MAESTRÍA EN AUDITORÍA DE TECNOLOGÍA DE LA INFORMACIÓN

DESARROLLO DE UN MECANISMO ÁGIL DE AUDITORÍA A LA SEGURIDAD INFORMÁTICA DE LA RED INALÁMBRICA 802.11 CON ARQUITECTURA AAA; CASO DE ESTUDIO: INSTITUTO ITSJOL

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

Magíster en Auditoría de Tecnologías de la Información

Por la estudiante:
Yasser Cesar ALVARADO SALINAS

Bajo la dirección de:
Rubén PACHECO VILLAMAR

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

Desarrollo de un mecanismo ágil de auditoría a la seguridad informática de la red inalámbrica 802.11 con arquitectura AAA; Caso de estudio: Instituto ITSJOL.

Development of an agile audit mechanism for the computer security of the 802.11 wireless network with AAA architecture; Case Study: ITSJOL Institute.

Yasser Cesar ALVARADO SALINAS[1]
Rubén PACHECO VILLAMAR [2]

Resumen

La computación inalámbrica facilita la movilidad y aumenta la productividad en las organizaciones, sin embargo, casi en la misma proporción, aumentan los riesgos de que dichas organizaciones se conviertan en víctimas de un ataque a la seguridad informática. En este artículo, se propone un mecanismo ágil para auditar la seguridad de la red inalámbrica basada en la arquitectura AAA, cuyo objetivo es evaluar la efectividad de los controles implementados. Para la construcción del mecanismo propuesto, se analizó la norma ISO 27002 junto con la metodología OSSTMM y las mejores prácticas de seguridad en redes inalámbricas, y para probar su utilidad se aplicó el modelo resultante en la ejecución de una auditoría ágil de seguridad, que proveyó elementos de juicio para determinar las deficiencias y el nivel de madurez de los controles de seguridad, así como las medidas de corrección necesarias. Una vez analizados los resultados se concluyó que el mecanismo funciona, que realmente es ágil, que provee un diagnóstico claro y medible del nivel de madurez de los controles en seguridad, y pautas para realizar nuevos proyectos y mejoras.

Palabras clave: Red inalámbrica, Seguridad, ISO 27002, OSSTMM, SSE-CMM.

Abstract

Wireless computing facilitates mobility and increases productivity in organizations; however, in almost the same proportion, they increase the risk that those organizations will become victims of an attack on computer security. In this article, we propose an agile mechanism to audit the security of the wireless network based on AAA architecture, whose objective is to evaluate the effectiveness of the implemented controls. For the construction of the proposed mechanism, the ISO 27002 standard was analyzed together with the OSSTMM methodology and the best security practices in wireless networks, and to test its usefulness, the resulting model was applied in the execution of an agile security audit, which provided elements of judgment to determine the deficiencies and the maturity level of the security controls, as well as the necessary corrective measures. Once the results were analyzed, it was concluded that the mechanism works, that it is really agile, that provides a clear and measurable diagnosis of the level of maturity of the controls in safety, and guidelines for making new projects and improvements.

Key words Wireless network, Security, ISO 27002, OSSTMM, SSE-CMM.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail valvarado@uees.edu.ec.
[2] Magíster en Ciencias en Telecomunicaciones. Universidad Espíritu Santo- Ecuador. E-mail rpachecov@uees.edu.ec

INTRODUCCIÓN

Las redes inalámbricas están en todas partes. Los usuarios las consideran prácticamente un bien de consumo masivo, y el no contar con este tipo de acceso en cualquier tipo de organización o empresa, sin importar su tamaño o naturaleza, se considera más bien una excepción o un caso muy especial. Es indiscutible que había una necesidad no cubierta y un mercado potencial esperando por la implementación de este tipo de soluciones antes de que aparecieran, por lo que su adopción masiva y pronta integración en las organizaciones, después de un periodo obligatorio de pruebas y errores, y de posteriores afinaciones, no fue realmente una sorpresa.

Entre las ventajas que las, ahora bastante maduras, tecnologías de acceso inalámbrico traen al día a día de cualquier institución están, por ejemplo: el incremento de la productividad, la reducción de los tiempos de puesta en marcha de áreas de conexión, y la movilidad, por nombrar algunas; aspectos no menores, con los que se ayuda a crear un ambiente de desempeño aceptable y acorde con las necesidades de la empresa actual.

Sin embargo, las comunicaciones inalámbricas parecen, a veces, ser víctimas de su propio éxito, debido a que su uso con frecuencia conlleva asumir riesgos asociados con la interferencia de la señal, tales como la interceptación y la intrusión, los mismos que pueden quebrantar la seguridad de una red inalámbrica y, por lo tanto, la seguridad de la red empresarial de la que forman parte, por ello se hace necesario la autenticación de usuarios y el cifrado de los datos que se transmiten (Touhill, Gregory, & Touhill, 2014).

Es así que, los administradores de red han implementado contramedidas para mitigar las amenazas, mediante el uso de protocolos de autenticación, autorización y registro de auditoría, conocidos también como la Arquitectura AAA, (por sus siglas en ingles *authentication, authorization, and accounting)*, lo que permite que solo los usuarios legítimos tengan acceso a la red inalámbrica. Este proceso que inicia con la verificación del nombre de usuario y contraseña. Después de la autenticación, el servidor determina los recursos a los cuales el usuario está autorizado a acceder. Por último, se realiza el proceso de registro de auditoría donde se identifica de donde se conectó el usuario y el tiempo que ha permanecido conectado (Meb, 2009), (Byung-Gil, Doo-Ho, Hyun-Gon, Sohn, & Parque, 2003). Dicha arquitectura ofrece elementos eficaces de control para mantener un ambiente inalámbrico seguro (Martínez & Gómez, 2009, pág. 86), (Liang & Wang, 2004), (Zhou, Xin, Nan , & Li, 2006), (Lorincz, Udovicic, & Begušić, 2007), (Alabady, 2008), (Li, Ma, & Yulong, 2012).

No obstante, las amenazas a la seguridad informática en la red inalámbrica siguen manifestándose a diario. Según ESET *Security Report* (2015) indica, que alrededor del 20% de los incidentes reportados corresponden a los accesos indebidos, y el 40% a ataques de denegación de servicio o también conocido como DoS (por sus siglas en inglés *Denial of Services)*. De igual forma, McAfee (2016) en su informe sobre amenazas, indica que el 33% de los incidentes reportados corresponden a ataques de DoS y un 18% a ataques de fuerza bruta. Además, CISCO (2015), en su informe anual de seguridad, afirma que cada día se detectan 50 mil intrusiones a la red. En efecto, el objetivo principal de un atacante común, en una red inalámbrica, son los dispositivos no autorizados y poco supervisados, debido a que estos dispositivos suelen estar mal administrados y, por lo tanto, son más propensos a contener vulnerabilidades, lo que puede comprometer a otros dispositivos de red, permitiendo a un atacante tomar el control de un sistema mediante el robo de las credenciales de acceso (Wagner, y otros, 2015), (ESET, 2017), (FORCEPOINT, 2017).

