MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

Análisis de un mecanismo de seguridad informática mediante El Manual de la Metodología Abierta de Testeo de Seguridad. Caso de estudio: Institución Pública del Ecuador

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por el estudiante:
Denis Neptalí SALINAS PINEDA

Bajo la dirección de:
Rayner Stalyn DURANGO ESPINOZA

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Febrero del 2017

Análisis de un mecanismo de seguridad informática mediante El Manual de la Metodología Abierta de Testeo de Seguridad. Caso de estudio: Institución Pública del Ecuador

Analysis of a computer security mechanism through of the Open Source Security Testing Methodology Manual. Case Study: Public Institution of Ecuador.

Denis Neptalí SALINAS PINEDA[1]
Rayner Stalyn DURANGO ESPINOZA[2]

Resumen

Entre las seguridades tecnológicas que toda organización debe realizar en su infraestructura que maneja las tecnologías de la información, son las redes de datos. Esta investigación analiza y evalúa estas vulnerabilidades en tres instituciones públicas para conocer lo robusto del mecanismo de las seguridades implementadas en estas organizaciones. La recopilación de la información se efectúa aplicando dos etapas de hackeo ético que son reconocimiento y exploración. Aplicando los lineamientos del *Open Source Security Testing Methodology Manual* (OSSTMM) enfocado en las redes de datos, con la finalidad de calcular los *Risk Assessment Values* (RAV) mediante el calculador proporcionado por el *Institute for Security and Open Methodologies* (ISECOM). Los valores obtenidos de la evaluación en las tres instituciones fueron 69,3881 RAVs, 67,9729 RAVs y 60,3295 RAVs, los cuales corresponden a la seguridad actual de la Institución A, B y C respectivamente; después de aplicar estrategias de gestión de seguridad informática de acuerdo a los lineamientos planteados por la OSSTMM, los nuevos valores de nivel de seguridad actual encontrados son 77,6363 RAVs, 75,2535 RAVs y 71,9043 RAVs con esto se garantiza la confidencialidad, integridad y disponibilidad de la información.

Palabras clave: Redes de datos, OSSTMM, RAV, Hackeo Ético.

Abstract

Among the technological securities that every organization must make in its infrastructure that manages the information technologies, are the data networks. This research analyzes and evaluates these vulnerabilities in three public institutions to know the robustness of the mechanism of the securities implemented in these organizations. The collection of the information is carried out applying two stages of ethical hacking that are recognition and exploration. Applying the guidelines of the *Open Source Security Testing Methodology Manual* (OSSTMM) focused on the data networks, in order to calculate the *Risk Assessment Values* RAVs using the calculator provided by *Institute for Security and Open Methodologies* (ISECOM). The values obtained from the evaluation in the three institutions were 69.3881 RAVs, 67.9729 RAVs and 60.3295 RAVs, which correspond to the actual safety of Institution A, B and C respectively; After applying security management strategies, the new security level values are 77,6363 RAVs, 75,2535 RAVs and 71,9043 RAVs, thereby guaranteeing the confidentiality, integrity and availability of the information.

Key words Data Network, OSSTMM, RAV, Ethical Hacking.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail dsalinas@uees.edu.ec.
[2] Magíster en Sistemas de Información Gerencial. Docente de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo-Ecuador. Email: rdurango@uees.edu.ec.

INTRODUCCIÓN

Salinas Sánchez (2013) manifiesta que actualmente, en las instituciones el grado de dependencia de las redes informáticas se incrementa a un ritmo acelerado y cualquier suceso que interrumpa el normal funcionamiento de éstas, puede complicar la continuidad del servicio que se presta. Una banda de hackers rusos realizó el mayor atraco bancario en la historia, según un estudio de la firma de seguridad cibernética Kaspersky con sede en Rusia. Cientos de millones de dólares fueron robados de 100 bancos en 30 países. Kaspersky publicó un informe alarmante de una operación mundial que se infiltró en los principales bancos y convirtió los cajeros automáticos en zombis escupe-efectivo (Kaspersky Lab, 2015).

De acuerdo al reporte del 2015 de ESET Latinoamérica (2016), indica que se consideraron 3044 encuestas aplicadas en Países latinoamericanos, del cual existieron ciertas preocupaciones en las empresas encuestadas que fueron las "Vulnerabilidades de software y sistemas" con un 58% de respuestas afirmativas, "Malware" con un 54% y en el tercer puesto "Acceso indebido a la información" con un 46%. Así mismo, el reporte menciona los incidentes de seguridad que afectaron a las empresas durante el 2015 fueron "la infección por Malware" ocupa el primer lugar con el 40%, mientras que en segunda posición se ubican los casos de "Phishing" con el 16% y en tercer lugar se encuentra el "Fraude interno/externo" con el 13%. En Ecuador "la infección por Malware" se encuentra en primera posición con el 51.9% y en base a Latinoamérica, Ecuador está en tercer lugar de los países más afectados por "la infección por Malware", en segundo lugar el "Phishing" con el 24%, en relación a los países de Latinoamérica, Ecuador se encuentra en primer lugar de los países más afectados por "Phishing".

Además, es importante destacar que una de las amenazas más importantes a la red de datos es el ataque de Denegación de Servicios (DoS), el mismo que consiste en ejecutar alguna forma de agotamiento de recursos directos o indirectos sobre el objetivo a través de la generación de tráfico específico, realizando así la interrupción con un impacto negativo en la preparación y continuidad del servicio, según (Zlomislić, Krešimir, & Vlado, 2014). Otro ataque comúnmente utilizado es el denominado "Ataque de fuerza bruta", el cual es un proceso que trata de "adivinar" una contraseña, según (Pazmiño Caluña, 2012). Conti, Dragoni, & Lesyk (2016) menciona que el ataque Man-In-The-Middle (MITM) es uno de los ataques más conocidos en seguridad informática, lo que representa una de las mayores preocupaciones de los profesionales de la seguridad, se enfoca en los datos reales que fluyen entre los puntos finales, y la confidencialidad e integridad de los datos en sí.

Cabe mencionar que, cuando se implementa un sistema informático en general, no termina solamente con la instalación del hardware y software, sino, se debe seguir algunos estándares tecnológicos sugeridos como educación a los usuarios internos ya que pueden ser utilizados para penetrar al sistema, además la verificación permanente de actualizaciones del software y hardware, ya que sin estas sugerencias existe la posibilidad de que nuestro sistema informático y la red sea vulnerable ante posibles intentos de intrusión, según (Morales Bonilla, 2015). Ramírez Montañez (2015), indica que se debe considerar que las características de seguridad informática quieren decir que se debe percibir el peligro, clasificarlo y de esta manera tratar de protegerse de los ataques y de los posibles daños. Esto significa que únicamente cuando se conocen las potenciales amenazas, agresores y sus diferentes intenciones en contra de un sistema o una organización, se puede adoptar las medidas de protección adecuadas, para que no se vulneren los recursos de la información.

