ANÁLISIS DE METODOLOGÍAS PARA PRUEBAS DE PENETRACIÓN MEDIANTE ETHICAL HACKING

ENNY ROCIO DIAZ BARRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROYECTO DE SEGURIDAD INFORMÁTICA II
YOPAL
2018

ANÁLISIS DE METODOLOGÍAS PARA PRUEBAS DE PENETRACIÓN MEDIANTE ETHICAL HACKING

ENNY ROCIO DIAZ BARRERA

Monografía elaborada como requisito de grado para optar el título de Especialista en Seguridad Informática

Director de Tesis
Ing. Martin Camilo Cancelado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROYECTO DE SEGURIDAD INFORMÁTICA II
YOPAL
2018

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

El proyecto de grado corresponde en decir el nivel de conocimiento sobre las metodologías de Ethical Hacking y en la posición se encuentra actualmente en el mundo digital. Decir las principales diferencias entre una y otra metodologías. Y Dado con el creciente número de ciber ataques, la filtración y el uso indebido de la información mediados por falta de seguridad de la red y equipos. En la actualidad el nivel de seguridad para los sistemas informáticos empresariales y personales ha convertido en un tema de gran importancia pero que por desconocimiento o falta de los recursos se deja a un lado o se resta importancia. Todo esto ha motivado a que los Hacker Éticos se coloquen en la tarea de desarrollar metodologías, guiones o Scripts novedosos, para así poder prevenir de los posibles ataques, pérdidas o sustracción de información privada. Entre las funciones de los Hacker éticos están la solución de las vulnerabilidades, mejorar procesos de seguridad y concientizar a los empresarios y demás usuarios, sobre la importancia de la implementación de un buen sistema de seguridad informática[1].

La demanda de tecnologías y procedimientos novedosos para administrar los sistemas de seguridad y almacenamiento, promovió el nacimiento de las pruebas de penetración, uno de los objetivos de estas pruebas es la identificación de vulnerabilidades de seguridad, mediante el uso de técnicas y herramientas

[1] **Reporte Digital. Seguridad y Hacking para beneficiar un negocio.** . [En línea]. https://reportedigital.com/negocios/tecnologia/seguridad-y-hacking/ .

específicas[2]. En este trabajo va a explicar las principales metodologías, mediante comparaciones, y análisis de ventajas y desventajas.

La estructura de cómo se va a dar desarrollo a cada una de los objetivos específicos propuestos, será dada por secciones, donde la primera se ira por un recorrido por los diferentes marcos como son el teórico, conceptual y legal; seguidamente se encuentra el diseño metodológico en el cual se describe los pasos a seguir a fin de recopilar la información más relevante.

[2] *Anonimo*. Pruebas de penetración y hacking ético. [En línea]. https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

1. TITULO

ANÁLISIS DE METODOLOGÍAS PARA PRUEBAS DE PENETRACIÓN MEDIANTE ETHICAL HACKING

2. DEFINICION DEL PROBLEMA

Al día de hoy, el funcionamiento de las sociedades humanas se basa en los sistemas informáticos, no solo en las instancias públicas o privadas sino también en el sector comercial, como también en lo que actualmente grandes conjuntos de datos que se componen con datos cotidianos de la población, lo que compramos o decimos, y que luego según resultados de análisis, se establecen perfiles para ofrecer los productos o servicios, de una forma personalizada.

La civilización se mueve a través de la información y el almacenamiento de la misma. Si los niveles de seguridad no son adecuados, la vulnerabilidad se aumenta y con ello los riesgos a un robo de datos, o cualquier ataque que realice un hacker con fines de manipular o destruir la información. Las razones para efectuar un ataque son diversas y se pueden asociar a un juego, un experimento para demostrar sus conocimientos, o un hacker que tiene los objetivos claros de robar información valiosa como contraseñas, cuentas bancarias, vulnerar la seguridad o esparcir un virus.

Aplicando las similares herramientas de ataque utilizadas por un hacker o Cracker se pueden realizar las prevenciones y protecciones a los sistemas informáticos.

Las amenazas sobre los sistemas informáticos basadas en usurpar la personalidad de usuarios autorizados para acceder y manipular indebidamente los datos de las empresas han llevado a que el tratamiento la seguridad informática sea

preponderante.[3] Todo lo anterior se puede prevenir y minimizar fortaleciendo el conocimiento sobre el Ethical Hacking y las herramientas que lo constituyen.

Para la presente investigación se tiene como orientación la siguiente pregunta: ¿Cómo el análisis de las principales metodologías de Ethical Hacking, permite a las personas y/o empresas identificar los mejores procedimientos para evaluar deficiencias en los sistemas de seguridad?

[3] FLOREZ, Rojas. Metodología para realizar Hacking Ético en bases de datos para para Positiva Compañía de Seguros S.A en la ciudad de Bogotá. Bogotá. 2017. 70p. Proyecto de Grado (Especialización en Seguridad Informática. Universidad Abierta y a Distancia. Escuela de Ciencias Básicas e Ingeniería. Especialización en Seguridad Informática.

3. JUSTIFICACIÓN

Dado que en los últimos años se han incrementado los ataques a los distintos tipos de empresas y/o organizaciones, a la vez que han evolucionado las técnicas de los atacantes para cometer delitos informáticos; surge la necesidad de evolucionar las formas de proteger los sistemas informáticos. Para el estudio comparativo, se toma como referencia las etapas que conforman el Ethical Hacking, en el cual se determinan las semejanzas y diferencias de las herramientas que sirven para hacer pruebas de penetración. En algunos países la inversión para tener una mejor seguridad informática ha crecido de forma acelerada, en otros el paso ha sido más lento; pero en última instancia hemos convergido todos en un mundo digital en el que la información es el activo intangible más valioso con el que contamos. Una de las maneras más recomendables es tomar medidas preventivas y predictivas usando las diferentes herramientas que el Ethical Hacking ofrece, permitiendo observar las falencias de las instalaciones.

Uno de los caminos es a través de las pruebas de penetración, que hacen uso de las técnicas utilizadas por los mismos atacantes para cometer sus delitos. Las pruebas de penetración nos ayudan a valorar los controles de protección, mostrar los puntos débiles que a simple vista no son evidentes. El rol del hacker ético es efectuar desde el punto de vista de un cracker un ataque controlado hacia la infraestructura informática de un cliente, detectando vulnerabilidades potenciales y explotando aquellas que le permitan penetrar las defensas de la red objetivo, pero sin poner en riesgo los servicios y sistemas auditados. Y todo esto con el solo propósito de alertar a la organización contratante de los riesgos de seguridad

informática presentes y cómo remediarlos.[4]

El proceso de Hacking ético no contempla solucionar todas las vulnerabilidades descubiertas por lo tanto su compromiso será solucionar las vulnerabilidades de riesgo “Alto", dejando a consideración del cliente la opción de aceptar el riesgo en vez de mitigarlo, y que el cliente decida el tratamiento que dará sobre las de otros impacto (Medio, Bajo), acorde con los propósitos de su negocio[5]

[4] *Anónimo*, Hacking etico101: Como hacer profesionalmente en 21 días o menos. [En línea]. Biblia del programador, 2017. [Citado 26-mayo-2018]. Disponible en internet: https://www.bibliadelprogramador.com/2017/06/hacking-etico-101-como-hackear.html

[5] Flores Rojano, J. A. (01 de Noviembre de 2018). METODOLOGÍA PARA REALIZAR HACKING ÉTICO EN BASES DE DATOS PARA POSITIVA COMPAÑÍA DE SEGUROS S.A EN LA CIUDAD DE BOGOTÁ. Bogota, Colombia.

4. OBJETIVOS

4.1 GENERAL

Analizar las principales metodologías de pruebas de penetración mediante Ethical Hacking.

4.2 ESPECIFICOS

- Consultar la funcionalidad de las principales metodologías de Ethical Hacking.
- Comparar fortalezas y debilidades de las metodologías.
- Analizar la forma y entorno de aplicación de las metodologías
- Presentar un documento que plantee el uso de cada una de las metodologías con el uso de Ethical Hacking.

5. MARCO REFERENCIAL

5.1 MARCO TEORICO

La seguridad informática, como las demás áreas, se basa en la minimización de riesgos con referencia a accesos o el mal uso de la información, por eso es bueno tener una gestión de riesgos, donde se valora y se cuantifica los datos, los equipos y software dentro de una organización, donde se usen implementación de medidas preventivas como políticas de seguridad que protejan contra un ataque de reemplazo, modificación o alteración de los datos almacenados.

Para hablar de hacking ético se hace necesario referirse a las herramientas de prevención y protección de datos. En Colombia se emitió un decreto (decreto 1377 de 2013[6]) que reglamenta parcialmente la ley de protección de datos (Habeas Data), donde la persona que acceda a información persona o de gran interés de uno, será multado desde 2000 salarios mínimo legales vigentes, Según la Superintendencia de Industria y Comercio, el derecho de protección de datos es aquel que tiene toda persona de conocer, actualizar y rectificar la información que haya sido recogido sobre ella en archivos y bases de datos de naturaleza pública o privada[7].

[6] Ministerio de comercio, Industria y Turismo. [En línea]. MinTIC, s.f, [Citado 26-mayo-2018]. Disponible en internet: http://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

[7] El Pais, Colprensa. Lo que tiene que sobre sobre la nueva ley de protección de datos. [En línea]. El Pais, 2013. [Citado 26-mayo-2018]. Disponible en internet: http://www.elpais.com.co/colombia/lo-que-tiene-que-saber-sobre-la-nueva-ley-de-proteccion-de-datos.html

Lo que se pretende es estar adelante de quienes intentan agredir a una organización haciendo pruebas y ataques propios con la ayuda de expertos informáticos y con el uso de diferentes técnicas de ataque digital. El hacking ético es la utilización de los conocimientos de seguridad en informática para realizar pruebas en sistemas, redes o dispositivos electrónicos, buscando vulnerabilidades que explotar, con el fin de reportarlas para tomar medidas sin poner en riesgo el sistema. Una técnica de seguridad es el cifrado de datos, que sirven para proteger datos confidenciales que se transmiten por satélite o por algún otro tipo de red de comunicaciones. El cifrado puede proveer protección adicional a secciones confidenciales de una base de datos. Los datos se codifican mediante algún algoritmo de codificación. Un usuario no autorizado que tenga acceso a los datos codificados tendrá problemas para descifrarlos, pero un usuario autorizado contara con algoritmos (o claves) de codificación o descifrado para interpretarlos[8].

Las pruebas de penetración son un método de encontrar brechas en la seguridad de la red. Los hackers éticos certificados u otros especialistas de seguridad de la información realizan pruebas de penetración, generalmente fuera de la red, aunque a veces también dentro de ésta. Las pruebas de penetración externa a menudo se realizan a ciegas, sin conocimiento de las medidas y del monitoreo de seguridad de red. Si la prueba de penetración externa infringe la red, esto también proporciona una idea de qué tan efectivas y eficientes son las medidas de seguridad en el caso de un incumplimiento.

Por lo general las pruebas internas de penetración incluyen el conocimiento de las medidas de seguridad interna, los evaluadores pueden tratar de violar la red de computadoras de empleados o utilizar otros métodos para evaluar las posibles

[8] ESCOBAR, Javier; RAMIREZ, Luis; ASPRINO, Omar. Integridad y Seguridad en los Sistemas de Bases de Datos. [En linea]. FACYT, s.f. [Citado 01-Noviembre-2018]. Disponible en internet: http://eduteka.icesi.edu.co/gp/upload/1275d0253997d62e90e9a7f6a5f107cc.pdf

brechas en la seguridad interna. También aquellos que monitorean la red deberían ser probados para evaluar sus respuestas a dicha violación de seguridad.[9]

Hay empresas que dedican gran parte de sus recursos a Investigación y Desarrollo. Tal es el caso de Hewlett Packard con su HP DVLabs[10], donde los expertos en vulnerabilidades y los desarrolladores aplican ingeniería inversa de vanguardia y técnicas de análisis para crear una amplia protección de amenazas para las redes de clientes. Los expertos en investigación de seguridad contra la vulnerabilidad controlan la actividad global de Internet, analizan las nuevas formas de ataque, detectan las vulnerabilidades al instante y crean filtros para prevención de intrusos (IPS) que se entregan de forma automática a los clientes de HP TippingPoint NGIPS para que tengan protección en tiempo real de la información que entra a la empresa.[11]

El método de Ethical Hacking es un término nuevo que nació a partir de las comunidades que están relacionadas con el uso del internet o todo lo que tenga que ver con los espacios virtuales que es desde el 1990. Actualmente la mayoría de la información se guarda en dispositivos de almacenamiento y en redes de datos, con los avances tecnológicos, es estos últimos años se ha empezado a utilizar con fuerza la nube que se encuentra sujeta a riesgos e inseguridades ya sean internas y externas a las organizaciones. Es por esto que muchas empresas tanto públicas como privadas han decido priorizar la protección de su información, sin embargo, los presupuestos asignados a esta gestión son limitados, por esta razón es necesario mantener implementados controles de seguridad para afrontar los riesgos

[9] Maggio, S. Actividades de monitoreo de seguridad interna y externa. [En linea]. Techlandia, s.f. [Citado 25-mayo-2018]. Disponible en internet: https://techlandia.com/actividades-monitoreo-seguridad-interna-externa-info_194844/

[10] Colaboradores Enter.co. El hacking Etico y su importancia para las empresas. [En Linea]. Enter.co, 2014. [Citado 25-mayo-2018]. Disponible en internet: http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/

[11] *Anonimo*, Hacking Etico. [En linea]. Corporacion Unificada Nacional de Educacion Superior, s.f. [Citado 26-mayo-2018]. Disponible en internet. https://auditoria2017.wordpress.com/hacking-etico/

a que está sometida la información en forma continua y no hacer inversiones grandes cuando ya se enfrenta a ataques informáticos.

La infraestructura tecnológica de una organización puede ser probada, analizada, y atacada en varias maneras, algunos de los más comunes modos de hacking ético son[12]:

Ataque Local
Ataque remoto
Ataques con equipos robado
Ataques a entradas físicas de la organización
Ataques por medio de equipos sin autenticación
Ataques con ingeniería social.

Un profesional de Hacker Etico, es un profesional de seguridad el cual debe conocer y tener en cuenta las sanciones legales a las que puede ser sometido y que son parte de las consecuencias de realizar las pruebas sin autorización. Es por esto que las actividades de hacking ético, análisis de vulnerabilidades, pruebas de penetración o auditorias de seguridad deben comenzar a realizarse una vez que se tenga un documento de autorización firmado por la Organización, el cual da permiso expreso al hacker a realizar este tipo de pruebas de red.[13]

La ciberdelincuencia es uno de los ambientes delictivos con más rápido crecimiento, debido a las facilidades de las nuevas tecnologías. Los ataques en contra de sistemas o redes de la información, como robo o adulteración de datos, estafas

[12] Escuela Politécnica Nacional. Utilización de Hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones. Alexander Verdesoto, 2007. [Citado 25-mayo-2018]. Disponible en internet. http://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD-1053.pdf

[13] MENDAÑO, Luis. Implementación de técnicas de hacking ético para el descubrimiento y evaluacion de vulnerabilidades de la red de una cartera de estado. Quito, 2016. 246p. Trabajo de Grado (Ingeniero en Electronica y Telecomunicaciones). Escuela Politecnica Nacional. Facultad de ingenieria electrica y electronica.

bancarias y comerciales, rodo de identidades, etc. Son parte de las actividades delictivas utilizando medios informáticos y a la vez diferentes técnicas como ingeniería social, malware avanzado con técnicas de ofuscación, inyección de código SQL, chantaje o ransomware, etc.[14]

Los estados miembros del consejo de Europa, convencidos de la necesidad de aplicar, con carácter frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional, preocupados por el riesgos de que las redes informáticas y la información electrónica sean utilizados igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenados y trasmitidas por medio de dichas redes, crean un convenio para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad delos sistemas, redes y datos informáticos, dicho convenio se llama Convenio de Budapest o convenio sobre la ciberdelincuencia.[15]

5.2 MARCO CONCEPTUAL

5.2.1 Hacking Ético: es un individuo en el que se confía para tratar de penetrar en las redes y / o sistemas informáticos de una organización utilizando los mismos conocimientos y herramientas que un pirata informático malintencionado, pero de una manera legal y legítima.[16]

5.2.2 Pruebas de penetración: se refieren a la explotación de un sistema de TI

[14] MENDAÑO, Luis. Implementación de técnicas de hacking ético para el descubrimiento y evaluacion de vulnerabilidades de la red de una cartera de estado. Quito, 2016. 246p. Trabajo de Grado (Ingeniero en Electronica y Telecomunicaciones). Escuela Politecnica Nacional. Facultad de ingenieria electrica y electronica.

[15] Council Of Europe. Convenio sobre la ciberdelicuencia. [En Linea]. OAS, 2001. [Citado 26-mayo-2018]. Disponible en Internet: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

[16] Escuela Politécnica Nacional. Utilización de Hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones. Alexander Verdesoto,

con el permiso de su propietario para determinar sus vulnerabilidades y debilidades. Es un proceso de prueba y validación de la postura y madurez de seguridad de la información de una organización. Los resultados de la piratería ética generalmente se utilizan para recomendar medidas preventivas y correctivas que mitiguen el riesgo de un ciberataque.[17]

5.2.3 Script: son pequeños programas que no son compilados, es decir, por lo general necesitan de un programa lector o interprete que codifique la información del script y lo lleve a lenguaje de máquina, para que la información sea procesada y ejecutada por el ordenador, son muy utilizados para interactuar con el sistema operativo del ordenador, de manera automatizada.[18]

5.2.4 Seguridad Informática: consiste en asegurar en que los recursos del sistema de información de una organización se utilizan de la manera que se decidió y que el acceso a la información allí contenida así como su modificación solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.[19]

5.2.5 Vulnerabilidad: es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.[20]

5.2.6 OSSTMM: Es uno de los estándares profesionales más complejos y comúnmente utilizados en Auditorias de seguridad para revisar la seguridad de los sistemas desde internet[21].

