ESTADO DEL ARTE ETHICAL HACKING

Docente

Osman Gonzalo Ferrer Marín

Estudiantes

John Jairo Pinto Gonzales

Samil Leonel Sanchez Acevedo

Fundación Universitaria Inpahu

Facultad ingeniería

Ingeniería de Software

Semillero de Investigación CiberSec

Bogotá Colombia

2019

Índice

Contenido

Resumen

El objetivo del presente proyecto es la implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades, las computadoras y todo dispositivo que use internet en todo el mundo son susceptibles de ser atacadas por crackers o hackers capaces de comprometer los sistemas informáticos y robar información valiosa, o bien borrar una gran parte de ella. Esta situación hace imprescindible conocer si estos sistemas y redes de datos están protegidos de cualquier tipo de intrusiones, los sistemas de información y los datos que estos almacenan, son actualmente los activos más valiosos de cualquier organización. El vertiginoso crecimiento y uso de las tecnologías de la información y las telecomunicaciones, trae consigo la aparición de agentes (internos o externos) que pueden aprovechar vulnerabilidades en dichos sistemas

Es así que se han implementado una serie de medidas a nivel de seguridad informática para blindar todos aquellos dispositivos existentes en las grandes organizaciones. Una de esas medidas se ha ejecutado a través del Ethical Hacking, mediante el cual es posible detectar el nivel de seguridad interno y externo de los sistemas de información de una organización, esto se logra determinando el grado de acceso que tendría un atacante con intenciones maliciosas a los sistemas informáticos con información crítica. Mediante el uso de las técnicas utilizadas por los ciber delincuentes, se puede evaluar la efectividad de los controles de seguridad establecidos para proteger la información.

Una vez identificadas todas las brechas de inseguridad informática, los expertos en esta modalidad de seguridad han diseñado una serie de estrategias y métodos para blindarse ante un inminente ataque a sus diferentes sistemas informáticos, lográndose el compromiso de toda una organización para que su operación no se vea afectada o comprometida ante eventos inseguros.

Palabras clave: Hacking ético, delito informático, ciber crimen, seguridad informática, hackers, crackers.

Abstract

The objective of this project is the implementation of ethical hacking techniques for the discovery and evaluation of vulnerabilities, computers and the entire device that use the internet worldwide are likely to be attacked by crackers or hackers that can compromise computer systems and steal valuable information, or delete a large part of it. This situation makes it essential to know if these systems and data networks are protected from any type of intrusion, the information systems and the data they store are currently the most valuable assets of any organization. The vertiginous growth and use of information and telecommunications technologies, brings the appearance of agents (internal or external) that may have vulnerabilities in these systems

Thus, a series of measures have been implemented at the level of computer security to shield all those devices devices in large organizations. One of these measures has been executed through Ethical Hacking, through which it is possible to detect the level of internal and external security of an organization's information systems, this is achieved by determining the degree of access that an attacker with malicious intentions has to computer systems with critical information. By using the techniques used by cyber criminals, you can evaluate the modification of security controls established to protect information.

Once all the gaps in computer insecurity have been identified, experts in this security technology have designed a series of strategies and methods to shield against an imminent attack on their different computer systems, recording the commitment of an entire organization for its operation not to be seen. affected or committed to unsafe events

.

Keywords: Ethical hacking, cybercrime, cybercrime, computer security, hackers, crackers.

Introducción

Colombia es un país donde la seguridad en sus diversas formas ha empezado a tomar importancia y conciencia en las altas direcciones de las empresas públicas y privadas, pero la mayoría no le ha dado la importancia real a los Sistemas de Seguridad Informática.

En Colombia se ha generado un crecimiento agigantado de los medios informáticos, su ubicación y disposición brindan la facilitad a las empresas de que todos sus procesos interactúen al unísono, facilitando la organización de la información personal y empresarial, ocasionando que se abra una infinidad de posibilidades para que los delincuentes busquen formas de conseguir datos de vital importancia para los usuarios, como lo son el acceso a claves bancarias, correos electrónicos, información sensible personal y empresarial, debido en su mayoría a causa de la instalación de software maliciosos en los computadores, celulares o cualquier otro dispositivo.

A pesar de la existencia de departamentos de informática y TIC en las empresas, muy pocas han implementado medidas de Seguridad en los sistemas informáticos tendientes a blindarlas ante posibles y eventuales ataques informáticos por hackers especializados.

En la Gestión Integral de Riesgos y conforme a eventos que han ocurrido a nivel interno en las empresas, se han detectado una serie de brechas en la Seguridad de los sistemas informáticos. Es así como los expertos en Seguridad Informática generaron una metodología denominada Hacking Ético, con el fin de identificar aquellas vulnerabilidades y brechas que representen riesgos a la seguridad de los sistemas informáticos empresariales.

Todos estos antecedentes y sus consecuencias inmediatas, ha generado que los expertos en Seguridad Informática se pregunten si las empresas poseen las herramientas adecuadas y fiables que las blinden ante estos posibles eventos.

Como consecuencia de estos eventos inesperados y adversos, se genera la necesidad de identificar las herramientas en Seguridad Informáticas que ayudan a blindar a las empresas ante ataques cibernéticos, los cuales para su oportuno tratamiento en primera instancia y para

contextualizar a las empresas, se inicia por definir la terminología relacionada con la Seguridad Informática, se continúa mostrando antecedentes reales sobre sobre la inseguridad informática a nivel nacional y se describen los métodos de Hacking Ético y Seguridad en los sistemas informáticos usados en las empresas del Sector Industrial

Todo esto redunda en la identificación de métodos y estrategias que blinden a las empresas ante ataques cibernéticos, procurando evitar, neutralizar o mitigar estos posibles eventos.

Dicho lo anterior y para que una organización pueda minimizar la probabilidad de pérdidas de activos de información por causa de la exposición a amenazas, se hace necesario el uso de herramientas como Sistemas de Gestión de la Seguridad de la Información, análisis de riesgos, gestión de vulnerabilidades, hacking ético, entre otras

1. FUNDAMENTOS TEÓRICOS

Este capítulo describe los fundamentos teóricos sobre los diferentes temas necesarios para el desarrollo del presente proyecto, tales como: seguridad informática, hacking ético: tipos de pruebas de penetración, tipos de hackers, fases del hacking ético. Se realizará una descripción de las herramientas de análisis de vulnerabilidades, así como se presenta un resumen de tres metodologías de hacking ético.

1.1.SEGURIDAD INFORMÁTICA[1]

La seguridad informática surge de la necesidad de proteger todos los elementos críticos que forman parte de un sistema de información que son: todos los datos, el hardware y software.

La seguridad informática no es un producto que se pueda adquirir, a la vez no puede ser considerado como un servicio, simplemente se debe considerar como un proceso clave para el rendimiento óptimo de una organización.

Si se toma a la seguridad como un proceso, este consiste en mantener un nivel aceptable de riesgo, por lo tanto, la seguridad informática es el proceso para asegurar que los recursos de la red sean usados para el fin que fueron creados y a la vez garantizar el acceso restringido a la información.

La seguridad informática tiene como objetivo la protección de la infraestructura de una red, en especial la información contenida o que circula por la misma; por lo tanto, se puede decir que es un conjunto de métodos, protocolos, herramientas, estándares, políticas orientados a proteger la privacidad de los datos y por ende minimizar los posibles riesgos de alteración, modificación o reemplazo de la información.

---

[1] Referencias:

Jara, H., y Pacheco, F. G. (2012). *Ethical hacking 2.0*. (1ª ed.). Buenos Aires: Fox Andina. Sandoval Méndez, L., y Vaca Herrera, A. (2013). *Implantación de Técnicas y Administración de Laboratorio para Investigación de Ethical Hacking*. Tesis de Ingeniería. Escuela Politécnica del Ejército, Ecuador.

Los elementos fundamentales de la seguridad informática son:

- La confidencialidad, para garantizar que solo las personas autorizadas tienen acceso a la información.
- La disponibilidad, para garantizar que los usuarios autorizados tengan acceso a la información en el momento que se requiera.
- La integridad, para asegurar que la información no ha sido adulterada en el camino por personas no autorizadas, y así garantizar la exactitud y totalidad de la información.
- La autenticidad, para garantizar el origen de la información.
- Protección de la información, para reducir las probabilidades de un evento inesperado mediante la aplicación de controles.

Un activo de información es un recurso o bien económica propiedad de una empresa considerado significativo ya que puede contener importante información. En el proceso de determinar el valor de cada activo intervienen cinco factores que son[2]:

- Vulnerabilidad: es la existencia de debilidades en el sistema, diseño o errores en implementación que pueden incitar a comprometer la seguridad del sistema inesperada e indeseablemente.
- Amenaza: es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño sobre los elementos de un sistema de información. Los cuatro tipos básicos de operación de las amenazas son:
    - Interrupción, hace referencia al impedimento de la comunicación entre dos entidades, lo que atenta directamente a la disponibilidad.
    - Intercepción, se da cuando los datos que son transmitidos en una comunicación entre dos entidades pueden ser vistos por un tercero, atenta contra la confidencialidad
    - Modificación: involucra a una tercera entidad entre los dos puntos principales de una comunicación, permitiéndole modificar la información que se transmiten en ambas direcciones, atenta contra la integridad.

---

2 Baltazár, J.M., y Campuzano, J.C. (2011). *Diseño e Implementación de un Esquema de Seguridad Perimetral para Redes de Datos*. Tesis de Ingeniería. Universidad Nacional Autónoma de México, México.

- Fabricación: es muy similar a la modificación, solo que en ese caso la información transmitida es completamente generada por una tercera entidad, atenta contra la integridad.

- Riesgo: Un riesgo está definido como la probabilidad de que una amenaza explote una vulnerabilidad, además si una amenaza explota una vulnerabilidad se lleva a cabo un ataque.
- Ataques: es un asalto en la seguridad del sistema que esta derivada desde una amenaza. Un ataque es cualquier acción que viola la seguridad.
- Control: se define como una medida de protección empleada, un control es un dispositivo, acción, procedimiento o técnica que elimina o reduce una vulnerabilidad.