Por lo anteriormente mencionado es importante realizar un análisis en la seguridad informática de la Institución Pública del Ecuador, en el departamento de TIC, mediante la utilización de evaluadores de vulnerabilidades y pruebas de escaneo de puertos en las redes de datos en un ambiente controlado, basándose en los

lineamientos planteados por el *Open Source Security Testing Methodology Manual OSSTMM*, para conocer el nivel de seguridad que posee la institución específicamente en las redes de datos para posterior plantear controles con la finalidad de mejorar el nivel de seguridad de la información. Con lo anteriormente descrito se responde a las siguientes interrogantes ¿Qué tan robusto es el nivel de seguridad Informática en la Institución Pública del Ecuador en las redes de datos?, ¿Cuáles son las principales vulnerabilidades que puedan generar un mayor impacto en la Institución Pública del Ecuador de acuerdo a la categorización de la herramienta Nessus? y ¿Mejoró el nivel de seguridad actual luego de aplicar las estrategias de gestión de seguridad informática de acuerdo a los lineamientos planteados por la OSSTMM?

MARCO TEÓRICO

OSTMM 3.0

Herzog (2010) menciona que el Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM) proporciona una metodología para una prueba exhaustiva de seguridad, se refiere como una auditoría OSSTMM. Una auditoría OSSTMM es una medida exacta de la seguridad a nivel operativo, que está vacío de las hipótesis y la evidencia anecdótica. Como metodología, que está diseñado para ser consistentes y repetibles. Como un proyecto de código abierto, que permite que cualquier analista de seguridad de aportar ideas para la realización de pruebas más precisas, accionable y eficientes de seguridad. Además, se permite la libre difusión de información y la propiedad intelectual.

Una auditoría requiere de pruebas en los tres canales. Este manual disecciona estos 3 canales en 5 secciones lógicas como se muestran y se detallan en la Figura 1 y en la Tabla 1 respectivamente.

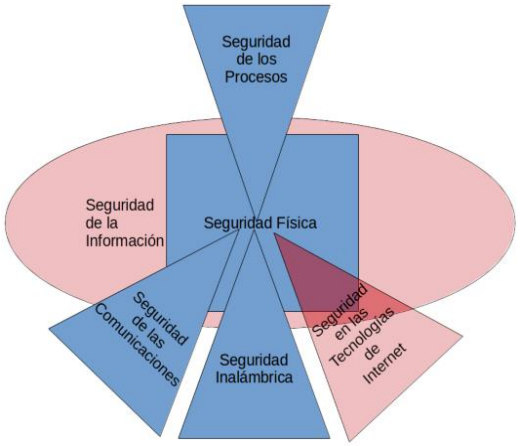

Figura 1 Alcance de la OSSTMM, (Herzog, 2010)

Clase	Canal	Descripción
La Seguridad Física (PHYSSEC)	Humano	Comprende el elemento humano de la comunicación donde la interacción es física psicológica.
	Física	Las pruebas de seguridad física donde el canal es a la vez físico y no de naturaleza electrónica.
La Seguridad del Espectro (SPECSEC)	Inalámbrica	Comprende todas las comunicaciones electrónicas, señales y emanaciones que tienen lugar sobre el espectro electromagnético conocido.
Seguridad en las Comunicaciones (COMSEC)	Telecomunicaciones	Comprende todas las redes de telecomunicación, digital o analógico, donde la interacción se lleva a cabo a través del teléfono establecido o líneas de redes telefónicas similares.
	Las Redes de Datos	Comprende todas las redes y sistemas de datos electrónicos donde la interacción se lleva a cabo a través de cable establecido y líneas de red con cable.

Tabla 1: Alcance de la OSSTMM, según (Herzog, 2010)

Con el Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM se generan ciertas métricas la cual es una medida constante que nos informa cuantitativamente de la relación de hechos que acontecen alrededor de una organización. Por analogía, en OSSTMM las métricas se usan para medir el grado de seguridad de nuestros activos. Se usan unos patrones denominados Rav (Risk Assesment Values), valores de evaluación de riesgos, según (Herzog, 2010).

Fases de la metodología

Herzog (2010) y Cruz Gavilánez (2016) mencionan que la metodología OSSTMM posee cuatro fases para que una evaluación de seguridad sea satisfactoria, estas son: *Fase de Inducción* se refiere a que el auditor inicia la evaluación entendiendo los requisitos, el alcance y las limitaciones de la auditoria, es decir estudia el entorno del activo de información**.** *Fase de Interacción* es el núcleo de la prueba de seguridad básica requiere conocer el alcance en relación con las interacciones con los objetivos transmitidos a las interacciones con los activos, en otras palabras se define el ámbito de la prueba con base de los objetivos planteados. *Fase de investigación* se trata de la información que descubre el analista, en esta fase, los diferentes tipos de valor de la información extraviada y mal gestionada como un activo se traen a la luz, dicho de otra manera, se recopila información que evidencia la mejora en la seguridad de los activos de información. *Fase de Intervención***,** estas pruebas se centran en los recursos de los objetivos, requieren en el ámbito de aplicación, esos recursos se pueden cambiar por estar, sobrecargados o murieron por causar la penetración o interrupción, es decir se enfoca en la penetración del activo de información.

Tipo de Pruebas

De acuerdo con el manual de la metodología OSSTMM existen varios tipos de pruebas los cuales son: *Blindaje o Hackeo ético* es uno de los procedimientos de exploración más utilizados, el auditor no posee ninguna información sobre el sistema que va a probar, es decir una auditoría a ciegas. *Doble Blindaje*: el auditor no tiene ninguna información del sistema que atacar, más en ese proceso el sistema no sabe que será atacado y ni qué pruebas serán realizadas. *Caja gris:* el auditor tiene poco conocimiento del sistema, en cuyo caso el sistema sabe que será atacado y qué pruebas serán ejecutadas por el auditor, con la finalidad de obtener informaciones específicas del sistema auditado. *Doble caja gris*: el auditor tiene poco conocimiento sobre el sistema que sabe que será atacado, más no tiene conocimiento de qué tipos de pruebas se aplicarán. *Tándem:* En este tipo de barrido el auditor tiene conocimiento sobre el sistema, que también tiene conocimiento que será atacado y qué procedimientos serán ejecutados en la prueba de invasión. *Inversa:* El auditor tiene conocimiento sobre lo que se va a evaluar, el sistema, no sabe que será atacado y ni qué procedimientos se utilizarán durante la prueba, según (Herzog, 2010) y (OLIVEIRA CIRQUEIRA, 2016).