5.2.7 Auditoria en Sistemas de Información: Es definida como cualquier auditoria que abarque la revisión y evaluación de todos los aspectos de

[17] **No hay ninguna fuente en el documento actual.**
[18] *Anonimo*.Que son los Script. [En Línea]. **No hay ninguna fuente en el documento actual.**
[19] *Anonimo*. Seguridad informatica. [En línea]. **No hay ninguna fuente en el documento actual.**
[20] **No hay ninguna fuente en el documento actual.**
[21] **No hay ninguna fuente en el documento actual.**

los sistemas automáticos de procesamiento de la información.[22]

5.2.8 Nmap: Es una aplicación multiplataforma usada para explorar redes uy obtener información acerca de los servicios, sistemas operativos y vulnerabilidades derivadas de la conjunción de estos.[23]

5.2.9 Exploits: Son una vía ya definida para romper la seguridad de un sistema aprovechando una vulnerabilidad. Un exploit se refiere a una parte del software, herramienta o técnica que se vale de una vulnerabilidad para poder obtener privilegios dentro de un sistema atacado.[24]

5.2.10 Metasploit: Utiliza gran cantidad de datos para ejecución de los ataques porque almacena en el sistema operativo todos los exploit conocidos hasta la fecha, por lo tanto, Metasploit para gestionar todos los exploits, módulos y auxiliares utiliza una base de datos en postgressql. [25]

5.2.11 Crackers: Puede considerarse como un subgrupo marginal de la comunidad de hackers, se dedican a violar la seguridad de un sistema informático de forma similar como lo haría un hacker, con la diferencia que realizan l intrusión con fines de beneficio personal o explícitamente para causar daño[26]

5.2.12 Objetivo de Evaluación: Un sistema tecnológico, producto, o componente que está identificado o sujeto a requerimientos o evaluaciones de

[22] **No hay ninguna fuente en el documento actual.**

[23] Seguridad Informática. ¿Qué es Nmap?. [En línea]. Seguridad Informatica, 2007. [Citado 25-Mayo-2018]. Disponible en Internet: https://seguinfo.wordpress.com/2007/06/27/¿que-es-nmap/

[24] *Alexander Verdesoto*. Utilización de Hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones. Escuela Politécnica Nacional, 2007. [Citado 25-mayo-2018]. Disponible en internet. http://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD-1053.pdf

[25] *Braulio Fernando Ortiz*. ¿Hacking Ético para detectar fallas en la seguridad informática en la intranet del gobierno provincial de Imbabura e implementar un sistema de gestión de seguridad de la información (SGCI), basado en la Norma ISO/IEC 27001:2005. Universidad Técnica del Norte, 2005. [En línea]. 2015. [Citado 25-mayo-2018]. Disponible en Internet:
http://repositorio.utn.edu.ec/bitstream/123456789/4332/1/04%20RED%20045%20TESIS.pdf

[26] *Alexander Verdesoto*. Utilización de Hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones. Escuela Politécnica Nacional, 2007. [Citado 25-mayo-2018]. Disponible en internet. http://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD-1053.pdf

seguridad. [27]

5.2.13 Magerit: El análisis de riesgos bajo las directrices de la metodología Magerit proporciona al usuario la herramienta completa, en una estructura sistemática en la que ofrece todo lo necesario para analizar los riesgos derivados del uso de las tecnologías de información y comunicación con el objetivo de descubrir cuáles son los riesgos a los que están expuestos.[28]

5.2.14 Ataque local: Se simula a un empleado o a otra persona autorizada la cual tiene una conexión legítima y autorizada a la red de la organización.[29]

5.2.15 Ataque Remoto. Se busca simular a un intruso tratando atacar al sistema por medio del internet[30]

5.2.16 Habeas Data: Es el derecho fundamental que tiene toda persona para conocer, actualizar y rectificar toda aquella información que se relacione con ella y que se recopile o almacene en bancos de datos.[31]

5.2.17 Penetración de Vulnerabilidades: Es realizado por los hackers éticos en donde intenta entrar a los sistemas burlando los mecanismos de control de acceso. Es donde, se prueban muchas de las amenazas identificados en la "evaluación de vulnerabilidades" para poder conocer el verdadero

[27] *Alexander Verdesoto*. Utilización de Hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones. Escuela Politécnica Nacional, 2007. [Citado 25-mayo-2018]. Disponible en internet. http://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD-1053.pdf

[28] *Braulio Fernando Ortiz.* ¿Hacking Ético para detectar fallas en la seguridad informática en la intranet del gobierno provincial de Imbabura e implementar un sistema de gestión de seguridad de la información (SGCI), basado en la Norma ISO/IEC 27001:2005. Universidad Técnica del Norte, 2005. [En línea]. 2015. [Citado 25-mayo-2018]. Disponible en Internet:
http://repositorio.utn.edu.ec/bitstream/123456789/4332/1/04%20RED%20045%20TESIS.pdf

[29]*Alexander Verdesoto*. Utilización de Hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones. Escuela Politécnica Nacional, 2007. [Citado 25-mayo-2018]. Disponible en internet. http://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD-1053.pdf

[30] *Alexander Verdesoto*. Utilización de Hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones. Escuela Politécnica Nacional, 2007. [Citado 25-mayo-2018]. Disponible en internet. http://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD-1053.pdf

[31] *Admin*. Educación Financiera. [En línea]. Coltefinanciera, s.f. [Citado 26-mayo-2018]. Disponible en internet: https://www.coltefinanciera.com.co/educacion-financiera/habeas-data

riesgo.[32]

5.3 MARCO LEGAL

La ley en Colombia en general es considerada una burla al pueblo y a la democracia, si los delitos son cometidos por personas del pueblo se aplica la mayor pena, pero si son realizados por gente de poder, la ley prácticamente no existe. La legislación en materia informática presenta muchos vacíos y no hay integración de las diferentes partes que la componen como son la penal, comercial, administrativo, entre otros; se evidencian casos donde ciertos tipos de personas reciben el "castigo", mientras que las personas detrás de toda la operación están libres continuando con su vida normal.

La legislación debe contemplar un castigo real, tanto para quien lo realiza como para quien lo induce o lo contrata, de igual forma. Es allí donde la legislación colombiana se debe plantear el comenzar por realizar un compendio de toda la normatividad, evitando los vacíos legales.

La problemática en Colombia es aún más grande, la incapacidad para tener presos (falta de cárceles), la existencia de un sistema penitenciario débil (formación, sueldos, educación, etc.) y la normatividad permisible, hacen que la aplicación de la ley sea muy difícil

Los delitos informáticos nacieron con la creación del computador y cada día son más frecuentes y destructivos; los daños causados se pueden medir en todos los aspectos, desde el psicológico hasta el monetario, en algunos casos hasta conducen al suicidio; pero lo más grave es que pueden ser realizados por personas de cualquier edad, y desde cualquier parte del mundo; a continuación, se presenta

[32] HERNANDEZ, Lirida. Hacking Etico para Dispositivos Móviles Inteligentes. Monterrey, 2012, 227p. Trabajo de Grado (Maestro en Ciencias en Tecnologías de Información). Instituto Tecnológico y de Estudios Superiores de Monterrey. Programa de Graduados de la Escuela de Ingeniería y Tecnología de Información.

un cuadro con algunos de estos delitos que están causando estragos en el mundo entero

La siguiente tabla que se mostrara, se nombrara algunos de los delitos informáticos que están causando problemas a nivel global y algunos del tiempo/multa que tendría que pagar en Colombia por cada delito que se cometa:

N°	Delito	Descripción	Pena
1	Sabotaje Informático	Dañar o destruir o modificar información de carácter electrónico (virus, gusanos, bombas lógicas, bombas cronológicas). Según los datos de la fiscalía, estos delitos alcanzaron la cifra de 143 casos registrados. No obstante, otras fuentes apuntan que podrían haberse dado muchos más casos.[33]	
2	Suplantación de Identidad[34]	También llamado delito de usurpación de estado civil o de identidad consiste en la acción apropiarse una persona de la identidad de otra, haciéndose pasar por ella para acceder a recursos y beneficios, actuando en el tráfico jurídico simulando ser la persona suplantada. Con este delito se trata de proteger la fe pública de la comunidad o la confianza en	6 meses a 3 años de prisión

[33] *Victor S. Manzhirova*. Los ocho delitos informáticos más comunes. [En Línea]. Tu Experto.com, 2015. [Citado 1-noviembre-2018]. Disponible en internet. https://www.tuexperto.com/2015/09/12/los-ocho-delitos-informaticos-mas-comunes/

[34] *Anonimo*.La usurpación de identidad. [En Línea]. LEGALITAS, 2015. [Citado 1-noviembre-2018]. Disponible en internet: https://www.legalitas.com/pymes-autonomos/actualidad/articulos-juridicos/contenidos/La-usurpacion-de-identidad

		la identificación de las personas. Por ello la jurisprudencia entiende que no es suficiente suplantar una identidad ficticia. Para poder cometer este delito el autor tiene que usurpar la identidad de una persona real, resultando impune la acción en el caso de que el culpable decidiera inventarse un personaje ficticio y hacerse pasar por él –suplantación de identidad-. Pensemos por ejemplo en quien faltando a la verdad se inventa un perfil ficticio crea un personaje y se hace pasar por él: la acción no tendría ninguna relevancia penal y resultaría impune.	
3	Piratería	Creación y distribución de copias de productos originales, sean libros, películas, canciones y entre otras.	
4	Pornografía Infantil	Actos con menores de edad, creación de videos haciendo actos sexuales. La Interpol, el FBI y autoridades en países latinoamericanos, especialmente en Argentina, Colombia, Brasil, Chile y Venezuela, realizan más esfuerzos para controlar el problema. Más de 280.000 casos al año de utilización de niños para pornografía en Internet, prostitución infantil, abuso sexual, venta de niños, práctica difundida y continuada del turismo sexual, se reportan solamente en Estados	

		Unidos, pero el número de casos no reportados es aún mayor si se tiene en cuenta el número de niñas y niños latinoamericanos utilizados para este aberrante delito.[35]	
5	Interceptación ilícita de datos informáticos[36]	Obstruyen datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático.	Prisión de 36 a 72 meses de vigencia
6	Violación de datos personales[37]	Sin estar facultado sustrae, vende, envía, compra, divulga o emplea datos personales almacenados en medios magnéticos	Prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos vigentes legales.
7	Daños Informáticos[38]	Cuando una persona que sin estar autorizada, modifica, daña, altera, borra, destruye o suprime datos del programa o documentos electrónicos y se hace en los recursos de TIC.	Prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos vigentes legales.

[35] *Munevar John*.Los Niños del Sexo! Pornografia Infantil en Internet. [En línea]. Semana. ,2002. [Citado 1-Noviembre-2018]. Disponible en Internet: https://www.semana.com/vida-moderna/articulo/los-ninos-del-sexo-pornografia-infantil-internet/50667-3

[36] *Murillo Garzon Yeimy Camila*. Delitos Informaticos y Entorno Juridico Vigente en Colombia. [En línea]. camaleo,sf. [Citado 1-Noviembre-2018]. Disponible en Internet: https://es.calameo.com/read/005340712f89c4b6bc86d

[37]*Murillo Garzon Yeimy Camila*. Delitos Informaticos y Entorno Juridico Vigente en Colombia. [En línea]. camaleo,sf. [Citado 1-Noviembre-2018]. Disponible en Internet: https://es.calameo.com/read/005340712f89c4b6bc86d

[38] *Murillo Garzon Yeimy Camila*. Delitos Informaticos y Entorno Juridico Vigente en Colombia. [En línea]. camaleo,sf. [Citado 1-Noviembre-2018]. Disponible en Internet: https://es.calameo.com/read/005340712f89c4b6bc86d

8	Xenofobia	Acciones de rechazo hacia un grupo de personas en particular a través de páginas, redes sociales y demás sitios en internet.	
9	Falsificación o Phising	Phishing es un ciberdelito por el que los ciberdelincuentes intentan conocer los datos confidenciales de cualquier usuario de internet, principalmente datos de acceso a diferentes servicios así como números de tarjetas de crédito o cuentas bancarias con el objetivo principal de robar dinero o conseguir datos bancarios con los que efectuar un fraude, es decir, compras a nuestro nombre. Su modus operandi es mediante el envío de un correo electrónico que nos reconduce a sitios web falsos construidos a imagen y semejanza de los auténticos. Por ello resulta tan importante no pulsar enlaces de correo que no conocemos, ni de ofertas increíbles.[39]	
10	Spam	El spam o correo basura se envía también junto con un enlace web o propuesta de negocio. Al hacer clic en este enlace o en respuesta a la propuesta de negocios, podemos ser objeto de phishing o instalar un malware en nuestro ordenador que proporcione nuestros datos	

[39] *J.Alfocea*. Ciberdelitos: Robo de identidad, Phishing y Spamming. [En línea].Delitos Informaticos.com, 2015. [Citado 1-Noviembre-2018]. Disponible en Internet: https://delitosinformaticos.com/04/2015/delitos/ciberdelitos-robo-identidad-phishing-spamming

		personales, bancarios, etcétera a los ciberdelincuentes. Una variedad de spam es el bombardeo de correo electrónico consistente en enviar grandes cantidades de correos electrónicos a la dirección de destino lo que provoca la caída de la dirección de correo electrónico o del servidor de correo.[40]	
11	Acceso Abusivo a un sistema informático[41]	Aprovechan la vulnerabilidad en el acceso a los sistemas de información o debilidades en los procedimientos de seguridad	Prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos vigentes legales.

Tabla1: Delitos informáticos

5.3.1 Acciones a nivel global.

Se ha visto que la importancia del termino Delito Informático ha hecho que las diferentes naciones estén adoptando este término en sus respectivas legislaciones un método para regular esta problemática que incrementa.

Las grandes potencias como Estados Unidos, Rusia, España, son reconocidos por tener grandes niveles de seguridad, pero aun así se le han podido infiltrar en sus

[40] *J.Alfocea*. Ciberdelitos: Robo de identidad, Phishing y Spamming. [En línea].Delitos Informaticos.com, 2015. [Citado 1-Noviembre-2018]. Disponible en Internet: https://delitosinformaticos.com/04/2015/delitos/ciberdelitos-robo-identidad-phishing-spamming

[41] *Murillo Garzon Yeimy Camila*. Delitos Informaticos y Entorno Juridico Vigente en Colombia. [En línea]. camaleo,sf. [Citado 1-Noviembre-2018]. Disponible en Internet: https://es.calameo.com/read/005340712f89c4b6bc86d

sistemas; se están empezando a destacar los esfuerzos generados por los países de México, Uruguay, chile y Colombia (COLCERT).

España fue uno de los países pioneros a nivel global en la implementación de marco normativos sobre el tratamiento de la información, creando en el año de 1994, la ley que trata sobre la firma digital, establecida en el Acta Federal de Abuso Computacional. Además los delitos informáticos y las sanciones para regular y contrarrestar, están escritas en la Ley Orgánica 10/1995, donde establece penas privativas de la libertad, en el 2007 el tribunal supremo español, para hacer frente a la estafa electrónica confirmo el tratamiento penitenciario[42].

En México se estableció la penalización para conductas que estén asociadas con revelación de secretos, acceso ilícito a sistemas y equipos de información, que son sancionables con castigadas con la cárcel y con altas multas[43]. En dicho país también se castiga la reproducción no autorizada de programas informáticos, según la Ley Federal del Derecho de Autor[44].

En Chile al ver el gran incremento de ataques informáticos, comenzó a crear una ley para contrarrestar dichos ataques/delitos, y es la Ley 19.223, que su aplicación comenzó en el año 1993 y que se refiere a la normatividad para sancionar los delitos informáticos. En dicha Ley se dice que se castigara con cárcel y sanciones pecuniarias a quienes llegue alterar o ir en contra de la pureza, idoneidad y calidad de la información[45].

En Uruguay se sanciono la primera ley en contra de los delitos informáticos en el año 2007, creando la ley 18.237, que fue categorizada como expediente electrónico, donde se define una amplia terminología en cuanto a procesos realizados a través

[42] ZAPATERO, Luis. Código de derecho Penal Europeo e Internacional, 2008
[43] Código Penal Federal, Articulo 167, Interrupción a comunicaciones alambicas, 2001
[44] Ley Federal del Derecho de Autor, Titulo IV, Capítulo IV, 2000.
[45] Ley 19.223 Delitos Informáticos, 1993.

de la red, por medio de dispositivos electrónicos, entendidos como firma electrónica, documento electrónico y trámites judiciales llevados a cabo en procesos judiciales[46].

5.3.2 Acciones en Colombia.[47]

En Colombia se considera un delito informático cuando una persona se apropia ilegalmente de información confidencial almacenada en un computador, en un correo electrónico, en un dispositivo móvil o USB. Incurrir en este delito puede generar una penalización que está amparada en Colombia desde el año 2009 bajo la Ley 1273, denominada "de la protección de la información y de los datos".

Hoy en día es sumamente importante estar informado sobre las acciones que se consideran delito informático, a continuación respondemos algunas de las interrogantes más comunes respecto al funcionamiento de esta ley en Colombia.

- *¿Qué se considera un delito informático?*

Es el acto de robar información y datos personales que están resguardados o contenidos en un medio electrónico.

- *¿Existe diferencia entre un delito informático y un delito clásico que sea realizado a través de medios electrónicos?*

La principal diferencia existente es que el delito informático vulnera la información y el dato privado de otra persona, mientras que el delito clásico informático es el ilícito realizado a través de medios electrónicos.