1.2.HACKING ÉTICO[3]

1.2.1. Introducción al Hacking Ético

El crecimiento progresivo del uso de la tecnología ha traído muchas ventajas a todos los usuarios de internet, hoy en día se tienen muchas aplicaciones en línea con lo cual ya no es necesario realizar trámites físicamente; pero a la vez este uso de aplicaciones o servicios que una organización ofrece a los usuarios ha llamado la atención de delincuentes informáticos, los cuales están más organizados, y también van adquiriendo día a día habilidades más especializadas para lograr sus objetivos y obtener mayores beneficios.

---

[3] Referencias:

Jara, H., y Pacheco, F. G. (2012). *Ethical hacking 2.0*. (1ª ed.). Buenos Aires: Fox Andina. Tori, Carlos. (2008). *Hacking Ético*.(1ª ed.). Rosario: El autor.

Certified Ethical Hacker Review Guide. Recuperado de: http://www.it-docs.net/ddata/863.pdf Reyes, Alejandro. (2010). *Ethical Hacking*. Recuperado de: *http*://www.seguridad.unam.mx/descarga.dsc?arch=2776

A medida que la tecnología ha avanzado los ataques o intrusiones pasaron de ser una simple ralentización de un equipo a causar daños mayores (daños de sistemas, robo de información, fraude informático, entre otros.) y con importantes pérdidas económicas. Para los administradores de las redes esto causa un desafío de seguridad por lo que en un intento por frenar estos daños

restringen los accesos, pero a la vez esto conlleva a que los delincuentes informáticos utilicen ataques más dañinos y estructurados.

Es por ello que la seguridad de toda empresa es esencial para mantener protegidos todos los datos, sistemas y servicios. La información que fluye de una organización pueden ser divulgadas perdiendo confidencialidad de la misma. Es así que muchas organizaciones, optan por contratar expertos para implementar técnicas de intrusiones bajo un ambiente controlado con el fin de conocer cómo se puede infiltrar en la red un atacante real, esta simulación permite encontrar brechas en la seguridad, las cuales pueden ser usadas para manipular información o suplantar identidades. Como resultado de estas pruebas, los administradores podrán realizar mejoras en las configuraciones, accesos e incluso un rediseño para reparar las fallas.

Hacking ético es un conjunto de técnicas que se utiliza para evaluar la seguridad de una red, medir la estrategia de defensa contra vectores de ataques[4] reales, mejorar la seguridad de los sistemas informáticos e identificar las vulnerabilidades de la red para luego analizarlos, medir su nivel de riesgo y recomendar soluciones apropiadas antes de que ocurra pérdida o robo de información.

Se puede decir que una definición completa y concisa de hacking ético es la del autor Alejandro Reyes Plata, que explica lo siguiente:

El objetivo fundamental del Ethical Hacking (hackeo ético) es explotar las vulnerabilidades existentes en el sistema de "interés" valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc. Con la intención de ganar acceso y "demostrar" que un sistema es vulnerable, esta información es de gran ayuda a las organizaciones al momento de tomar las medidas preventivas en contra de posibles ataques malintencionados. Dicho lo anterior, el servicio de Ethical Hacking consiste en la simulación de posibles escenarios donde se reproducen ataques de manera

[4] Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.

controlada, así como actividades propias de los delincuentes cibernéticos, esta forma de actuar tiene su justificación en la idea de que: "Para atrapar a un intruso, primero debes pensar como intruso" (Reyes, 2010, p. 1).

Así mismo, se puede decir que una definición muy acertada de hacker ético es la del autor Pekka Himanen en su libro "La ética del hacker y el espíritu de la era de la información", que explica lo siguiente:

En el centro de nuestra era tecnológica se hallan unas personas que se autodenominan hackers. Se definen a sí mismos como personas que se dedican a programar de manera apasionada y creen que es un deber para ellos compartir información y elaborar software gratuito. No hay que confundirlos con los crackers, los usuarios destructivos cuyo objetivo es el de crear virus e introducirse en otros sistemas: un hacker es un experto o un entusiasta de cualquier tipo que pude dedicarse o no a la informática. La ética del trabajo para el hacker se funda en el valor de la creatividad, y consiste en combinar la pasión con la libertad. El dinero deja de ser un valor en sí mismo y el beneficio se cifra en metas como el valor social y el libre acceso, la transparencia y la franqueza (Himanen, 2002, p. 2).

De aquí que los valores fundamentales de un hacker ético sean: pasión, libertad, conciencia social, verdad, anti-corrupción, igualdad social, libre acceso a la información, accesibilidad, actividad, creatividad, curiosidad, interés, preocupación responsable, entre otros.

1.2.2. Tipos de Hackers

- Hacker de sombrero negro o crackers

  Son las hackers maliciosos o delincuentes informáticos, conocidos como crackers, estas personas buscan continuamente romper las seguridades de un sistema de información para provocar daños con beneficios personales y/o monetarios. Estos delincuentes informáticos por lo general buscan el camino de menor resistencia, ya sea por alguna vulnerabilidad, un error humano o cualquier tipo de fallo en la seguridad.

- Hacker de sombrero gris

  Son aquellos que dependiendo de las circunstancias trabajan en ocasiones de manera ofensiva y otras de manera defensiva, ocasionalmente superan los límites de la legalidad.
- Hacker de sombrero blanco

  Son aquellos que utilizan sus habilidades con fines defensivos, de manera que en base a sus destrezas pueden localizar amenazas e implementan contramedidas
- Hacker Ético

  Los hackers éticos son los profesionales de seguridad con amplios conocimientos y habilidades, los cuales realizan ataques a los sistemas informáticos en nombre de los propietarios, esto en busca de fallos de seguridad con la finalidad de proporcionar un informe con todas las vulnerabilidades encontradas y posibles remediaciones.

1.2.3. Tipos de Pruebas de Penetración

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

- Pruebas de penetración con objeto: se buscan vulnerabilidades en elementos específicos de los sistemas informáticos críticos de la organización.
- Pruebas de penetración sin objeto: esta prueba consiste en examinar la totalidad de los componentes de los sistemas informáticos presentes en la organización.
- Pruebas de penetración ciega: se utiliza únicamente la información pública disponible. Esta prueba de penetración trata de simular los ataques de un ente externo a la organización.
- Pruebas de penetración informadas: aquí se utiliza la información privada, otorgada por la organización acerca de sus sistemas informáticos. En este tipo de pruebas se trata de simular ataques realizados por usuarios internos de la organización que tienen determinado acceso a información privilegiada.

- Pruebas de penetración externas: son realizadas desde lugares externos a las instalaciones de la organización. El objetivo de esta prueba es evaluar los mecanismos perimetrales de seguridad informática de la organización.
- Pruebas de penetración internas: es realizada dentro de las instalaciones de la empresa con el objetivo de evaluar las políticas y los mecanismos internos de seguridad de la organización.

1.2.4. Modalidades de Hacking Ético

- Hacking ético externo caja blanca: la organización nos facilita información de la infraestructura para poder realizar las pruebas, normalmente direcciones IP. El resultado es un informe de todas las vulnerabilidades halladas, así como un conjunto de recomendaciones para solucionar cada una de ellas.
- Hacking ético externo caja negra: principalmente es igual que la modalidad de caja blanca, con la diferencia que la organización no facilita ningún tipo de información. Esta modalidad es la que se lleva a cabo en el desarrollo del presente proyecto.
- Hacking ético interno: se examina la red desde adentro, para hacer frente a la amenaza de intento de intrusión, bien por un empleado que pueda realizar un uso indebido o una persona con acceso a los sistemas o un hacker que hubiera conseguido penetrar en la red.

1.2.5. Fases del Hacking Ético

Un ataque se lleva a cabo mediante cinco fases, conocido también como el círculo del hacking, los cuales son reconocidos por *Certified Ethical Hacker*[5]- Certificado Hacker Ético:

[5] El Certificado Hacker Ético es una certificación profesional proporcionada por el Consejo Internacional de Comercio Electrónico (EC-Council).

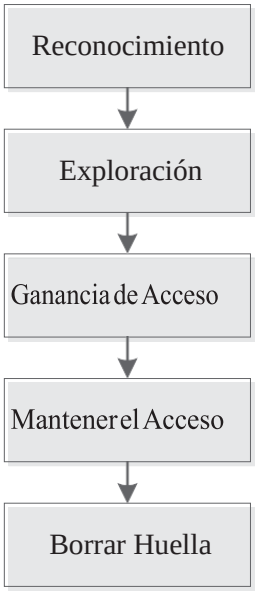


Figura 1.1 Fases del hacking ético

1.2.5.1.1. Reconocimiento

Es la fase de preparación en la cual se busca recolectar toda la información esencial del objetivo mediante el uso de diferentes herramientas y técnicas. Existen dos tipos de reconocimiento que son:

1.2.5.1.2. Reconocimiento Pasivo

El reconocimiento pasivo implica la recolección de la información sin tener un contacto directo o conocimientos particulares del blanco a atacar. Este tipo de reconocimiento puede ser tan simple como vigilar un edificio para ver la entrada y salida de los empleados de la organización. Sin embargo, este tipo de reconocimiento se lo hace a través de la web, en busca de información sobre una organización o una persona.

1.2.5.1.3. Reconocimiento Activo

El reconocimiento activo implica la recolección de la información mediante el contacto directo con el objetivo, esto implica un sondeo de la red para descubrir direcciones IP's, hosts, servicios que se ejecutan en la red. Este reconocimiento aumenta el riesgo de ser detectado.

El reconocimiento activo como el pasivo son de gran importancia, debido a la información que se obtiene.

Esta fase es en la que normalmente les toma más tiempo a los hackers ya que de esta depende la estrategia que se utilizará para realizar los siguientes pasos. Por lo general es relativamente fácil descubrir qué tipo de servidores web se están utilizando, así como los sistemas operativos que emplea una organización. Esta información permite encontrar alguna vulnerabilidad relacionada con la versión del sistema operativo y explotar la debilidad para obtener acceso al sistema.

