamiento.

- **En cuanto a lugar y sistemas a monitorear:** se clasifican los IDS dependiendo donde y que sistemas tienen que monitorear. Estos son:

  - **HIDS (“HOST IDS”)**

    Estos IDS detectan intrusiones a nivel de HOST o a nivel de un equipo de cómputo, verificando alteraciones que pudo presentar el sistema operativo, así como también analizar los logs del equipo en busca de actividades sospechosas.

    Las principales tareas realizadas por un Host IDS son:

    a) Analizar los registros de actividad (Logs) del núcleo (Kernel) del sistema operativo, para detectar posibles infiltraciones.

b) Verificar la integridad de los archivos ejecutables, a fin de detectar posibles modificaciones de los mismos (Integrity check). Herramientas como Tripwire facilitan esta función.

c) Explorar periódicamente y planificadamente los programas privilegiados (setuid de sistemas UNIX/LINUX).

d) Auditoría periódica de los permisos asignados a los recursos del sistema.

e) Buscar y evaluar periódicamente de vulnerabilidades de software conocidas.

f) Revisar detalladamente el proceso de instalación de nuevas aplicaciones en el sistema, a fin de poder detectar caballos de Troya u otros códigos malignos.

- **MHIDS (MULTIHOST IDS)**

  Este IDS permite detectar actividades sospechosas detectados en varios hosts, por esto se les conoce como IDS Distribuidos (DIDS, Distributed IDS).

- **NIDS (NETWORK IDS)**

  Estos IDS se encargan de monitorear el tráfico de red (contenido de los paquetes) en busca de actividades sospechosas, tráfico anómalo que evidencian intentos de

intrusión. Entre las distintas situaciones de tráfico anómalo, se puede citar las siguientes:

a) Enrutamiento anormal de los paquetes de datos.
b) Fragmentación de paquetes deliberada.
c) Utilización de una dirección IP no válida o en desuso en uno de los tramos de red internos (IP Spoofing).
d) Afluencia de paquetes DNS con identificadores consecutivos, que incluyen la supuesta respuesta a una misma encuesta (situación típica de un ataque de DNS Spoofing).
e) Invasión de paquetes TCP SYN desde una o varias direcciones (situación típica de un ataque de denegación de servicio del tipo de SYN Flooding).
f) Invasión de paquetes ICMP o UDP de eco (típicos de ataques como Smurf y Fraggle).
g) Falsa correspondencia entre las direcciones MAC conocidas y las direcciones IP de los equipos.
h) Tormentas de tráfico ARP, que podrían revelar un intento de envenenamiento de las tablas ARP (situación típica de un ataque de ARP Spoofing).

SNORT, es un sistema conocido que verifica que paquetes de una red resultan sospechosos, para ello emplea una base de datos de reglas que verifican el contenido y los formatos de cabecera de los paquetes de datos. También se pueden descargar reglas desde el internet, estas permiten catalogar nuevos tipos de incidentes, exploits y vulnerabilidades de sistemas informáticos.