[46] Ley 18.237, Expediente Electrónico, 2007.
[47] *Anónimo*. Acciones que son consideradas un delito informático en Colombia. [En línea].Tus Abogados y Contadores, 2018. [Citado 1-Noviembre-2018]. Disponible en Internet: https://tusabogadosycontadores.co/blog/acciones-que-son-consideradas-un-delito-informatico-en-colombia/

- *¿Se considera un delito informático una amenaza hecha vía e-mail?*

Este hecho no se considera un delito informático, sin embargo en caso de que se solicite cualquier cantidad de dinero esto sería extorsión a través de medios electrónicos, aunque aun así no se considera delito informático. Este caso se considera una extorsión clásica, es como si la misma amenaza se hiciera por medio de una nota, una llamada, o cualquier otro medio.

- *¿Ingresar al computador personal de una persona y extraer información sin su permiso puede considerarse delito informático?*

Sí, efectivamente esto es considerado en Colombia un delito informático y una violación de datos personales, acto penalizado en la Ley 1273 del año 2009.

- *¿Cuál es la pena mínima impuesta en Colombia para los delitos informáticos?*

En nuestro país, la pena mínima establecida es de cuatro años de cárcel. Pero además de ello, la ley establece que a quien se le impute este delito no tendrá la posibilidad de modificar la medida de aseguramiento, motivo por el cual no se tendrán beneficios como el de prisión domiciliaria.

- *¿Enviar correos electrónicos desde la cuenta de otras personas se considera un delito informático?*

Aunque este acto es un delito, no necesariamente se considera informático, para serlo deben ser usados los datos de la supuesta víctima, pero si solo se utiliza el correo electrónico sería un delito clásico mejor conocido como “violación de datos personales”.

- *¿Desconocer las normas puede exculpar a una persona de haber cometido un delito informático?*

Expertos consultados aseguran que ignorar la norma no excluye a una persona de de la responsabilidad sobre un posible delito informático. En este sentido el Estado colombiano presume que todos sus ciudadanos conocen las leyes, por lo que no se está exento de ser juzgado como un delincuente informático.

- *¿Revisar el correo electrónico o las redes sociales de un hijo menos de edad es un delito informático?*

En el caso específico de un menor de edad se puede considerar que no, ya que los padres de familia tienen la plena autorización por derecho para acceder a los perfiles y cuentas de correo de sus hijos, incluso esto es una buena práctica para controlar con quienes se contactan los menores.

- *¿Existen en Colombia sanciones económicas por el delito informático?*

Los delitos informáticos en Colombia tienen la sanción económica más altas del Código Penal de este país. La pena económica más baja está en 100 salarios mínimos mensuales legales vigentes, cerca de los 60 millones de pesos, mientras que la máxima puede alcanzar los 600 millones de pesos, cantidad que también depende del delito en el cual se haya incurrido.

- ¿Puede considerarse la piratería como un delito informático?

Aunque es un delito de violación a la propiedad intelectual, no puede definirse como un delito informático, a pesar de ser un ilícito que se consuma a través de medios electrónicos. En este caso no hay vulneración de la información, ya que lo que se protege son los derechos morales e intelectuales del autor.

En todo caso lo más importante es el pleno conocimiento de las leyes colombianas, las cuales ya determinan claramente lo que puede ser considerado como un delito informático o no, aunque en ocasiones el desconocimiento de algunos fiscales o

jueces, hace que delitos informáticos sean juzgados como delitos clásicos, ubicando al delito informático como una circunstancia de agravación que se usa para aumentar la pena.

6. DISEÑO METOLOGICO

El presente trabajo está enfocado hacia la modalidad de *Monografía,* a través del cual se "Le permite al estudiante el desarrollo de una investigación con base en la revisión de mesas documentales"[48].

6.1 Tipo De Investigación

La metodología para el desarrollo del este trabajo de grado, se basara en los planteamientos definidos en materia de la seguridad de la información y hacer un análisis en las diferentes metodologías de Ethical Hacking.

Principalmente se busca en el análisis de las diferentes metodologías que componen a la Ethical Hacking, y esto con el fin de encontrar las vulnerabilidades y

[48] *UNAD*. Obtenido de Alternativas para Grado-ECBTI. [En línea]. Universidad Abierta y a Distancia, s.f. [Citado 1-Noviembre-2018]. Disponible en Internet: https://academia.unad.edu.co/ecbti/oferta-academica/alternativas-para-grado

fortalezas de cada una de ellas, para que al final lleguemos a la creación de un informe de su aplicación.

6.2 Técnicas e Instrumentos de recolección de información

Para la realización de este trabajo, se utilizara todas las fuentes bibliográficas posibles (En todos los idiomas posibles, para tener una mejor investigación), relacionadas con los conceptos de Ethical Hacking, las metodologías, esto con el fin de establecer antecedentes y/o tener unas buenas bases en la investigación y así dar un buen desarrollo al trabajo propuesto.

Las técnicas que se utilizaran en la recolección de información elegida para el desarrollo, son: las encuestas, entrevista y por último la observación.

6.2.1 Entrevista: Por medio de preguntas adecuadas es posible socializar la temática con la que se está tratando o investigando y conocer los puntos de vista, hasta el nivel de conocimiento de las personas sobre la seguridad de la información, los hackers, o en si los conceptos básicos de Ethical Hacking.

6.2.2 Observación: Esta técnica permite entrar en contacto de forma directa a la problemática del poco conocimiento y las pocas formas de implementación en el nivel de la seguridad de la información.

7. ETHICAL HACKING

Escuchamos sobre piratería en las noticias todo el tiempo, desde Anonymous hasta noticias falsas, ataques de denegación de servicio y violaciones de datos, parece que los malos siempre están causando estragos. Y es verdad; los malos están haciendo todo tipo de daños, desde los molestos (spam) hasta los destructivos (ataques cibernéticos que roban datos personales, o algo peor)[49].

¿Quiénes son?

Un hacker ético (también conocido como hacker de sombrero blanco) es el mejor profesional de seguridad. Los hackers éticos saben cómo encontrar y explotar vulnerabilidades y debilidades en varios sistemas, como un hacker malicioso (o un hacker de sombrero negro). De hecho, ambos usan las mismas habilidades; sin embargo, un hacker ético utiliza esas habilidades de manera legítima y legal para tratar de encontrar vulnerabilidades y corregirlas antes de que los malos puedan llegar e intentar ingresar. El rol de un hacker ético es similar al de un probador de penetración, pero implica deberes más amplios. Se rompen en sistemas legal y éticamente. Esta es la principal diferencia entre los hackers éticos y los hackers reales: la legalidad[50].

¿Qué es?[51]

Aparte de las tareas de prueba, los hackers éticos están asociados con otras responsabilidades. La idea principal es replicar a un pirata informático malintencionado en el trabajo y, en lugar de explotar las vulnerabilidades con fines

[49] *Jayanthi Manikandan*. Who's an Ehical Hacking? [En línea]. Simplilearn, 10- Octubre- 2018. [Citado 1-Noviembre-2018]. Disponible en Internet: https://www.simplilearn.com/roles-of-ethical-hacker-article
[50] *Jayanthi Manikandan*. Who's an Ehical Hacking? [En línea]. Simplilearn, 10- Octubre- 2018. [Citado 1-Noviembre-2018]. Disponible en Internet: https://www.simplilearn.com/roles-of-ethical-hacker-article
[51] *Jayanthi Manikandan*. Who's an Ehical Hacking? [En línea]. Simplilearn, 10- Octubre- 2018. [Citado 1-Noviembre-2018]. Disponible en Internet: https://www.simplilearn.com/roles-of-ethical-hacker-article

maliciosos, buscar contramedidas para reforzar las defensas del sistema. Un hacker ético podría emplear todas o algunas de estas estrategias para penetrar en un sistema:

- Escanear puertos y buscar vulnerabilidades: un hacker ético utiliza herramientas de escaneo de puertos como Nmap o Nessus para escanear sus propios sistemas y encontrar puertos abiertos. Se pueden estudiar las vulnerabilidades con cada uno de los puertos y se pueden tomar medidas correctivas.

- Un hacker ético examinará las instalaciones de parches y se asegurará de que no puedan ser explotados.

- El hacker ético puede involucrarse en conceptos de ingeniería social como el buceo en basureros: hurgar en los contenedores de basura en busca de contraseñas, gráficos, notas adhesivas o cualquier cosa con información crucial que pueda usarse para generar un ataque.

- Un hacker ético también puede emplear otras técnicas de ingeniería social como navegar por los hombros para obtener acceso a información crucial o jugar la carta de bondad para engañar a los empleados para que se desprendan de sus contraseñas.

- Un hacker ético intentará evadir IDS (sistemas de detección de intrusos), IPS (sistemas de prevención de intrusos), honeypots y firewalls.

- Rastreando redes, evitando y descifrando el cifrado inalámbrico, y secuestrando servidores web y aplicaciones web.

- Los hackers éticos también pueden manejar problemas relacionados con el robo de computadoras portátiles y el fraude de empleados.

- Detectar qué tan bien reacciona la organización ante estas y otras tácticas ayuda a probar la solidez de la política de seguridad y la infraestructura de seguridad. Un hacker ético intenta los mismos tipos de ataques que un hacker malicioso intentaría, y luego ayuda a las organizaciones a fortalecer sus defensas.

7.1 Tipos de Tests de intrusión[52].

Las empresas que se dedican a realizar pruebas de penetración, luego de analizar las necesidades del cliente, las enfocan en las siguientes perspectivas:

- **Tests de intrusión con objetivo:** se busca las vulnerabilidades en componentes específicos de los sistemas informáticos que son de mayor importancia para la empresa.

- **Tests de intrusión sin objetivo:** a diferencia de la prueba de penetración con objetivo esta prueba examina la totalidad de los componentes en los sistemas informáticos presentes en la empresa.

[52] *Maiken Menendez Mendez*. Ethical hacking: Test de intrusion. Principales Metodologías. [En línea]. Monografías, *S.f.* [Citado 1-Noviembre-2018]. Disponible en Internet: https://www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethical-hacking-test-intrusion-metodologias.shtml

- **Tests de intrusión ciega:** se utiliza únicamente la información pública disponible sobre la empresa. Esta prueba de penetración trata de simular los ataques de un ente externo a la empresa.

- **Tests de intrusión informada:** se utiliza información privada, otorgada por la empresa, sobre sus sistemas informáticos. Esta prueba de penetración trata de simular ataques hechos por un ente interno a la empresa y con cierto grado de información privilegiada.

- **Tests de intrusión externa:** se realiza de manera externa a las instalaciones de la empresa. La motivación de esta prueba es evaluar los mecanismos perimetrales de seguridad informática de la empresa.

- **Tests de intrusión interna:** es realizada dentro de las instalaciones de la empresa con el motivo de probar las políticas y los mecanismos internos de seguridad de la empresa.

El resultado de este servicio le brinda al cliente un documento con una lista detallada de las vulnerabilidades encontradas y certificadas (eliminación de falsos positivos). Adicionalmente el documento provee una lista de recomendaciones a aplicar, sobre la cual los responsables de seguridad de la organización pueden apoyar su programa de control.

7.2 Ámbito de las pruebas[53].

[53] *Anonimo*. Test de Intrusion. [En línea].Internet Security Auditors ISecAuditors, *S.f*. [Citado 1-Noviembre-2018]. Disponible en Internet: https://www.isecauditors.com/test-de-intrusion

Para realizar estos ataques se utilizarán tanto técnicas como herramientas de hacking. Las herramientas utilizadas serán las mismas que las utilizadas en el mundo underground por los propios hackers para realizar los ataques, así como herramientas creadas por el equipo técnico de Internet Security Auditors para realizar los Test de Intrusión y elaboradas a partir de las pautas definidas en los estándares OSSTMM, ISSAF PTES.

1. **Análisis de la Información Pública:**

El éxito de una intrusión depende, en gran medida, del nivel de conocimiento que dispone el atacante sobre los sistemas objetivo. Es decir, cuanta más información, detallada y precisa disponga, mayor probabilidad de conseguir su propósito. Para ellos se realizarán análisis de las webs corporativas, metadatos, redes sociales, ofertas de trabajo, listas negras y reputación, foros y webs externas a la entidad. Y búsquedas en Internet de información relacionada con la entidad, marca o servicio entre otros datos:

- Análisis de webs corporativas.
- Análisis de metadatos.
- Análisis de redes sociales.
- Análisis de ofertas de trabajo.
- Análisis de listas negras y reputación.
- Análisis de foros y webs externas a la entidad.
- Análisis de otras fuentes de información.

2. **Análisis de Seguridad a Nivel de Red:**

El análisis de la red consiste en la recolección de datos y la obtención de información y políticas de control de los sistemas analizados, con el objetivo de obtener la máxima información acerca de los componentes hardware y software, así como sobre la disposición de todos estos elementos. Para realizar este análisis de la red se seguirán los siguientes pasos:

- Sondeo de red.
- Mapa de red.
- Escaneo de puertos.
- Identificación de servicios.
- Identificación de sistemas operativos.

3. **Análisis de Seguridad a Nivel de Sistemas**:

La detección de vulnerabilidades se realiza tanto de forma automática como de forma manual y, en ambos casos, se lleva a cabo una fase de validación de las vulnerabilidades identificadas para descartar falsos positivos.
Para realizar este análisis de los sistemas se ejecutan las siguientes actuaciones:

- Análisis de actualizaciones.
- Análisis de Configuraciones.
- Identificación de vulnerabilidades no publicadas.
- Análisis de sistemas de autenticación.

4. **Análisis de Seguridad a Nivel de Aplicaciones**:

El análisis a nivel de aplicación está limitado a aquellas aplicaciones accesibles desde Internet, y sigue la filosofía de caja negra. Es decir, no se dispone de

información privilegiada sobre la aplicación (como credenciales de autenticación) y no se incluye en el alcance el análisis del código fuente de la aplicación. El motivo de esta metodología de trabajo es la de simular la actuación real de un atacante que, a través de las aplicaciones auditadas y sin disponer de información sobre las mismas, intenta comprometer la seguridad de la aplicación:

- Inventario de aplicaciones.
- Análisis de la configuración en la infraestructura.
- Análisis de sistemas de autenticación.
- Análisis del esquema de autorización.
- Análisis de la gestión de sesiones.
- Análisis del mecanismo de validación de datos.

5. **Análisis de los Sistemas de Seguridad**:

En muchas ocasiones, estos dispositivos y herramientas pueden no encontrarse debidamente configurados y/o monitorizados, con lo que su efectividad puede verse reducida en gran medida. Entre estos sistemas de seguridad, se analizarán los siguientes:

- Análisis de Firewalls.
- Análisis de WAF (Web Application Firewall)
  - Detección e identificación del WAF.
  - Análisis del comportamiento del WAF frente a distintos ataques.
  - Evasión del WAF.
- Análisis de IDS / IPS.

- Análisis de Antivirus/ Antimalware.

Resultados

Informe

Se elabora un informe detallado donde se incluye:

- Resumen ejecutivo de alto nivel con la clasificación de los resultados.
- Detalle de todas las pruebas realizadas especificando su objetivo.
- Resultados obtenidos en los diferentes test que se han realizado con descripciones paso a paso del proceso de detección y explotación de cada vulnerabilidad.
- Recomendaciones que permitan solucionar de la forma más acertada los problemas de seguridad encontrados.
- Clasificación de los problemas de seguridad según su nivel de peligro, incluyendo valores CVSS. Esto permitirá a la empresa poder elaborar un plan de actuación eficiente para resolver estos problemas de seguridad.