1.2.5.1.4. Exploración (Escaneo)

Esta etapa depende de la información obtenida en la fase de reconocimiento para explorar una red y lanzar un ataque mediante la identificación de vulnerabilidades. Las herramientas que suele usarse en esta fase pueden incluir: escaneo de puertos, mapeadores de red, barridos, escáner de vulnerabilidades.

1.2.5.1.5. Ganancia de Acceso

En esta fase es donde realmente entra el desempeño de un Hacker, ya que aquí es donde las vulnerabilidades encontradas en las etapas anteriores son explotadas para tener acceso a un sistema. En esta etapa el hacker puede escalar privilegios para obtener un completo control del sistema, así los sistemas intermedios que están conectados a la red también se encuentran comprometidos.

Los ataques pueden ser a nivel de: sistema operativo, red, aplicaciones web, destrezas o mediante el aprovechamiento de configuraciones por defecto o mal configuradas.

Algunos tipos de ataques pueden ser: desbordamiento de búfer (Buffer Oveflow), denegación de servicio (DoS Denial of Service), secuestro de sesión (Session hijacking), romper o adivinar claves usando varios métodos como ataques de fuerza bruta o ataques diccionarios (Password cracking), ataques Man-in-the-middle.

1.2.5.1.6. Mantener el Acceso

Una vez que se ha conseguido el acceso al sistema comprometido lo que se busca es mantener ese acceso para futuras intrusiones o ataques, esto se puede realizar mediante el uso de puertas traseras (backdoors), troyanos o rootkits[6]. En esta etapa el hacker puede usar algunas herramientas como sniffers para capturar todo el tráfico de la red incluyendo sesiones de Telnet y FTP.

En esta etapa se puede tener la habilidad de subir, bajar, modificar o manipular cualquier tipo de archivos, alterando el funcionamiento de las aplicaciones y configuraciones de los sistemas operativos.

Todos los sistemas comprometidos se pueden utilizar para futuros ataques.

1.2.5.1.7. Borrado de Huellas

Una vez que el hacker ha ganado el acceso lo que hace, es descubrir y destruir toda la evidencia de sus actividades, esto con el efecto de mantener el acceso y seguir usando el sistema comprometido, para eliminar evidencias de la violación al sistema y/o para evitar acciones legales.

1.2.6. Beneficios del Hacking Ético

Mediante prácticas de hacking ético es posible detectar el nivel de seguridad de una organización, las cuales son las mismas metodologías que usaría un atacante real, de esta forma se podrá medir el grado de exposición que se tiene.

Las pruebas de penetración realizadas por un hacker ético se enfocan en clasificar y comprobar las vulnerabilidades, mas no en el impacto que estas representen a la organización. De aquí que el hacking ético debe ser un paso previo al análisis de seguridad o riesgos.

---

[6] **Rootkit** es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.

Al finalizar las pruebas de penetración los resultados son entregados mediante un documento que contiene una lista detallada de las vulnerabilidades encontradas, a la vez que se provee recomendaciones para solucionar los fallos de seguridad. Es importante la entrega de un informe tanto técnico como ejecutivo, de esta manera se garantiza que los empleados técnicos como los administrativos entiendan y tomen conciencia de los riesgos potenciales que la organización presenta y así poder tomar medidas preventivas.

Los beneficios que se obtienen al realizar un hacking ético son muchos, pero de manera general los más importantes son:

- Ofrecer un panorama muy claro acerca de las vulnerabilidades encontradas, lo cual sirve para que se puedan aplicar medidas correctivas a tiempo.
- Deja al descubierto configuraciones no adecuadas en aplicaciones instaladas en los sistemas (routers, servidores, firewall, sistemas de cómputo, switches) los cuales pueden desencadenar graves problemas de seguridad.
- Identificación de fallas en sistemas a falta de actualizaciones.
- Disminuir el tiempo de respuesta requerido para afrontar situaciones adversas.

Cabe mencionar que es muy importante tener en cuenta los aspectos legales en la realización de un hacking ético los cuales deben tenerse muy presentes tanto por las organizaciones que prestan el servicio como por quienes lo contratan, estos aspectos abarcan la confidencialidad, es decir que a la información que se obtenga de la realización de estas pruebas no se le dé un mal manejo o uso más allá de los fines previstos por las pruebas.

En lo que respeta a la organización que contrata el servicio, esta debe garantizar que la información que se provee de las pruebas de penetración es fidedigna para que los resultados sean congruentes y certeros.

1.3.METODOLOGÍAS DE HACKING ÉTICO

Aun sabiendo que la información de una empresa es el activo más valioso, existen fallos de seguridad en la administración, lo cual genera la necesidad de realizar un análisis de los sistemas y verificar si se han cerrado o mitigado las brechas de seguridad. Los encargados de tecnología o directores de área, recurren a grupos de profesionales que ejecuten un análisis de seguridad realizando diferentes pruebas y ataques controlados para poner a prueba dicha seguridad, y verificar si los sistemas son vulnerables a algún tipo de intrusión y evaluar los tiempos de respuesta de las organizaciones ante un ataque real.

Todos los datos recopilados y procesados por los profesionales encargados de realizar la evaluación de vulnerabilidades tienen como base diferentes metodologías de hacking ético hoy por hoy existentes, con el fin de mantener un orden en su ejecución sin descuidar ningún punto de la red, con una correcta y clara presentación de la información obtenida, entre las metodologías más importantes tenemos: OSSTMM, ISSAF, OWASP.

1.3.1. **OSSTMM7**

Manual de la Metodología Abierta de Testeo de Seguridad por su siglas en ingles OSSTMM (Open-Source Security Testing Methodology Manual), es una metodología de pruebas de seguridad ejecutadas en los diferentes niveles de operación.

Este proyecto inicia en el año 2000 con un crecimiento y aceptación por los canales de seguridad. Para el año 2005, OSTMM ya no es considerado solo un marco de mejores prácticas, sino que se convirtió en una metodología para asegurar la seguridad del nivel de operación. En el 2006, el OSSTMM pasa de ser un test en soluciones de firewall y routers a ser un estándar.

Hoy por hoy el ambiente de redes en las organizaciones tiende a ser cada vez más complejo y con infraestructura de diferentes tipos, con la introducción al mercado de las telecomunicaciones de soluciones como; operaciones remotas, virtualización, cloud computing, etc. Las metodologías para una evaluación de

[7] Herzog, Peter. *OSSTMM 3 Open Source Security Testing Methodology Manual, Contemporary Security Testing and analysis*. ISECOM.

vulnerabilidades tiene que ajustarse a dichos requerimientos, para lo cual la OSSTMM realizó algunos cambios en sus versiones y de esta manera cubre pruebas para diferentes ambientes o canales, los cuales son: humano, físico, inalámbrico, telecomunicaciones y redes de datos.

Este manual proporciona un marco común y un estándar permitiendo realizar paso a paso las tareas necesarias para que tanto administradores como profesionales de la seguridad lo utilicen para analizar y ejecutar pruebas de intrusión en los sistemas de redes, con el fin de evaluar los niveles de seguridad informática, y plasmar los resultados de una manera cuantificable.

Su principal propósito está centrado en proporcionar un manual científico para la caracterización precisa de seguridad operacional (OpSec), mediante el análisis y la correlación de los resultados de prueba en una forma confiable y consistente. Algo que se destaca a gran escala de este manual, es su adaptabilidad para cualquier tipo de auditoría, incluyendo pruebas de penetración, hacking ético, análisis de vulnerabilidades, análisis de seguridad, red-teaming[8], blue-teaming[9], entre otras.

El contenido del Manual OSSTMM tiene una estructura dividida por 15 capítulos, con los cuales cubre todos los requisitos necesarios para realizar un buen trabajo de evaluación y auditoría de la seguridad de la información.

Los tres primeros capítulos brindan una base teórica para nivelar conocimientos y fundamentar el contenido futuro que posee el manual, de igual manera hace referencia a la terminología principal empleada en dicho manual, como también directrices para poder aprovechar al máximo los lineamientos de la metodología, a tal punto de realizar un trabajo de un alto nivel y con resultados óptimos para la infraestructura evaluada y respetando los acuerdos planteados de ambas partes.

---

[8] Red-Teaming: prueba encubierta, en donde sólo un grupo selecto de directores sabe de ella. Esta prueba es la más real y evita se realicen cambios de última hora que hagan pensar que hay un mayor nivel de seguridad en la organización.

[9] Blue-Teaming: el personal de informática conoce sobre las pruebas.

El manual ha optado por dividir el análisis en tres clases, los cuales a su vez se dividen en 5 canales diferentes con los cuales cubren todos los frentes de vulnerabilidad que se puedan presentar, de la siguiente manera:

CLASES	CANALES	DESCRIPCIÓN
Seguridad Física (PHYSSEC)	Humano	Comprende el elemento humano de la comunicación donde la interacción puede ser física o psicológica.
	Físico	Pruebas de seguridad física donde los canales son físicos y de naturaleza no-electrónica. Comprende el elemento tangible de seguridad donde la interacción requiere esfuerzo físico o un transmisor de energía para manipular.
Seguridad del Espectro (SPECSEC)	Wireless	Comprende todas las comunicaciones, señales, y emanaciones que tienen lugar sobre el espectro electromagnético conocido. Esto incluye la seguridad de comunicaciones electrónicas (ELSEC[10]), seguridad de señales (SIGSEC[11]) y seguridad de emanaciones (EMSEC[12]).

[10] ELSEC, son las medidas para negar el acceso no autorizado a la información derivada de la intercepción y el análisis de las radiaciones de comunicaciones electromagnéticas.

[11] SIGSEC, son las medidas para proteger las comunicaciones inalámbricas de accesos no autorizados.

[12] EMSEC, son las medidas para prevenir las emanaciones de las máquinas, que de ser interceptado y analizado podría revelar información transmitida, recibida y ser manipulada o de otro modo ser procesada por equipos de sistemas de información.