Por otro lado, tendencias como la utilización de tabletas personales y teléfonos móviles inteligentes en los entornos empresariales, BYOD, (por sus siglas en inglés *Bring Your Own*

Device), abonan con más situaciones de riesgo y están generando nuevos retos de seguridad en las organizaciones, por el mismo hecho de conectarse a recursos críticos de la empresa por medio de una conexión inalámbrica (CISCO, 2012). A tal nivel ha llegado la afectación que los expertos de seguridad de CISCO aseveran que, la violación a la seguridad en las redes inalámbricas se da, mayoritariamente, por causa de los dispositivos móviles.

Al respecto, ESET *Security Report* (2015) asegura que el 42% de las empresas encuestadas ni siquiera poseen una política definida para la gestión de BYOD. Sin embargo, la demanda de las organizaciones por el uso de las redes inalámbricas y dispositivos inteligentes sigue en aumento. Intel (2016) en su informe anual de desempeño, proyecta que para el año 2019 existirán 2.600 millones de conexiones inalámbricas adicionales. Así mismo, CISCO (2015), afirma que para el año 2020, habrá un total de 37.000 millones de dispositivos inteligentes conectados a una red inalámbrica. Ante el inminente escenario que se aproxima, las empresas u organizaciones están obligadas a revisar y mejorar las contramedidas adoptadas en sus infraestructuras para garantizar la seguridad en la red inalámbrica.

Para contrarrestar o detener los ataques y mitigar los impactos que estos puedan tener en la seguridad de la red inalámbrica, se debe tomar acciones para anticiparse a las diversas amenazas existentes. No obstante, frecuentemente la evaluación de las políticas a implementar y la selección de los controles de defensa en la red se deja a un juicio más bien subjetivo por parte de los administradores de la red (Wagner, y otros, 2015). Por último, ESET *Security Report* (2015), indica que solo el 42% de las empresas encuestadas ha efectuado una auditoría interna y solo el 27% tiene un plan de respuesta a incidentes.

Por consiguiente, las organizaciones se enfrentan a amenazas que evolucionan constantemente, y que emplean métodos cada vez más sofisticados de ataque para abatir las defensas implementadas en la red (CISCO, 2016), (ESET, 2015). En esta nueva coyuntura, la seguridad ya no es responsabilidad únicamente del departamento de TI o de los administradores de red, sino que más bien involucra a toda la organización, incluidas las áreas directivas.

La solución a lo antes mencionado, no solo depende de instalar nuevo hardware o software, o de cambiar la configuración a los equipos, o de implementar medidas de seguridad en la red inalámbrica (Chui, 2009), sino también, dependerá principalmente de evaluar constantemente la seguridad inalámbrica en la organización (Lehembre, 2006), (Bautts, Dawson, & Purdy, 2005), con el fin de obtener la información necesaria para ejecutar las acciones pertinentes de mejora, puesto que si no se realiza de esta manera, sería similar a un proceso en que el paciente se auto médica, sin consultar o haber recibido un diagnóstico previo de algún experto. Por lo tanto, es necesario realizar previamente una evaluación para identificar y mitigar vulnerabilidades en las redes (Lehembre, 2006), (Bautts, Dawson, & Purdy, 2005).

Respecto a esto, Silva y Ludwig (2011) proponen el desarrollo de una metodología para la auditoría de redes inalámbricas, para ayudar a mejorar la seguridad de la misma. De igual forma, Ferreira et al. (2015), proponen un método para reducir al mínimo los agujeros de seguridad en redes WLAN. Por último, Cheng et al. (2014), diseñan un nuevo mecanismo útil para la monitorización inalámbrica y técnicas de blindaje en la red.

No obstante, la idea de utilizar una metodología ágil de auditoria es para verificar los requerimientos de seguridad en varias áreas comprometidas dentro de la organización, y por medio de la evaluación, lograr juzgar con mucha precisión la seguridad en las infraestructuras de red de datos, como lo establece Valencia Blanco (2013); USER (2011); Jara y Pacheco (2012, pág. 230).

Por lo tanto, Kaklauskas y Rathos (2014), en su investigación para probar la función de seguridad en la red inalámbrica emplean el manual de la metodología abierta de comprobación de la seguridad, también conocido como OSSTMM (por sus siglas en ingles *Open Source Security Testing Methodology Manual*), utilizada para evaluar las redes inalámbricas de la ciudad Šiauliai, la cuarta ciudad más grande de Lituania. De igual forma, Caicedo, De La Cruz, y Taimal (2010) emplearon la metodología precitada para garantizar la ejecución de pruebas de seguridad a la red inalámbrica en un ambiente de evaluación donde probaron un modelo de autenticación.

Además, existen trabajos relacionados con el estándar ISO/IEC 27002; como por ejemplo el caso de Iqbal et al. (2009), que desarrollaron una base de datos de la norma ISO, la misma que permite el uso eficaz de la norma. De igual manera, Horváth y Jakub (2009), muestran que la norma tiene la característica de ser flexible puesto que se aplicaron 88 de los 133 controles en una organización pequeña. Por último, la norma ISO es la norma más utilizada y la metodología estructurada más reconocida dedicada a la seguridad de la información (Talib, Adel , & Barachi, 2011)

Es así que, para efectos del presente estudio se ha elegido a la metodología abierta OSSTMM y la norma ISO 27002. Ésta última permite medir el éxito de los controles de seguridad, y la mejora de la eficacia de la seguridad de la información (Talib, Khelifi, & Ugurlu, 2012), (Hsu, Nat. Taiwan University, Wang, & Lu, 2016). Mientras que la metodología OSSTMM fue la primera metodología para incluir factores humanos en las pruebas, teniendo en cuenta el hecho establecido de que los seres humanos son fuentes de riesgos para el sistema. Además, los dos documentos comparten un componente dedicado a evaluar la seguridad en las redes inalámbricas.

Por todo lo expuesto, se ha definido como objeto de la investigación, que sirve de base para la elaboración del presente artículo, desarrollar un mecanismo ágil de auditoría mediante el análisis de la metodología OSSTMM, en conjunto con la norma ISO 27002 y las mejores prácticas de la industria, para la evaluación de la seguridad informática de la red inalámbrica 802.11 basada en arquitectura AAA. El resto de este documento se organiza de la siguiente manera: la segunda sección presenta la descripción de los protocolos de seguridad de la red inalámbrica, las amenazas a la red inalámbrica y las metodologías de evaluación a la seguridad informática; la tercera sección ofrece la metodología utilizada para la elaboración del mecanismo ágil de auditoría; la cuarta sección muestra y analiza los resultados obtenidos en la ejecución de los pilotos experimentales, finalmente, la quinta sección ofrece la conclusión y las direcciones para investigaciones e implementaciones futuras.

MARCO TEÓRICO

Esta investigación se fundamenta en la Teoría Matemática de la Comunicación propuesta por Shannon y Weaver (1949), que se ocupa de la transmisión de los símbolos de comunicación (Barchini, Sosa, & Herrera, 2004). De igual manera, el componente disciplinar en la cual se basará el presente trabajo son las Tecnologías de la información y comunicación, definida por Laudon (1997), la misma que involucra dispositivos físicos y de software en las redes de transmisión de datos.

Cabe indicar que el objeto de estudio se centra en la seguridad informática de la red inalámbrica de área local con el estándar IEEE 802.11 sobre una arquitectura AAA. A continuación se presenta la fundamentación teórica que sustentan esta investigación.