Superficie de ataque

La superficie de ataque de un sistema se ha definido como el subconjunto de recursos del sistema como métodos, canales y datos; que potencialmente pueden ser utilizados por un ciberdelincuente para ejecutar un ataque, según (Manadhata & Wing, 2011).

Porosidad

Cuando se analiza el estado de la seguridad que se puede visualizar, donde existe la posibilidad de interacción y donde no lo hay. Sabemos que algunas, todas, o incluso ninguna de estas interacciones pueden ser necesarias para las operaciones. Dado que el analista de seguridad puede no saber en este momento la justificación de negocio para todos estos puntos interactivos, nos referimos a esto como porosidad. La porosidad se reduce la separación entre una amenaza y un acceso. Ésta se clasifica como uno más de 3 elementos, la visibilidad, acceso, o la confianza que describe su función en las operaciones que permite aún más los controles

adecuados que se añaden durante la fase de remediación de mejora de la protección, según (Herzog, 2010).

Controles

Herzog (2010) plantea que un control es un mecanismo que se establece sobre el activo para que influya en el impacto de las amenazas y sus efectos, cuando se requiere alguna interacción. Para obtener una verdadera protección de los activos es necesario definir una serie de controles, aunque en este aspecto se debe tener cuidado de colocar más controles de los necesarios, puesto que éstos a su vez, pueden incrementar el número de interacciones y por ende ampliar vulnerabilidad del sistema.

Controles de Clase A. De Interactividad: Los controles de la clase A, influyen directamente en la interacción en relación con la Visibilidad, Acceso y Confianza; éstos son: *Autenticación* que es un control de credenciales basados en el proceso de identificación y posteriormente autorización, *Compensación* es un control que tiene que ver con un contrato entre el propietario de los activos y su parte interactiva. *Dominación* es un control sobre todas las interacciones para mantener la protección de los activos ante un evento de una falla o corrupción, *Continuidad* es un control que asegura las interacciones ocurran únicamente de acuerdo con los procesos definidos y *Resistencia o capacidad de recuperación* es un control sobre todas las interacciones para mantener la interactividad con el activo ante un evento de corrupción o falla, (Herzog, 2010).

Controles de Clase B. De Procedimiento: Los de la clase B son usados para crear procesos defensivos, estos controles no influyen directamente en las interacciones sino más bien se encargan de proteger el activo una vez que la amenaza se presenta; son también conocidos como Controles de Proceso y son *Confidencialidad* es un control que asegura que un activo desplegado o intercambiado entre las partes interactivas no pueda ser conocido fuera de esas partes. *No Repudio* es un control que previene que el activo niegue su rol en cualquier interacción, además garantiza que ninguna persona responsable de la interacción pueda negar el acceso a la misma. *Privacidad* control que asegura que un activo que es accedido, desplegado o intercambiado entre partes, no puede ser conocido fuera de ese entorno. *Integridad* es un control que asegura que las partes interactuantes conocen cuándo un activo y los procesos han cambiado. Alarma es un control que notifica que una interacción está ocurriendo o ha ocurrido. Es una notificación apropiada y precisa de las actividades que violan o intentan violar cualquiera de las dimensiones de la seguridad, (Herzog, 2010).

Limitaciones

Este es el estado actual de los límites percibidos y conocidos de los canales, operaciones y controles, tal como se verifican en la auditoría. Los tipos de limitación se clasifican por la forma en que interactúan con la seguridad y la seguridad operacional. Por lo tanto, las opiniones sobre el impacto, la disponibilidad en el medio silvestre, la dificultad de realizar y la complejidad no se utilizan para clasificarlos, (Herzog, 2010).

Vulnerabilidad es la falla o error que: (a) niega el acceso a activos para personas o procesos autorizados, (b) permite acceso privilegiado a activos o personas o procesos no autorizados, o Dentro de un escenario definido; *Debilidad* son todos los posibles defectos o errores que interrumpan, reducen, abusan o anulan específicamente los efectos de los cinco controles de interactividad: autenticación, indemnización, resiliencia, subyugación y continuidad, (Fiaschetti, y otros, 2015).

Preocupación Se deben considerar todos los posibles defectos o errores que interrumpan, reducen, abusan o anulan los efectos del flujo o ejecución de los cinco controles del proceso: no repudio, confidencialidad, privacidad, integridad y alarma; *Anomalía* se deben considerar todos los elementos no identificables o desconocidos que no pueden ser contabilizados en operaciones normales, generalmente cuando la

fuente o destino del elemento no puede ser entendido. (Fiaschetti, y otros, 2015).

Hackeo ético

Rahman, Rasel, Noman, & Alim (2016) describe que hackeo ético es una manera proactiva de seguridad de la información y también se conoce como pruebas de penetración, pruebas de intrusión y agrupación de redes. Además, el hackeo ético es una evaluación de la debilidad de la seguridad y evidencia las vulnerabilidades potenciales de la seguridad de la información, según (V.V.N. SURESH, 2014).

Etapas del hackeo ético

Juneja (2013) indica que las fases del hackeo ético son: 1) *Reconocimiento*, el cual consiste en obtener la mayor cantidad de información del objetivo, las herramientas que se pueden utilizar son: Who.is, dmitry, entre otras. 2) *Exploración,* la cual se refiere a un escaneo de los puertos del equipo, nmap es una herramienta para realizar la exploración y Nessus es otro aplicativo que evalua las vulnerabilidades del sistema de seguridad de una institución. 3) *Explotación,* en esta fase se realiza el ataque propiamente dicho, con la ayuda de ciertas herramientas especializadas como Metaexploit, esto se efectúa conociendo las vulnerabilidades del objetivo. 4) *Mantener Acceso,* se basa en obtener el acceso a un determinado servicio de forma prolongada.

Hacker

PRASAD (2014) define al termino hacker como una persona que accede a ordenadores y a la información almacenada en computadoras sin obtener permiso.