CLASES	CANALES	DESCRIPCIÓN
Seguridad de Comunicaciones (COMSEC)	Telecomunicaciones	Comprende todas las redes de telecomunicaciones, digitales o analógicas, donde la interacción tienen lugar a través del teléfono establecido o líneas de la red de telefonía similar.
	Redes de Datos	Comprende todos los sistemas y redes de datos electrónicos, donde la interacción tiene lugar a través de cable establecido y líneas de la red de cable.

Tabla 1.1 Canales de la Metodología OSTMM

El manual OSSTMM maneja un modelo llamado OPSEC[13], el cual se superpone sobre los objetivos para análisis de vectores y canales, es simple de aplicar, debido a que se realiza un conteo de los controles para cada punto interactivo de acceso o confianza, algo muy importante en este manual, es la cuantificación de la superficie de riesgo, la cual se realiza por medio del RAV, esta escala de medida ayuda a cuantificar la cantidad de interacciones incontroladas con el objetivo de evaluación y es calculado por el equilibrio cuantitativo entre operaciones, limitaciones y controles, es importante aclarar que RAV, no mide el riesgo para la superficie de ataque, más bien permite su medida.

Una vez entendido el manejo del manual con sus parámetros y su terminología, dedica un capítulo a cada canal (Humano, Físico, Wireless, Telecomunicaciones, Redes de Datos), dentro del cual se revisan cuatro fases: fase de introducción, fase de interacción, fase de encuesta y fase de intervención. Cada fase presenta diferente grado de profundidad en la auditoría, pero cada uno de ellas no es menos importante que otra.

---

[13] OPSEC (seguridad operacional) es un proceso analítico que clasifica los activos de información y determina los controles necesarios para proteger estos activos.

Finalmente en el capítulo 13 podemos encontrar la presentación de reportes de auditoría de pruebas de seguridad o también conocido como STAR (Security Test Audit Report), por su siglas en inglés, con el cual se presenta un resumen ejecutivo con las actividades realizadas y plasmando los resultados obtenidos.

1.3.2. ISSAF14

Marco de evaluación de la seguridad del sistema de información, más conocido como ISSAF (Information Systems Security Assessment Framework), por sus siglas en inglés, fue desarrollado por la OISSG para cubrir las necesidades de organizaciones o empresas que se desenvuelven en un ambiente donde su información es un activo más de la empresa. Muchas empresas descuidan la seguridad de la información, tratando de alcanzar sus metas, es aquí donde OISSG enfoca sus objetivos al desarrollar ISSAF, ofreciendo nuevas capacidades de negocios con la integración de la tecnología al desarrollo de actividades empresariales.

ISSAF es un documento de referencia para la evaluación de la seguridad que estandariza los procesos de pruebas de los sistemas de seguridad, una de sus grandes diferencias con respecto a otros documentos o manuales de evaluación de vulnerabilidades, es que en este documento se encuentra no solo una guía paso a paso de cómo llevar un análisis de la seguridad sino que también facilita las herramientas que muy probablemente entregue la información necesaria para llenar las distintas plantillas de este documento, también indica el cómo y el por qué las medidas de seguridad deberían ser evaluadas.

ISSAF está dirigido a: asesores de vulnerabilidades internas o externas, responsables de la seguridad perimetral, ingenieros y consultores de seguridad, administradores de proyectos de evaluación de seguridad, administradores de redes y sistemas, técnicos y administradores funcionales, grupo de seguridad de la información.

---

[14] OISSG (Open Information Systems Security Group), *Infomation Systems Security Assessment Framework (ISSAF)* Draft 0.2.1, Date: April 30, 2006

El marco de referencia de ISSAF se encuentra desarrollado por 5 fases definidas como: planeación, evaluación, tratamiento, acreditación y mantenimiento, con lo cual estructura la gestión de la seguridad y asegura la viabilidad de compromisos orientados al trabajo, por otro lado presenta un marco de referencia para gestión de compromisos que definen acuerdos con el cliente sobre las tareas a realizar en el proyecto de análisis y explotación de vulnerabilidades, también contiene una sección de mejores prácticas que ayudan a su implementación.

Es muy importante los primeros 9 capítulos para la ejecución del proyecto de análisis debido a que los mismos hacen referencia al marco teórico, se da una visión general de la metodología ISSAF así como sus objetivos, presenta la gestión de contratos y acuerdos donde se especifican consejos claros a tomar en consideración a la hora de implementar el proyecto, se realiza una evaluación del riesgo enfocado al beneficio de la empresa evaluando sus activos y su criticidad de operación. Los capítulos 7, 8, 9 son guías de evaluación para determinar o identificar el nivel de las políticas de seguridad establecidas en las organizaciones, así mismo, presenta modelos de políticas.

En la sección de evaluación de seguridad y control técnico se implementa la metodología de pruebas de penetración, la misma que se divide en 3 fases, conformadas por:

- Fase I: Planeación y preparación.

  Esta fase comprende los pasos iniciales para realizar las pruebas: entrevistas para intercambiar información, planificación, alcance, escalada de privilegios, realización del cronograma, especificación del equipo que trabajará, tiempos de pruebas, entre otros arreglos. Todo esto con el fin de realizar el acuerdo que será firmado entre ambas partes y de esta manera tener la base de trabajo y una protección jurídica.
- Fase II: Evaluación.

  Esta fase a la vez se divide en: recopilación de la información, mapeo de la red, identificación de vulnerabilidades, penetración, ganancia de

acceso y escalamiento de privilegios, enumeración, comprometer usuarios/sitios remotos, mantener el acceso, cubrir pistas.

- Fase III: Reporte, limpieza y destrucción de huellas.

  Esta fase final consiste de un reporte bien estructurado que contenga el resumen de la gestión, alcance, herramientas utilizadas, cronograma real de las pruebas, resultados de las pruebas, así como recomendaciones para remediar los fallos encontrados. Además toda la información que se ha obtenido debe ser borrada al finalizar el trabajo así como se deberán borrar todas las huellas.

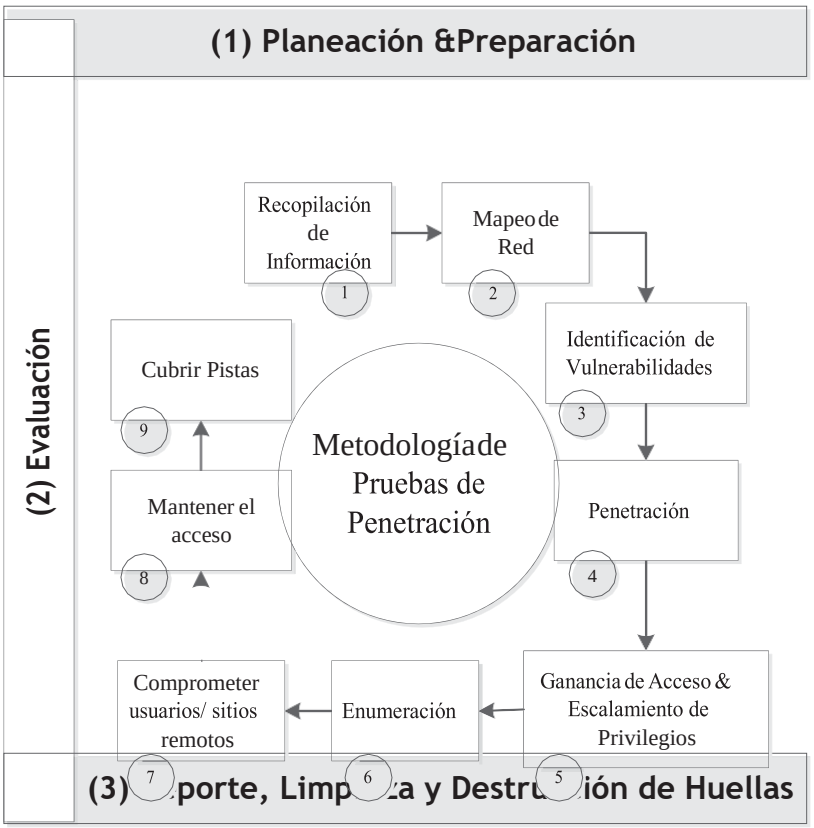


Figura 1.2 Metodología ISSAF

En la parte final del manual se realiza un análisis de la seguridad física, ingeniería social, gestión de operaciones de seguridad, gestión de cambios, concientización de la seguridad, gestión de incidentes.

1.3.3. OWASP15

El Proyecto Abierto de Seguridad de Aplicaciones Web o más conocida como OWASP (Open Web Application Security Project) por sus siglas en inglés, es un proyecto abierto a nivel mundial enfocado en mejorar la seguridad en software de aplicaciones, motivando y fomentando de esta manera a los desarrolladores independientes y desarrolladores adjudicados a alguna organización, a elaborar su trabajo brindando confiabilidad en las aplicaciones desarrolladas para el desempeño de negocios.

El mundo está lleno de aplicaciones web, y por tal razón se requiere de un estándar de desarrollo que permita llevar de manera ordenada todo el contenido de internet, si se realiza un análisis de las actividades en línea que efectúa una persona a lo largo de su vida día tras día, se puede evidenciar que la tecnología nos ha facilitado bastantes procesos, como: pago de servicios básicos, acceso a correo, trasferencias, acceso a documentación, etc., incluso se realiza todo esto desde algún aplicativo instalado en teléfono inteligente. Sin embargo, si cada usuario conociera el verdadero riesgo que conlleva utilizar estos aplicativos celulares o computacionales muy probablemente no lo utilizaría, pero tal acción se interpretaría como dar un paso atrás para el desarrollo tecnológico. Es esa la razón crucial de brindar confianza al usuario final para utilizar un programa, y aun sabiendo que los desarrolladores son personas con defectos y virtudes, es muy probable que cometan errores dentro de sus incontables líneas de código al elaborar las tan anheladas aplicaciones. Habiendo tomado este referente se nos hace racional enfocarnos en la seguridad de la información y la seguridad de los códigos fuente que ponemos a disposición del mundo.

OWASP es una comunidad abierta formada por un grupo de voluntarios apasionados por la seguridad informática dedicados a colaborar con la corrección y evolución de aplicaciones web, que relaciona los errores que normalmente se realiza a nivel de código de aplicaciones por los desarrolladores de los mismos, para evaluar los riesgos que puede generar

---

[15] OWASP Open Web Application Security Project, testing Guide 4.0, 2014 The OWASP Foundation.

estos errores a la empresa y genera un plan de corrección de las aplicaciones encontradas con riesgos.