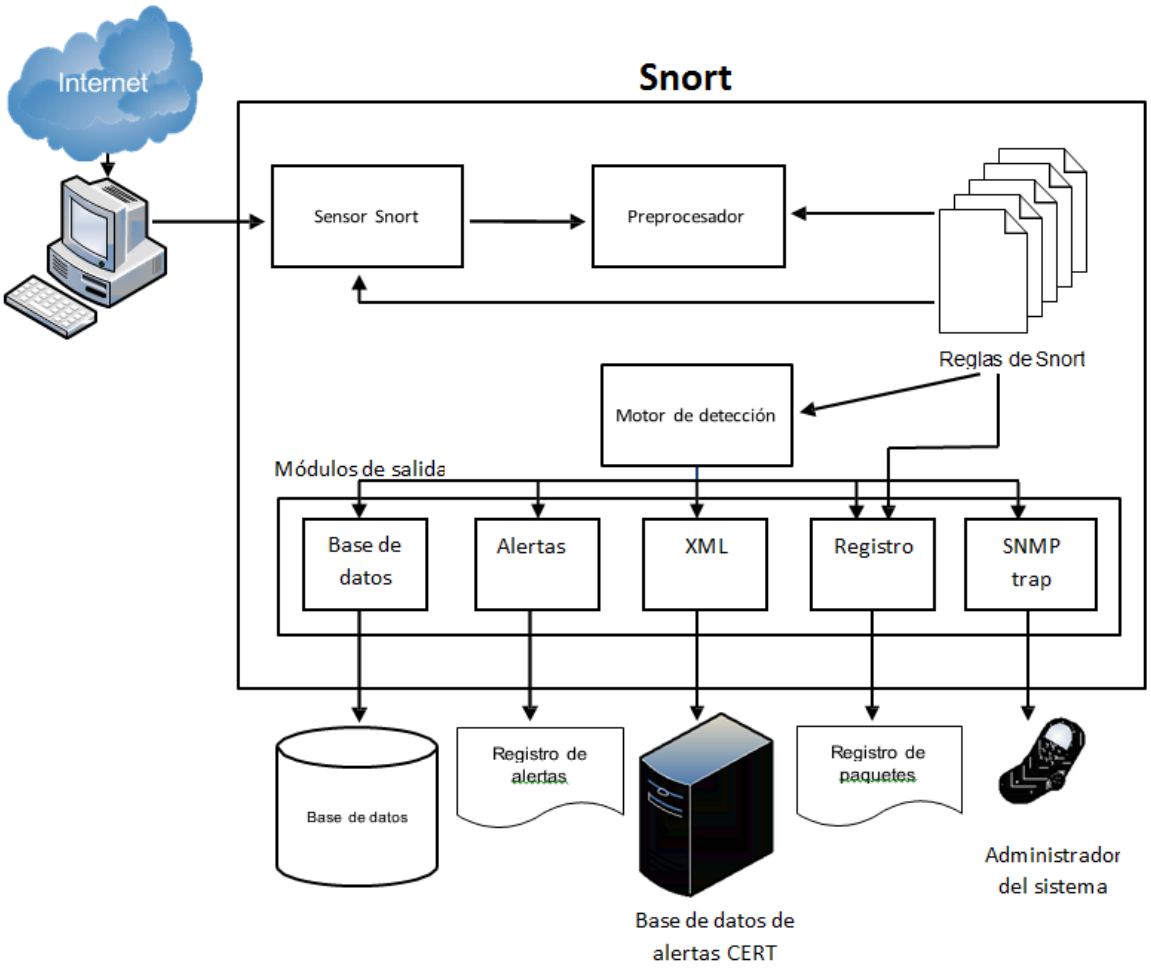

Figura 27 Arquitectura del IDS Snort

Fuente: www.snort.org, 2014

a) **Módulo de captura de paquetes**: realiza la captura del tráfico que circula por la red, aprovecha los recursos de procesamiento y minimiza la pérdida de paquetes.

Snort requiere de una biblioteca sniffing de paquetes; libpcap que fue escogida para la captura de paquetes de la tarjeta de red y puede ser controlada sobre todas las combinaciones de hardware y Sistemas Operativos; e incluso sobre WIN32 con winpcap. La facilidad de capturar paquetes

raw permite que el sistema operativo esté disponible a otras aplicaciones.

Un paquete raw es un paquete que se encuentra en su forma original una vez haya atravesado la red del cliente al servidor, es decir toda la información se encuentra intacta e inalterada por el sistema operativo.

b) **Decodificador:** Está organizado alrededor de las capas de los protocolos de Enlace de Datos y TCP/IP. Snort posee capacidades de decodificación para protocolos Ethernet, SLIP y PPP.

Un paquete sigue el siguiente flujo de datos moviéndose a través del decodificador de paquetes, como se puede ver en la figura 3.7.