8. METODOLOGIAS

8.1 OSSTMM

OSSTMM (Open Source Security Testing Methodology Manual) proporciona una metodología para una exhaustiva prueba de seguridad, en este documento se referencia como una auditoría OSSTMM. Una auditoría OSSTMM es una medición precisa de la seguridad a nivel operacional, lo cual evita suposiciones y evidencia anecdótica. Como una metodología, está diseñada para ser consistentes y repetible. Como un proyecto de fuente abierta, permite a cualquier profesional en pruebas de seguridad contribuir con ideas para realizar pruebas de seguridad más precisas, concretas y eficientes. Además esto permite la libre difusión de información y propiedad intelectual.[54]

EL OSSTMM 2.1, Incluye un marco de trabajo que describe las fases que habría que realizar para la ejecución de la auditoría. Se ha logrado gracias a un consenso entre más de 150 expertos internacionales sobre el tema, que colaboran entre sí mediante Internet. Se encuentra en constante evolución y actualmente se compone de las siguientes fases[55]:

[54]*CABALLERO QUEZADA,Alonso*. Introduction a OSSTMM (Open Source Security Testing Methodology Manual). [En Línea]. reydes, 2015. [Citado 1-noviembre-2018]. Disponible en Internet: http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual

[55] *Anónimo*. OSSTMM, Manual de la Metodología Abierta de Testeo de Seguridad. [En Línea]. DragonJAR, *s.f.* [Citado 1-noviembre-2018]. Disponible en Internet: https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml

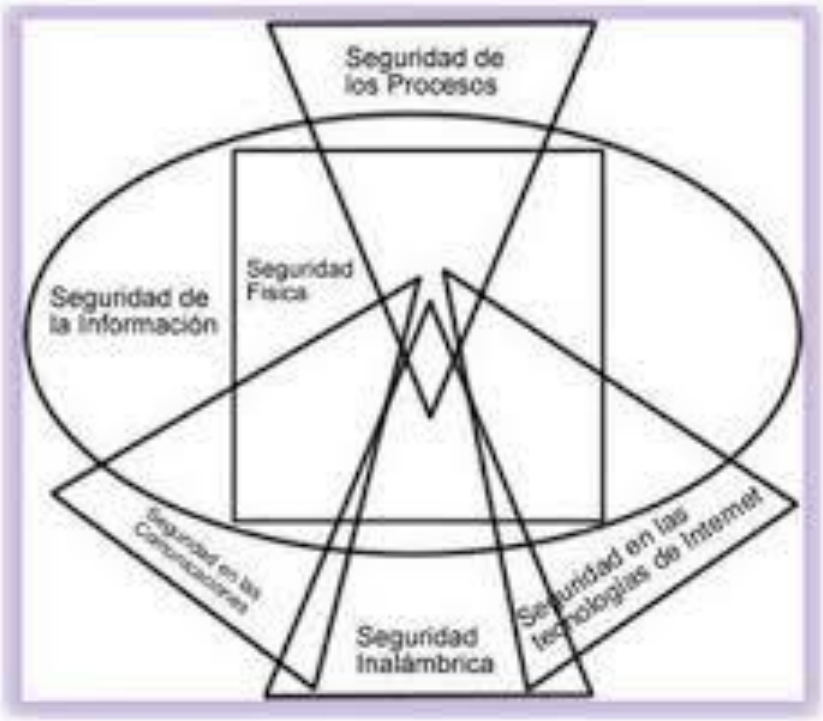

Figura 1. Esquema de la Metodología

Fuente: (Prandini & Ramili, 2010)

Sección A -Seguridad de la Información

1. Revisión de la Inteligencia Competitiva
2. Revisión de Privacidad
3. Recolección de Documentos

Sección B – Seguridad de los Procesos

1. Testeo de Solicitud
2. Testeo de Sugerencia Dirigida
3. Testeo de las Personas Confiables

Sección C – Seguridad en las tecnologías de Internet

1. Logística y Controles

2. Exploración de Red
3. Identificación de los Servicios del Sistema
4. Búsqueda de Información Competitiva
5. Revisión de Privacidad
6. Obtención de Documentos
7. Búsqueda y Verificación de Vulnerabilidades
8. Testeo de Aplicaciones de Internet
9. Enrutamiento
10. Testeo de Sistemas Confiados
11. Testeo de Control de Acceso
12. Testeo de Sistema de Detección de Intrusos
13. Testeo de Medidas de Contingencia
14. Descifrado de Contraseñas
15. Testeo de Denegación de Servicios
16. Evaluación de Políticas de Seguridad

Sección D – Seguridad en las Comunicaciones

1. Testeo de PBX
2. Testeo del Correo de Voz
3. Revisión del FAX
4. Testeo del Modem

Sección E – Seguridad Inalámbrica

1. Verificación de Radiación Electromagnética (EMR)
2. Verificación de Redes Inalámbricas [802.11]
3. Verificación de Redes Bluetooth
4. Verificación de Dispositivos de Entrada Inalámbricos
5. Verificación de Dispositivos de Mano Inalámbricos
6. Verificación de Comunicaciones sin Cable
7. Verificación de Dispositivos de Vigilancia Inalámbricos

8. Verificación de Dispositivos de Transacción Inalámbricos
9. Verificación de RFID
10. Verificación de Sistemas Infrarrojos
11. Revisión de Privacidad

Sección F – Seguridad Física

1. Revisión de Perímetro
2. Revisión de monitoreo
3. Evaluación de Controles de Acceso
4. Revisión de Respuesta de Alarmas
5. Revisión de Ubicación
6. Revisión de Entorno

Figura 2. Logo ISSTMM 2.1

Fuente: http://www.isecom.org/research/

De manera sencilla se identifican una serie de actividades de testeo específicas por área, sobre las que se comprueban las especificaciones de seguridad, integradas con las verificaciones realizadas en las revisiones rutinarias. Con esta metodología, se realiza un esfuerzo para convertir en predecible **QUE** se debe de probar, **COMO** se puede hacer y **CUANDO** es necesario ejecutarlo. De esta manera se aumenta la calidad del desarrollo, ya que la seguir esta metodología, se tiene la certeza de que se cumplen unos objetivos prefijados.

Un aspecto importante de esta metodología, es que no solo se centra en los aspectos eminentemente técnicos de seguridad tradicionales, sino que abarca aspectos sobre los responsables del testeo. Trata de estandarizar las credenciales del desarrollador a cargo del test, el formato de los resultados, crear un código ético, un plan temporal de ejecución, etc… Un aspecto muy importante de la metodología, es la incorporación del concepto de Valores de Evaluación de Riesgo, que permiten diferenciar y clasificar las diferentes problemáticas[56]. con la versión 3, OSSTMM abarca prueba desde todos los canales, humano, físico, inalámbrico, telecomunicación, y redes de datos.

Esto también lo hace perfectamente confortable para pruebas de computación en la nube, infraestructuras virtuales, middleware de mensajería, infraestructuras de comunicación móvil, ubicaciones de alta seguridad, recursos humanos, computación confiable, y cualquier proceso lógico el cual cubra todos los diversos canales y requiera un diferente tipo de prueba de seguridad.

Un conjunto de métricas de superficie de ataque, denominado ravs, proporciona una herramienta poderosa y altamente flexible la cual proporciona una representación

[56] *Anónimo*. Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM). [En Línea]. Marco de Desarrollo de la Junta de Andalucía, *s.f.* [Citado 1-noviembre-2018]. Disponible en Internet: http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/551

gráfica del estado, y muestra cambios en el estado a través del tiempo. Esto se integra bien con un "tablero" de gestión y es beneficiosa para pruebas internas y externas, permitiendo la comparación/combinación de las dos. La gestión del riesgo cuantitativo puede ser hecho desde el reporte con los hallazgos de la auditoría OSSTMM, proporcionando un resultado mejorado debido a resultados más precisos libres de error, sin embargo, se podría encontrar la gestión de confianza propuesta aquí superior a la gestión del riesgo.

OSSTMM incluye información para planificar el proyecto, cuantificar resultados, y las reglas del contrato para realizar auditorías de seguridad. La metodología puede ser fácilmente integrada con leyes y política existentes para asegurar una auditoría exhaustiva a través de todos los canales.[57] OSSTMM plantea categorizaciones estándar, que permiten identificar claramente el alcance de cada una de las actividades, evitando inconvenientes en tal sentido[58]:

1. Búsqueda de Vulnerabilidades: Orientado principalmente a realizar comprobaciones automáticas de un sistema o sistemas dentro de una red.

2. Escaneo de la Seguridad: Orientado a las búsquedas principales de vulnerabilidades en el sistema que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles en el sistemas y análisis individualizado.

[57] *CABALLERO QUEZADA, Alonso*. Introduction a OSSTMM (Open Source Security Testing Methodology Manual). [En Línea]. reydes, 2015. [Citado 1-noviembre-2018]. Disponible en Internet: http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual

[58] *Anónimo*. Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM). [En Línea]. Marco de Desarrollo de la Junta de Andalucía, *s.f.* [Citado 1-noviembre-2018]. Disponible en Internet: http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/551

3. Test de Intrusión: Se plantean test de pruebas que se centran en romper la seguridad de un sistema determinado.

4. Evaluación de Riesgo: se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.

5. Auditoria de Seguridad: Se refiere a la continua inspección que sufre el sistema por parte de los administradores que controlan que se cumplan las políticas de seguridad definidas.

6. Hacking Ético: Orientado a tratar de obtener, a partir de los test de intrusión, objetivos complejos dentro de la red de sistemas.

   Una nueva versión ha salido y es la OSSTMM 3, y esta ha dado un cambio radical a algunos puntos de la metodología, que permiten aumentar la efectividad del manual, pero podría requerir un esfuerzo extra a quienes ya veníamos trabajando con las versiones anteriores del OSSTMM, algunos de los cambios que he visto en esta versión 3.0 son[59]:

   - La metodología fue re-escrita totalmente, revisando minuciosamente cada uno de sus puntos.
   - Re-ordenado el Mapa de Seguridad.
   - Nuevo concepto de dashboards, que nos permite organizar más fácilmente los datos procedentes de los RAVs y explicarlos mejor.
   - Se explican mejor y se le da más relevancia a los Valores de la Evaluación de Riesgo o RAVs.

[59] *Anónimo*. OSSTMM, (Open Source Security Testing Methodology Manual) 3.0. [En Línea]. DragonJAR, *s.f.* [Citado 1-noviembre-2018]. Disponible en Internet: https://www.dragonjar.org/osstmm-open-source-security-testing-methodology-manual-3-0.xhtml

- Seguramente hay muchos más, pero aun no termino de leerlo.

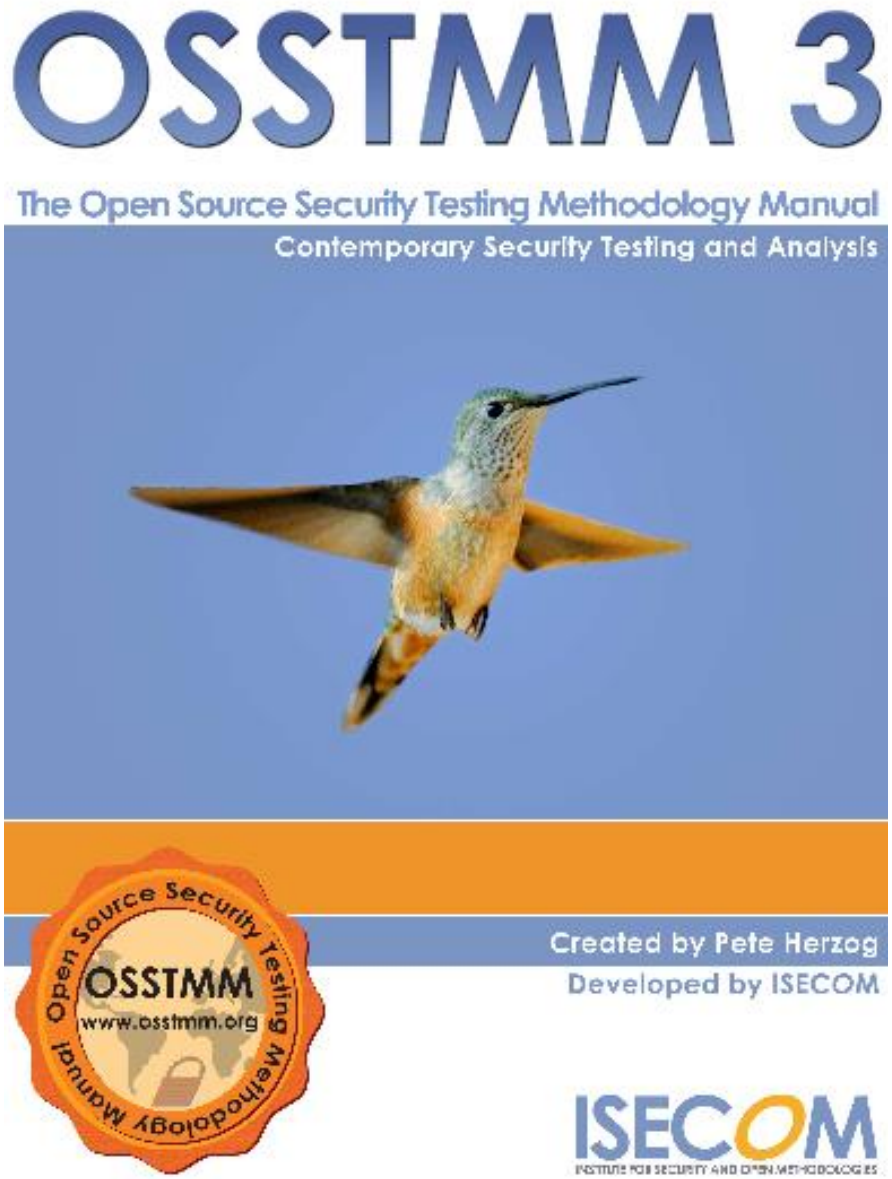

Figura 3. Logo OSSTMM 3

Fuente: http://www.isecom.org/mirror/OSSTMM.3.pdf

8.2 ISSAF

Figura 4. Logo ISSAF

Fuente: http://www.oissg.org/issaf.html

ISSAF (Information Systems Security Assessment Framework) e OISSG (Open Information System Security Group), es uno de los frameworks más interesantes dentro del ámbito de metodología de testeo. Realiza un análisis detallado de todos los posibles aspectos que afectan al 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 revisado por expertos en cada una de las áreas de aplicación. Estos criterios de evaluación a su vez, se componen de los siguientes ítems:

- Una descripción del criterio de evaluación.
- Puntos y objetivos a cubrir.
- Los prerrequisitos para conducir la evaluación.

- El proceso mismo de evaluación.
- El informe de los resultados esperados.
- Las contramedidas y recomendaciones.
- Referencias y Documentación Externa.

Para organizar de forma sistemática las labores de testeo, dichos “Criterios de Evaluación”, se han catalogado, desde los aspectos más generales, como pueden ser los conceptos básicos de la “Administración de Proyectos de Testeo de Seguridad”, hasta técnicas tan puntuales como la ejecución de pruebas de Inyección de Código SQL o como las “Estrategias del Cracking de Contraseñas”[60].

8.2.1 Historia y Visión General de ISSAF

ISSAF está evolucionando constantemente un marco que puede modelar los requisitos de control interno para la seguridad de la información. Al definir las pruebas junto con los dominios a probar, se busca unificar las políticas de administración con las operaciones técnicas para garantizar que haya una alineación completa entre todos los niveles intermedios.

ISSAF cubre las principales plataformas de tecnología de la información, la mayoría de los procesos operativos relacionados con TI de alto nivel, y está destinado a ser aplicable a las principales verticales de la industria, como la banca, la fabricación y los servicios. Esta ubicuidad de ISSAF está destinada a facilitar su adopción como el marco de evaluación de seguridad preferido por los departamentos de TI de todo el mundo. En el proceso de esta adopción, OISSG busca posicionarlo como la base para acreditar los sistemas de seguridad de la información de una organización al

[60] *Anónimo*. Metodologia y Frameworks de testeo de la seguridad de las aplicaciones. [En Línea]. Marco de Desarrollo de la Junta de Andalucía, *s.f.* [Citado 1-noviembre-2018]. Disponible en Internet: http://www.juntadeandalucia.es/servicios/madeja/sites/default/files/historico/1.3.0/contenido-recurso-216.html

nivel de las especificaciones técnicas que han sido probadas y probadas por los principales profesionales de la seguridad en todo el mundo[61].

8.2.2 Acerca de ISSAF[62].

El Marco de Evaluación de la Seguridad del Sistema de Información (ISSAF) es una revisión por pares marco estructurado que clasifica la evaluación de seguridad del sistema de información en varios Dominios y detalles de evaluación específica o criterios de prueba para cada uno de estos dominios. Apunta hacia proporcionar entradas de campo sobre evaluación de seguridad que reflejen escenarios de la vida real. ISSAF debería principalmente para cumplir con los requisitos de evaluación de seguridad de una organización y puede además, se utilizará como referencia para satisfacer otras necesidades de seguridad de la información. ISSAF incluye la faceta crucial de los procesos de seguridad y, su evaluación y fortalecimiento para obtener una imagen completa de las vulnerabilidades que puedan existir[63].

La información en ISSAF está organizada en criterios de evaluación bien definidos, cada uno de los cuales tiene sido revisado por expertos en la materia en ese dominio. Estos criterios de evaluación incluyen[64]:

• Una descripción de los criterios de evaluación.

---

[61] *Anónimo*. INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK (ISSAF). [En Línea]. Open Information Systems Security Group OISSG, *s.f.* [Citado 1-noviembre-2018]. Disponible en Internet: http://www.oissg.org/issaf.html

[62] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

[63] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

[64] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

• Sus fines y objetivos.
• Los requisitos previos para realizar las evaluaciones.
• El proceso para la evaluación.
• Muestra los resultados esperados
• Contramedidas recomendadas
• Referencias a documentos externos.

El marco general es amplio, elegimos proporcionar la mayor cantidad de información posible sobre el suponiendo que sería más fácil para los usuarios eliminar material en lugar de desarrollarlo. El Marco de Evaluación de la Seguridad del Sistema de Información (ISSAF) es un documento saliente que se ampliará, modificará y actualizará en el futuro.

8.2.3 Objetivos del ISSAF[65].

- Actuar como un documento de referencia de extremo a extremo para la evaluación de seguridad.

- Estandarizar el proceso de evaluación de seguridad del sistema de información.

- Establecer el nivel mínimo de proceso aceptable.

- Proporcionar una línea de base en la que se puede (o debería) realizar una evaluación

- Para evaluar las protecciones implementadas contra el acceso no autorizado.

[65] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

- Actuar como referencia para la implementación de seguridad de la información.

- Fortalecer los procesos y tecnologías de seguridad existentes.
- Evalúe las políticas y los procesos de seguridad de la información de la organización y asegúrese de que cumplan con los requisitos de la industria y que no violen las leyes y regulaciones aplicables.

- Identificar la infraestructura de sistemas de información crítica requerida para el negocio de las organizaciones.

- Procesa y evalúa su seguridad.

- Realizar evaluaciones de vulnerabilidad y pruebas de penetración para resaltar las vulnerabilidades del sistema:

- identificando así debilidades en sistemas, redes y aplicaciones.
- Evaluar los controles aplicados a varios dominios de seguridad mediante:
- Encontrar configuraciones erróneas y corregirlas o Identificar los riesgos relacionados con las tecnologías y abordarlas o Identificar los riesgos dentro de las personas o los procesos de negocios y abordarlos
- Fortalecimiento de procesos y tecnologías existentes.

- Priorizar las actividades de evaluación según la criticidad del sistema, los gastos de prueba y los beneficios potenciales.

- Educar a las personas en la realización de evaluaciones de seguridad.

- Educar a las personas sobre sistemas de seguridad, redes y aplicaciones.

- Proporcionar información sobre:

- La revisión de los procesos de registro, monitoreo y auditoría.
- La construcción y revisión del Plan de Recuperación de Desastres.
- La revisión de las preocupaciones de seguridad de outsourcing.