Al momento el manual de OWASP se encuentra en la versión 4, liberada en el 2014, la misma que mejora la versión anterior en tres aspectos fundamentales:

- Implementación de la guía de desarrolladores y la guía de revisión de código, con el fin de evaluar los controles de seguridad descritos en la propia guía del desarrollador
- Introducción de cuatro nuevos capítulos y controles con un alcance de 87.
- Finalmente alienta a la comunidad a compartir sus experiencias y evaluaciones con el fin de mejorar y ampliar la base del conocimiento

La guía OWASP se encuentra formada por 5 capítulos para su interpretación e implementación: prefacio, características de la guía de pruebas, marco de pruebas de OWASP, pruebas de seguridad de aplicaciones web y reportes.

Para un mejor entendimiento del manual, se introduce un capítulo que sirve como marco teórico el mismo que cubre aspectos importantes además de indicar que es la guía OWASP, también cubre fundamentos importantes de la seguridad informática, gestión de riesgos, pruebas de penetración, entre otras.

Se dedica un capítulo que se enfoca principalmente al personal del área de desarrollo, enfocándose a presentar una guía de un modelo genérico de desarrollo, el cual los lectores deberían seguirlo de acuerdo al proceso de la organización, este modelo se divide en 5 faces de implementación: antes de comenzar el desarrollo, durante la definición y diseño, durante el desarrollo, durante la implementación, mantenimiento y operaciones.

La metodología dedica un capítulo muy importante a la hora de realizar pruebas de seguridad sobre las aplicaciones que se encuentran en producción o que están en proceso de sacar a producción, el mismo tiene como objetivo probar y explicar cómo las pruebas de vulnerabilidades se evidencian dentro de la aplicación debido a la deficiencia con controles de identificación de seguridad. Este capítulo describe 12 subcategorías de la metodología de pruebas de penetración de aplicaciones web, cada una de estas subcategorías

posee la referencia necesaria para ejecutar las pruebas que se presentan, como son: un resumen, como ejecutarlas, técnicas, herramientas, entre otros, ítems que nos ayudarán a realizar las pruebas de seguridad a las aplicaciones de una manera precisa y concisa. Estas subcategorías son:

- Pruebas de introducción y objetivos.
- Pruebas para la recolección de la información.
- Pruebas para la configuración.
- Pruebas de gestión de incidentes.
- Pruebas de autenticación.
- Pruebas de autorización.
- Pruebas de gestión de sesiones.
- Pruebas de validación de ingreso.
- Pruebas de error de código.
- Pruebas para cifrado débil.
- Prueba lógica de negocios.
- Pruebas de clientes – sitio.

Finalmente tendremos un capítulo que nos guía para elaborar los reportes obtenidos durante nuestra fase de pruebas o el proceso de evaluación, es la parte más importante de nuestro trabajo debido a que es aquí donde detallamos toda la información obtenida para entregar a las autoridades pertinentes, por ende, este reporte tiene que ser lo más claro posible y resaltar todo el riesgo encontrado a lo largo de la evaluación.

1.3.4. Comparación de las Metodologías

Para la comparación de las metodologías se consideran los parámetros tomados como referencia en el proyecto de titulación "Análisis de riesgos y vulnerabilidades de la infraestructura tecnológica de la secretaria nacional de gestión de riesgos utilizando metodologías de ethical hacking", las cuales se describen a continuación:

[16] Acosta Naranjo, O.A. (2013). *Análisis de riesgos y vulnerabilidades de la infraestructura tecnológica de la secretaria nacional de gestión de riesgos utilizando metodologías de ethical hacking*. Tesis de Ingeniería. Escuela Politécnica Nacional, Ecuador.

CARACTERÍSTICAS	METODOLOGÍAS		
	OSSTMM	ISSAF	OWASP
Permite realizar pruebas y análisis de seguridad a cualquier sistema informático.	SI	SI	NO
Establece requisitos previos para la evaluación.	NO	SI	NO
Define áreas de alcance.	NO	SI	SI
Contiene plantillas para realizar las pruebas.	SI	SI	SI
Detalla técnicas para cada prueba.	NO	SI	SI
Contiene pruebas de ejemplos y resultados.	NO	SI	SI
Recomienda herramientas para cada prueba.	NO	SI	SI
Presenta procesos de análisis y evaluación de riesgos.	SI	SI	SI
Define dimensiones de seguridad a evaluar.	SI	NO	NO
Enumera y clasifica las vulnerabilidades encontradas.	NO	SI	NO
Genera reportes e informes.	SI	SI	SI
Presenta contramedidas y recomendaciones.	NO	SI	NO
Contiene referencias a documentos y enlaces externos.	NO	SI	SI
Presenta Evaluación a aplicaciones Web.	SI	SI	SI
Mantiene actualizaciones al día.	SI	NO	SI
Es un estándar.	SI	NO	SI
Presenta acuerdos de confidencialidad.	SI	SI	NO

Tabla 1.2 Comparación de Metodologías.

Se puede observar en la tabla 1.2, que cada metodología presenta parámetros importantes, por lo que para la implementación del presente proyecto se considera sugerencias de cada una dependiendo de la fase que se realice.

1.4.PROTOCOLOS SIMPLES PARA GESTIÓN DE REDES17

Entre los protocolos para gestión de redes podemos nombrar los siguientes:

- Protocolo de control de transmisión (TCP)

  Es una de los principales protocolos de la capa de transporte del modelo TCP/IP. Este protocolo garantiza que los datos serán entregados a su destino sin errores y en el mismo orden en que se transmitieron, también proporciona mecanismos para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto del puerto.

  TCP está documentado en el RFC 793 y sus principales características son:

  - ✓ Orientado a la conexión: permite que dos máquinas que están comunicadas controlen su estado de la transmisión.
  - ✓ Operación Full-Duplex: una conexión TCP es un par de circuitos virtuales, cada uno en una dirección. Solo los dos sistemas finales sincronizados pueden usar la conexión.
  - ✓ Revisión de errores: una técnica de checksum es usada para verificar que los paquetes no estén corruptos.
  - ✓ Acuses de recibo: sobre el recibido de uno o más paquetes, el receptor regresa un acuse de recibo al transmisor indicando que recibió el paquete.
  - ✓ Control de flujo: si el transmisor está desbordando el buffer del receptor por transmitir demasiado rápido, el receptor descarta paquetes. Los acuses fallidos que llegan al transmisor le alertan para bajar la tasa de transferencia o dejar de transmitir.

---

[17] Villalobos B., V. A. (2014). Protocolos simples para gestión de redes. Recuperado de: http://es.slideshare.net/EquipoSCADA/unidad-vi-tema-8-scada

- ✓ Servicio de recuperación de paquetes: el receptor puede pedir la retransmisión de un paquete, si el paquete no es notificado como recibido.

- Protocolo de internet (IP)

  El protocolo IP es parte de la capa de Internet del conjunto de protocolos TCP/IP. Es uno de los protocolos de internet más importantes ya que permite el desarrollo y transporte de datagramas de IP (paquetes de datos), aunque sin garantizar su entrega. En realidad, el protocolo IP procesa datagramas IP de manera independiente al definir su representación, ruta y envío.

  Las principales características de este protocolo son:

  - ✓ Protocolo no orientado a conexión.
  - ✓ Fragmenta paquetes si es necesario.
  - ✓ Direccionamiento mediante direcciones IP lógicas de 32 bits.
  - ✓ Si un paquete no es recibido, este permanecerá en la red mediante un tiempo finito.
  - ✓ Realiza el "mejor esfuerzo" para la distribución de paquetes.
  - ✓ Tamaño máximo de paquetes de 65635 bytes.

  Solo se realiza verificación por suma al encabezado del paquete, no a los datos que éste contiene.

- Protocolo de control de transmisión / Protocolo de internet (TCP/IP)

  El protocolo de red TCP/IP se podría definir como el conjunto de protocolos básicos de comunicación de redes, que permite la transmisión de información en redes de ordenadores.

  En algunos aspectos TCP/IP representa todas las reglas de comunicación para internet, y se basa en la noción de dirección IP, es decir, en la idea de brindar una dirección IP a cada equipo de la red para poder enrutar paquetes de datos.

Debido a que el conjunto de protocolos TCP/IP originalmente se creó con fines militares, está diseñado para cumplir una cierta cantidad de criterios, entre ellos:

- ✓ Dividir mensajes de paquetes.
- ✓ Usar un sistema de direcciones.
- ✓ Enrutar datos en la red.
- ✓ Detectar errores en la transmisión de datos.

- Protocolo UDP

UDP (User Datagram Protocol) es un protocolo no orientado a conexión de la capa de transporte del modelo TCP/IP. Se limita a recoger el mensaje y enviar el paquete por la red. Para garantizar la llegada el protocolo exige a la máquina de destino del paquete que envió un mensaje (un eco), si el mensaje no llega se envía de nuevo.

UDP es un protocolo sencillo que implementa un nivel de transporte orientado a datagramas, tiene las siguientes características:

- ✓ No es orientado a conexión.
- ✓ No es fiable por tres razones: pueden perderse datagramas, pueden duplicarse datagramas y pueden desordenarse datagramas.

- Protocolo de resolución de dirección (ARP)

El protocolo ARP tiene un papel clave entre los protocolos de capa de internet relacionados con el protocolo TCP/IP, ya que permite que se conozca la dirección física de una tarjeta de interfaz de red correspondiente a una dirección IP, por eso se lo llama protocolo de resolución de direcciones.

Para que las direcciones físicas no puedan conectar con las direcciones lógicas, el protocolo ARP interroga a los equipos de la red para averiguar sus direcciones físicas y luego crea una tabla de búsqueda entre las direcciones lógicas y físicas en una memoria caché.