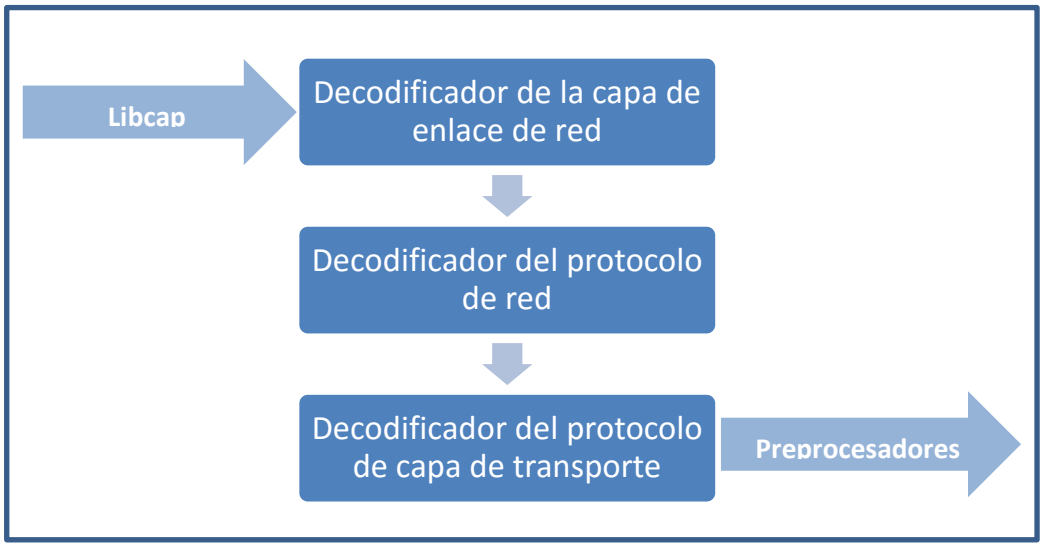

Figura 28 Flujo de datos del decodificador

c) **Preprocesadores:** para entender al preprocesador es importante recordar la forma de comunicación de un sistema,

conocer la función de un protocolo, como por ejemplo TCP/IP, que es un protocolo basado en capas, como se muestra en la figura 3.8. Cada capa del protocolo tiene una funcionalidad y necesita de una información para trabajar correctamente.

Los datos que se transmiten por la red en paquetes de forma individual, pueden llegar a su destino de forma desordenada, siendo el receptor el encargado de ordenar los paquetes y darles sentido.

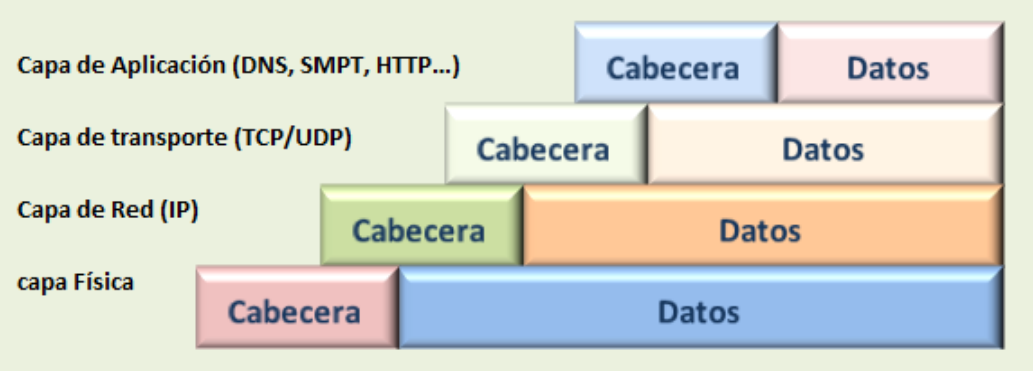

Figura 29 Capas TCP/IP

Fuente: es.ccm.net, 2016

La intrusión depende del módulo Preprocesador, aquí se interpreta y se ordena la información que viaja por la red de manera caótica, para luego aplicar reglas y buscar un determinado ataque.

Tabla 7

Preprocesadores para Snort

Preprocesador	Descripción
Frag3	El preprocesador frag3 se basa en la fragmentación IP de los módulos de snort. Frag3 permite una ejecución más rápida que frag2 y permite técnicas de antievasión.
stream4 y stream4_reasemble	Proporciona un flujo de ensamblado TCP y capacidades de análisis para poder rastrear hasta 100.000 conexiones simultáneas.
Flow	Permite unificar el estado que mantiene los mecanismos de Snort en un único lugar. Desde la versión 2.1.0 sólo se implementaba el detector portscan, pero a largo plazo muchos subsistemas de Snort utilizan flow.
stream5	Es un módulo de reensablado que intenta suplantar a stream4 y a flow. Permite rastrear tanto comunicaciones TCP como UDP.
Sfportscan	Es un módulo desarrollado por sourcefire para detectar el primer paso de un ataque: el escaneo de puertos.
rpc_decode	Permite normalizar múltiples registros RPC fragmentados en un único registro.
perfomance monitor	Permite medir en tiempo real el funcionamiento de Snort. El funcionamiento de éste preprocesador se lo verá más tarde.
http_inspect y http_inspect_server	Es un decodificador genérico para analizar el tráfico http. Permite trabajar tanto para analizar las respuestas de los clientes como de los servidores.
Smtp	Es un decodificador SMTP para los clientes de correo electrónico.
ftp/Telnet	Permite decodificar el tráfico ftp y telnet para buscar cualquier actividad anormal. Se utiliza para analizar tanto las respuestas de los clientes como de los servidores.
Ssh	Permite analizar el tráfico ssh de clientes y servidores.
dce/rpc	Analiza el tráfico SMB (compartir archivos y carpetas de Windows).
dns	Permite analizar el tráfico de DNS para detectar diferentes tipos de ataques.