- Cumplimiento de las normas legales y reglamentarias

- Crear conciencia de seguridad

- Gestión eficaz de proyectos de evaluación de seguridad

- Protección contra la explotación de la ingeniería social.

- Revisión de control de seguridad física.

Proporcionar procedimientos muy detallados para el testing de sistemas de información. La metodología de test de penetración ISSAF está diseñada para evaluar las redes de trabajo, sistemas y control de aplicaciones[66].

8.2.4 El Framework[67]

[66] *Anónimo*. Metodología ISSAF. [En Línea]. Prezi, *25 de Marzo de 2015*. [Citado 1-noviembre-2018]. Disponible en Internet: https://prezi.com/5ssonumqypgo/metodologia-issaf/

[67] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

La seguridad puede ser una prioridad inmediata si el sitio web corporativo ha sido vandalizado o si una bomba lógica destruye registros corporativos cruciales, o si el sistema de correo electrónico corporativo fue el responsable de promulgar un virus conocido o un fraude basado en la subversión de procesos automatizados fue descubierto después del hecho. En estos casos, las preguntas anteriores se convierten en la base para iniciar un programa que busca abordar los problemas que han surgido. Sin embargo, en los casos que no presentan una necesidad imperiosa de cambio, también puede haber problemas que pueden afectar seriamente las posibilidades de supervivencia a largo plazo de la organización. La información que se filtra a los competidores, como planos o estimaciones para una licitación, puede no ser tan clara y un peligro actual como las instancias anteriores, pero puede erosionar seriamente las posibilidades de la empresa de obtener una ventaja crucial en el mercado[68].

Las cuatro fases respectivamente son Planificación, Evaluación, Tratamiento y acreditación. Cada una de estas fases tiene paquetes de trabajo específicos que son genéricos para todas las organizaciones, independientemente de su tamaño, sus áreas de resultados clave específicas y su ubicación geográfica. A través de la secuenciación de sus respectivos paquetes de trabajo, estas fases se centran en la entrega de resultados específicos, ya sea un entregable o un estado de cosas deseado. Los resultados de estas fases son seguidos por operaciones actividades diseñadas para integrar lo entregable o para mantener el estado alcanzado, factible y eficazmente[69].

[68] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

[69] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

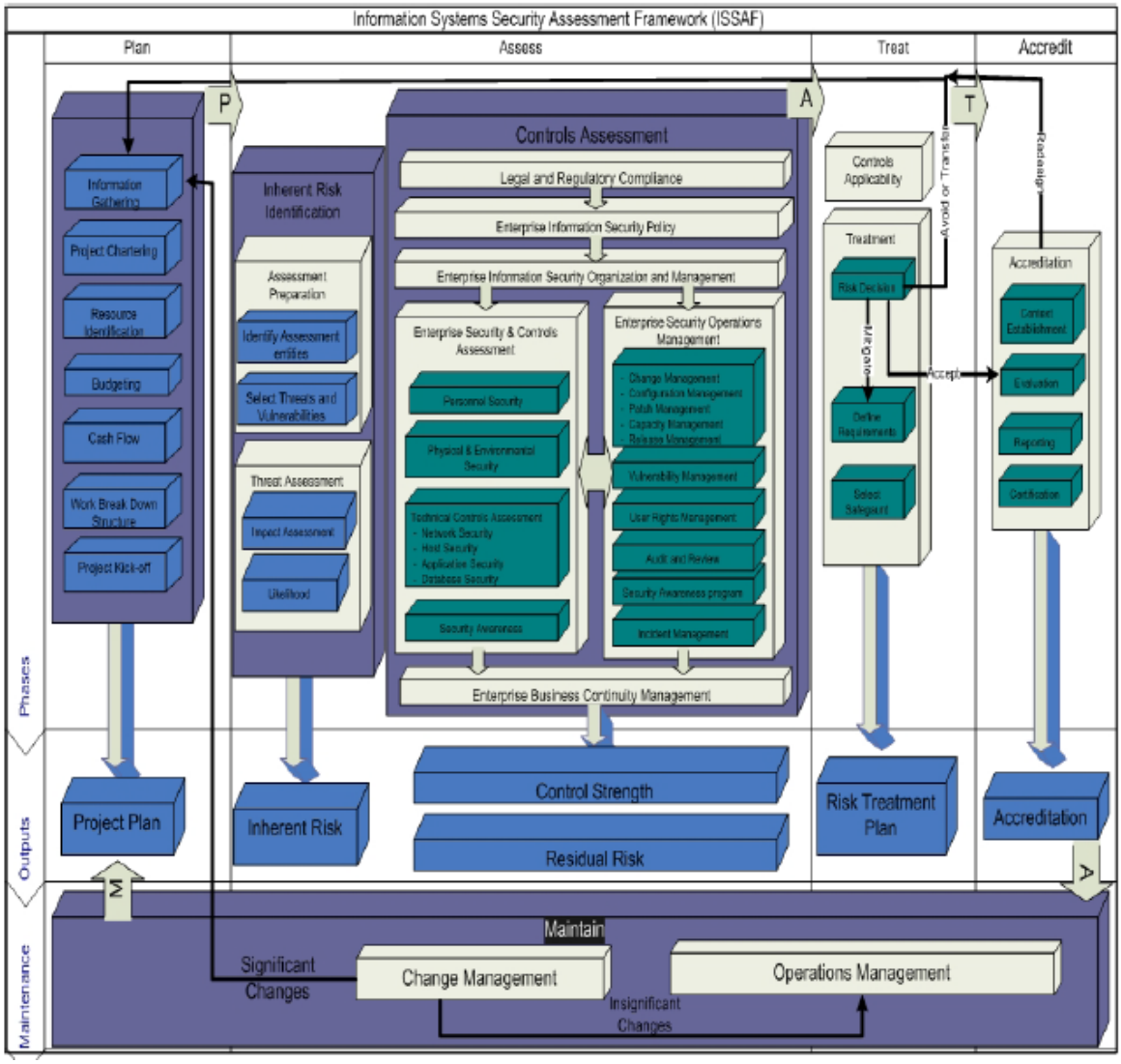

Figura 5. Fases ISSAF

Fuente: http://www.oissg.org/files/issaf0.2.1.pdf

8.2.4.1 Fase 1. Planeación[70].

[70] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

"Esta fase comprende los pasos iniciales para el intercambio de información, planificar y prepararse para la prueba"[71].

Las iniciativas de seguridad normalmente no tienen el mismo conjunto de eventos de activación dentro de las organizaciones. En algunos casos, un cambio en la administración podría resultar en un enfoque en la seguridad como un requisito crítico. En otros casos podría ser desencadenado por la realización de las pérdidas causadas por la interrupción de los sistemas. Si un auditor está preocupado por el período de retención de los registros de actividad del sistema, no puede presentar un caso de negocios a menos que sea capaz de justificar la necesidad de respaldar los registros de actividad con los requisitos legales o de cumplimiento específicos basados en no rechazo en los que basa sus requisitos en. Si existe una dependencia comercial de un servicio de información en particular, como el correo electrónico, corresponde al propietario del proceso de la función comercial en cuestión identificar las pérdidas potenciales que podrían acumularse en una hora, un día o una semana de interrupción de los sistemas causada por un virus u otra amenaza probable[72].

Por lo tanto, la recopilación de información busca reunir una imagen completa de la infraestructura de tecnología de la información para que sirva de base para la siguiente fase, a saber, la evaluación de riesgos. ISSAF ha reunido un conjunto de preguntas que pueden servir de base para la recopilación de esta información en un documento titulado ISSAF - Cuestionario de recopilación de información. Se recomienda que el profesional de seguridad recopile esta información y analice sus hallazgos antes de pasar a la siguiente etapa, es decir, preparar el caso de negocios para alinear la gestión de la seguridad como una prioridad. Se recomienda identificar

[71] *Anónimo*. Metodología ISSAF. [En Línea]. Prezi, *25 de Marzo de 2015*. [Citado 1-noviembre-2018]. Disponible en Internet: https://prezi.com/5ssonumqypgo/metodologia-issaf/

[72] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

los factores críticos de éxito (resultados deseados) y luego mapearlos a todos los procesos comerciales internos clave, incluidos los ciclos de ingresos y gastos, como paso inicial; Esto facilitará la identificación de qué procesos de negocio son más críticos para el negocio, y esto a su vez ayudará a priorizar qué sistemas son críticos para estos procesos[73].

Usando la carta del proyecto, es posible identificar a un alto nivel los recursos que probablemente se necesitarán para entregar los resultados requeridos. Los recursos pueden ir desde personas, productos, procesos, herramientas, conocimientos y apoyo político. El objetivo de esta actividad es investigar el tipo y los costos potenciales de los recursos que se requerirán para ejecutar este proyecto. Normalmente las iniciativas de seguridad se basan en cartas del proyecto, como contratar a un proveedor externo para implementar un firewall seguro, o contratar a un auditor para identificar las debilidades de control en los sistemas empresariales. El proceso de reunión y discusión de las iniciativas propuestas con los proveedores puede ayudar a aclarar las áreas de costos clave que probablemente resultarán de una implementación del plan propuesto[74].

Iniciativas El objetivo clave de esta fase es comprender si este proyecto es factible desde un punto de vista financiero y de recursos humanos. En este punto, es probable que la carta del proyecto requiera una revisión adicional para restringir o ampliar el alcance en función de la corrección o validación de los muchos supuestos que habrían impulsado la definición de la carta anterior. Esto es bastante normal y debe tratarse como un resultado de valor agregado de esta actividad en particular. La primera salida de la fase de identificación de recursos es la preparación de una RFP que se emite a los proveedores que suministrarán los recursos necesarios. Las

[73] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

[74] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

pautas para preparar esta RFP, así como una estructura de muestra, se proporcionan en los apéndices para futuras referencias[75].

- Flujo de efectivo: Es importante preparar lo siguiente:

- Cuenta de resultados (pérdidas y ganancias)
- Hoja de balance

A menos que se preparen estas declaraciones pro forma, el equipo financiero no podrá realizar un análisis financiero básico, como la preparación de los cronogramas de depreciación / amortización, identificar el aumento en los costos operativos causados por las nuevas contrataciones, la capacitación necesidades, etc.

- Estructura de desglose del trabajo:

Una estructura de desglose del trabajo (WBS) esencialmente crea un marco que agrupa e integra los paquetes de trabajo individuales que trabajarán en concierto para entregar los resultados del proyecto. Los paquetes de trabajo son una colección de tareas relacionadas que generalmente lleva a cabo un unidad integral, como un equipo o un individuo o a través de la automatización. Esta estructura se compone de un esquema jerárquico que desglosa progresivamente las actividades en partes cada vez más pequeñas hasta que la parte final se traduce en un paquete de trabajo asignable[76].

- Comienzo del proyecto:

[75] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf
[76] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

El propósito principal del inicio del proyecto es designar formalmente al gerente del proyecto. Esto garantiza que el gerente del proyecto tenga la visibilidad necesaria y la autoridad funcional para tomar las decisiones necesarias para entregar los resultados del proyecto definidos. La WBS se utiliza para iniciar el proyecto, y las discusiones posteriores se utilizan para generar un sentido de propiedad dentro de los miembros del equipo que se han reunido para este proyecto. El resultado clave de la puesta en marcha del proyecto es la matriz o cuadro de Responsabilidad, Acreditación, Consulta, Información (RACI), que designa quién es Responsable, quién acreditará los entregables, quién debe ser consultado y quién debe ser informado. A lo largo del proyecto. El gráfico RACI se convierte en el documento clave que se utilizará para gestionar todas las comunicaciones del proyecto[77].

- Salida – Plan del proyecto:

Sobre la base de los resultados anteriores, se prepara el plan final del proyecto, integrando horarios y recursos a las estructuras de desglose del trabajo. Este plan inicial del proyecto servirá como línea de base para monitorear y controlar la ejecución real de los resultados y resultados proyectados.

Tenga en cuenta que la fase de planificación anterior fue diseñada para ser genérica y se puede usar tanto para hacer frente a una tarea de la unidad como la compra e implementación de un nuevo firewall, así como para volver a diseñar toda la arquitectura corporativa de TI si necesario.

En resumen[78]:

[77] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

[78] *Anónimo*. Metodología ISSAF. [En Línea]. Prezi, *25 de Marzo de 2015*. [Citado 1-noviembre-2018]. Disponible en Internet: https://prezi.com/5ssonumqypgo/metodologia-issaf/

Las actividades que se hacen en esta Fase serian:

- Identificación de las personas de contactos de ambas partes.
- Apertura de Reunión para identificar el alcance.
- El enfoque y la metodología.
- Las fechas exactas.
- Los tiempos de prueba.
- La escalada de privilegios.

8.2.4.2 Fase 2. Evaluación[79]

"En esta fase se concreta el test de penetración, que se realiza a través de 9 capas, cada capa representa un mayor nivel de acceso a los activos de la información"[80].

La fase de evaluación proporciona un enfoque holístico para evaluar los riesgos de seguridad de la información en una empresa. Esta fase aboga por realizar evaluaciones de riesgos de seguridad de la información desde la perspectiva de los objetivos empresariales de la empresa y los riesgos asociados. Esto aseguraría la alineación de los riesgos empresariales de la empresa con los riesgos en relación con la naturaleza y el alcance del uso de la tecnología de la información para el logro de los objetivos comerciales de una empresa. Los riesgos inherentes identificados durante la evaluación se utilizan para identificar riesgos específicos que se derivan de la naturaleza y el alcance del uso de la tecnología de la información en la empresa. Los riesgos de la tecnología de la información identificados se utilizan para formular los requisitos de seguridad y control de la empresa[81].

[79] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf
[80] *Anónimo*. Metodología ISSAF. [En Línea]. Prezi, *25 de Marzo de 2015*. [Citado 1-noviembre-2018]. Disponible en Internet: https://prezi.com/5ssonumqypgo/metodologia-issaf/
[81] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

8.2.4.2.1 Recolección de información[82]: En la recopilación de la información se deben explorar todos los medios de los cuales podamos conseguir algún tipo de información.

- Motores de búsqueda, noticias, correos, blogs.
- Documentos internos, listas de visitantes, controles de accesos.

8.2.4.2.2 Mapeo de la red de trabajo[83]: Desde la capa anterior tomamos la información pertinente a la red, analizamos la posible topología de la empresa, existen gran cantidad de herramientas o aplicaciones que se pueden aplicar en esta etapa. Ejemplo NMAP.

8.2.4.2.3 Identificación de vulnerabilidades[84]:

- Escaneo de vulnerabilidades posibles ya identificadas.
- Listar y enumerar las vulnerabilidades encontradas.
- Calcular el posible impacto de las vulnerabilidades encontradas.
- Identificar las posibles rutas de ataque y posibles espacios de explotación.

8.2.4.2.4 Penetración[85]: El auditor intentara eludir las medidas de seguridad para tratar de llegar lo más lejos posible en cuanto al nivel de acceso de la información se refiere.

8.2.4.2.5 Obtener acceso y escalada de privilegios[86]: Se confirman y se documentan las intrusiones posibles. En esta etapa también se pretende

[82] *Anónimo*. Metodología ISSAF. [En Línea]. Prezi, *25 de Marzo de 2015*. [Citado 1-noviembre-2018]. Disponible en Internet: https://prezi.com/5ssonumqypgo/metodologia-issaf/
[83] *Anónimo*. Metodología ISSAF. [En Línea]. Prezi, *25 de Marzo de 2015*. [Citado 1-noviembre-2018]. Disponible en Internet: https://prezi.com/5ssonumqypgo/metodologia-issaf/
[84] *Anónimo*. Metodología ISSAF. [En Línea]. Prezi, *25 de Marzo de 2015*. [Citado 1-noviembre-2018]. Disponible en Internet: https://prezi.com/5ssonumqypgo/metodologia-issaf/
[85] *Anónimo*. Metodología ISSAF. [En Línea]. Prezi, *25 de Marzo de 2015*. [Citado 1-noviembre-2018]. Disponible en Internet: https://prezi.com/5ssonumqypgo/metodologia-issaf/
[86] *Anónimo*. Metodología ISSAF. [En Línea]. Prezi, *25 de Marzo de 2015*. [Citado 1-noviembre-2018]. Disponible en Internet: https://prezi.com/5ssonumqypgo/metodologia-issaf/

obtener privilegios de administrador, para evitar bloqueos que se podrían presentar por los antivirus, firewall y otros mecanismos de seguridad.

8.2.4.2.6 Enumeración adicional[87]:

- Obtener contraseñas por ejemplo las registradas en el archivo SAM de Windows o con los archivos /etc/passwd y /etc/shadow de Linux.
- Obtener contraseñas en textos planos.
- Mapear redes internas.

8.2.4.2.7 Comprometer usuarios remotos y sitios[88]: Las comunicaciones entre usuarios a través de sitios remotos y redes empresariales pueden ser con métodos de autenticidad cifrado, ejemplo VPN, pero esto no es garantía de que los extremos no hayan sido intervenidos.

8.2.4.2.8 Mantener el acceso[89]: Software de túnel, puertas traseras y rootkits entre otros, no soy muy utilizados ya que es posible que un atacante los descubra y obtenga acceso y privilegios del sistema.

8.2.4.2.9 Cubrir rastros[90]: Es normal que se lleve a cabo este paso durante las pruebas para que sea lo más transparente posible. En este paso se ocultan archivos y se borran los registros ya que si un atacante obtiene acceso a nuestro sistema tratara de borrar cualquier registro o evidencia.