- Protocolo simple para la administración de red (SNMP)

Es un protocolo que permite administrar y diagnosticar una red. Es un estándar de administración de redes basado en un conjunto de protocolo TCP/IP, que permite la consulta a los diferentes elementos que constituyen una red.

El sistema de administración de red se basa en dos elementos principales: un supervisor y agentes. El supervisor es el terminal que le permite al administrador de red realizar solicitudes de administración. Los agentes son entidades que se encuentran al nivel de cada interfaz. Ellos conectan a la red los dispositivos administrados y permiten recopilar información sobre los diferentes objetos.

Toda la información de los equipos está en una base de datos MIB (Management Information Base). Esta base de datos con estructura de árbol es recogida por el agente del protocolo simple para la gestión de red y comunicada al sistema de administración de red.

2. UNA NUEVA EXPERIENCIA EN SEGURIDAD HACKING ÉTICO*

Situación actual de Colombia ante la seguridad informática

En la actualidad Colombia ha ocupado en puesto muy crítico en lo relacionado a las vulnerabilidades detectadas y encontradas en sus plataformas informáticas, la mayoría de las empresas colombianas han sido y están expuestas a una gran cantidad de amenazas que vulneran la seguridad de sus sistemas informáticos, se genera una incertidumbre de cuan seguras pueden estar sus plataformas, redes informáticas, es ahí donde se le empieza a dar importancia y a mantener la seguridad de los sistemas informáticos, ya que si se vulnera su seguridad traerá como consecuencias ataques informáticos que pueden poner en riesgo la integridad de su información, imagen y bienes de la empresa u organización.

Es de vital importancia que las empresas u organizaciones opten por implementar medidas que contrarresten cualquier ataque a sus sistemas informáticos, tomen las medidas de seguridad pertinentes a fin de dar continuidad a sus negocio, que no se vean afectadas por manos y mentes criminales, dañinas, donde su fin en unos casos puede ser causar daño y estragos colocando a la empresa en un estado crítico o donde otros solo quieren causar un impacto social, pero que a la mirada de otros como personas, empresas, organizaciones, el mismo gobierno, puede generar un impacto negativo en contra de la organización así no haya sido su intensión que se ocasionara o en su defecto si existía una responsabilidad por no haber acatado sugerencias o implementado medidas de seguridad y control a fin de evitar ataques a sus sistemas informáticos.

Los ataques informáticos siempre generarán traumatismos a la información sensible de cada organización, puesto que puede verse afectada en su integridad, modificada inadecuadamente, convertirse en pública, teniéndose en cuenta que puede ser información privilegiada tanto de la organización como de sus clientes, proveedores, contratistas, personas en misión, cooperados, etc., que al dejarse expuesta puede originar brechas más profundas en la organización que serán aprovechas por los ciberdelincuentes.

* Para la elaboración del documento se tomó como referencia la asignatura nuevas tendencias.

En Colombia se ha generado un crecimiento agigantado de los medios informáticos, su ubicación y disposición brindan la facilitad a las empresas de que todos sus procesos interactúen al unísono, facilitando la organización de la información personal y empresarial, ocasionando que se abra una infinidad de posibilidades para que los delincuentes busquen formas de conseguir datos de vital importancia para los usuarios, como lo son el acceso a claves bancarias, correos electrónicos, información sensible personal y empresarial, debido en su mayoría a causa de la instalación de software maliciosos en los computadores, celulares o cualquier otro dispositivo

Diferentes medios de comunicación manifiestan la vulnerabilidad de los sistemas informáticos de las empresas, mostrando en una forma real las consecuencias que estos presentan a las organizaciones.

> Los riesgos y amenazas a la seguridad informática de las empresas son evidentes. Solo en Colombia, el año pasado el Departamento de Delitos Informáticos de la Policía Nacional recibió 7118 denuncias por parte de víctimas de delitos informáticos, evidenciando un aumento del 40% con respecto al 2014. Las pérdidas económicas derivadas por estos actos representan al país alrededor del 0,14%, según el Banco Mundial (2014) del PIB Nacional, es decir, cerca de US$500 millones aproximadamente. (Manrique Horta. 2016. Diariamente en Colombia hay 10 millones de ataques informáticos. Diario del Huila).

Es evidente que Colombia y sus empresas han dejado al descubierto una infinidad de brechas de seguridad informática, las cuales son aprovechadas por los ciberdelincuentes.

Como consecuencia de todos estos antecedentes, las empresas colombianas han implementado mecanismos para protegerse de posibles ataques que afecten su integridad, su estabilidad económica y social, siendo conscientes de que están frente a una globalización tecnológica donde su información privada y sensible puede ser hurtada y dársele un mal manejo por posibles delincuentes informáticos que se encuentran diariamente en el mundo cibernético.

Actualmente el ciberdelincuente para obtener información personal o financiera de las personas cuenta con herramientas para acceder a todo el historial de su víctima, dentro de estas se encuentra el software malicioso malware, el cual por sus características informáticas puede estar oculto en un archivo adjunto de un correo electrónico, el cual una vez abierto empiezan a ejecutar una serie de funciones programadas en el sistema operativo de este software y en muchas ocasiones se vuelve casi invisible para el antivirus de la empresa. Este es uno de los tantos métodos que puede utilizar el ciberdelincuente para acceder a la información de la empresa o de las personas que allí laboran. De esto se hablará más adelante una vez se relacionen algunos métodos usados por los ciberdelincuentes.

Es un hecho que Colombia se ha ganado un puesto privilegiado, primero por ser un país donde se presentan a diaria un sinfín de ataques ciberdelincuentes a empresas nacionales, pero también como el primer o segundo país del Latinoamérica que más ataques cibernéticos ocasionan a otros países.

EL Periódico el Espectador, Sección de Tecnología, redacta un informe dando a conocer lo siguiente

> Colombia lidera lista de ataques informáticos en países de habla hispana. Cuatro de los cinco ataques más comunes son realizados por Colombia. En el informe anual realizado por Digiware, primer integrador de seguridad informática de Latinoamérica, se reveló que Colombia es el país de habla hispana que genera más ataques informáticos en Latinoamérica, luego siguen Argentina, Perú, México y Chile. (Colombia lidera lista de ataques informáticos. 2014. Periódico el Espectador).

Son varios los antecedentes que enlutan a nuestro país ocasionados por delitos informáticos, es así que se muestra otra noticia, donde evidencia estos hechos

> En Colombia las cifras de delitos informáticos van en aumento. Colombia es actualmente el tercer país en Latinoamérica donde más se cometen. Se calcula que 187 denuncias mensuales son interpuestas por fraude a

> diferentes bancos. Así lo reveló en los últimos días el Colegio Colombiano de Juristas, que explicó que la lista de esta modalidad de delito la encabezan Brasil y México. Algunos de los delitos electrónicos que más se presentan en el país y que, según expertos de la Fiscalía, van en aumento son acceder a bases de datos de bancos u otras entidades sin permiso, sustraer archivos de computadores, ingresar a redes sociales y correos ajenos y clonar tarjetas bancarias. (En Colombia las cifras de delitos informáticos van en aumento. 2102. El País).

3. NORMATIVIDAD VIGENTE EN SEGURIDAD INFORMÁTICA

Colombia en el ámbito de la seguridad informática ha dejado entrever que es muy vulnerable ante los ataques de la delincuencia informática, las brechas identificadas son ocasionadas por descuido, impericia, negligencia y falta de una cultura de seguridad informática, no se han establecido unos protocolos de seguridad eficaces y eficientes que de verdad lleven a muchas empresas colombianas a blindarse ante los ataques por parte de los delincuentes informáticas y/o a cómo enfrentar estas situaciones.

A pesar de existir una norma técnica colombiana como es la NTC-ISO/IEC 27001 Tecnología de la información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información (SGSI) y una ley como la 1273 de 2009 Ley de Delitos Informáticos en Colombia, se sigue evidenciando que a pesar de tener a la mano todas estas ayudas y herramientas legales, no invierten ni se concientizan de la necesidad de hacer uso de ellas. Se demuestra que las empresas son reactivas más no preventivas ante todas estas situaciones que afectan la seguridad, integridad de sus activos intangibles como es la información sensible. Son muchas las empresas y gobiernos que han caído por no tomar acciones preventivas que lleven a blindar y contrarrestar acciones negativas que van en detrimento de la estabilidad y bienes de la empresa y sus asociados de negocio, no sin dejar de mencionar que el principal afectado es la persona como tal, el ser humano que está al frente y es el soporte y piedra angular de ese conglomerado empresarial.

El Gobierno Colombiano con el fin de ejercer control en el sector de las tecnologías de información y Comunicaciones ha emanado una serie de normas legales de estricto cumplimiento, de las cuales se nombrarán algunas de relevancia e importancia a nivel empresarial y personal.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "De la Protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales. (Ley 1273. 2009. De la protección de la información y de los datos. Ministerio del interior y de justicia. República de Colombia. Gobierno Nacional. Bogotá.)

El 30 de julio de 2009 el entonces presidente Álvaro Uribe Vélez decretó la ley 1341 la cual le garantiza a Colombia un marco normativo por el cual se modifica el código penal, se crea un nuevo régimen tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones

> Artículo 1°. Objeto. La presente ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes

> del territorio nacional a la Sociedad de la Información. (Ley 1341. 2009. Políticas públicas que regirán el sector de las tecnologías de la información y las comunicaciones. Ministerio del Interior y de Justicia. República de Colombia. Gobierno Nacional. Bogotá).

En el año 2012 el Gobierno Nacional Decreto la Ley Estatutaria 1581 del 17 de octubre de 2012 por la cual se dictan disposiciones generales para la protección de datos personales Habeas Data en Colombia

Artículo 1°. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. (Ley Estatutaria 1581. 2012. Protección de datos personales Habeas Data en Colombia. República de Colombia. Gobierno Nacional. Bogotá.).