Hacker ético

Chandrika (2014) explica que un hacker ético es un experto en computadoras y redes que ataca un sistema de seguridad en nombre de sus propietarios, buscando vulnerabilidades que un hacker malicioso podría explotar. Así mismo, Abdulrahman (2015) describe a un hacker ético como a una persona profesional en computadoras y redes que ejecutan muchos ataques en un sistema de red con el conocimiento de sus propietarios, buscando vulnerabilidades que un hacker criminal podría usar para comprobar un sistema de seguridad de red,

Tipos de hackers

Chandra Behera & Dash (2015) menciona que un hacker de sombrero negro tiene buen conocimiento sobre la piratería informática. Ellos usan sus habilidades para propósitos destructivos. Ellos rompen la seguridad en sistemas y redes, ya sea por diversión o para ganar dinero por medios ilegales. Obtienen acceso no autorizado y destruyen / roban datos confidenciales y causan problemas a su objetivo.

Bhawana, Ankit, & Shashikala (2014), describe que un hacker de sombrero blanco son personas autorizadas y pagadas por las empresas, con buena intención y posición moral. También se les conoce como "Técnicos de TI". Su trabajo es proteger Internet, las empresas, las redes informáticas y los sistemas de crackers. Algunas compañías pagan a los profesionales de TI para intentar hackear sus propios servidores y computadoras para probar su seguridad. El Hat Hacker blanco también es llamado como un Hacker Ético.

Chowdappa, Lakshmi, & Kumar (2014), indica que Un hacker de sombrero gris hereda las propiedades tanto de un hacker de Sombrero Negro y del hacker de sombrero blanco. Un hacker de sombrero gris recopila información y entra en un sistema informático para violar la seguridad, con el fin de notificar al administrador que hay lagunas en la seguridad y el sistema puede ser hackeado. Entonces ellos mismos ofrecen el remedio. Son muy conscientes de lo que es correcto y lo que está mal, pero a veces actúan en una dirección negativa. Un sombrero gris puede romper la seguridad de la organización, y puede explotarla y desfigurarla.

Pero por lo general hacen cambios en los programas existentes que pueden ser reparados.

Pilares de la seguridad Operacional OpSec

Según Toth Gastón (2014), la seguridad de la información se basa en tres principios que son confidencialidad, integridad y disponibilidad, conocidos comúnmente como la tríada CIA, por sus iniciales en inglés (Confidentiality, Integrity, Availability). En una organización es imprescindible generar normas, políticas y protocolos que ayuden a cumplir cada una de las características mencionadas anteriormente.

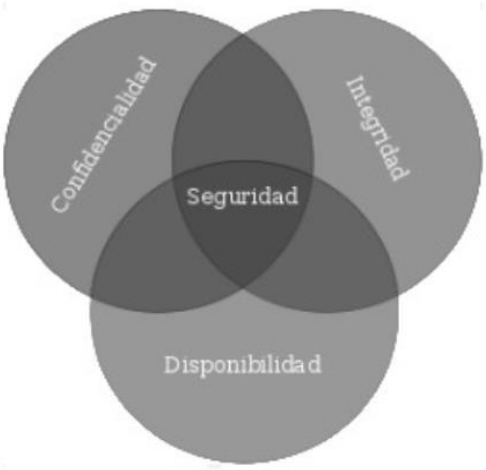

Figura 2 Tríada CIA, Fuente:(Toth Gastón, 2014)

La Confidencialidad es la propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados**.** *La Integridad* es la propiedad de salvaguardar la exactitud e integridad de los activos**.** *La Disponibilidad* se trata de asegurar de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados, según (Fuertes, Guagalango Vega, & Moscoso Montalvo, 2011). Por otro lado, Daniel, William, Ling, Lai, & Tevanotai (2014) describe que la confidencialidad, integridad y disponibilidad es el modelo bien conocido en cuanto a seguridad de la información. *La Confidencialidad* evita que la información de un usuario pueda ser accedida por otro. *La Integridad* mantiene la exactitud de la información. *La Disponibilidad* hace que la información sea accesible para el usuario en cualquier momento y en cualquier lugar.

Así mismo; Rahman, Rasel, Noman, & Alim (2016) manifiesta que, l*a confidencialidad* es una característica que se aplica a la información y para proteger y preservar la confidencialidad de la información hay asegurarse de que no esté disponible o no se da a conocer a las entidades no autorizadas. En este ámbito, las entidades incluyen a las personas y procesos. Para preservar la integridad de la información se debe proteger la exactitud e integridad de la información y los métodos que se utilizan para procesar y administrarla.

Vulnerabilidad

La vulnerabilidad se refiere a un fallo o debilidad en un sistema informático el cual puede permitir que un delincuente informático tenga acceso sin autorización, violar la confidencialidad, integridad y disponibilidad de los datos, según (Ortiz Aristizábal, 2015). Desde una perspectiva diferente una vulnerabilidad es la posibilidad que existe de que una amenaza se materialice en contra de un activo de la organización, no todos los activos son vulnerables a la misma amenaza según (López, 2010).

Amenazas

Una amenaza representa cualquier evento que modifica, interrumpe, intercepta o destruye la información de una organización. De acuerdo al área donde se produzcan las amenazas se clasifican en Amenazas externas y Amenazas internas. *Amenazas externas*, se originan fuera de la organización dentro de los cuales se puede encontrar los gusanos, virus, caballos de Troya, intentos de ataques informáticos. *Amenazas internas*, son las que provienen dentro de la organización y pueden resultar muy costosas ya que el posible atacante conoce donde se encuentra la información sensible y puede moverse en la organización con facilidad, según (Parra Correa & Porras Díaz, 2007). Así mismo el Esquema Nacional de Seguridad (2012), detalla que una amenaza es una causa potencial de un suceso que puede provocar daños a un

sistema de información o a una organización, las amenazas pueden afectar a cada activo.

Riesgos

Los riesgos son problemas potenciales, que pueden afectar a los sistemas de información o a los equipos de cómputo. Si no se tienen las medidas adecuadas para salvaguardar los datos y la información; dichos riesgos se pueden presentar por las vulnerabilidades y amenazas en cualquier momento, por lo tanto los riesgos se pueden clasificar en: Riesgos de integridad, Riesgos de relación, Riesgos de acceso, Riesgos de utilidad, Riesgo de infraestructura, según (Solarte Solarte, ENRIQUEZ ROSERO, & Benavides Ruano, 2015). López (2010) define a riesgo a la probabilidad de que una amenaza se materialice o no valiéndose de una vulnerabilidad. Cuando se presente un riesgo una organización puede elegir de tres alternativas las cuales son: a) Asumir el riesgo sin hacer nada, b) Aplicar medidas para disminuirlo o anularlo, c) Transferir el riesgo.