[87] *Anónimo*. Metodología ISSAF. [En Línea]. Prezi, *25 de Marzo de 2015*. [Citado 1-noviembre-2018]. Disponible en Internet: https://prezi.com/5ssonumqypgo/metodologia-issaf/
[88] *Anónimo*. Metodología ISSAF. [En Línea]. Prezi, *25 de Marzo de 2015*. [Citado 1-noviembre-2018]. Disponible en Internet: https://prezi.com/5ssonumqypgo/metodologia-issaf/
[89] *Anónimo*. Metodología ISSAF. [En Línea]. Prezi, *25 de Marzo de 2015*. [Citado 1-noviembre-2018]. Disponible en Internet: https://prezi.com/5ssonumqypgo/metodologia-issaf/
[90] *Anónimo*. Metodología ISSAF. [En Línea]. Prezi, *25 de Marzo de 2015*. [Citado 1-noviembre-2018]. Disponible en Internet: https://prezi.com/5ssonumqypgo/metodologia-issaf/

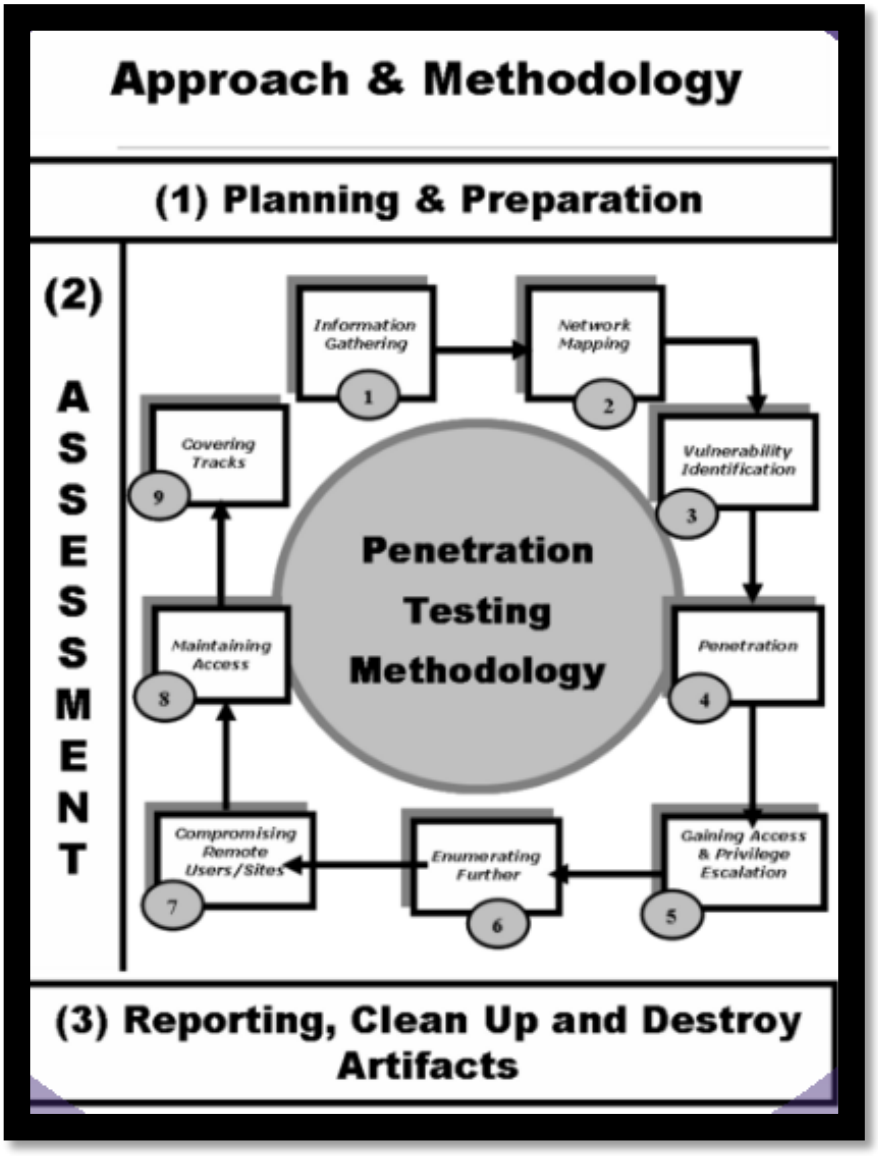

Figura 6. Nueve capas de Fase de Evaluación

Fuente: https://prezi.com/5ssonumqypgo/metodologia-issaf/

8.2.4.3 Fase3. Tratamiento[91]

[91] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

El tratamiento de riesgos proporciona una plataforma para tomar una decisión sobre los riesgos residuales, a través de la selección de salvaguardas, el desarrollo de planes de implementación y el suministro de documentación precisa para la implementación y el proceso de toma de decisiones. La decisión de riesgo es una etapa importante en la que la gerencia ejecutiva y otras partes interesadas revisan su documentación y toman la decisión de aceptar, mitigar, transferir o evitar el riesgo. Una vez que se toma esta decisión, se hacen planes para implementar el resultado y se buscan aprobaciones para los requisitos presupuestarios. Otra tarea importante en el proceso de tratamiento de riesgos es que cuando se toma una decisión para mitigar un riesgo, se selecciona la selección de controles para mitigar el riesgo y se desarrolla un plan de proyecto para implementar los controles. Le sugerimos que utilice la plantilla del Plan de tratamiento de riesgos en el ISSAF para este proceso.

8.2.4.4 Fase 4. Acreditación[92]

El proceso de acreditación implica evaluar los controles que se han seleccionado para la implementación en el ámbito de la certificación. Los resultados de la evaluación determinan la acreditación de la certificación ISSAF a una organización

8.2.4.5 Fase 5. Mantenimiento[93]

Se requerirá que las organizaciones certificadas ISSAF demuestren el cumplimiento de la acreditación ISSAF de manera continua. Para garantizar esto, OISSG realizará evaluaciones / revisiones de cumplimiento programadas regularmente. La

[92] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

[93] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

frecuencia de esta revisión se basará en el tamaño de la organización y el alcance de la acreditación.

8.2.5 Gestión de Compromisos[94]

Un compromiso es agrupar las actividades que, cuando se juntan, logran un objetivo y una meta. Un compromiso siempre tiene un comienzo y un final reconocibles. Este documento proporciona una visión general sobre la gestión de compromisos para los compromisos de evaluación de seguridad. El compromiso de evaluación de seguridad implica numerosas tareas e involucra a varias partes. Dicho compromiso requiere la planificación del compromiso desde el inicio y la actividad de gestión a lo largo del desarrollo del compromiso. Esta sección describe los aspectos de la gestión del compromiso de un compromiso de evaluación de seguridad. Las siguientes pautas pueden utilizarse directamente para proporcionar un plan de gestión de compromiso al cliente.

8.2.6 Buenas practicas – Pre Evaluación, Evaluación y Post Evaluación[95]

En los últimos años, el proceso de evaluación de seguridad ha evolucionado desde un conjunto variado de ataques llevados a cabo por aficionados hasta un proceso de evaluación maduro y revisable con sólidos límites legales y resultados bien definidos. Independientemente de la Evaluación de Vulnerabilidad, las Pruebas de Penetración y / o la Evaluación de Seguridad, hay ciertas cosas que el evaluador debe tener en cuenta al evaluar la fortaleza de la seguridad de una empresa. Una evaluación bien definida, probada y estructurada puede ayudar enormemente a fortalecer sus defensas; también presenta problemas nuevos y complejos con los

[94] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

[95] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

que tendrá que lidiar. P.ej. Aspectos legales, consulte la sección Base de conocimientos para obtener más detalles sobre esto.

8.2.7 Evaluación de riesgos[96]

En el entorno empresarial extremadamente competitivo de hoy, las organizaciones se ven cada vez más obligadas a reducir costos y aumentar la rentabilidad, la Administración Senior de organizaciones en todo el mundo está poniendo mayor énfasis en el Retorno de las Inversiones (ROI) y el Costo v / s Beneficio empresarial de cada dólar gastado. La tecnología de la información, que forma parte integral del entorno empresarial actual, también debe demostrar las justificaciones de costo-beneficio y un nivel aceptable de ROI para todos los gastos de TI. La seguridad de los sistemas de información es una inversión en TI que está constantemente bajo la lupa de la alta gerencia, dado que se están gastando millones de dólares en evaluaciones e implementaciones de seguridad. Para agravar esto, la Alta Dirección también tiene que lidiar con un grupo de adictos que hablan un lenguaje extraño que es casi etéreo para ellos, lo que lleva a un mayor escepticismo entre la Alta Dirección.

Dado este escenario, se ha vuelto extremadamente importante para los profesionales de Seguridad de los Sistemas de Información de todo el mundo para alinear sus evaluaciones e implementaciones con el negocio y sus objetivos comerciales estratégicos. La demostración de cómo y dónde contribuye la seguridad de los sistemas de información al negocio es de suma importancia hoy en día. Para lograr esto, una evaluación de riesgos de tecnología con una evaluación de riesgos de negocios es el orden del día para facilitar la integración de

[96] OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf

los objetivos de negocios con los objetivos de seguridad de los sistemas de información.

Por lo tanto, el riesgo es una función del valor de los activos, amenazas y vulnerabilidades y se puede calcular de la siguiente manera:

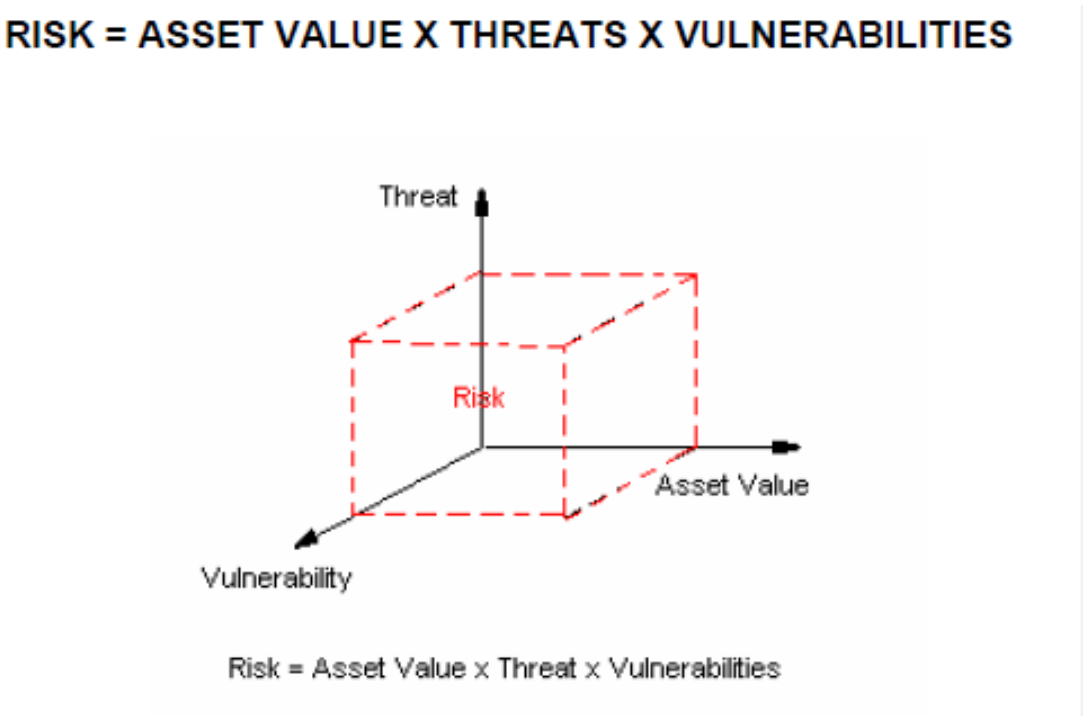

Figura 7. Función de Riesgo

Fuente: https://prezi.com/5ssonumqypgo/metodologia-issaf/

El tema de la evaluación de riesgos y en realidad cómo llevar a cabo un ejercicio de evaluación de riesgos puede ser al principio confuso y alucinante. Sin embargo, si se siguen algunas reglas básicas y la metodología adecuada, un ejercicio de evaluación de riesgos tiende a ser muy fructífero e interesante para el negocio. Esta área del marco le proporciona procedimientos prácticos y herramientas para permitirle ejecutar efectivamente su propio ejercicio de evaluación de riesgos. El ejercicio se puede llevar a cabo a través de talleres en los que los interesados de los Sistemas de información intercambian ideas sobre los riesgos que enfrenta la

empresa y acuerdan las prioridades. Un "facilitador" es ideal para este tipo de ejercicio para facilitar el taller y mantener las discusiones enfocadas y dentro de los límites.

El proceso general en pocas palabras será el siguiente:

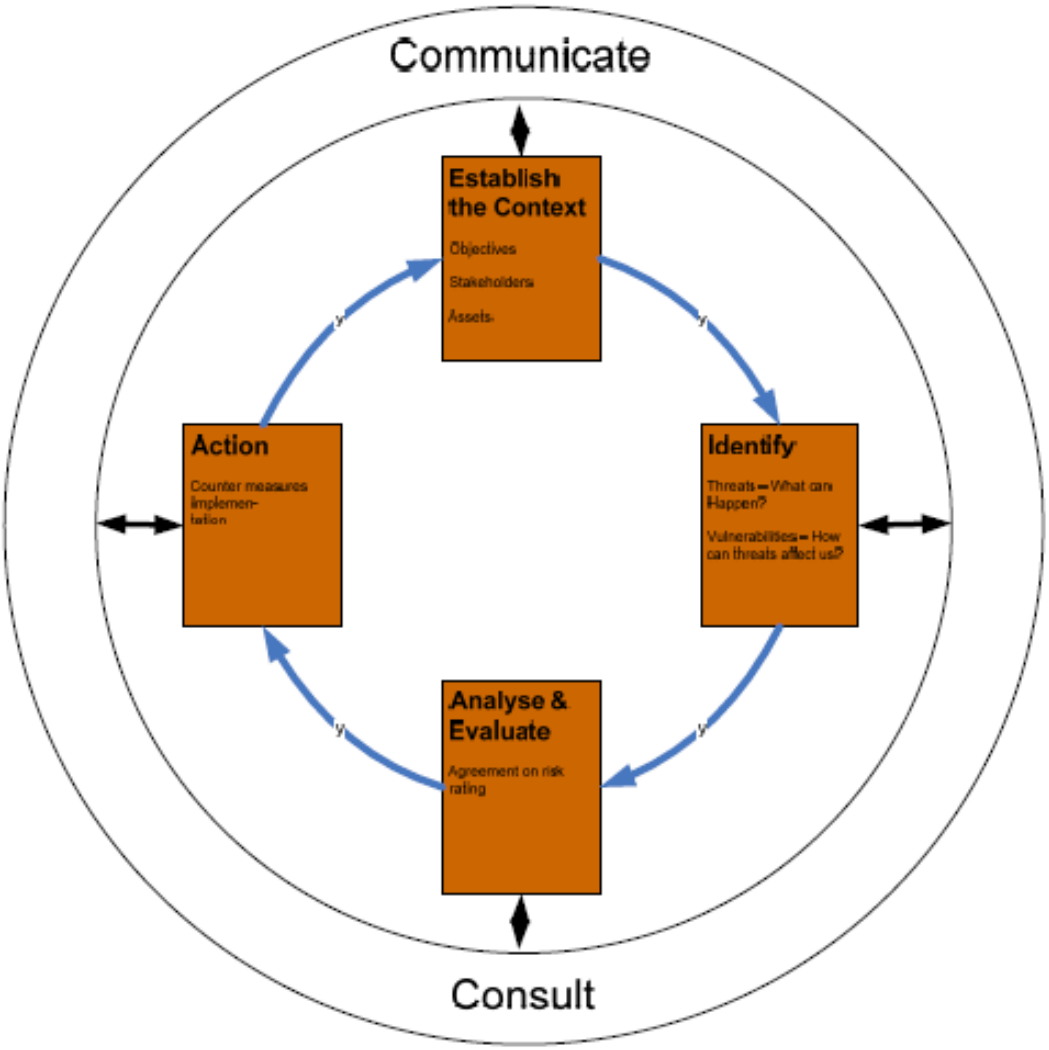

Figura 8. Procesos de la evaluación del Riesgo

Fuente: https://prezi.com/5ssonumqypgo/metodologia-issaf/

8.3 OWASP

Figura 9. Logo de OWASP

Fuente: https://www.owasp.org/index.php/Austin

Todo mercado de tecnología vibrante necesita una fuente de información imparcial sobre las mejores prácticas, así como un cuerpo activo que abogue por estándares abiertos. En el espacio de Seguridad de la aplicación, uno de esos grupos es el Proyecto de seguridad de la aplicación web abierta (u OWASP para abreviar). **El Open Web Application Security Project** (OWASP) es una organización benéfica sin fines de lucro mundial centrada en mejorar la seguridad del software. Nuestra misión es hacer visible la seguridad del software , para que las personas y las organizaciones puedan tomar decisiones informadas. OWASP se encuentra en una posición única para proporcionar información imparcial y práctica sobre AppSec a individuos, corporaciones, universidades, agencias gubernamentales y otras organizaciones en todo el mundo. Operando como una comunidad de profesionales con ideas afines, OWASP emite herramientas de software y documentación basada en el conocimiento sobre la seguridad de las aplicaciones[97].