El Gobierno Nacional el día 11 de abril de 2016 a través del Consejo Nacional de Política Económica y Social aprobó la nueva política de Seguridad Digital CONPES 3854 de 2016 que reemplaza al 3701 del 2011, en el cual se establece una política de seguridad y defensa contra posibles ataques digitales a las entidades del Estado, convirtiendo a Colombia en el primer país de Latinoamérica y uno de los primeros en el mundo, en incorporar plenamente las recomendaciones y las mejores prácticas internacionales en gestión de riesgos de seguridad digital emitidas recientemente por la Organización para la Cooperación y el Desarrollo Económicos “OCDE”. (CONPES 3854. 2016. Política Nacional de Seguridad Digital. Departamento Nacional de Planeación. República de Colombia. Bogotá).

En esta política se establecen nuevos lineamientos y directrices de seguridad digital y se tienen en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación.

El CONPES 3854 de 2016 de Seguridad Digital integra los objetivos de defensa del país en relación con la lucha contra el crimen y la delincuencia en Internet, para lo cual se centra en la implementación de cinco frentes de acción específicos, los cuales se mencionan a continuación, así:

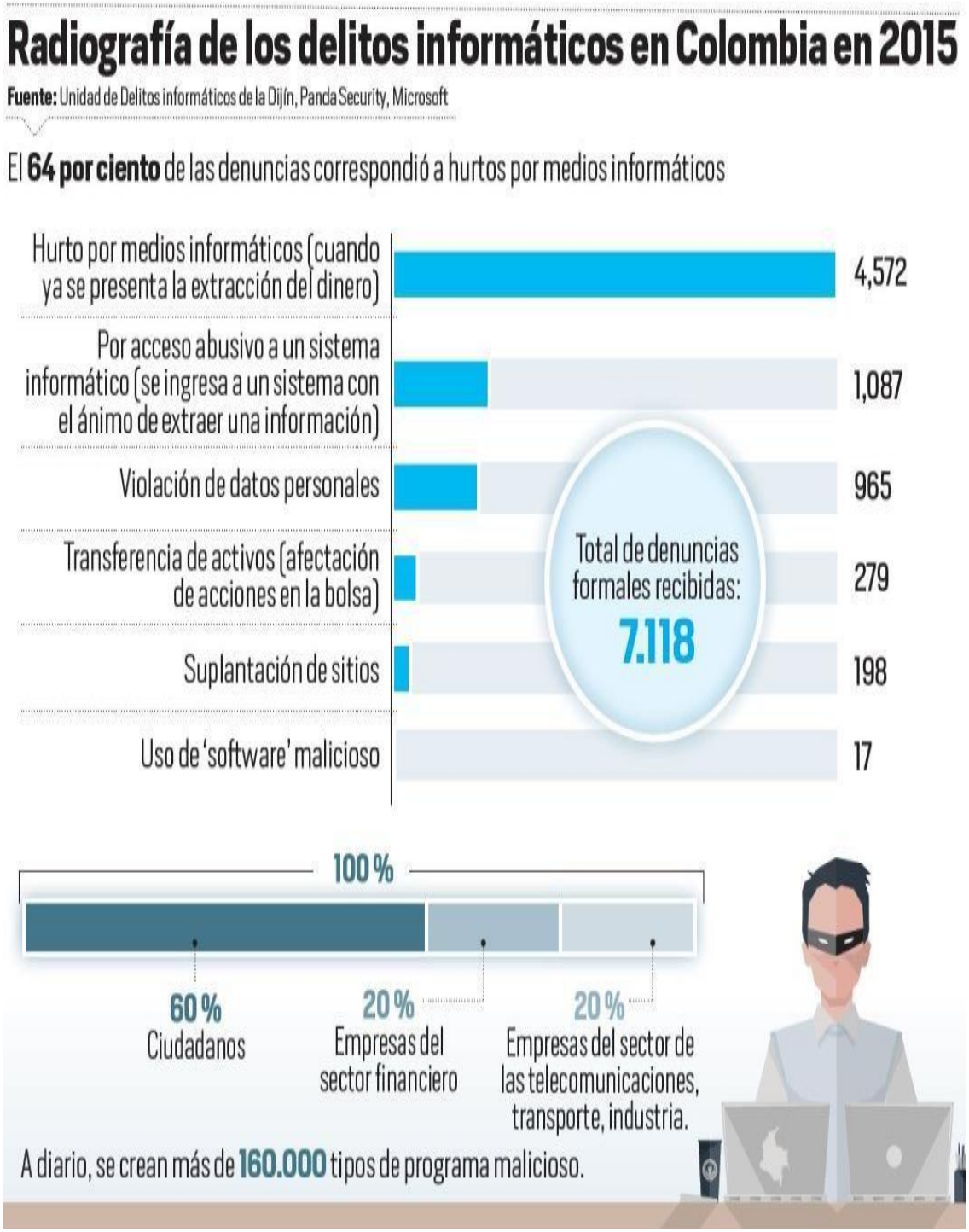
- Establecer un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos.
- Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.
- Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.
- Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.
- Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional.

Dicho lo anterior y para que una organización pueda minimizar la probabilidad de pérdidas de activos de información por causa de la exposición a amenazas, se hace necesario el uso de herramientas como Sistemas de Gestión de la Seguridad de la Información, análisis de riesgos, gestión de vulnerabilidades, hacking ético, entre otras

4. RADIOGRAFÍA DE LOS DELITOS INFORMÁTICOS EN COLOMBIA

Diferentes medios de comunicación escrita, en este caso el Periódico El Tiempo, muestra una radiografía de los delitos informáticos en Colombia en el año 2015, donde a través de unidades especializadas como la del Grupo DIJIN de la Policía Nacional, suministran información real sobre las condiciones y situación actual por la que pasa el país frente a los delitos informáticos. (Medina. (2016). En 2015, cibercrímen generó pérdidas por US$ 600 millones en Colombia. Radiografía de los delitos informáticos en Colombia en 2015. El Tiempo).

Figura No. 1: Radiografía de los delitos informáticos en Colombia en 2015.



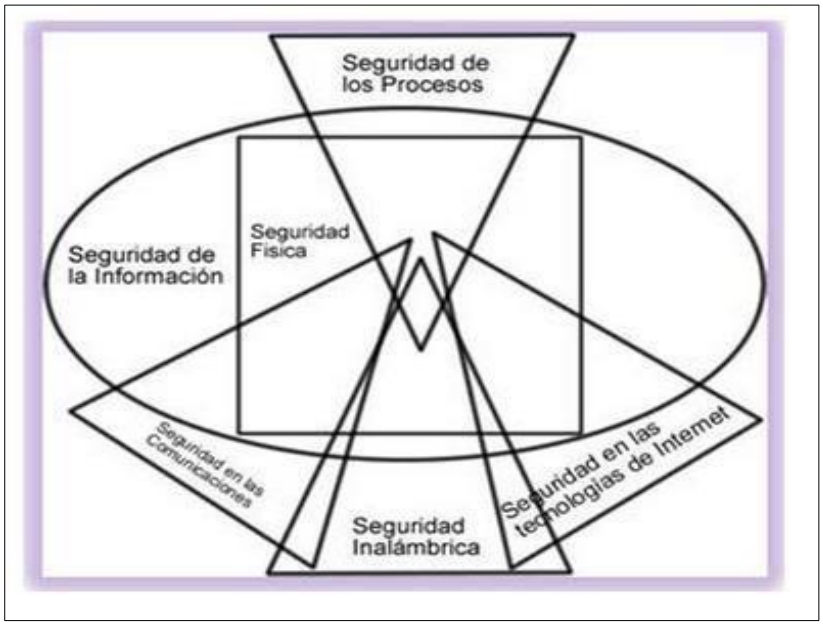
Fuente: Medina. (2016). En 2015, cibercrímen generó pérdidas por US$ 600 millones en Colombia. Fuente. El Tiempo. Recuperada de http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604

Este estudio nos muestra en forma real de cómo el hurto por medios informáticos se ha convertido en una de los delitos más comunes en Colombia. El 64% de las denuncias generadas ante autoridades judiciales soportan el actuar del ciudadano colombiano en pro de tratar de controlar este flagelo y como las personas y empresas están dejando de lado el temor a denunciar, esto no teniendo en cuenta la gran cantidad de personas y empresas que no lo hacen. La vulnerabilidad de que son objeto los sistemas informáticos en las empresas y a nivel personal, dejar entrever las brechas en seguridad informática, carencia de medidas y protocolos de seguridad que le hacen fácil al ciberdelincuente actuar sin temor.

Es así como se muestra y evidencia otras formas de cómo los ciberdelincuentes acceden a los sistemas informáticos en las empresas. Estas son: Acceso abusivo a un sistema informático, violación de datos personales, transferencia de activos, suplantación de sitios, uso de software malicioso.

Según el Mapa de Seguridad propuesto por el OSSTMM, las secciones a las cuales se aplican el hacking ético son las siguientes:

Figura No. 5: Mapa de Seguridad propuesto por el OSSTMM.



Fuente: Mapa de Seguridad propuesto por el OSSTMM: 2012. Hacking ético: mitos y realidades. Revista seguridad defensa digital | 1 251 478, 1 251 477. Seguridad cultura de prevención para TI. Recuperado de http://revista.seguridad.unam.mx/numero-12/hacking-%C3%A9tico-mitos- y-realidades

4.1. **Seguridad Física**: Las empresas han generado una serie de protocolos de seguridad física a fin de proteger sus activos informáticos, dentro de los procedimientos se encuentran:

- Revisión periódica del perímetro.
- Revisión de monitoreo.
- Evaluación de controles de acceso.
- Revisión de respuesta de alarmas.
- Revisión de ubicación.
- Revisión del entorno.

4.2. **Seguridad** de las Comunicaciones: Se crean protocolos de seguridad a fin de proteger sus telecomunicaciones digitales y analógicas y las redes de datos que se relacionan con todos los sistemas electrónicos y redes de datos cableados.

4.3. **Seguridad** Inalámbrica: Se crean protocolos de seguridad a fin de proteger todas sus comunicaciones electrónicas, señales y emanaciones de señales que se producen en el espectro electromagnético.