Estándar IEEE 802.11

El estándar IEEE 802.11, fue definido para las redes inalámbricas de área local (WLAN, *Wireless Local Area Network*) en el año 1997. Actualmente las redes WLAN, se han convertido en una necesidad tanto para las organizaciones como para los entornos domésticos debido a los

beneficios de movilidad y escalabilidad que ofrecen, a diferencia de las redes cableadas tradicionales. (Thomas, Willis, & Craig, 2006). En efecto, las organizaciones han adaptado su arquitectura operacional a las redes Wi-Fi y con esto los usuarios móviles incrementan sus demandas por más datos, más cobertura y mayor disponibilidad en redes de conectividad inalámbrica. Debido a esto el estándar IEEE 802.11 ha evolucionado constantemente para compensar esta creciente necesidad (Buritica, 2016). En enero del año 2014, la IEEE estableció una nueva versión conocida como 802.11ac, la misma que duplica las capacidades de velocidad de datos de la versión 802.11n, para proporcionar un rendimiento en gigabit (Perahia & Stacey, 2013).

Protocolos de seguridad de la red WLAN

Entre los protocolos de seguridad de una red inalámbrica común está, inicialmente, el protocolo de cifrado inalámbrico, también conocido como WEB (por sus siglas en inglés *Wireless Encryption Protocol*). Posteriormente apareció el protocolo de punto de acceso inalámbrico, llamado también WPA (por sus siglas en ingles *Wireless Access Point*). Este protocolo integra mecanismos mucho más robustos que el anterior protocolo, mejorando la autenticación, control de acceso, la integridad y la confidencialidad (Navarro & Ascencio, 2016), (Bellido, 2013).

Por último, en el año 2004, fue ratificado el estándar IEEE 802.11i, también se le conoce por el nombre WPA2, considerado hasta la actualidad un mecanismo eficiente puesto que incluye un fuerte algoritmo de cifrado como lo es AES (*Advanced Encryption Standard*, Cifrado Avanzado Estándar) el mismo que utiliza 128 bits como tamaño de bloque y para las claves utiliza 128, 192 o 256 bits (Mathews & Hunt, 2007). Por consiguiente, cada uno de estos mecanismos emplea un algoritmo criptográfico con el fin de proveer seguridad en la conexión y privacidad en los datos (Martínez & Gómez, 2009, pág. 85), (Poddar & Choudhary, 2014, pág. 1), (Méndez, Mosquera, & Trujillo, 2015).

Además, una característica del estándar WPA2 es la administración de claves, que brindan dos tipos de sistemas de gestión de claves: el uso de un servidor de autenticación para generar y gestionar claves, o el uso de claves previamente compartidas. Aunque la implementación completa del protocolo 802.11i normalmente no permite claves pre-compartidas, no obstante, esta opción está disponible para hacer la aplicación más fácil para los usuarios domésticos y de pequeñas empresas (Prodanovic & Simic, 2007).

Algoritmo criptográfico

La característica principal de un algoritmo criptográfico es la de convertir un mensaje claro en un texto cuyo contenido es totalmente incomprensible, llamado texto cifrado, el mismo que solo puede ser entendido por una persona autorizada para el efecto que hace uso de una o más llaves para realizar el proceso de descifrado del mensaje (Fulgueira, Fuenteseca, & Hernández, 2015).

Arquitectura AAA

La arquitectura AAA permite proporcionar la autenticación centralizada, autorización y auditoría para el acceso a la red. Estos tres elementos son usados para proteger al usuario de la red, prevenir ataques, facilitar la administración de los recursos de forma adecuada y evitar accesos no autorizados (Nakhjiri, 2005), (Yago, 2008).

Protocolos de Autenticación

La autenticación consiste en la identificación de un usuario previamente para tener acceso a la red, para tal efecto se presentan las credenciales respectivas y se procede con la verificación de la identidad, para determinar que es el usuario que dice ser (Joshi, y otros, 2008), (Díaz, Alzórriz, & Ruiz, 2014), (Nakhjiri, 2005).

Protección y Prevención

Según el reporte de seguridad de ESET (2015) se indica que en los siete últimos años las empresas se han valido de tres controles de

seguridad para la protección y prevención de su arquitectura tecnológica y que hasta en la actualidad siguen siendo útiles, como son el antivirus, el firewall y los respaldos de información. Además, otro elemento de protección y prevención son lineamientos estipulado en las políticas de seguridad apegadas a un al cumplimiento de algún estándar o norma y por último están las auditorías internas.

Por consiguiente, Intel (2016) indica que es necesario que las medidas de protección y prevención estén integradas por tecnología, procesos y herramientas, que contribuya a contrarrestar las amenazas presentes. Por último, en el reporte anterior de ESET (2015) recomienda que se debe asignar el presupuesto suficiente al departamento de TI o al encargo de la seguridad, fomentar actividades de capacitación y concientización en los usuarios, implementar medidas de cifrado de la información y la doble autenticación.

Ramachandran (2011) recomienda como medida de protección en redes inalámbricas el uso de WPA2-PSK con una contraseña fuerte. En entornos empresariales para la asegurar la autenticación, usar WPA2-Enterprise con EAP-TLS, puesto que ha demostrado ser irrompible.

Firewall

Definido de manera simple, un firewall o cortafuegos es “un punto de estrangulación de una red (normalmente una red interna) a otra (normalmente Internet)” (Syngress, Liu, & Miller, 2006, pág. 74). Además, tiene la característica de controlar el acceso a la información y a la red de datos por lo que garantiza un entorno se red físicamente seguro. Al respecto, Preetham (2002) asegura que un firewall permite evitar amenazas a los equipos de una red, puesto que proporciona una barrera de seguridad entre la red local y la red externa como el internet.

Sistemas de detección/protección de intrusos

Castillo (2006) define a un Sistema de Detección de Intrusos (IDS) como la combinación de hardware y software que permite, haciendo uso de alguna alarma o indicador, detectar acciones inusuales de los usuarios en la red que se han realizado o que se estén ejecutando en ese instante. Las investigaciones realizadas han determinado que existen dos técnicas que permiten realizar la detección de intrusos a un sistema de red. El primero responde a los usos mal intencionados o que no están permitidos en un sistema, enfocándose en el estudio de los patrones conocidos. El segundo se centra en la detección de anomalías, que consisten en las desviaciones de un comportamiento normal de un usuario en la red (Tejvir, Vimmi, & Dheerendra, 2014).

Para Capano (2015) los sistemas inalámbricos de detección de intrusos también conocido como WIDS (por sus siglas en ingles *Wireless intrusion detection systems*) y los sistemas inalámbricos de protección contra intrusos, llamados también WIPS (por sus siglas en ingles *wireless intrusion protection systems*), son utilizados para proteger continuamente una red inalámbrica de intrusos. Un WIDS, consta de un sistema de sensores encargados de supervisar la red en busca de dispositivos no autorizados, tales como puntos de acceso falsos. Mientras que en un WIPS, está encargado de detectar dispositivos no autorizados y toma medidas para mitigar la amenaza al contener el dispositivo y separarlo de la red inalámbrica. Estos dos sistemas, realizan el monitoreo de la red inalámbrica constantemente, y la característica de resaltar es que no requieren de administración. Además los WIDS y WIPS escuchan todo el tráfico que genera la red inalámbrica para detectar y prevenir la intrusión inalámbrica. Un WIPS consta de tres componentes: un servidor, una consola de administración y sensores distribuidos.