[97] The OWASP Foundation. The OWASP. [En línea]. OWASP, s.f. [Citado 01-Noviembre-2018]. Disponible en internet: https://www.owasp.org/index.php/Main_Page

El objetivo de este proyecto según la OWASP top 10(2013), es crear conciencia acerca de la seguridad en aplicaciones mediante la identificación de algunos de los riesgos más críticos que enfrentan las organizaciones.[1] Así mismo estos riesgos de seguridad son referenciados en artículos científicos, tesis de pregrado y postgrado, libros de seguridad y organizaciones como MITRE,[2] SANS, PCI DSS, DISA, FCT.[98]

El proyecto abierto de seguridad en aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a habilitar a las organizaciones para desarrollar, comprar y mantener aplicaciones confiables. Todas la herramientas, documentos, foros y capítulos de OWASP son gratuitos y abierto a cualquiera interesado en mejorar la seguridad de aplicaciones. Abogamos por resolver la seguridad de aplicaciones como un problema de gente, procesos y tecnología porque las soluciones más efectivas incluyen mejoras en todas estas áreas. OWASP es un nuevo tipo de organización. Nuestra libertad de presiones comerciales nos permite proveer información sobre seguridad en aplicaciones sin sesgos, práctica y efectiva. OWASP no está afiliada a ninguna compañía de tecnología, aunque soportamos el uso informado de tecnologías de seguridad comerciales. Parecido a muchos proyectos de software de código abierto, OWASP produce muchos materiales en una manera abierta y colaborativa. La Fundación OWASP es una entidad sin ánimo de lucro para asegurar el éxito a largo plazo del proyecto.[99]

OWASP Foundation (Overview Slides) es una asociación profesional de miembros globales y está abierta a cualquier persona interesada en aprender más sobre la seguridad del software. Los capítulos locales se ejecutan de forma independiente y están guiados por el Chapter_Leader_Handbook . Como una asociación profesional

[98] *Anónimo*. OWASP Top10. [En Línea].WIKIPEDIA, *01 de Noviembre de 2018*. [Citado 1-noviembre-2018]. Disponible en Internet: https://es.wikipedia.org/wiki/OWASP_Top_10
[99] *Anónimo*. Sobre OWASP. [En Línea]. OWASP, *11 de noviembre de 2014*. [Citado 1-noviembre-2018]. Disponible en Internet: https://www.owasp.org/index.php/Sobre_OWASP

sin fines de lucro, su apoyo y patrocinio de cualquier lugar de reunión o refrigerio es deducible de impuestos. Las contribuciones financieras solo deben hacerse en línea utilizando el botón de donación de capítulo autorizado en línea. Para ser un **ALTAVOZ** en CUALQUIER Capítulo de OWASP en el mundo, simplemente revise el acuerdo del orador y luego comuníquese con el líder del capítulo local con los detalles sobre qué OWASP PROJECT, investigación independiente o tema de seguridad de software relacionado le gustaría presentar.[100]

Todos los materiales de OWASP están disponibles bajo la aprobada Licencia FLOSS. Si opta por convertirse en una organización miembro de OWASP, puede también usar la licencia comercial que le permite usar, modificar y distribuir todos los materiales de OWASP dentro de su organización bajo una licencia sencilla.[101]

En OWASP, encontrarás gratis y abierto[102]:

• Herramientas y estándares de seguridad de aplicaciones.
• Libros completos sobre pruebas de seguridad de aplicaciones, seguros Desarrollo de código, y revisión segura de código.
• Presentaciones y videos.
• Hojas de trucos sobre muchos temas comunes.
• Controles de seguridad estándar y bibliotecas.
• Capítulos locales en todo el mundo.
• Investigación de vanguardia.
• Amplias conferencias a nivel mundial.
• Listas de correo.

[100] The OWASP Foundation. Austin. [En línea]. OWASP, s.f. [Citado 01-Noviembre-2018]. Disponible en internet: https://www.owasp.org/index.php/Austin
[101] *Anónimo*. Sobre OWASP. [En Línea]. OWASP, *11 de noviembre de 2014*. [Citado 1-noviembre-2018]. Disponible en Internet: https://www.owasp.org/index.php/Sobre_OWASP
[102] *www.owasp.org*. OWASP Top10-2017. [En Línea].OWASP, *sf.* [Citado 1-noviembre-2018]. Disponible en Internet: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

El software inseguro está socavando nuestra infraestructura financiera, sanitaria, de defensa, energética y otras infraestructuras críticas. A medida que nuestro software se vuelve cada vez más complejo y conectado, la dificultad de lograr la seguridad de la aplicación aumenta exponencialmente. El rápido ritmo de los procesos modernos de desarrollo de software hace que los riesgos más comunes sean esenciales para descubrir y resolver de manera rápida y precisa. Ya no podemos permitirnos tolerar problemas de seguridad relativamente simples como los presentados en este Top 10 de OWASP.[103]

OWASP Top 10 fue lanzado por primera vez en 2003, con actualizaciones en 2004 y 2007. La versión 2010 fue renovada para dar prioridad al riesgo, no sólo a la prevalencia. La edición 2013 sigue el mismo enfoque. Los documentos del OWASP top 10 comenzaron a publicarse desde el 2004, haciendo un total de cuatro actualizaciones hasta la fecha, estos son además del Owasp top 10-2004 el Owasp top 10-2007, Owasp top 10-2010 y Owasp top 10-2013. Hay una versión inicial del 2003 pero no hay detalles en la página del proyecto más que la lista de los riesgos de seguridad de ese entonces.[104]

OWASP Top 10-2003	OWASP Top 10-2004	OWASP Top 10-2007	OWASP Top 10-2010	OWASP Top 10-2013	OWASP Top 10-2016

[103] *www.owasp.org*. OWASP Top10-2017. [En Línea].OWASP, *sf*. [Citado 1-noviembre-2018]. Disponible en Internet: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

[104] *Anónimo*. OWASP Top10. [En Línea].WIKIPEDIA, *01 de Noviembre de 2018*. [Citado 1-noviembre-2018]. Disponible en Internet: https://es.wikipedia.org/wiki/OWASP_Top_10

A1-Entrada no validada	A1-Entrada no validada	A1-Secuencia de comandos en sitios cruzados XSS	A1-Inyección	A1-Inyección	A1 - Verify for Security Early and Often
A2-Control de acceso interrumpido	A2-Control de acceso interrumpido	A2-Fallas de inyección	A2-Secuencia de comandos en sitios cruzados XSS	A2-Pérdida de autenticación y gestión de sesiones	A2 - Parameterize Queries
A3-Administración de cuentas y sesión interrumpida	A3-Administración de autenticación y sesión interrumpida	A3-Ejecución de ficheros malintencionados	A3-Pérdida de autenticación y gestión de sesiones	A3-Secuencia de comandos en sitios cruzados XSS	A3 - Encode Data
A4-Fallas de cross site scripting XSS	A4-Fallas de cross site scripting XSS	A4-Referencia insegura y directa a objetos	A4-Referencia directa insegura a objetos	A4-Referencia directa insegura a objetos	A4 - Validate All Inputs
A5-Desbordam	A5-Desbordam	A5-Falsificación de	A5-Falsificación de	A5-Configuración de	A5 - Implement Identity

iento de bufer	iento de bufer	peticiones en sitios cruzados CSRF	peticiones en sitios cruzados CSRF	seguridad incorrecta	and Authentication Controls
A6-Fallas de inyección de comandos	A6-Fallas de inyección	A6-Revelación de información y gestión incorrecta de errores	A6-Defectuosa configuración de seguridad	A6-Exposición de datos sensibles	A6 - Implement Appropriate Access Controls
A7-Problemas de manejo de errores	A7-Manejo inadecuado de errores	A7-Pérdida de autenticación y gestión de sesiones	A7-Almacenamiento criptográfico inseguro	A7-Ausencia de control de acceso a las funciones	A7 - Protect Data
A8-Uso inseguro de criptografía	A8-Almacenamiento inseguro	A8-Almacenamiento criptográfico inseguro	A8-Falla de restricción de acceso a URL	A8-Falsificación de peticiones en sitios cruzados CSRF	A8 - Implement Logging and Intrusion Detection
A9-Fallas de administración	A9-Negación de servicio	A9-Comunicaciones inseguras	A9-Protección insuficiente en la capa	A9-Uso de componentes con vulnerabilid	A9 - Leverage Security Framewor

remota(no aplicable)			de transporte	ades conocidas	ks and Libraries
A10-Configuración indebida de servidor web y de aplicación	A10-Administración de configuración insegura	A10-Falla de restricción de acceso a URL	A10-Redireccion es y reenvíos no validados	A10-Redireccio nes y reenvíos no validados	A10 - Error and Exception Handling

TABLA2: Historia de OWASP

8.3.1 Top 10 Vulnerabilidades más comunes[105]

OWASP, cada cierto tiempo, realiza un informe recogiendo las vulnerabilidades más comunes dentro de las aplicaciones web. Con este informe, podremos estar al tanto de dichas vulnerabilidades y podremos emplearlo para comprobar si nuestra aplicación tiene alguna de las que aparecen en dicho informe. También, ofrecen herramientas de detección y consejos sobre medidas a tomar para solucionar dicha vulnerabilidad.

A continuación, vamos a enumerar las 10 vulnerabilidades más comunes del informe realizado hasta 2013 y vamos a aportar una breve descripción sobre cada una de las vulnerabilidades:

1. Inyección: este ataque se produce cuando datos no confiables son enviados a un intérprete (ya sea del sistema operativo, de una base de datos o cualquier intérprete) como parte de un comando o consulta. Los

[105] *VINDEL Rafael*. Introducción a OWASP. [En Línea]. Adictos al trabajo, *07 de marzo de 2016*. [Citado 1-noviembre-2018]. Disponible en Internet: https://www.adictosaltrabajo.com/2016/03/07/introduccion-a-owasp/

datos hostiles introducidos por el atacante pueden engañar al intérprete haciendo que se ejecuten comandos no intencionados o accediendo a información sobre la que no se está autorizado. Uno de los ejemplos más significativos de este tipo de ataque es *SQL Injection*.

2. Pérdida de autenticación y gestión de sesiones: este tipo de ataque se produce cuando los mecanismos de la aplicación relacionados con la autenticación, autorización y control de sesiones son, frecuentemente, implementados de forma incorrecta o su configuración no se ha realizado de forma correcta. Esto provoca que un usuario malicioso pueda obtener las credenciales de un usuario, el identificador de la sesión o, incluso, el identificador de acceso y hacerse pasar por dicho usuario accediendo a todos sus datos. Uno de los ejemplos puede ser la gestión de la sesión mediante la propia página.

3. Secuencia de comandos en sitios cruzados (XSS): este tipo de ataque ocurre cuando se obtienen datos no confiables y se envían directamente al navegador web. Esto provoca que se puedan ejecutar comandos no deseados en el navegador del usuario. Estos comandos pueden obtener desde las credenciales de acceso del usuario como instalar ciertos programas maliciosos.
4. Referencia directa insegura a objetos: este tipo de ataque ocurre cuando no se controlan los accesos a recursos sobre los que un usuario no debería tener acceso. En las aplicaciones, la mayoría de las veces, existen distintos usuarios y cada usuario tiene una serie de recursos sobre los que tiene acceso y otros sobre los que no debería tener acceso. Un ejemplo podría ser el acceso a una tabla de base de datos sobre la que un determinado usuario no debería tener acceso (una tabla de gestión sobre la que sólo el administrador debería tener acceso).

5. Configuración de seguridad incorrecta: este tipo de ataque ocurre cuando se han realizado malas configuraciones en las aplicaciones, en los servidores de las aplicaciones, en las bases de datos o en la configuración del propio sistema operativo. Es importante tener todo el *software* bien actualizado con la última versión disponible (esperando a que no haya vulnerabilidades de día 0) y que todas las librerías o *frameworks* que use la aplicación también estén actualizadas ya que muchos cambios que se realizan en las versiones tienen que ver con aspectos de seguridad.
6. Exposición de datos sensibles: este tipo de ataque ocurre cuando se puede acceder de forma fácil a datos de carácter sensible almacenados en la aplicación. Cuando, por ejemplo, se almacenan las credenciales de los usuarios sin codificar o si la comunicación del servidor no es segura a la hora de realizar un pago con una tarjeta de crédito.
7. Ausencia de control de acceso a funciones: este tipo de ataque ocurre cuando se acceden a funciones del servidor sobre las que un usuario no debería tener permiso. Cuando, por ejemplo, el servicio de listado de usuario sólo debería estar disponible por la aplicación, pero cualquier usuario puede también acceder a esta información.
8. Falsificación de peticiones en sitios cruzados: este tipo de ataque ocurre cuando se realizan peticiones HTTP falsificadas del ordenador de la víctima a una aplicación web vulnerable.
9. Utilización de componentes con vulnerabilidades conocidas: este tipo de ataque ocurre cuando se emplean librerías o *frameworks* que contienen vulnerabilidades. Es por esto que es importante actualizar estos componentes o revisar el histórico de revisiones para comprobar las mejoras de seguridad implementadas.

10. Redirecciones y reenvíos validados: este tipo de ataque ocurre cuando, al re direccionar al usuario a otra página, no se comprueba que el destino sea válido. Es por esto que se puede redirigir a un usuario a una página que contenga contenido malicioso para robar las credenciales de dicho usuario.

Una vez se han visto los 10 ataques más comunes, es importante destacar que casi siempre se usan ataques combinados para aprovecharse de todas las vulnerabilidades. Se puede hacer un ataque de *SQL Injection* para acceder a una tabla sobre la que el usuario no debería tener permiso para tener acceso a credenciales no codificadas de los usuarios del sistema. Por lo que es importante centrarse en todas y cada una de estas vulnerabilidades.

8.3.2 Herramientas[106]

OWASP también realiza una serie de proyectos con el objetivo de darnos herramientas para afianzar la seguridad de nuestras aplicaciones. Estos proyectos se pueden acceder desde el siguiente enlace.

A continuación, se muestran algunos de estos proyectos junto con una breve descripción de cada uno de ellos:

- Zed Attack Proxy: es una herramienta de *pentesting* que nos ayuda a encontrar vulnerabilidades en nuestras aplicaciones. Es recomendable el uso por gente con cierta experiencia en términos de seguridad.

[106] *VINDEL Rafael*. Introducción a OWASP. [En Línea]. Adictos al trabajo, *07 de marzo de 2016*. [Citado 1-noviembre-2018]. Disponible en Internet: https://www.adictosaltrabajo.com/2016/03/07/introduccion-a-owasp/

- OWTF: es una herramienta de *pentesting* que es, quizás, un poco más sencilla que la herramienta anterior.

- Dependency Check: es una herramienta que nos permite analizar todas las dependencias de nuestra aplicación y comprobar si existen vulnerabilidades dentro de ellas.

- Mobile Security Project: es una herramienta que nos permite realizar *pentesting* sobre aplicaciones móviles.

- SSL advanced forensic tool: es una herramienta que nos permite mostrar información sobre SSL y los certificados.

Existen muchos proyectos más y es recomendable echar un vistazo a todos ellos ya que nos ayudan (y mucho) a nuestro objetivo de asegurar la seguridad en las aplicaciones.

9. ANALISIS DE VULNERABILIDADES[107]

El proceso de análisis de vulnerabilidades implica reconocer, medir y priorizar las vulnerabilidades de un sistema de información. Se indicara a continuación el procedimiento para un análisis de vulnerabilidades:

- Comprobar si el equipo está activo
- Escanear puertos
- Identificar las vulnerabilidades potenciales y generar un reporte
- Clasificar las vulnerabilidades y determinar un plan de acciones para su mitigación.
- Clasificar y priorizar los activos de la empresa e iniciar la gestión de riesgos
- Documentar las acciones realizadas y generar un informe de los resultados
- Iniciar un proceso continuo de seguridad.

9.1 Clasificación de Vulnerabilidades[108]

- Errores de configuraciones
- Instalaciones por defecto
- Buffer Overflows
- Servidores sin parches
- Contraseñas por defecto

[107] LOPEZ LOPEZ, Agustin. Estudio de Metodologías para Pruebas de Penetración a Sistemas Informáticos, México D.F, 2011, 123, Trabajo de Grado (Estudio de Metodologías para Pruebas de Penetración a Sistemas Informáticos). Instituto Politécnico Nacional. Departamento Superior de Ingeniería Mecánica y Eléctrica Sección de Estudios de Posgrado e Investigación.

[108] LOPEZ LOPEZ, Agustin. Estudio de Metodologías para Pruebas de Penetración a Sistemas Informáticos, México D.F, 2011, 123, Trabajo de Grado (Estudio de Metodologías para Pruebas de Penetración a Sistemas Informáticos). Instituto Politécnico Nacional. Departamento Superior de Ingeniería Mecánica y Eléctrica Sección de Estudios de Posgrado e Investigación.

- Servicios abiertos
- Fallas en las aplicaciones
- Fallas en los sistemas operativos
- Fallas en los diseños

El análisis de vulnerabilidades es un examen para identificar las debilidades de un sistema o aplicación que podrían ser aprovechadas por un atacante. De igual es puesta a prueba la efectividad de los procedimientos y los controles de seguridad ante posibles ataques.

9.2 Herramientas para el análisis de vulnerabilidades[109]

- QUALYS Scanner
- Cycorp Cycsecure Scanner
- eEye Retina Network Security Scanner
- Foundstone Professional Scanner
- GFI LANguard Network Security Scanner
- ISS Internet Scanner
- Saint Vulnerability Scanner
- Symantec Netrecon Scanner
- Shadow Security Scanner
- Open Source Nessus

Antes de utilizar cualquier herramienta, es importante comprender su funcionamiento, que este actualizado y haberlo probado en un ambiente de laboratorio. El análisis de vulnerabilidades se debe realizar de forma periódica.

[109] LOPEZ LOPEZ, Agustin. Estudio de Metodologías para Pruebas de Penetración a Sistemas Informáticos, México D.F, 2011, 123, Trabajo de Grado (Estudio de Metodologías para Pruebas de Penetración a Sistemas Informáticos). Instituto Politécnico Nacional. Departamento Superior de Ingeniería Mecánica y Eléctrica Sección de Estudios de Posgrado e Investigación.

10. ESTUDIO COMPARATIVO DE METODOLOGIAS DE PRUEBAS DE PENETRACIÓN DE ETHICAL HACKING

Por medio de este estudio comparativo de cada una de las principales metodologías con respecto a las etapas del Ethical Hacking, para poder determinar las diferencias, semejanzas, debilidades y fortalezas.