METODOLOGÍA.

Para el desarrollo del presente trabajo se utiliza un enfoque cuantitativo, ya que con este tipo de investigación se presenta resultados en métricas o RAVs, utilizando los lineamientos del Manual de la Metodología Abierta de Testeo de Seguridad, por sus siglas en inglés OSSTMM de manera específica en las redes de datos en tres instituciones públicas. Además este trabajo elaborado tiene un alcance descriptivo debido a que es un caso de estudio de tres instituciones públicas de diferente actividad económica.

Para la evaluación se utiliza un computador portátil Core I3 de 2,40 GHZ, en la que se crea una máquina virtual con un disco duro de 30 GB y 4 GB de RAM, la cual alojará la distribución de Kali Linux de 64 bits versión 2016.2, posterior a la instalación del Sistema Operativo, se instala la herramienta Nessus 6.9.3 para Kali Linux de 64 bits, esta herramienta se utiliza para escanear vulnerabilidades.

Además, se utiliza el sitio web Whois.domaintools.com, para encontrar información sobre el dominio de las tres instituciones públicas, un complemento a esto se ejecuta la herramienta de Kali Linux dmitry que arroja información del dominio y posibles subdominios. Posteriormente se ejecuta un comando de rastreo de rutas, por ejemplo: “tracert” para visualizar los saltos que existen desde el equipo escáner hasta el dominio y sus posibles subdominios.

Para realizar el escaneo de puertos TCP abiertos, la versión del Sistema Operativo y los servicios iniciados se utiliza la herramienta ZENMAP, la cual es la versión gráfica de NMAP, aplicando un escaneo intenso mediante el comando: “nmap –p 1-65535 –T4 –O –A –v XX.XX.XX.XX”; posterior a esta información se levanta el servicio del software Nessus para realizar un “escaneo básico de red”, la misma que nos arroja las vulnerabilidades existentes en las direcciones de las IP escaneadas; Para el estudio, se toma la referencia de Nessus que arroja una lista de vulnerabilidades categorizada de acuerdo a su severidad como son: crítica, alta, media y baja.

Con la información obtenida, se conoce cuáles son las vulnerabilidades más frecuentes de cada institución evaluada; además se calcula el nivel de seguridad con el calculador RAV (Risk Assessment Values), el cual se encuentra disponible en la página web del Instituto de Seguridad y Metodologías Abiertas por sus siglas en inglés ISECOM, sólo se debe introducir los valores requeridos para la Seguridad Operacional (Visibilidad, Acceso y Confianza), Controles de tipo A (Autenticación, Indemnización, Resistencia, Subyugación y Continuidad), Controles de tipo B (No Repudio, Confidencialidad, Privacidad, Integridad y Alarma) y Limitaciones (Exposición, Vulnerabilidad, Debilidad, Preocupación y Anomalías); posterior al cálculo de los RAVs se proponen mejoras para un posible incremento del nivel de seguridad actual de las instituciones y por último se recalcularán los RAVs para conocer

si el nivel de seguridad de las instituciones mejoró.

ANÁLISIS DE RESULTADOS

Resultados de la evaluación en las Instituciones públicas.

La evaluación de la seguridad en las redes de datos en la fase de exploración con la utilidad Nessus, la cual proporcionó un total de 433 vulnerabilidades de mayor frecuencia entre ellas se tomaron las vulnerabilidades críticas con una frecuencia de 14, vulnerabilidades altas con un frecuencia de 7 y vulnerabilidades de severidad media con una frecuencia de 173, las mismas que se detallan en la Tabla 2.

Severidad	Vulnerabilidad	Instituciones			Total
		A	B	C	
Críticas	MS14-066: Una vulnerabilidad en SChannel podría permitir la ejecución remota de código (2992611) (cheque sin credenciales)			5	**5**
	MS15-034: Una vulnerabilidad en HTTP.sys podría permitir la ejecución remota de código (3042553) (cheque sin credenciales)			4	**4**
	Detección de versiones no admitidas del Sistema operativo Unix		1		**1**
	MS11-030: Una vulnerabilidad en la resolución de DNS podría permitir la ejecución remota de código (2509553) (comprobación remota)			1	**1**
	MS11-058: Vulnerabilidades en el servidor DNS podrían permitir la ejecución remota de código (2562485) (comprobación remota)			1	**1**
	MS11-058: Las vulnerabilidades en el servidor DNS podrían permitir la ejecución remota de código (2562485) (chequeo sin credenciales)			1	**1**
	Detección de Instalación sin soporte Microsoft Windows Server 2003			1	**1**
Total de vulnerabilidades críticas		**0**	**1**	**13**	**14**
Alta	Acceso no autenticado al servidor VNC			1	**1**
	Envenenamiento de cache del campo de predicción del ID del DNS		1		**1**
	Nombre de agente de comunidad SNMP predeterminado	1			**1**
	MS12-020: Las vulnerabilidades de Escritorio remoto podrían permitir la ejecución remota de código (2671387) (cheque sin credenciales)			1	**1**
	Acceso no autenticado del servidor VNC: Captura de pantalla			1	**1**
	OpenSSL Heartbeat Divulgación de información (Heartbleed)			1	**1**
	Vulnerabilidad OpenSSL 'ChangeCipherSpec' MiTM			1	**1**
Total de vulnerabilidades altas		**1**	**1**	**5**	**7**
Media	El certificado SSL no es confiable	1	10	19	**30**
	Certificado SSL firmado utilizando algoritmo de hash débil		9	17	**26**
	SSL Cifrado de Mediana Fuerza Compatible	1	2	19	**22**
	Soporta Suites de cifrado de tamaño de bloques de 64-bit (SWEET32)	1	2	19	**22**
	Certificado SSL auto-firmado	1	2	13	**16**
	Detección de protocolos SSL Versión 2 y 3	1		14	**15**
	SSLv3 Padding Oracle en la vulnerabilidad de cifrado heredado degradado (PODDLE)	1		14	**15**
	Servidor Telnet sin cifrar	6	1	3	**10**
	SSH Soporta Algoritmos débiles	3	3	3	**9**
	Vulnerabilidad de ataque SSL DROWN (Descifrando RSA con encriptación obsoleta y debilitado)	1		7	**8**
Total de vulnerabilidades medias		**16**	**29**	**128**	**173**
TOTAL		**52**	**70**	**311**	**433**