VLAN

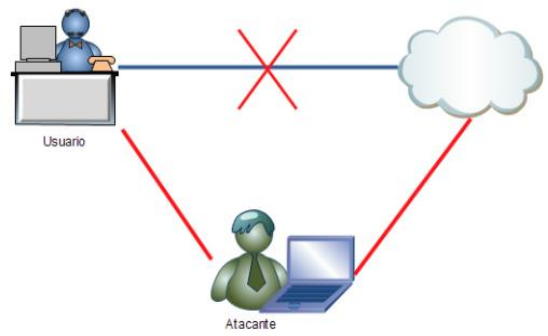
Para Wall (2004) las redes virtuales de área local (VLAN, *virtual local área network*) representan la separación lógica de las redes

físicas, es decir que al hacer uso de una VLAN permitirá efectuar una división entre los dispositivos físicos de conexión en diferentes redes virtuales, las cuales poseen sus propias características. Además, indica que el uso de las VLAN en la empresa, contribuyen a la escalabilidad, seguridad, disponibilidad y ahorro de costes de la red global de la red.

Amenazas sobre las redes inalámbricas

Los ataques a las redes inalámbricas son cada más sofisticados y difíciles de detectar, por lo que es necesario múltiples niveles de defensa para la protección de la red. Entre los muchos riesgos de seguridad conocidos, están los ataques de hombre en el medio (MITM, *man in the middle*) y *spoofing*, que suponen una importante amenaza de intrusión para redes inalámbricas, puesto que permite a los atacantes secuestrar una conexión ya establecida por un usuario legítimo (Mookiah, Walsh, Greenstad, & Dandekar, 2013). Al respecto, Joshi y otros (2008) indican que el ataque MITM, se produce cuando un atacante se posiciona en medio de una comunicación entre un usuario común y el servidor, interceptando, de esta forma, todas las transmisiones, lo que le permite al atacante capturar todos los datos no cifrados como las credenciales de acceso a algún servicio.

Gráfico 1: Ataque MITM



Fuente: Elaborado por los autores.

Al respecto sobre *spoofing* o falsificación, Earle (2006) lo describe como la acción de imitar a un usuario legitimo con el objetivo de acceder a un recurso que está protegido por alguna forma de autenticación o autorización. Generalmente este ataque implica que el atacante establezca un punto de acceso falso para conseguir un cliente valido, quien después de conectarse al AP falso, entrega, sin saberlo, información de autenticación que puede ser utilizar para actos maliciosos en la red corporativa.

Sobre el ataque de *Hotspots* falsos o AP falso, Wall (2004) indica que consiste básicamente en que el atacante, desde un punto exterior a la organización, levante un punto de acceso y en muchos casos con el mismo nombre de SSID para confundir a los usuarios invitándolos a identificarse. Los usuarios que sucumben a este tipo de ataque son afectados por la implantación de algún código malicioso que frecuentemente son indetectables por los antivirus.

De igual forma, sobre el ataque de Denegación de Servicio, Beggs (2014) afirma que las redes inalámbricas son inherentemente vulnerables a este tipo de ataques y es difícil localizar al atacante. Este ataque consiste en que el atacante evita que un usuario legítimo tenga acceso a la red inalámbrica provocando que no esté disponible o su bloqueo permanente. Sin embargo, para redes corporativas que migran al estándar 802.11n, existe la posibilidad de usar canales más grandes y menos concurridos. Además algunos puntos de acceso (APs) actuales pueden configurar los canales de forma automática para detectar y evadir la interferencia. No obstante, un atacante experimentado encontrará otras formas de cumplir su cometido, como por ejemplo, consumir los recursos del AP o mantener los canales ocupados. Lo recomendable es usar dispositivos de comunicación actuales que proporcionen protección enmarcada en la gestión 802.11w.

Norma ISO 27002

La norma ISO 27002:2013, considerada una guía para mejorar la seguridad de la información, es un estándar internacional, donde se expone de manera explícita, para algunos ámbitos de aplicación, varias sugerencias para cumplir con 35 objetivos y con cada uno de los 114 controles definidos. Está

estrechamente relacionada con la norma ISO 27001, encargada de ayudar a las empresas que requieran establecer un programa de gestión de la seguridad de la información o mejorar sus prácticas actuales de seguridad de la información. (Sangkyun, 2011).

Para Moeller (2013) la norma ISO 27002 estipula todas las sugerencias para los controles que se deben implementar en una organización para garantizar la seguridad de la información y estar preparado para responder ante una amplia gama de amenazas que van desde errores provocados por humanos y fallas de equipos hasta robos, fraudes, vandalismo, sabotaje, incendio e inundación. Sin embargo el marco de gestión que proporciona a ISO 27001 contribuye a la correcta integración de las prácticas de seguridad con la alta gerencia, es decir que este estándar está diseñado para medir, supervisar y controlar la gestión de seguridad desde una perspectiva de arriba hacia abajo.

El tema de la gestión de seguridad de la información es muy amplio y de gran impacto en las organizaciones puesto que involucra todas las formas de información, no solo los de las tecnologías de información sino también la documentación, propiedad intelectual, los conocimientos, entre otros. Por lo que para contribuir a la implementación de la norma se requiere la cooperación de la alta gerencia, por la potestad que posee ésta, de fomentar el cumplimiento de la norma en todas las áreas, y no dejar la responsabilidad únicamente al área técnica, los que frecuentemente se limitan a proponer soluciones más concretas como solo controles, sin prestar atención a marcos estandarizados que son más amplios y cubren los riesgos de la información que involucra al personal interno, contratistas y proveedores (Bustamante & Osorio, 2014).

Por último, el cumplimiento de la norma ISO 27002 constituye una marca de confianza en la seguridad global de la organización, así como la ISO 9000 se ha convertido en una garantía de calidad. La norma ISO/IEC 27002:2013 contiene 114 controles, 35 objetivos de control agrupados en 14 cláusulas, tal como se muestra en la Tabla 1. A diferencia de su antecesora, la versión 2005 estaba compuesta de 133 controles, 39 objetivos de control agrupados en 11 cláusulas (Mesquida, 2012), (Gomes, 2008).

. ***Tabla 1:*** *Clausulas de la norma ISO 27002:2012*

Clausulas	Categorías	controles
5. Políticas de seguridad	1	2
6. Aspectos organizativos de la seguridad de la información	2	7
7. Seguridad ligada a los recursos humanos	3	6
8. Gestión de activos	3	10
9. Control de Accesos	4	14
10. Cifrado	1	2
11. Seguridad Física y ambiental	2	15
12. Seguridad en la operativa	7	14
13. Seguridad en las Telecomunicaciones	2	7
14. Adquisición, Desarrollo y Mantenimiento de los SI	3	13
15. Relación con los Suministradores	2	5
16. Gestión de incidentes en la seguridad de la información	1	7
17. Seguridad en la gestión de la Continuidad Negocio	2	4
18. Cumplimiento	2	8
TOTAL	**35**	**114**

Fuente: Norma ISO 27002:2012

Por consiguiente, para implementar la norma ISO 27002, la empresa deberá identificar sus necesidades y requisitos de seguridad de la información puesto que si se omite este principio y se implementan todos los controles de la norma, se estaría despilfarrando recursos y afectando a su eficiencia en los procesos (Montesino, Baluja, & Porvén, 2013), (Martelo, Madera, & Betín, 2015), (Heru, Mohammad, & Yong, 2011).