Fuente: www.snort.org, 2014

d) **Reglas:** estas son patrones que se buscan dentro de los paquetes de datos. Estas reglas son utilizadas para comparar paquetes recibidos y generar alertas en caso de coincidir con la firma y paquetes.

A continuación se verificará algunas reglas de Snort, y el formato de las mismas para poder realizar su configuración.

Reglas de Protocolo: son dependientes del protocolo que se está analizando, por ejemplo en el protocolo Http está la palabra reservada uricontent.

Reglas de Contenido Genéricas: especifica patrones de búsqueda, ya sean binarios o ASCII, muy útil para buscar exploits los cuales suelen terminar en cadenas de tipo “/bin/sh”.

Reglas de Paquetes Malformados: verifican si existe alguna anomalía en sus cabeceras, este tipo de reglas no miran en el contenido ya que primero se comprueban las cabeceras.

Reglas IP: este tipo de reglas analiza con contenido y sin él, se aplican directamente sobre la capa IP, y son comprobadas para cada datagrama IP, si el datagrama luego es Tcp, Udp o Icmp se realizará un análisis del datagrama con su correspondiente capa de protocolo.

Estructura de reglas

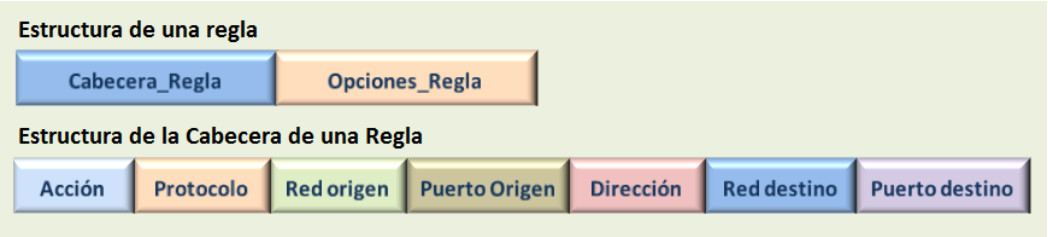

Figura 30 Estructura de una Regla y una Cabecera

Fuente: es.ccm.net, 2016

Cabecera de una regla: establece el origen y destino de la comunicación y realiza una acción sobre dicha información. Su estructura es:

<acción> <protocolo> <red origen> <puerto origen> <dirección> <red destino> <puerto destino>

Ejm: alert tcp $EXTERNAL_NET any → $HOME_NET 53

e) El motor de detección

La responsabilidad principal del motor de detección es descubrir en el paquete cualquier intrusión existente. El tiempo de respuesta y la carga del motor de detección se definen por los siguientes factores:

- Las características de la máquina.
- Las reglas definidas.
- Velocidad interna del bus usado en la máquina Snort.
- Carga en la red.

El motor de detección puede aplicar las reglas en distintas partes del paquete. Estas partes son las siguientes:

La cabecera IP: Puede aplicar las reglas a las cabeceras IP del paquete.

La cabecera de la capa de Transporte: Incluye las cabeceras TCP, UDP e ICMP.

La cabecera del nivel de la capa de Aplicación: Incluye cabeceras DNS, FTP, SNMP y SMPT.

Payload del paquete: significa que se puede crear una regla que el motor de detección use para encontrar una cadena que esté presente dentro del paquete.

f) Módulos de salida

Los módulos de salida o plugins básicamente controlan el tipo de salida generada por estos sistemas.

Los módulos de salida son Syslog, Database y Unified, que es un formato binario genérico para exportar datos a otros programas.