Tabla 2 Listado de vulnerabilidades encontradas mediante la utilización de Nessus

Para cada una de las vulnerabilidades críticas que están relacionadas con los productos de la plataforma Microsoft. Esto implica que las vulnerabilidades MS11-058: Vulnerabilidades en el servidor DNS podrían permitir la ejecución remota de código (2562485) (comprobación remota), la vulnerabilidad MS14-066: Una vulnerabilidad en SChannel podría permitir la ejecución remota de código (2992611) (cheque sin credenciales), la vulnerabilidad MS15-034: Una vulnerabilidad en HTTP.sys podría permitir la ejecución remota de código (3042553) (cheque sin credenciales) y la vulnerabilidad MS11-030: Una vulnerabilidad en la resolución de DNS podría permitir la ejecución remota de código (2509553) (comprobación remota) se debe instalar los parches de actualización proporcionados por Microsoft usando el código proporcionado durante el escaneo. En cuanto a la vulnerabilidad de Detección de Instalación sin soporte Microsoft Windows Server 2003, se debe actualizar a una versión de Windows que tenga soporte actualmente. En relación a la vulnerabilidad de detección de versiones no admitidas del Sistema operativo Unix, se debe actualizar a una versión de Unix que tenga soporte actualmente.

Las vulnerabilidades de alta severidad como el Acceso no autenticado al servidor VNC, se recomienda deshabilitar el tipo de seguridad Sin Autenticación. En relación a la vulnerabilidad: Envenenamiento de cache del campo de predicción del ID del DNS se recomienda contactarse con su proveedor de servidor DNS para obtener un parche. En cuanto a la vulnerabilidad de Nombre de agente de comunidad SNMP predeterminado, se debe deshabilitar el Protocolo Simple de Administración de Red por sus siglas en inglés SNMP en caso de no utilizarlos o a su vez cambiar la cadena de comunidad predeterminada. En el caso de MS12-020: Las vulnerabilidades de Escritorio remoto podrían permitir la ejecución remota de código (2671387) (cheque sin credenciales) se debe instalar los parches de actualización proporcionados por Microsoft usando el código proporcionado durante el escaneo.

Continuando con el análisis de vulnerabilidades de severidad alta se destaca la vulnerabilidad Acceso no autenticado del servidor VNC: Captura de pantalla se debe deshabilitar el tipo de seguridad "Sin autenticación". Con relación a la vulnerabilidad: OpenSSL Heartbeat Divulgación de información (Heartbleed) se recomienda actualizar a OpenSSL 1.0.1g o posterior; como alternativa, recompile OpenSSL con el indicador 'DOPENSSL_NO_HEARTBEATS' para deshabilitar la funcionalidad vulnerable. En cuanto a la Vulnerabilidad OpenSSL 'ChangeCipherSpec' MiTM, se debe actualizar OpenSSL 0.9.8 Los usuarios de SSL / TLS (cliente y / o servidor) deben actualizar 0.9.8za o superior.

Por otro lado, las vulnerabilidades de severidad media como el certificado SSL no es confiable, se recomienda comprar o generar un certificado adecuado para este servicio. En base a la vulnerabilidad certificado SSL firmado utilizando algoritmo de hash débil se debe contactarse con la Autoridad de Certificación para que se vuelva a emitir el certificado. En relación a la vulnerabilidad SSL Cifrado de Mediana Fuerza Compatible se recomienda reconfigurar la aplicación afectada si es posible para evitar el uso de cifrado de intensidad media. En cuanto a la vulnerabilidad que soporta Suites de cifrado de tamaño de bloques de 64-bit (SWEET32) se debe reconfigurar la aplicación afectada, si es posible, para evitar el uso de todos los cifrados de bloques de 64 bits; como alternativa, coloque limitaciones en el número de solicitudes que se permiten procesar sobre la misma conexión TLS para mitigar esta vulnerabilidad.

Continuando con el análisis de vulnerabilidades de severidad media, se encuentra la vulnerabilidad del Certificado SSL auto-firmado, para lo cual se recomienda comprar o generar un certificado adecuado para este servicio. En cuanto a la vulnerabilidad de detección de protocolos SSL Versión 2 y 3, se debe consultar la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0. Utilice TLS 1.1 (con conjuntos de cifrado aprobados) o superior en su

lugar. En base a SSLv3 Padding Oracle en la vulnerabilidad de cifrado heredado degradado (PODDLE) se recomienda deshabilitar SSLv3. Los servicios que deben soportar SSLv3 deben habilitar el mecanismo TLS Fallback SCSV hasta que se pueda desactivar SSLv3.

En el mismo contexto se encuentra la vulnerabilidad el servidor Telnet sin cifrar para lo cual se debe deshabilitar el servicio Telnet y utilice SSH en su lugar. En cuanto a la vulnerabilidad de SSH Soporta Algoritmos débiles, se recomienda contactarse con el proveedor o consulte la documentación del producto para eliminar las cifras débiles.

Efectuando un resumen complementario de la Tabla 2 se puede constatar que existen en la Institución A, existen cero vulnerabilidades críticas, una vulnerabilidad alta y dieciséis vulnerabilidades media; con un total de 52 vulnerabilidades detectadas. En la institución B, existen una vulnerabilidad crítica, una vulnerabilidad alta y veintinueve vulnerabilidades media; con un total de 70 vulnerabilidades encontradas. En la institución C, existen trece vulnerabilidades críticas, cinco vulnerabilidades media y ciento veintiocho vulnerabilidades media; con un total de 146 vulnerabilidades.

Cálculo de los criterios de los RAVs

Después de efectuar las dos etapas del hackeo ético en las tres instituciones públicas, se realiza el cálculo de los criterios de los RAVs de igual manera en las tres instituciones, esto se calcula con la información recopilada. Este cálculo proporcionó para la Seguridad Operacional ***OpSec*** un valor total de 396, para los Controles de Clase A un valor de 57, en base a los Controles de Clase B un valor de 25 y en relación a las Limitaciones un valor de 396; cabe indicar que éstos valores pertenecen a la sumatoria de las tres instituciones evaluadas, los mismos que se pueden visualizar en la Tabla 3.