Metodología OSSTMM

El Manual de la Metodología Abierta de Testeo de Seguridad o también conocido como "OSSTMM" (por sus siglas en ingles *Open Source Security Testing Methodology Manual*),

es una metodología estándar, comúnmente utilizados para realizar pruebas de seguridad. Por su naturaleza, la metodología se puede adaptar a cualquier tipo de operación de auditoría, como pueden ser pruebas de penetración, evaluaciones de seguridad y vulnerabilidad, hacking ético, entre otros. Además, OSSTMM define seis diferentes tipos de pruebas o test de seguridad, que se detallan a continuación: 1) Blindaje o Hacking Ético; 2) Doble blindaje, Auditoría de caja negra o Pruebas de Penetración; 3) De caja gris; 4) De doble caja gris; 5) Test tándem o secuencial; y 6) Inverso. La elección de la prueba más adecuada para ser aplicada dependerá de las necesidades de la organización (Silva, Machado, Oliveira, & Amorim, 2007), (Valdez, 2013).

La metodología OSSTMM emplea el término "canal" para clasificar las diferentes áreas de seguridad de interés dentro de una organización, incluyendo seguridad física, seguridad en comunicación y seguridad de espectro. Por tanto, en el caso de una auditoría de seguridad exhaustiva es necesario la ejecución de pruebas de los tres canales, sin embargo, también es aceptable seleccionar las pruebas que se desean según necesidades específicas. Por esta razón, la metodología realiza una división de los tres canales en cinco secciones lógicas, tal como se detalla en la tabla 2 (Wilhelm, 2013).

Tabla 2: Ámbito de la OSSTMM

Canal	Sección	Descripción
Seguridad Física	Humano	Personal comprometido con la organización
	Físico	Objetos tangibles de la organización
Seguridad de las comunicaciones	Redes de datos	Sistemas electrónicos y redes de datos
	Telecomunicaciones	Comunicación es digitales y analógicas
Seguridad del espectro	Comunicaciones inalámbricas	Señales Electromagnéticas empleadas

Fuente: Valdez (2013)

Mejores prácticas

La Comunidad de Prácticas APS (2012) define las buenas prácticas como la experiencia de una intervención que ha generado resultados positivos en un contexto específico mejorando la resolución de problemas o dificultades que surgen en las operaciones diarias. Para el presente estudio se han considera las recomendaciones de las buenas prácticas de las siguientes instituciones: a) CISCO; b) ESET; c) Instituto Nacional de Cyberseguridad de España; y d) Instituto de Seguridad de Consenso de Evaluación de Preparación Operativa.

Herramientas de Pruebas de penetración

Cardwell (2013) describe algunas herramientas para efectuar las pruebas de penetración en la red inalámbrica, entre las que se mencionan están: a) Aircrack-ng, esta herramienta sirve para evaluar la seguridad inalámbrica; b) Aireplay-ng se utiliza combinación con la herramienta con la herramienta anterior para la captura de tráfico; c) Airmon-ng es utilizada para colocar una tarjeta de red inalámbrica en modo monitor para recibir todo el tráfico de la red 802.11; d) Airodump-ng es empleado como un analizador de protocolo para capturar paquetes inalámbricos 802.11 sin procesar; e) Airpwn es una herramienta que permite lanzar un ataque escuchando los paquetes transmitidos entre el usuario y el punto de acceso, buscando un patrón específico para luego realizar el ataque, tal como *spoofing* (fingiendo ser alguien más); f) Kismet es un poderosa herramienta que realiza no sólo la dirección de puntos de acceso, sino que también realiza las funciones de un IDS; g) Ssidsniff utilizada para buscar puntos de acceso y para capturar y guardar tráfico inalámbrico en un archivo; h) Ettercap Es una poderosa herramienta que puede usarse como un sniffer, realizar ataques de hombre en el medio (MiTM) y efectuar envenenamiento de ARP.

Además, en el desarrollo de esta investigación se encontraron algunas distribuciones de Linux que integran un sinnúmero de herramientas que facilitan la realización de pruebas y auditoría de

redes inalámbricas, las cuales son las siguientes: Kali Linux, BackTrack y WifiSlax.

Según Ali y Heriyanto (2011), indican que para efectuar las pruebas de penetración es necesario hacer uso de una metodología, la cual define un conjunto de reglas, prácticas, procedimientos y métodos que se persiguen e implementan durante al auditoría de seguridad de la información. Por tanto, la metodología de pruebas de penetración define una hoja de ruta con ideas prácticas para evaluar correctamente la seguridad de red inalámbrica. Al respecto, Johns (2015), propone una metodología para pruebas basada en estándares internacionales, la misma que consta de 6 etapas que se detallan a continuación: 1) Reconocimiento; 2) Ataques y penetración; 3) Ataques del cliente; 4) Entrar en la red; 5) Valoración de vulnerabilidad; y 6) Explotación y captura de datos.

Mecanismo ágil de seguridad propuesto

El término mecanismo adquiere diferentes significados, dependiendo principalmente del campo de conocimiento y del contexto donde se aplica, en este caso el contexto es la seguridad de la información en redes inalámbricas. Al respecto, Erfani S. (2003), define al mecanismo de seguridad como el conjunto de técnicas eficientes y esquemas utilizados para implementar la seguridad, por lo que es necesario la combinación de varias metodologías, normas y buenas prácticas para construir un mecanismo de seguridad eficaz, que permita contrarrestar ataques o amenazas a la seguridad de la información. De igual forma, Ochoa Ovalles y Cervantes Sánchez (2012), consideran al mecanismo de seguridad como una herramienta de seguridad o técnica diseñada “para detectar, prevenir o recobrarse de un ataque de seguridad”. Además, indican que los mecanismos integran diversidad de controles para ser implementados y ejecutados (pág. 3).

Por lo tanto, el término mecanismo puede ser utilizado para referirse a un funcionamiento o una metodología que integra varios componentes de distintas metodologías y manuales de buenas prácticas. En síntesis, para aclarar esta idea, y relacionarlo con los conceptos de los expertos, anteriormente mencionados, el Diccionario de la Real Academia Española (RAE), define mecanismo como un “Conjunto de las partes de una máquina en su disposición adecuada” (RAE, 2016). Es decir, que el conjunto de varias partes compatibles y adaptables permiten el funcionamiento adecuado de un mecanismo. Por último, la Master en Ciencias Cintia Quezada, Administradora del Laboratorio de Redes y Seguridad de la Universidad Nacional Autónoma de México, corrobora estas definiciones e indica que los controles deben estar enfocados la confidencialidad, integridad, disponibilidad, no repudio, controles de acceso y autenticación (Quezada Reyes, 2015).