Plugins snort

A continuación se resumen algunos módulos y complementos existentes para Snort:

Tabla 8

Complementos de Snort

Nombre	Comentario	Url
Spade	Módulo detector de Anomalías	http://majorgeeks.com/Sam_Spade_d594.html
Inline Snort	Sistema de prevención de intrusos	http://snort-inline.sourceforge.net/
BRO	NIDS que usa una gran variedad de módulos para el análisis de protocolos.	http://www.bro-ids.org/
SAM	Monitor de Alertas de Snort.	http://www.darkaslight.com/projects/sam
Snort Log Parser	Analiza los mensajes del archivo de alertas de Snort.	http://linux-bsdcentral.com/index.php/content/view/17/28/
IDS Policy Manager	Facilita el manejo de los preprocesadores y de las salidas de Snort.	http://www.activeworx.org/Default.aspx?tabid=55
ACID	Consola web para visualizar los registros de Snort.	http://acidlab.sourceforge.net/
BASE	Evolución de ACID.	http://sourceforge.net/projects/secureideas/

Fuente: www.snort.org, 2014

Sistemas que utilizan Snort: Son muchas las arquitecturas que integran Snort como sistema de detección de intrusos, por ejemplo:

a) SPP-NIDS: Arquitectura para detección de intrusos, que soporta las reglas SNORT.

b) High Performance Software, Hardware Network Intrusion and Detection System: Propone un sistema que ejecuta una versión mejorada de Snort haciendo uso de FPGAs.

c) Snort Híbrido: Implementación de Snort como IDS híbrido (detección de anomalías y de uso indebido).

d) Intrusion Detection and Prevention: Combinación de Snort con un sistema de prevención de Intrusos, IPS.

e) SANTA-G: Monitoriza el framework que usa el RGMA (Relational Grid Monitoring Architecture).

Existe también una versión de Snort que realiza el análisis de redes inalámbricas, se llama AirSnort y su único propósito es romper la encriptación WEP (obteniendo así la contraseña de encriptación) de todas las redes inalámbricas que se encuentren en el radio de alcance del dispositivo inalámbrico que utilice la herramienta.

CAPÍTULO IV. PROPUESTA METODOLÓGICA PARA REALIZAR PRUEBAS DE PENETRACIÓN EN AMBIENTES VIRTUALES

4.1 Introducción

En la actualidad existen diferentes mecanismos de evaluación de las medidas de protección de una organización y de sus servicios expuestos a internet, por esto es importante analizar la efectividad de los controles de seguridad implantados realizándose una batería de acciones planificadas que simulan el comportamiento de un atacante.

Un test de penetración tiene el propósito de generar un informe técnico en el que se ponga de manifiesto la identificación del riesgo, la probabilidad de su ocurrencia, el impacto en la organización y la estimación de su gravedad así como las correspondientes recomendaciones.

No existe ninguna metodología que se ajuste a algún trabajo específico, sin embargo como resultado de este trabajo investigativo se proporciona una metodología detallada para realizar pruebas de penetración en ambientes virtuales.

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

- Planificación y preparación de la prueba de penetración
- Evaluación
- Informe, limpieza y destrucción de objetos

4.2 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, se debe especificar:

- Antecedentes de la organización
- Obtener los permisos necesarios para la participación del equipo en las pruebas de penetración.
- Recepción de informes de pruebas de penetración realizados anteriormente.
- Acordar la no divulgación de la información.
- Es recomendable contar con un asesor jurídico que entienda el manejo de documentos legales en términos de tecnología de la información.
- Descripción detallada de:
    - Herramientas que se utilizarán en las pruebas de penetración.
    - Requisitos de hardware y software para la ejecución de pruebas de penetración.
    - Fechas exactas del desarrollo de ejecución y entrega de informes finales.

4.3 Ejecución

En esta fase se realiza la prueba de penetración con un enfoque por capas, estas son:

4.3.1 Recolección de Información

En esta fase se recoge la mayor cantidad de información posible sobre los sistemas de información, como por ejemplo:

- Rangos de direcciones IP asignados
- Direcciones IP de servicios tercerizados
- Dirección física de la empresa
- Números telefónicos
- Nombres de personas y cuentas de correo electrónico
- Fuentes de información
- Análisis de la página WEB
- Existencia de redes inalámbricas (WiFi)

Esta etapa es esencial porque se recopila la información requerida para completar la prueba de penetración; el evaluador debe identificar los puntos más vulnerables más probables y centrarse en ellos, generalmente el tiempo y los recursos son limitados.