10.1 Similitudes:

A continuación se enlistaran las similitudes de las metodologías de nuestro estudio:

- Según las necesidades de la organización, se determina los tipos de pruebas que se debe realizar y los servicios que serán revisados.
- Se debe obtener el permiso de la alta gerencia de la organización para realizar la prueba de penetración.
- Se debe especificar las obligaciones y limitaciones del pentester.
- Se debe definir los alcances de las pruebas, se establece los límites de la prueba en términos de acciones y de los resultados esperados.
- Se debe especificar los criterios y los procedimientos a realizar en caso
- Se tiene que preparar un documento legal de la prueba de penetración, en la cual se indique las reglas, las condiciones y todos los aspectos legales de las pruebas que se pretende realizar.
- Creación de un contrato de confidencialidad.
- Realizar la identificación de los requisitos de cumplimiento de seguridad del cliente.

- Si se desea realizar algún tipo de entrevista, encuesta, se debe primeramente proporcionar las preguntas y deben ser aprobadas por el gerente o el comité de la empresa, para así luego de ser aprobadas se pueden ser aplicadas.
- Especificar los niveles de acceso a los sistemas y/o red.
- Especificar el hardware, software que el equipo que hará las pruebas van a utilizar.
- Si se llega a hacer contratos se debe explicar claramente los límites y los peligros de cada prueba de seguridad como parte del contrato
- Si llegase a haber el caso de hacer las pruebas vía remotamente, el contrato debe incluir de donde debe partir el análisis por su dirección, dirección IP y también su número de contacto.
- Todos los contratos deben tener los nombres de contacto de emergencia y sus respectivos numero telefónicos.

11. CONCLUSIONES

- El analizar las principales metodologías de pruebas de penetración mediante Ethical Hacking, permite identificar los aspectos relevantes para tener en cuenta a la hora de establecer la seguridad de la información sólida.

- La seguridad informática permite analizar la funcionalidad que comprende el análisis de la organización. La segregación de funciones y gestión de las actividades de procesamiento de datos, también los sistemas informáticos, donde busca la adecuación de los mismos a los fines que fueron diseñados.

- La buena gestión de la seguridad informática sea en pequeñas o grandes empresas o ya sea en un los documentos de una persona, se traduce en asegurar toda la información, en todos los aspectos o en todos áreas que comprende la empresa o equipo personal.

- A medida que aumenta la demanda en el conocimiento del aseguramiento de la información por las constantes innovaciones en los ataques de hackers, es importante tener en cuenta que metodologías son útiles conociendo sus debilidades y/o fortalezas.

- Es importante que las empresas sin importar su régimen comercial le puedan garantizar a todos sus clientes y/o usuarios la información que ellos están suministrando este en un lugar seguro, ya sea en la iniciación de algún servicio o cualquier servicio que soliciten datos personales, donde se garantice que esos datos no lleguen a personas

- Con el estudio a profundidad de las principales metodologías de Ethical Hacking, permite que las personas estén más enteradas sobre su funcionamiento, y el entorno de las aplicaciones.

12. RESULTADOS

Los resultados logrados mediante el desarrollo del presente trabajo de grado, cumple básicamente en documentar y concientizar a las personas, a la empresas sin importar su régimen económico y a los administradores de tecnología acerca de la importancia que tiene la implementación de cualquier metodología para realizar Ethical Hacking con el fin de proteger su información.

BIBLIOGRAFIA

(s.f.). Admin. Educación Financiera. [En línea]. Coltefinanciera, s.f. [Citado 26-mayo-2018]. Disponible en internet: https://www.coltefinanciera.com.co/educacion-financiera/habeas-data.

(s.f.). Alexander Verdesoto. Utilización de Hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones. Escuela Politécnica Nacional, 2007. [Citado 25-mayo-2018]. Disponible en inte.

(s.f.). Alexander Verdesoto. Utilización de Hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones. Escuela Politécnica Nacional, 2007. [Citado 25-mayo-2018]. Disponible en inte.

(s.f.). Anonimo, Hacking Etico. [En linea]. Corporacion Unificada Nacional de Educacion Superior, s.f. [Citado 26-mayo-2018]. Disponible en internet. https://auditoria2017.wordpress.com/hacking-etico/.

(s.f.). Anónimo, Hacking etico101: Como hacer profesionalmente en 21 días o menos. [En línea]. Biblia del programador, 2017. [Citado 26-mayo-2018]. Disponible en internet: https://www.bibliadelprogramador.com/2017/06/hacking-etico-101-como-hackear.html.

(s.f.). Anonimo. [En Linea]. DragonJAR. (s.f.) [Citado 25-mayo-2018]. Disponible en Internet: //www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de testeo-de-seguridad.xhtml.

(s.f.). Anonimo. ¿Qué es el hackig etico y para que sirve?. [En linea] SocialeTic. (s.f.).[Citado 25-Mayo-2018]. Disponible en Internet: https://www.socialetic.com/que-es-el-hacking-etico-y-para-que-sirve.html.

(s.f.). Anonimo. Acciones que son consideradas un delito informático en Colombia. [En línea].Tus Abogados y Contadores, 2018. [Citado 1-Noviembre-2018]. Disponible en Internet: https://tusabogadosycontadores.co/blog/acciones-que-son-consideradas-un-delito-informa.

(s.f.). Anónimo. INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK (ISSAF). [En Línea]. Open Information Systems Security Group OISSG, s.f. [Citado 1-noviembre-2018]. Disponible en Internet: http://www.oissg.org/issaf.html.

(s.f.). Anónimo. Metodología ISSAF. [En Línea]. Prezi, 25 de Marzo de 2015. [Citado 1-noviembre-2018]. Disponible en Internet: https://prezi.com/5ssonumqypgo/metodologia-issaf/.

(s.f.). Anónimo. Metodologia y Frameworks de testeo de la seguridad de las aplicaciones. [En Línea]. Marco de Desarrollo de la Junta de Andalucía, s.f. [Citado 1-noviembre-2018]. Disponible en Internet: http://www.juntadeandalucia.es/servicios/madeja/sites/defau.

(s.f.). Anónimo. OWASP Top10. [En Línea].WIKIPEDIA, 01 de Noviembre de 2018. [Citado 1-noviembre-2018]. Disponible en Internet: https://es.wikipedia.org/wiki/OWASP_Top_10.

(s.f.). Anonimo. Pruebas de penetración y hacking ético. [En línea]. Secure Information Technologies. 2008. [Citado 25-Mayo-2018]. Disponible en internet. https://secureit.com.mx/pruebas-de-penetracion-y-hackeo-etico/.

(s.f.). Anonimo. Seguridad informatica. [En linea]. Seguridad Informaticas MR. (s.f.). [Citado 25-Mayo-2018]. Disponible en Internet: https://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA.

(s.f.). Anónimo. Sobre OWASP. [En Línea]. OWASP, 11 de noviembre de 2014. [Citado 1-noviembre-2018]. Disponible en Internet: https://www.owasp.org/index.php/Sobre_OWASP.

(s.f.). Anónimo. Sobre OWASP. [En Línea]. OWASP, 11 de noviembre de 2014. [Citado 1-noviembre-2018]. Disponible en Internet: https://www.owasp.org/index.php/Sobre_OWASP.

(s.f.). Anonimo. Test de Intrusion. [En línea].Internet Security Auditors ISecAuditors, S.f. [Citado 1-Noviembre-2018]. Disponible en Internet: https://www.isecauditors.com/test-de-intrusion.

(s.f.). Anonimo.La usurpación de identidad. [En Línea]. LEGALITAS, 2015. [Citado 1-noviembre-2018]. Disponible en internet: https://www.legalitas.com/pymes-autonomos/actualidad/articulos-juridicos/contenidos/La-usurpacion-de-identidad.

(s.f.). Anonimo.Que son los Script. [En Linea]. Culturacion. (s.f.). [Citado 25-Mayo-2018]. Disponible en Internet: http://culturacion.com/que-son-los-scripts/.

(s.f.). Anonimo.Seguridad informatica es una vulnerbilidad. [En linea]. CodeJobs, 2012. [Citado 25-Mayo-2018].Disponible de Internet: https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo. Obtenido de https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

Avila, D. L. (Noviembre de 2011). *Repositorio Uisrael*. Obtenido de http://repositorio.uisrael.edu.ec/bitstream/47000/164/1/UISRAEL-EC-SIS-378.242-397.pdf

Bortnik, S. (s.f.). *Revista de Universidad Nacional Autonoma de Mexico*. Obtenido de https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

(s.f.). Braulio Fernando Ortiz. ¿Hacking Ético para detectar fallas en la seguridad informática en la intranet del gobierno provincial de Imbabura e implementar un sistema de gestión de seguridad de la información (SGCI), basado en la Norma ISO/IEC 27001:2005. Un.

Caluña, A. A. (2011). *Repositorio ESPOCH*. Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/1726/1/98T00005.pdf

(s.f.). Colaboradores Enter.co. El hacking Etico y su importancia para las empresas. [En Linea]. Enter.co, 2014. [Citado 25-mayo-2018]. Disponible en internet: http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/.

(s.f.). Council Of Europe. Convenio sobre la ciberdelicuencia. [En Linea]. OAS, 2001. [Citado 26-mayo-2018]. Disponible en Internet: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

Digital, C. D. (3 de Diciembre de 2013). *YouTube*. Obtenido de https://www.youtube.com/watch?v=VUtYjgLSAsg

ENTER.CO. (28 de Febrero de 2014). Obtenido de http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/

(s.f.). ESCOBAR, Javier; RAMIREZ, Luis; ASPRINO, Omar. Integridad y Seguridad en los Sistemas de Bases de Datos. [En linea]. FACYT, s.f. [Citado 01-Noviembre-2018]. Disponible en internet: http://eduteka.icesi.edu.co/gp/upload/1275d0253997d62e90e9a7f6a5f107cc.pdf.

(s.f.). Escuela Politécnica Nacional. Utilización de Hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones. Alexander Verdesoto, 2007. [Citado 25-mayo-2018]. Disponible en inte.

Ethical Hack. (28 de Mayo de 2017). Obtenido de http://ehack.info/tipos-de-pruebas-de-penetracion/

Flores Rojano, J. A. (01 de Noviembre de 2018). METODOLOGÍA PARA REALIZAR HACKING ÉTICO EN BASES DE DATOS PARA POSITIVA COMPAÑÍA DE SEGUROS S.A EN LA CIUDAD DE BOGOTÁ. Bogota, Colombia.

Freeman, R. (s.f.). Freeman, R. Ethical hacking what is it and why would i need it [En linea]. It Governance, 2016.[Citado 25-Mayo-2018]. Disponible en :

https://www.itgovernance.co.uk/blog/ethical-hacking-what-is-it-and-why-would-i-need-it/.

Giraldo, B. (2016 de Noviembre de 2016). *B-SECURE*. Obtenido de https://www.b-secure.co/blog/ethical-hacking-mas-alla-de-una-guia-tecnica

Gomez Santiago, M. A., Venegas Tamayo, C. D., & Yañez Hernandez, V. (2010). *Instituto Politecnico Nacional*. Obtenido de Escuela Superior de Computo: https://viclab.files.wordpress.com/2010/11/docfinal_pub.pdf

Guzman, I. S. (Noviembre de 2016). *Universidad Del Claustro De Sor Juana*. Obtenido de http://www.ucsj.edu.mx/pdf/EticaHackerSeguridadVigilancia.pdf

Hernandez, J. A. (2015). *Ciber Security Group*. Obtenido de http://ucys.ugr.es/download/taller1/Taller1_Intro_hacking.pdf

(s.f.). HERNANDEZ, Lirida. Hacking Etico para Dispositivos Móviles Inteligentes. Monterrey, 2012, 227p. Trabajo de Grado (Maestro en Ciencias en Tecnologías de Información). Instituto Tecnológico y de Estudios Superiores de Monterrey. Programa de Graduados de la .

(s.f.). http://repositorio.utn.edu.ec/bitstream/123456789/4332/1/04%20RED%20045%20TESIS.pdf.

(s.f.). J.Alfocea. Ciberdelitos: Robo de identidad, Phishing y Spamming. [En línea].Delitos Informaticos.com, 2015. [Citado 1-Noviembre-2018]. Disponible en Internet: https://delitosinformaticos.com/04/2015/delitos/ciberdelitos-robo-identidad-phishing-spamming.

(s.f.). J.Alfocea.Ciberdelitos: Robo de identidad, Phishing y Spamming. [En línea].Delitos Informaticos.com, 2015. [Citado 1-Noviembre-2018]. Disponible en Internet: https://delitosinformaticos.com/04/2015/delitos/ciberdelitos-robo-identidad-phishing-spamming.

(s.f.). Jayanthi Manikandan. Who’s an Ehical Hacking? [En línea]. Simplilearn, 10-Octubre- 2018. [Citado 1-Noviembre-2018]. Disponible en Internet: https://www.simplilearn.com/roles-of-ethical-hacker-article.

(s.f.). Las amenazas sobre los sistemas informáticos como la que representan usuarios que pueden usurpar la personalidad de usuarios autorizados para acceder y manipular indebidamente los datos de las empresas ha llevado que el tratamiento de los temas relacionad.

(s.f.). LOPEZ LOPEZ, Agustin. Estudio de Metodologías para Pruebas de Penetración a Sistemas Informáticos, México D.F, 2011, 123, Trabajo de Grado (Estudio de Metodologías para Pruebas de Penetración a Sistemas Informáticos). Instituto Politécnico Nacional. Depar.

(s.f.). Maggio, S. Actividades de monitoreo de seguridad interna y externa. [En linea]. Techlandia, s.f. [Citado 25-mayo-2018]. Disponible en internet: https://techlandia.com/actividades-monitoreo-seguridad-interna-externa-info_194844/.

(s.f.). Maiken Menendez Mendez. Ethical hacking: Test de intrusion. Principales Metodologías. [En línea]. Monografías, S.f. [Citado 1-Noviembre-2018]. Disponible en Internet: https://www.monografias.com/trabajos71/ethical-hacking-test-intrusion-metodologias/ethic.

(s.f.). MENDAÑO, Luis. Implementación de técnicas de hacking ético para el descubrimiento y evaluacion de vulnerabilidades de la red de una cartera de estado. Quito, 2016. 246p. Trabajo de Grado (Ingeniero en Electronica y Telecomunicaciones). Escuela Politecni.

MIeres, J. (12 de Noviembre de 2010). *CEH*. Obtenido de http://www.it-docs.net/ddata/863.pdf

(s.f.). Munevar John.Los Niños del Sexo! Pornografia Infantil en Internet. [En línea]. Semana. ,2002. [Citado 1-Noviembre-2018]. Disponible en Internet: https://www.semana.com/vida-moderna/articulo/los-ninos-del-sexo-pornografia-infantil-internet/50667-3.

(s.f.). Murillo Garzon Yeimy Camila. Delitos Informaticos y Entorno Juridico Vigente en Colombia. [En línea]. camaleo,sf. [Citado 1-Noviembre-2018]. Disponible en Internet: https://es.calameo.com/read/005340712f89c4b6bc86d.

(s.f.). OPEN INFORMATION SYSTEMS SECURITY. Information Systems Security Assessment Framework (ISSAF) draft 0.2.1. [En línea]. [Consultado el 1 de Noviembre 2018]. Consultado en: http://www.oissg.org/files/issaf0.2.1.pdf.

(s.f.). Ortega, B. M. Auditoria de sistemas de informacion. Gestiopolis.[En Linea]. 2012. [Citado 25-Mayo-2018]. Disponible en Internet: https://www.gestiopolis.com/auditoria-de-sistemas-de-informacion/.

Rizzo, J. A. (2013). *Repositorio Puce*. Obtenido de repositorio.puce.edu.ec/bitstream/handle/22000/11352/TESIS-PUCE- Rizzo Raza Jeniffer.pdf?sequence=1

Rojas, E. F. (s.f.). *Universidad Piloto de Colombia.* Obtenido de http://polux.unipiloto.edu.co:8080/00002050.pdf

Roopkumar, B. K. (Diciembre de 2014). *Louisiana State University*. Obtenido de https://digitalcommons.lsu.edu/cgi/viewcontent.cgi?article=4237&context=gradschool_theses

Salcedo, N. E. (3 de Octubre de 2012). *Prezi.com*. Obtenido de https://prezi.com/8xeq7tpsieyb/tecnicas-de-ethical-hacking/

Sandoval Mendez, L. C., & Vaca Herrera, A. E. (Mayo de 2013). *Repositorio espe*. Obtenido de https://repositorio.espe.edu.ec/bitstream/21000/6483/1/T-ESPE-047094.pdf

Seguridad Informatica. (27 de Junio de 2007). Obtenido de https://seguinfo.wordpress.com/2007/06/27/¿que-es-nmap/

(s.f.). Seguridad Informática. ¿Qué es Nmap?. [En línea]. Seguridad Informatica, 2007. [Citado 25-Mayo-2018]. Disponible en Internet: https://seguinfo.wordpress.com/2007/06/27/¿que-es-nmap/.

Seguridad para todos. (6 de Octubre de 2011). Obtenido de http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

(s.f.). UNAD. Obtenido de Alternativas para Grado-ECBTI. [En línea]. Universidad Abierta y a Distancia, s.f. [Citado 1-Noviembre-2018]. Disponible en Internet: https://academia.unad.edu.co/ecbti/oferta-academica/alternativas-para-grado.

(s.f.). Victor S. Manzhirova. Los ocho delitos informáticos más comunes. [En Línea]. Tu Experto.com, 2015. [Citado 1-noviembre-2018]. Disponible en internet. https://www.tuexperto.com/2015/09/12/los-ocho-delitos-informaticos-mas-comunes/.

(s.f.). www.owasp.org. OWASP Top10-2017. [En Línea].OWASP, sf. [Citado 1-noviembre-2018]. Disponible en Internet: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.

(s.f.). www.owasp.org. OWASP Top10-2017. [En Línea].OWASP, sf. [Citado 1-noviembre-2018]. Disponible en Internet: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.