Con esta finalidad, se pretende desarrollar un mecanismo ágil de seguridad, integrado por los estándares y metodologías como: ISO 27002, OSSTMM y las recomendaciones de las buenas prácticas, para evaluar el diseño, la administración y la seguridad de la red inalámbrica. Además, se hará uso del modelo de madurez CMM para identificar el nivel de madurez en el que se encuentra la organización. En consecuencia, la finalidad del mecanismo ágil de auditoría es la de evaluar los controles implementados para resguardar la operatividad de la red inalámbrica, permitiendo identificar falencias o carencias en la arquitectura inalámbrica de una organización, de una forma eficiente, logrando en el menor tiempo posible, obtener resultados fiables, que muestren el nivel de madurez de la seguridad y las mejoras o correcciones a realizar; de ahí el nombre de mecanismo ágil.

Además, el mecanismo ágil, considerado de manera analógica un resumen inteligente, (permite hacer una evaluación de la seguridad inalámbrica) contribuye a la ejecución de una auditoría a los controles de seguridad informática de la red inalámbrica con arquitectura AAA, reduciendo considerablemente el tiempo que tomaría hacerlo con una metodología completa o con

estándar tradicional. Sin embargo, es necesario aclarar que no se desfavorece a ninguna de las metodologías conocidas. En todo caso, se puede asegurar que el mecanismo ágil de seguridad es adaptable y flexible. Además, aborda ampliamente diversos componentes y enfoques con la finalidad de brindar una solución efectiva y eficiente, acorde a las necesidades actuales de la seguridad de la información en redes inalámbricas de área local.

Ahora bien, las contramedidas consideradas para mitigar una posible explotación de vulnerabilidades se agrupan en lo que se conoce como controles. En el contexto de la seguridad informática un control se clasifica en 3 tipos distintos, acompañados de un nivel de madurez o cumplimiento. Los tipos de controles son: controles preventivos, controles detectivos y controles correctivos (Ndaw, Mendy, & Ouya, 2016, pág. 622). La presente ejecución del mecanismo ágil de auditoría evaluará los controles preventivos y detectivos implementados para asegurar la infraestructura de red inalámbrica. Sin embargo, las indicaciones o puntualizaciones que se emitirán, en caso de hallar falencias en el control evaluado, conllevará implementar acciones correctivas para mejorar el nivel de seguridad actual.

Karygiannis y Owens (2002), recomiendan que deben existir 3 tipos controles en tres áreas primordiales con la finalidad de proteger a los dispositivos portátiles en una red inalámbrica, estos controles son los siguientes: controles de gestión, controles operacionales y controles técnicos (págs. 5-31). Así mismo, Noor y Mohamad (2010), afirman que los controles de seguridad deben agruparse en 3 categorías que son: controles de gestión, controles técnicos y controles operacionales. Los controles técnicos son las medidas de seguridad que se efectúan y ejecutan primordialmente en los equipos de comunicación, es decir, contramedidas que ya están incorporados en hardware, software y firmware de los equipos informáticos o dispositivos inalámbricos. En consecuencia, los controles de gestión no pueden funcionar independientemente; debe y normalmente se complementa con otros dos aspectos: el técnico y el operativo. (Hurley , y otros, 2006). De igual forma, Erfani (2003), señala que la seguridad en la red informática, dependerá de los controles empleados a nivel lógico y físico, es decir, medidas preventivas y detectoras, tanto en la instalación del hardware como en la configuración del software. Por último, con el mismo enfoque, la guía de seguridad de Red Hat, especifica tres clases de controles que se deben atender, los mismos que son: controles Físicos, controles técnicos y controles administrativos. Estas categorías permiten alinear y garantizar una correcta implementación de la seguridad de la información en una red informática (Red Hat, 2011).

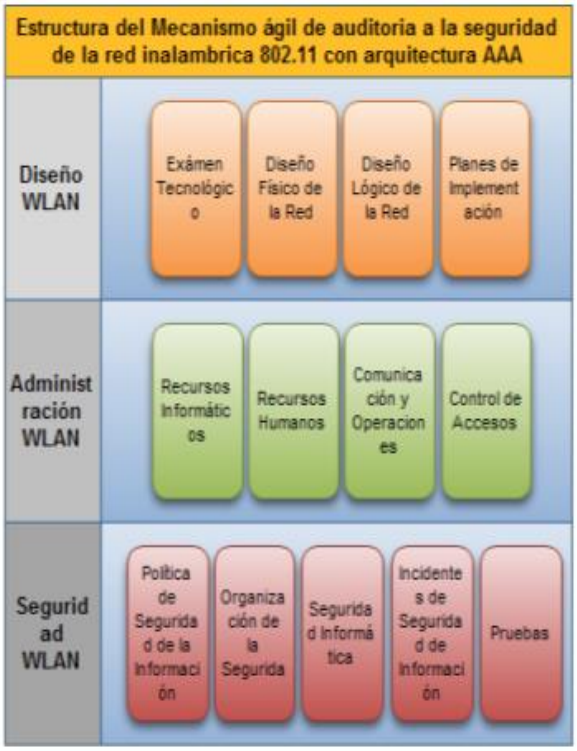
Sin embargo, es necesario considerar una etapa primordial de las redes de datos, conocida como el diseño de la red, etapa en la cual se planificó detenidamente para determinar los servicios que prestaría la red, los tipos de aplicaciones informáticas, la cantidad de usuarios, la ubicación estratégica de los puntos de acceso y otros factores adicionales que en conjunto forman el segmento más largo del diseño de una red. Además, es indispensable considerar el compromiso de la gerencia para identificar, definir y aplicar estrategias y controles de seguridad a la red inalámbrica (Hurley , y otros, 2006).

Por último, es importante definir políticas o normas de seguridad informática para el uso de la red y de los equipos o dispositivos inalámbricos. La política de seguridad debería cercar todas las tecnologías inalámbricas dentro de una organización, como dispositivos inteligentes y ordenadores portátiles. De ahí que la ventaja de contar con una política que cubre todas las comunicaciones inalámbricas ayudará a prolongar su ciclo vital y adaptarse fácilmente a nuevas tecnologías (Earle, 2006, pág. 260) (Zamora Márquez & Plá Feria, 2007).

Por lo tanto, considerando todo lo expuesto anteriormente sobre los controles de seguridad,

para el presente mecanismo ágil de auditoría, se definen tres dominios principales, 13 subdominios y 170 controles de verificación encargados de evaluar la seguridad de la red inalámbrica en una organización. Los tres dominios de evaluación son los siguientes: 1) Diseño WLAN; 2) Administración WLAN y 3) Seguridad WLAN. En el Grafico 2 de muestra los subdominios del mecanismo propuesto.

Gráfico 2: Dominios y subdominios del mecanismo propuesto.