4.3.2 Mapeo de la red de trabajo

En esta etapa con la ayuda de herramientas y aplicaciones se busca descubrir información técnica sobre anfitriones y redes que participan en la prueba, como:

- Encontrar anfitriones
- Puerto y servicio de exploración
- Perímetro de la cartografía de la red (router, firewall)
- Identificación de los servicios críticos
- Sistema operativo toma de huellas dactilares
- Rutas identificación con administración información base
- Servicio de toma de huellas dactilares

La cartografía de la red ayudará a determinar probables puntos débiles y e importantes para la organización evaluada. También contribuirá a que se confirme o descarte ciertas hipóptesis sobre el

sistema de información (por ejemplo: software, hardware, configuración, arquitectura, la relación con otros recursos y su relación con procesos de negocio).

En esta etapa se trata de identificar:

- Máquinas o equipos
- Sistemas operativos, firewalls, antivirus, dispositivos perimetrales, enrutamiento y topología de la red en general que forman parte de la organización de destino.
- Contenido de la red (hosts, servers, routers y otros dispositivos) y cómo funciona con los protocolos y sistemas operativos.
- Direcciones de correo electrónico, nombres NetBIOS, las exportaciones NFS, nombres de host, etc.

4.3.3 Identificación de vulnerabilidades

Antes de empezar con el trabajo el responsable de realizar las pruebas de penetración deberá realizar ciertas actividades:

- Identificar los servicios vulnerables mediante banners de servicios.
- Realizar el análisis de vulnerabilidades en base a vulnerabilidades conocidas, o de bases de datos públicas, como security focus, etc.
- Verificar falsos positivos y falsos negativos.
- Enumerar y clasificar las vulnerabilidades descubiertas.
- Identificar las rutas de ataque y escenarios para la explotación.

En esta etapa se proporciona las directrices para el equipo que realizará las pruebas de penetración, este equipo tomará datos necesarios en la topología de red para encontrar posibles fallos de red, servidores, servicios y otros recursos de información que se adjunta. Con esta información podrá ser capaz de construir un listado de servidores vulnerables.

Los escáneres de vulnerabilidad, CGI y otras herramientas se pueden utilizar para identificar las vulnerabilidades y adaptarlas a ataques conocidos. Con esta información el responsable de realizar las pruebas de penetración podrá con las herramientas de escaneo realizar ajustes finos a fin de evitar los falsos positivos, falsos negativos y centrarse en las cuestiones relevantes, y mala calidad de la evaluación.

El objetivo de esta etapa es primero contar con la existencia real de las vulnerabilidades, y se logra:

- Haciendo coincidir las versiones vulnerables de servicios de vulnerabilidades conocidas y teóricas, que recorren la red en direcciones no deseadas.
- Las pruebas de servicios web en busca de vulnerabilidades como XSS y de inyección de SQL
- La localización de contraseñas débiles y cuenta-
- Escalada de privilegios.

En esta etapa se realiza una revisión de todas las vulnerabilidades detectadas por la herramienta de evaluación seleccionada. Se interpreta los resultados en base a la gravedad de la vulnerabilidad y criticidad de los activos.

Se debe dar a conocer al personal de TI todas las vulnerabilidades identificadas ya que conocen de mejor manera los

sistemas implementados y protegerlos de manera inmediata de las vulnerabilidades identificadas.

Cuando se prepara el resumen de vulnerabilidades detectadas se debe considerar la gravedad del riesgo, basada en el impacto de procesos de negocio. La clasificación puede diferir significativamente de la clasificación de riesgo técnico.

La clasificación de riesgo de las vulnerabilidades generalmente es efectuada por las herramientas de escaneo con una relativa precisión, sin embargo se da mayor valor agregado a las pruebas de penetración cuando se realiza un análisis basado en impacto que tienen las vulnerabilidades en el negocio de la organización de destino, así se podrán aplicar las correcciones y justificar su presupuesto.

El evaluador primero debe entregar un primer borrador sobre los hallazgos encontrados en la prueba de penetración, este documento debe ser revisado en conjunto con los responsables de la organización de manera puedan identificar correcta y oportunamente el impacto que estos pueden tener en el negocio y los ajustes que deben hacer. También se entregará un informe técnico en el que se describe generalmente los resultados reportados por las herramientas.