Categoría	Operaciones	Institución			Total
		A	B	C	
OpSec	Visibilidad	10	16	16	**42**
	Acceso	68	78	208	**354**
	Confianza	0	0	0	**0**
Total OpSec		**78**	**94**	**224**	**396**
Controles Clase A	Autenticación	15	19	20	**54**
	Indemnización	0	0	0	**0**
	Resistencia	0	0	0	**0**
	Subyugación	0	0	0	**0**
	Continuidad	0	2	1	**3**
Total Controles Clase A		**15**	**21**	**21**	**57**
Controles Clase B	No Repudio	1	2	2	**5**
	Confidencialidad	5	6	9	**20**
	Privacidad	0	0	0	**0**
	Integridad	0	0	0	**0**
	Alarma	0	0	0	**0**
Total Controles Clase B		**6**	**8**	**11**	**25**
Limitaciones	Vulnerabilidades	40	58	244	**342**
	Debilidad	15	19	20	**54**
	Preocupación	0	0	0	**0**
	Exposición	0	0	0	**0**
	Anomalías	0	0	0	**0**
Total Limitaciones		**55**	**77**	**262**	**396**

Tabla 3 Cálculo de los criterios RAVs

Con los valores detallados en la Tabla 3, se procede a ingresar en el calculador de *Métricas de seguridad de superficie de ataque*, proporcionado por la ISECOM, y el nivel de seguridad actual por institución se evidencia en la Tabla 4.

Institución	Seguridad Actual
A	69,3881 RAVs
B	67,9729 RAVs
C	60,2970 RAVs

Tabla 4 Nivel de Seguridad Actual

En la Tabla 4 se refleja el nivel de seguridad actual de las tres instituciones evaluadas, en la Institución A el nivel de seguridad es de **69,3881**

RAVs de seguridad actual y una brecha de seguridad de **31,96 RAVs**, en la Institución B el nivel de seguridad actual es de **67,9729 RAVs** con una brecha de seguridad de **33,37 RAVs** y en la institución C la seguridad actual es de **60,2970 RAVs** y una inseguridad de **42,26 RAVs**. Herzog (2010) indica que con el objetivo de mejorar el nivel de seguridad actual se aplican las estrategias de gestión de seguridad informática de acuerdo a los lineamientos planteados por la OSSTMM, los cuáles son: Mover el activo y crear una barrera entre él y la amenaza, cambiar la amenaza a un estado inofensivo y destruir la amenaza.

Mejora el nivel de la Seguridad actual de los casos de estudio.

En la Tabla 3 se encuentran los criterios RAVs obtenidos del hackeo ético y en la Tabla 4 se encuentra el nivel de seguridad actual calculado en RAVs, los cuáles se mejoran aplicando las estrategias de gestión de seguridad informática descritos anteriormente los mismos se visualizan en la tabla 5.

En base a los valores obtenidos en la porosidad de acceso en las instituciones A, B, y C exceden a los controles encontrados, para contrarrestar este aspecto, es vital implementar controles de interacción y controles de proceso, además de disminuir la porosidad cerrando los puertos lógicos ya que se encuentran en estado abierto de manera innecesaria. Con esto la disponibilidad, integridad y confidencialidad de la información no se ve afectada.

Asimismo, en el ámbito de las limitaciones existen vulnerabilidades, que por lo general son debido que no se encuentran actualizados los Sistemas Operativos, aplicaciones, Antivirus, entre otros; para disminuir las vulnerabilidades se activa las actualizaciones de lo antes mencionado. Por otro lado, se eliminan las debilidades aplicando en la autenticación un límite de intentos de inicio de sesión.

Categoría	Operaciones	Institución			Total
		A	B	C	
OpSec	Visibilidad	10	16	16	**42**
	Acceso	33	34	77	**144**
	Confianza	0	0	0	**0**
Total OpSec		**43**	**50**	**93**	**186**
Controles Clase A	Autenticación	15	19	20	**54**
	Indemnización	2	2	2	**6**
	Resistencia	0	0	0	**0**
	Subyugación	0	0	0	**0**
	Continuidad	1	2	2	**5**
Total Controles Clase A		**18**	**23**	**24**	**65**
Controles Clase B	No Repudio	4	5	12	**21**
	Confidencialidad	15	19	20	**54**
	Privacidad	0	0	0	**0**
	Integridad	0	0	0	**0**
	Alarma	2	2	2	**6**
Total Controles Clase B		**21**	**26**	**34**	**81**
Limitaciones	Vulnerabilidades	10	20	32	**62**
	Debilidad	0	0	0	**0**
	Preocupación	0	0	0	**0**
	Exposición	0	0	0	**0**
	Anomalías	0	0	0	**0**
Total Limitaciones		**10**	**20**	**32**	**62**

Tabla 5 Cálculo de los criterios RAVs con la mejora

CONCLUSIONES

En el presente trabajo se realizó un hackeo ético en las redes de datos en tres instituciones públicas, alineados con el Manual de la Metodología Abierta de Testeo de Seguridad en la cual se detallan los siguientes hallazgos: en la **Institución A** en el primer examen se evidenció un nivel de seguridad actual de **69,3881 RAVs**, luego de la implementación de controles se constató que la seguridad actual es de **77,6363 RAVs** con un incremento de **8,2482 RAVs**; en la **Institución B** en la primera prueba de hackeo ético la seguridad actual fue de **67,9729 RAVs** y posterior a las mejoras la seguridad actual es de **75,2535 RAVs** con un mejoramiento de **7,2806 RAVs** y por último en la **Institución C** en la

primera evaluación la seguridad actual fue de **60,2970 RAVs** y después de aplicar las estrategias de gestión de seguridad informática la seguridad actual es de **71,9043 RAVs** con un aumento de **11,6073 RAVs** .

Además, con la primera evaluación a las redes de datos de las instituciones A, B y C se deduce que el nivel de seguridad actual es equivalente a una seguridad informática baja, luego de mover el activo y crear una barrera entre él y la amenaza, cambiar la amenaza a un estado inofensivo y destruir la amenaza y posterior a estos controles se realizó otro examen a las redes de datos a las instituciones A, B y C se evidenció que el nivel de seguridad actual es equivalente a una seguridad informática media.

Esta evaluación de las redes en una organización permite al Administrador de red tener una visión del estado de la seguridad de las redes de datos cuantificada, con la finalidad disminuir las debilidades del sistema de red y por ende incrementar la seguridad actual de la organización; por lo tanto este examen de vulnerabilidades se considera parte de una Auditoría Informática, debido a que ésta se considera como el estudio para conocer los procesos, métodos, vulnerabilidades.