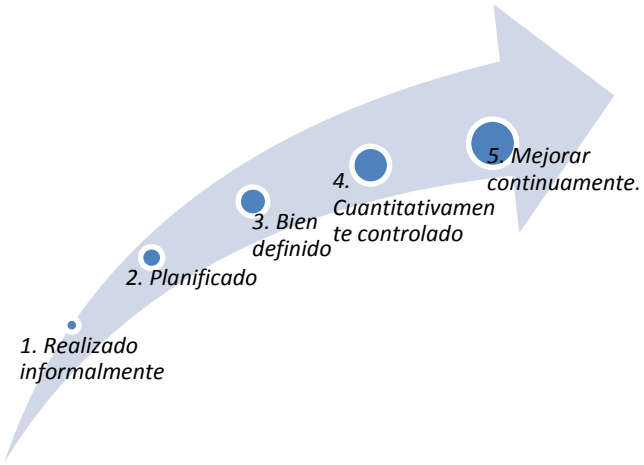
Fuente: Elaborado por los autores

Nivel de madurez

El estándar ISO 21827:2008 especifica el Sistema de Ingeniería de Seguridad - Modelo de Madurez de Capacidad (*SSE-CMM, Systems Security Engineering - Capability Maturity Model*), que describe las características necesarias que deben existir en una organización para garantizar la seguridad. El modelo está dirigido a la seguridad de TI de una organización, puesto que es un estándar métrico que cubre todo el ciclo de vida, incluidas las actividades de desarrollo, explotación, mantenimiento y desmantelamiento; incluye también las interacciones concurrentes con otras disciplinas, como sistemas, software, hardware, factores humanos así como la gestión, operación y mantenimiento del sistema (Shoemaker & Sigler, 2015, pág. 197), (Organización Internacional para la Estandarización [ISO], 2008).

El modelo SSE-CMM o ISO 21827 es aplicable a todas las organizaciones de ingeniería de seguridad, incluyendo entidades gubernamentales, comerciales y académicas. Como se muestra en el Gráfico 3, el nivel más alto de madurez tiene asignado una valoración de 5, niveles que empiezan con: 1. Realizado informalmente; 2. Planificado; 3. Bien definido; 4. Cuantitativamente controlado; y 5. Mejorar continuamente (Macaulay, 2006).

Gráfico 3: El Modelo de madurez de la seguridad SSE-CMM



Fuente: Macaulay (2006).

Adicionalmente, para efectos del presente mecanismo, es conveniente incorporar el nivel 0 al modelo de madurez, con la razón de indicar cuando hay carencia de controles. Por consiguiente, cabe señalar que la puntuación de maduración, varía de 0 a 5, tal como se detalla en la siguiente tabla.

Tabla 3: Descripción de los niveles de madurez

Valor	Nivel de Madurez	Descripción
0	No realizado	Carece de controles o no planes de seguridad en su lugar.
1	Realizado informalmente	Las prácticas de control se realizan generalmente sobre una base ad hoc. Aunque existen medidas individuales Las prácticas no son formalmente adoptadas, rastreadas y reportadas.
2	Planificado	La planificación de la realización del proceso, la formación en la realización del proceso, asignación de recursos al proceso y la asignación de responsabilidad de la realización del proceso son todos dirigidas. Los procesos están planificados, implementados y son repetibles.
3	Bien definido	Además de ser repetibles, los procesos utilizados son más maduros: documentados, aprobados e implementados en toda la organización. La diferencia con el nivel anterior es que el proceso se planifica y se administra utilizando un proceso estándar.
4	Cuantitativamente controlado	La diferencia del nivel anterior es que el proceso definido es cuantitativamente entendido y controlado, es decir, el proceso se mide y verifica. (Se audita)
5	Mejorar continuamente	A diferencia del nivel anterior, en esta etapa los procesos estándar definidos se revisan y actualizan periódicamente. La gestión incluye la evaluación periódica de los procesos y la posterior optimización del proceso.

Fuente: ISO 21827:2008

Con este modelo de madurez, se podrá conocer el nivel de madurez en el que se encuentra la organización en temas de seguridad. Para ello, se debe conocer el grado de madurez de cada uno de los 3 dominios del mecanismo ágil de auditoría, para promediar sus valores y obtener el nivel de madurez de la seguridad de la red inalámbrica de la organización. Además, el mecanismo realizará las sugerencias de las contramedidas a implementar para mejorar la seguridad de la red.

METODOLOGÍA.

Enfoque de la investigación

El enfoque para esta investigación será Mixto. Con el enfoque Cualitativo nos permitirá conocer las sugerencias de las normas o estándares que cumplen efectivamente con el propósito de garantizar la seguridad de la información en la red inalámbrica 802.11. Mientras que, con el enfoque cuantitativo, se podrán ponderar ciertos aspectos de las metodologías, las pruebas de penetración, resultados y controles a implementar para mejorar la seguridad de la red.

Tipo de Investigación

Según Cortes e Iglesias (2004), indican que los estudios descriptivos buscan identificar propiedades de un fenómeno por medio de un análisis, “recolectando datos sobre una serie de cuestiones y se efectúan mediciones sobre ellas, buscan especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice” (pág. 20).

Para el desarrollo metodológico de la presente investigación se empleó una investigación descriptiva, permitiendo así identificar propiedades y características relevantes de los controles de seguridad proporcionados por las norma o estándares seleccionados, seguidamente se efectúa un análisis de los indicadores a tomar en cuenta para evaluar la seguridad de la red, con lo que se logró obtener una lista para las mediciones del cumplimiento de los indicadores de estudio, resultando en la medición del nivel de madurez de la seguridad de la red.

Por otro lado, Ramón (2006), afirma que la Investigación Experimental se efectúa “mediante la manipulación de una variable experimental no comprobada, en condiciones rigurosamente controladas con el fin de descubrir de qué modo

o por que causa se produce una situación o fenómeno particular" (pág. 106).

Para el estudio, es necesario un escenario de pruebas, por lo que se optó por aplicar el mecanismo ágil de auditoría en una institución de educación de nivel superior. Con el caso de estudio se logró recabar valores numéricos que facilitó visualizar los resultados finales.

Por lo tanto, el tipo de investigación será descriptivo-experimental. Primero la investigación descriptiva permitirá identificar las características principales de los controles de los estándares seleccionados. Ayudará a establecer los factores determinante que serán considerados para la propuesta del mecanismo de seguridad. Asimismo, la parte experimental nos ayudara aplicar el mecanismo en una institución de educación de nivel superior. De este experimento obtendremos valores que permitirán aplicar técnicas para el tratamiento de la información.

Diseño

El diseño de esta investigación sigue el proceso investigativo planteado por: Quivy y Van Camplenhoudt (2000), quien plantea siete fases agrupadas en tres componentes principales: la Ruptura, la Estructuración y la Comprobación.

a. La ruptura

En esta primera etapa se desarrolló el planteamiento del problema, que sirvió como punto de partida y el hilo conductor para el desarrollo de este trabajo. Para tal efecto, se realizó el análisis de la revisión de la literatura en temas relacionados con la seguridad informática en redes inalámbricas 802.11, como por ejemplo los reportes anuales de las empresas de seguridad reconocidas para identificar los tipos de ataques que han sufrido, analizar sus vulnerabilidades así como las acciones de mejoras que han adoptado. Además, se analizaron las metodologías ISO 27002, OSSTMM y las sugerencias de las mejores prácticas, para la evaluar la seguridad de las redes inalámbricas 802.11.

b. La estructuración

En esta etapa se determinó la estructuración teórica para soportar la posible respuesta a la problemática presentada en el desarrollo del trabajo. Se seleccionan las características relevantes de cada metodología para definir el mecanismo de seguridad, para lo cual se realizó: 1) Análisis bibliográfico de las metodologías ISO 27002 junto con la metodología OSSTMM y las mejores prácticas; 2) Selección de las herramientas informáticas a utilizar para las pruebas de penetración; y 3) Diseñar un mecanismo ágil de auditoría a la seguridad informática de la red inalámbrica 802.11 con arquitectura AAA.

c. La comprobación

Para verificar la efectividad del modelo propuesto se aplicó el mecanismo de auditoría a la seguridad informática de la red inalámbrica 802.11 de la red inalámbrica del Instituto Tecnológico Superior José Ochoa León (ISTJOL), lo que permitió identificar controles deficientes y el nivel de madurez de la seguridad. Además los resultados obtenidos permitieron tener información valiosa, la misma que fue socializada con el encargado de la red Wi-Fi y docentes del área de Sistemas. Por lo tanto, en este punto se realizaron los siguientes pasos: 1) Aplicación del mecanismo ágil de auditoría a la seguridad informática de la red inalámbrica 802.11, en el ITSJOL; 2) Generar el informe ejecutivo de auditoría; y 3) Análisis de los resultados obtenidos y la socialización de los controles correctivos a realizar.