4.3.4 Penetración

Una vez seleccionadas las herramientas de penetración, se realiza algunas pruebas para verificar que resultados se obtienen, estas pruebas son realizadas a medida, es decir con código y herramientas manipuladas, y hechas a medida.

4.3.5 Obtener Acceso y escalada de privilegios

Ganar privilegios desde el más elemental hasta el “root”, de esta manera se asegura el control de los sistemas.

Las actividades en esta sección permitirán a los evaluadores confirmar y documentar la intrusión probable y/o propagación de ataques automatizados. Esto permite una mejor evaluación del impacto en el conjunto de los sistemas de información de la organización.

Obtener privilegio en el acceso mínimo es posible gracias a la obtención de acceso a través de varios medios a las cuentas sin privilegios, incluyendo:

- Descubrimiento de combinaciones de nombre de usuario / contraseña.
- Descubrimiento de contraseña por defecto o contraseñas en blanco en las cuentas del sistema.
- Aprovechar la configuración predeterminada del proveedor (como los parámetros de configuración de red, contraseñas y otros).
- Descubrimiento de servicios públicos que permiten ciertas operaciones en el sistema, como creación de archivos de lectura y escritura.

Para alcanzar el objetivo de la evaluación ya sea un sistema específico o una red puede requerir que los sistemas intermedios se vean comprometidos, estos posibles saltos intermedios pueden ser routers, firewalls, servidores o estaciones de trabajo, etc.

El objetivo final se ha cubierto, el evaluador tiene los privilegios administrativos sobre el sistema, es decir cuentas administrativas como administrador, root, SISTEMA, etc.

4.3.6 Enumeración de objetivos

Ataque a passwords, esnifar tráfico de red y analizarlo, hacernos con “cookies”, direcciones de correo (mensajes incluidos), routers y redes (passwords por defecto), mapeo completo de la red.

4.3.7 Comprometer usuarios remotos y sitios

El auditor y asesor deberían tratar de comprometer los sistemas y hacerse con el máximo de contraseñas y sistemas. Una vez conseguido le dará acceso a sistemas tanto dentro como fuera dela red objetivo. Usar firewall en escritorios remotos de los usuarios para tratar de contener e acceso a cualquier parte de la red.

Un solo agujero es suficiente para dejar al descubierto toda una red, independientemente de qué tan seguro puede ser la red perimetral. Cualquier sistema es tan seguro como el más débil.

Las comunicaciones entre usuarios remotos, sitios y redes empresariales se pueden proporcionar con la autenticación y el cifrado, usando tecnologías como VPN, así se podrá asegurar que los datos en tránsito por la red no pueden ser vulnerados, sin embargo no se garantiza que parte de la comunicación sea vulnerable.

4.3.8 Mantener Acceso

No es recomendable utilizar para pruebas de penetración canales encubiertos, instalación de puerta de atrás y el despliegue de rootkits, ya que existe enorme riesgo que durante la prueba estos queden abiertos y sean detectados por un intruso.

Para el uso de canales encubiertos es importante:

- Identificar el canal encubierto que se pueda utilizar.
- Seleccionar la mejor herramienta disponible para el canal encubierto.
- Realizar la configuración metódica del canal encubierto en la Red.
- Realizar pruebas usando la técnica de detección común.

Las puertas traseras (Backdoors) se pueden crear de varias maneras:

- Uso de rootkits.
- Mediante la apertura de un puerto.
- Al permitir que el sistema de destino se conecte al servidor.
- Mediante la creación de un oyente para una determinada secuencia de paquetes que a su vez abren un puerto.

4.3.9 Cubrir pistas

Esta etapa es una práctica habitual durante las pruebas de penetración, se trata de actuar lo más abierto posible (excepto cuando lo solicite el cliente), producir información detallada y los registros de todas las actividades.

Cubrir las pistas es importante, porque se debe ocultar las actividades y herramientas utilizadas durante y después de la prueba de intrusión, y así proteger el sistema de los peligros a los que estuvo expuesto.

La importancia de esta etapa se entiende fácilmente, pero por lo general subestimada. Después de que un atacante ha comprometido con éxito un sistema, le va a gustar que se mantenga sin alertar al administrador, por razones obvias. Cuanto más tiempo el atacante

permanece en un sistema comprometido, mejores serán las posibilidades de alcanzar sus metas en la red.