4.4. **Seguridad** en las tecnologías de internet: Se generan por los expertos en seguridad informática protocolos de seguridad a fin de evitar que los sistemas informáticos de la empresa sean objeto de intrusiones por parte de ciber delincuentes. Se crean barreras a través de software especializado en detectar intrusiones, antivirus confiables, pero ante todo procedimientos de control por parte de todo aquel que tenga acceso a los sistemas informáticos de la empresa. Se apoyan en pruebas de intrusión periódicas a las aplicaciones web a fin de detectar cualquier brecha o vulnerabilidad que pueda generar inseguridad a sus sistemas informáticos.

4.5. **Seguridad** del resguardo de información: Se generan formas de resguardar la información utilizando medios de almacenamiento confiables, sean a través de dispositivos o en la contratación de empresas confiables que administren su información.

4.6. **Seguridad** de los procesos: Este es uno de los métodos más representativos a nivel de la empresa, ya que se generan por parte de la empresa políticas de seguridad informáticas a modo de blindar a toda la organización ante ataques por ciber delincuentes. Se crean protocolos de seguridad informática a fin de evitar el acceso a su información privilegiada y sensible, donde

por voluntad propia o involuntariamente un empleado puede dar acceso a un ciber delincuente a los sistemas informáticos de la organización a través de medios como el teléfono, e-mail, chat, redes sociales, etc.

Las empresas colombianas y en especial las del Sector Industrial, enfrentan un reto muy importante para consolidar sus negocios y potenciar su prestigio ante clientes, proveedores, socios estratégicos, contratistas entre otros y, para lograr todo esto es blindándose ante todo ataque y vulneración a sus sistemas informáticos, generando políticas y protocolos de seguridad a fin de controlar, mitigar todo acto inseguro que genere inestabilidad y coloque en juego la continuidad de su negocio.

5. Conclusiones

En la actualidad Colombia ha ocupado en puesto muy crítico en lo relacionado a las vulnerabilidades detectadas y encontradas en sus plataformas informáticas, la mayoría de las empresas colombianas han sido y están expuestas a una gran cantidad de amenazas que vulneran la seguridad de sus sistemas informáticos.

En Colombia se ha generado un crecimiento agigantado de los medios informáticos, su ubicación y disposición brindan la facilitad a las empresas de que todos sus procesos interactúen al unísono, facilitando la organización de la información personal y empresarial, ocasionando que se abra una infinidad de posibilidades para que los delincuentes busquen formas de conseguir datos de vital importancia para los usuarios, como lo son el acceso a claves bancarias, correos electrónicos, información sensible personal y empresarial, debido en su mayoría a causa de la instalación de software maliciosos en los computadores, celulares o cualquier otro dispositivo.

Los riesgos y amenazas a la seguridad informática de las empresas son evidentes. Solo en Colombia, el año pasado el Departamento de Delitos Informáticos de la Policía Nacional recibió 7118 denuncias por parte de víctimas de delitos informáticos, evidenciando un aumento del 40% con respecto al 2014. Las pérdidas económicas derivadas por estos actos representan al país alrededor del 0,14%, según el Banco Mundial (2014) del PIB Nacional, es decir, cerca de US$500 millones aproximadamente.

Colombia en el ámbito de la seguridad informática ha dejado entrever que es muy vulnerable ante los ataques de la delincuencia informática, a pesar de existir una norma técnica colombina como es la NTC-ISO/IEC 27001 Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI) y una ley como la 1273 de 2009 Ley de Delitos Informáticos en Colombia, se sigue evidenciando que a pesar de tener a la mano todas estas ayudas y herramientas legales, no invierten ni se concientizan de la necesidad de hacer uso de ellas.

Los departamentos con menos acceso a la red han sido catalogados como uno de los más chocados y atacados por los ciberdelincuentes, no se aleja mucho de la realidad que es debido igual que muchos otros a la falta de blindajes adecuados ante este accionar delincuencial. En lo corrido de este año se han presentado en el Valle del Cauca 1700 denuncias por delitos informáticos, cifra que convirtió a este departamento en el más golpeado del país por esta modalidad delictiva.

Colombia ocupa el segundo y tercer puesto a nivel latinoamericano como uno de los países que más ciberataques ocasionan a otros países. Así como Colombia ataca a otros países, igual Colombia es el blanco predilecto de muchos otros países del mundo, más debido a las vulnerabilidades que presentan sus sistemas informáticos.

El Hacker Ético, mediante el uso de técnicas utilizadas por los ciber delincuentes, evalúa la efectividad de los controles de seguridad establecidos por las empresas para proteger su información digital sensible, el cual mediante un informe menciona e identifica los sistemas en los que se ha logrado penetrar y muestra la información sensible, confidencial obtenida.

En este medio del Hacking Ético es común escuchar sobre el Hacker de Sombrero Blanco o Caja Blanca o Hacker de Sombrero Negro o Caja Negra, que no es más que la forma legal o ilegal de cómo se obtiene información de un sistema informático o como se violenta su seguridad, con o sin autorización de los propietarios. En este caso los dueños de empresas pequeñas, medianas y grandes, por los antecedentes anteriormente mencionados y que se han visto afectados por ataques de ciber delincuentes, han optado por contratar los servicios de personas expertas en hackear sistemas informáticos (Hacker Ético), con el fin de determinar qué tan vulnerables y expuestos se encuentran sus sistemas informáticos ante ataques por parte de los ciber delincuentes.

Las empresas Colombianas y en especial las del Sector Industrial del Departamento del Valle del Cauca, enfrentan un reto muy importante para consolidar sus negocios y potenciar su prestigio ante clientes, proveedores, socios estratégicos, contratistas entre otros y, para lograr todo esto es blindándose ante todo ataque y vulneración a sus sistemas informáticos, generando políticas y protocolos de seguridad a fin de controlar, mitigar todo acto inseguro que genere inestabilidad y coloque en juego la continuidad de su negocio.

6. Referencias

Manrique Horta. (2016). Diariamente en Colombia hay 10 millones de ataques informáticos. Diario del Huila. Recuperado de http://diariodelhuila.com/economia/%E2%80%9Cdiariamente-en- colombia-hay-10-millones-de-ataques-informaticos%E2%80%9D-cdgint20160312211955155)

Colombia lidera lista de ataques informáticos. (2014). Periódico el Espectador. Recuperado de http://www.elespectador.com/tecnologia/colombia-lidera-lista-de-ataques-informaticos-paises- de-articulo-523201)

En Colombia las cifras de delitos informáticos van en aumento. (2102). El País. Recuperado de http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van- aumento)

Valle del Cauca, el departamento más golpeado por los delitos informáticos. (2013). El País. Recuperado de http://www.elpais.com.co/elpais/judicial/noticias/valle-cauca-departamento- golpeado-por-delitos-informaticos)

Delitos informáticos se han incrementado un 100% en Cali. (2015). El País. Recuperado de http://www.elpais.com.co/elpais/judicial/noticias/delitos-informaticos-han-incrementado-100- cali)

En 2015, cibercrímen generó pérdidas por US$ 600 millones en Colombia. (2016). El Tiempo. Recuperado de http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos- informaticos-se-denuncian-en-colombia/16493604

Medina. (2016). En 2015, cibercrímen generó pérdidas por US$ 600 millones en Colombia. Radiografía de los delitos informáticos en Colombia en 2015. El Tiempo. Recuperada de http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se- denuncian-en-colombia/16493604

Delitos informáticos se han incrementado un 100% en Cali. (2015). El País. Recuperado de http://www.elpais.com.co/elpais/judicial/noticias/delitos-informaticos-han-incrementado-100- cali)

En 2015, cibercrímen generó pérdidas por US$ 600 millones en Colombia. (2016). El Tiempo. Recuperado de http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos- informaticos-se-denuncian-en-colombia/16493604

Cortes Ignacio, Del Castillo Arturo. (2013). Cibercrímen. Encuesta de fraude en Colombia 2013. KPMG Forensic Services. KPMG en Colombia. Pp 33. Recuperado de https://www.kpmg.com/CO/es/IssuesAndInsights/ArticlesPublications/Documents/Encuesta%20de%20Fraude%20en%20Colombia%202013.pdf

El hacking ético y su importancia para las empresas. (2014). Enter.Co. Recuperado de (http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/

Guevara. (2012). Hacking ético: mitos y realidades. Revista seguridad defensa digital | 1 251 478, 1 251 477. Seguridad cultura de prevención para TI. Recuperado de http://revista.seguridad.unam.mx/numero-12/hacking-%C3%A9tico-mitos-y-realidades)

Medina. (2016). En 2015, cibercrímen generó pérdidas por US$ 600 millones en Colombia. Radiografía de los delitos informáticos en Colombia en 2015. El Tiempo. Recuperada de http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se- denuncian-en-colombia/16493604

Ataque cibernético de Colombia a otros países. Día 22 de septiembre de 2016. 07:41 horas. Tercer puesto. Recuperada de http://map.norsecorp.com/#/?geo=latAmer

Ataques cibernéticos de Colombia hacia otras naciones. Septiembre 22 de 2016 07:47 horas. Tercer lugar. Recuperado de http://map.norsecorp.com/#/?geo=latAmer

Ataques de Colombia hacia otras naciones. Septiembre 22 de 2016 08:22 horas. Segundo lugar. Recuperado de http://map.norsecorp.com/#/?geo=latAmer

Mapa de Seguridad propuesto por el OSSTMM. (2012). Hacking ético: mitos y realidades. Revista seguridad defensa digital | 1 251 478, 1 251 477. Seguridad cultura de prevención para TI. Recuperado de http://revista.seguridad.unam.mx/numero-12/hacking-%C3%A9tico-mitos-y- realidades

Ley 1273. 2009. De la protección de la información y de los datos. Ministerio del interior y de justicia. República de Colombia. Gobierno Nacional. Bogota

Ley 1341. 2009. Políticas públicas que regirán el sector de las tecnologías de la información y las comunicaciones. Ministerio del Interior y de Justicia. República de Colombia. Gobierno Nacional. Bogotá.

Ley Estatutaria 1581. 2012. Protección de datos personales Habeas Data en Colombia. República de Colombia. Gobierno Nacional

CONPES 3854. 2016. Política Nacional de Seguridad Digital. Departamento Nacional de Planeación. República de Colombia. Bogotá