El presente trabajo tuvo como limitaciones el estudio de instituciones de la misma actividad económica, además no se logró realizar el examen en todos los servicios debido a que se encuentran centralizados en un lugar geográficamente distante, recursos económicos y el permiso debido para tener acceso a todos los activos de la red de datos por parte de las Autoridades de cada Institución. Asimismo, por temas de tiempo no se evaluó todos las instancias propuestos por la OSSTMM, debido a todos los elementos que poseen los demás canales, por tal motivo el cálculo de la seguridad informática actual de las instituciones no están completas.

En futuras investigaciones, este trabajo puede ser implementado en cualquier entidad ya sea privada o pública incluyendo todas las etapas del hackeo ético, además utilizar todas las instancias del Manual de la Metodología Abierta de Testeo de Seguridad y por último implementar un mecanismo estándar de aplicación de controles para que la Seguridad de la Información en una Organización sea robusta. Además se puede aplicar otro tipo de hackeo como OWASP (*Open Web Application Security Project*) o ISSAF (*Information Systems Security Assessment Framework*).

Referencias Bibliográficas

Abdulrahman, M. S. (2015). Ethical Hackers. *IT e-Magazine*(5).

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

Chandra Behera, M. P., & Dash, M. C. (2015). Ethical Hacking: A Security Assessment Tool to Uncover Loopholes and Vulnerabilities in Network and to Ensure Protection to the System. *International Journal of Innovations & Advancement in Computer Science IJIACS, 4*, 54-61.

Chandrika, V. (2014). ETHICAL HACKING: TYPES OF ETHICAL. *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), 11*(1), 43-48.

Chowdappa, K., Lakshmi, S., & Kumar, P. (2014). Ethical Hacking Techniques with Penetration Testing. *(IJCSIT) International Journal of Computer Science and Information Technologies, 5*(3), 3389-3393.

Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man In The Middle Attacks. *IEEE, 18*(3), 2027 - 2051.

Cruz Gavilánez, Y. d. (Marzo de 2016). Metodología OSSTMM para la detección de errores de seguridad y vulnerabilidad en sistemas operativos

de 64 bits a nivel de usuario final. Riobamba, Chimborazo, Ecuador: Escuela Superior Politécnica de Chimborazo.

Daniel, W., William, K., Ling, M., Lai, S., & Tevanotai, A. (2014). Awareness in e-Banking Security and usage. *Information Science, Electronics and Electrical Engineering (ISEEE), 2014 International Conference on, 2*, 1176 - 1150. doi:10.1109/InfoSEEE.2014.6947856

ESET Latinoamérica. (21 de Abril de 2016). *WELIVESECURITY.* Recuperado el 22 de 06 de 2016, de ESET Security Report Latinoamérica 2016: http://www.welivesecurity.com/wp-content/uploads/2016/04/eset-security-report-latam-2016.pdf

Esquema Nacional de Seguridad. (2012). *MAGERIT versión 3 (idioma español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* España: Ministerio de Hacienda y Administraciones Públicas.

Fiaschetti, A., Lanna, A., Panfili, M., Mignanti, S., Pietrabissa, A., Delli Priscoli, F., . . . Morgagni, A. (2015). Attack-Surface metrics, OSSTMM and Common Criteria based approach to “Composable Security” in Complex Systems. *WSEAS TRANSACTIONS on SYSTEMS, 14*, 187-202.

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

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

Juneja, G. K. (2013). ETHICAL HACKING: A TECHNIQUE TO ENHANCE INFORMATION SECURITY. *International Journal of Innovative Research in Science, Engineering and Technology, 2*(12), 7575 - 7580.

Kaspersky Lab. (17 de Febrero de 2015). *CNN Expansión (Pan-Regional): Lo que sabemos del mayor 'hackeo' bancario de la historia*. Recuperado el 02 de Abril de 2016, de http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/ultimas-noticias/2015/cnn-expansion-pan-regional-lo-que-sabemos-del-mayo

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

Manadhata, P., & Wing, J. (27 de Mayo de 2011). An Attack Surface Metric. *IEEE Transactions on Software Engineering, 37*(3), 371-386.

Morales Bonilla, J. E. (23 de Julio de 2015). Aplicación de Hacking Ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución. Quito, Ecuador.

OLIVEIRA CIRQUEIRA, S. (26 de Febrero de 2016). Auditoria de segurança utilizando teste de invasão de redes em ambientes de tecnologia da informação. Brasilia, Brasil: Centro Universitário de Brasília Instituto CEUB de Pesquisa e Desenvolvimento - ICPD.

Ortiz Aristizábal, D. F. (2015). Desarrollo de metodología para hallazgos de vulnerabilidades en redes corporativas e intrusiones controladas. Bogotá, Colombia.

Parra Correa, C. A., & Porras Díaz, H. (2007). Las Amenazas Informáticas: Peligro latente para las organizaciones actuales. *Gerencia Tecnológica Informática, 6*(16), 85-97.

Pazmiño Caluña, A. A. (16 de Marzo de 2012). Aplicación de Hacking Ético para la Determinación de Vulnerabilidades de Acceso a Redes Inalámbricas WiFi - See more at: http://dspace.espoch.edu.ec/handle/123456789/1726#sthash.zAkIq3bE.dpuf. Riobamba, Ecuador.

PRASAD, S. (2014). Ethical Hacking and Types of Hackers. *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), 11*(2), 24-27.

Rahman, A., Rasel, S., Noman, A., & Alim, A. (2016). Vulnerability Assessments in Ethical Hacking. *American Journal of Engineering Research (AJER), 5*(5), 1-5.

Ramírez Montañez, J. E. (2015). Análisis, evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la Alcaldía de Pamplona Norte de Santander. Pamplona, Colombia: Universidad Nacional Abierta y a Distancia UNAD.

Salinas Sánchez, J. A. (Mayo de 2013). Diseño y construcción de una red IP virtualización para la aplicación de hacking ético. Ecuador.

Solarte Solarte, F. J., ENRIQUEZ ROSERO, E. R., & Benavides Ruano, M. d. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL – RTE, 28*(5), 492-507.

Toth Gastón, S. J. (31 de Marzo de 2014). Implementación de la guía NIST SP800-30 mediante la utilización de OSSTMM. Neuquén, Argentina: Universidad Nacional de Comahue.

V.V.N. SURESH, K. (noviembre de 2014). Ethical Hacking and Penetration Testing Strategies. *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), 11*(2), 21-23.

Zlomislić, V., Krešimir, F., & Vlado, S. (2014). Denial of Service Attacks: An Overview. *Information Systems and Technologies (CISTI), 2014 9th Iberian Conference on* (págs. 1-6). Barcelona: IEEE.