4.4 Informe, limpieza y destrucción de información

Una vez se han culminado todos los casos de prueba definidos en el alcance del trabajo, se debe generar un informe escrito que describe los resultados detallados y las recomendaciones pertinentes para mejorar la seguridad; no obstante, en caso de identificar un punto crítico durante la ejecución de las pruebas, se debe informar de inmediato. Adicionalmente, toda la información que se crea y/o almacena en los sistemas de prueba debe ser eliminada; si por alguna razón esto no es posible, todos los archivos (con su localización) deben ser mencionados en el informe técnico para que sean eliminados posteriormente

4.4.1 Informes

El informe como mínimo debe contener:

En todo el tiempo en que se realiza las pruebas de penetración, se identifican puntos críticos y estos deben ser reportados inmediatamente para garantizar que la organización es consciente de ello. Este punto crítico debe ser discutido y a la vez establecer medidas para proteger la información.

Una vez haya culminado las pruebas de penetración es importante elaborar un informe en el que se describa los resultados detallados de las pruebas, y recomendaciones para la mejora. El informe debe seguir una estructura bien documentado, en que se incluya:

- Resumen de Gestión

- Alcance del proyecto
- Herramientas que se han utilizado (incluyendo exploits)
- Fechas y horarios de las pruebas reales sobre los sistemas
- Una lista de todas las vulnerabilidades identificadas con las recomendaciones incluidas en la forma de resolver los problemas encontrados.
- Una lista de acciones correctivas y soluciones recomendadas.

4.4.2 Limpieza y destrucción de la información

Toda la información que se crea y/o almacena en los sistemas probados deben ser removidos, si esto es por alguna razón no es posible todos estos archivos con su respectiva localización deben ser mencionadas en el informe para que el personal técnico del cliente elimine estos después de que se haya recibido el informe.

La organización debe crear lineamientos para seguir un estándar de mejores prácticas en base a las recomendaciones del informe de pruebas de penetración. Las auditorías periódicas de una organización, reducen la exposición a vulnerabilidades. Las políticas y directrices de seguridad incluyen:

- Política de normas de la organización: Especifica la utilización de tecnologías, procedimientos y parámetros con el fin de asegurar la información.
- Lineamientos de uso aceptable: Específica el uso aceptable de los recursos Web en la organización.
- Roles y responsabilidades: Especifica los roles y

responsabilidades de los administradores y los usuarios de las aplicaciones Web.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- 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.

- Una prueba de penetración permite evaluar de manera planificada y en tiempos establecidos la protección de los sistemas de información de una organización.

- Con el análisis del marco teórico se evidenció la realidad del Ecuador y el mundo en la cantidad de vulnerabilidades de los sistemas de información, así como los robos y fraudes en las redes sociales.

- Según Publicación especial 800-115 de NIST la herramienta evaluada muestra como esta alcanza eficaz y eficientemente los objetivos relacionados con la detección de vulnerabilidades en sistemas de información.

- Con el análisis de las diferentes metodologías y herramientas se identificaron las principales vulnerabilidades que se pueden presentar en ambientes virtuales en base los niveles de seguridad que previenen accesos no autorizados sin sacrificar el rendimiento de los sistemas de información.

- 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.

- 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.

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

- La Metodología propuesta contribuyo para que todas personas que realizan trabajos relacionados con las evaluaciones de seguridad, realicen pruebas de penetración de manera planificada y obtengan resultados confiables que beneficien a la organización.

- La Metodología propuesta contribuyo para que todas personas que realizan trabajos relacionados con las evaluaciones de seguridad, realicen pruebas de penetración de manera planificada y obtengan resultados confiables que beneficien a la organización

5.2 Recomendaciones

- Definir una herramienta de pruebas de penetración en base a la metodología propuesta, que permita identificar de manera oportuna los posibles puntos vulnerables que pueden poner en riesgo la información de la organización. Esto evitará sacrificar el desempeño o disponibilidad de los sistemas de información que sean parte de la prueba de penetración.

- Las personas encargadas de realizar pruebas de penetración deben contar con suficientes conocimientos legales, que permitirán alcanzar los objetivos trazados en base al cumplimiento de la ley.

- Una vez concluida las pruebas de penetración, es importante desarrollar una matriz en la que se describa todos los puntos críticos encontrados, de manera que ayuden eficiente y oportunamente al establecimiento de acciones que permitan precautelar la información de la organización.

5.3 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/