Alcance de la investigación

El alcance fue de carácter experimental. Se desarrolló un mecanismo ágil de auditoría de la seguridad informática de la red inalámbrica 802.11 con arquitectura AAA, basado en la norma ISO 27002, la metodología OSSTMM y las sugerencias de las mejores prácticas.

Luego, como caso de estudio, se lo aplico el mecanismo en una Institución de Educación Superior, se generó el informe ejecutivo con análisis gráfico, se identificó el nivel de madurez correspondiente a cada dominio evaluado y se socializo las acciones de mejoras con el responsable de la red inalámbrica.

Variables de estudio

Se ha definido como variable independiente la completitud e importancia de los controles implementados para garantizar la seguridad de la red inalámbrica.

De igual manera se ha establecido como variable dependiente, el nivel de madurez evaluado en el cumplimiento de dichos controles.

Población y Muestra

Para el desarrollo de la presente investigación se consideró los estudiantes y docentes de la carrera de Análisis de Sistemas del Instituto Tecnológico Superior José Ochoa León, en la ciudad de Pasaje, en la provincia de El Oro. En la siguiente tabla se detalla la población identificada.

Tabla 4: Población y Muestra

Población	Involucrados cantidad	Muestra
Docentes	22	22
Estudiantes	380	175
TOTAL	**395**	**172**

Fuente: Secretaría General del ITSJOL.

Método para recolectar datos

Escala Likert para medir el grado de madurez del control implementado en la organización. Esta escala le permitirá al auditor ubicar el nivel de cumplimiento del control. Para el análisis de la información recolectada se lo efectuar mediante estadística descriptiva.

Además, otra técnica utilizada fueron las encuestas, aplicadas a administradores de red y personal de seguridad informática. Para el análisis de los datos se utilizaron estadística descriptiva.

Por último, la técnica de la observación se utiliza el caso de estudio para aplicación del mecanismo diseñado para la evaluación de seguridad de la red inalámbrica 802.11 el que proveerá de información cuantitativa que permitirá la medición, clasificación y categorización de lo observado. El análisis de los datos se lo efectuará de manera gráfica por medio del análisis de frecuencias y estadística descriptiva.

ANÁLISIS DE RESULTADOS

La primera aplicación del mecanismo ágil de auditoría en la institución, permitió corregir y ajustar la eficiencia del mecanismo de verificación, como por ejemplo ciertos controles que estaban duplicados o que tenían la misma intención, así como disminuir la exigencia del mecanismo, es decir, que según el modelo de madurez, en primera instancia se definió que el nivel aceptable seria el nivel 4 (controlado), posteriormente se estableció que el nivel aceptable debía ser el nivel 2 (planificado), puesto que la intención del mecanismo es de verificar que el control exista.

En la segunda aplicación del mecanismo, se logró obtener valiosos resultados para el análisis correspondiente. Cabe indicar que al tratarse de variables ordinales, que fueron utilizadas para medir el nivel de madurez de la seguridad inalámbrica, es imposible determinar la distancia entre sus categorías, por lo tanto se realiza el análisis grafico de los resultados obtenidos en la evaluación y luego las frecuencias de los niveles de madurez seleccionados.

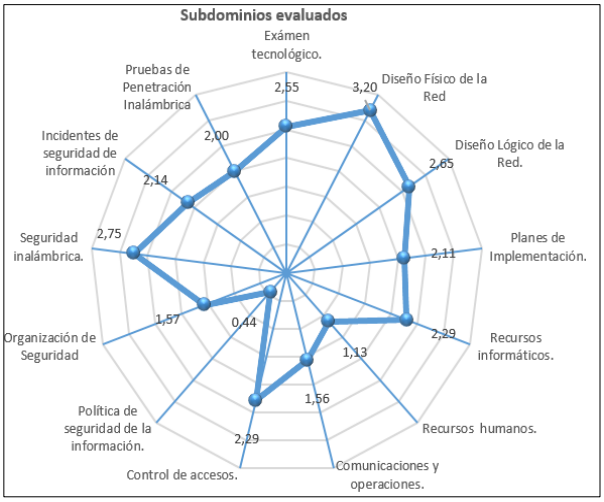
Análisis gráfico

En primera instancia, se efectúa un análisis de los valores obtenidos en cada subdominio, dicho valor corresponde al promedio del conjunto de controles verificados correspondientes a cada uno de los 13 subdominios evaluados, donde se

observa que existen algunos valores promedios que se encuentran por debajo del nivel aceptable (2 planificado), como lo es el subdominio de recursos humanos que alcanza un valor de 1.13 (con respecto al valor máximo que es 5); el subdominio de comunicaciones y operaciones tiene 1.56; de igual forma el subdominio de operación de la seguridad alcanza un valor de 1.57; y por último el valor más bajo de todos, que pertenece al subdominio de política de seguridad de información con un valor de 0.44.

Sin embargo, los otros 9 subdominios alcanzan valores comprendido entre 2 y 3, es decir que existen controles que han sido planificados y otros que están bien definidos, que aunque no están optimizados (5 mejora continua), cumplen un rol efectivo pero no eficiente en la institución.

Gráfico 4: Subdominios evaluados



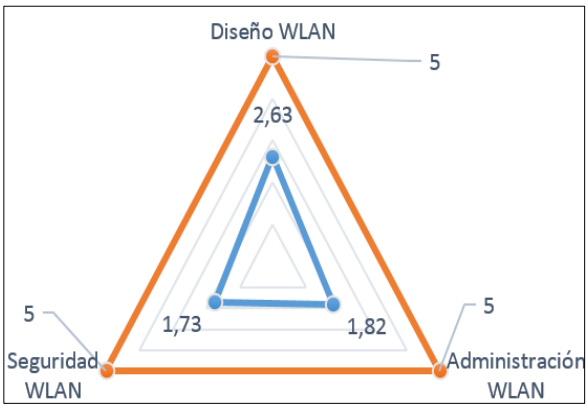
Fuente: Elaborado por el autor.

De igual forma, se analiza los resultados de cada uno de los 3 dominios que componen el mecanismo ágil de auditoría, para ello se promedian los valores obtenidos de los subdominios pertenecientes a cada dominio. Por ejemplo al primer dominio: Diseño de WLAN, le corresponde 3 subdominios, que al promediar sus resultados alcanza un valor de 2.63, que corresponde a un nivel de madurez aceptable, sin embargo, es un estado que necesariamente debe mejorar.

Así mismo, el dominio, Administración WLAN alcanza una valoración de 1.82, lo que representa un nivel deficiente, debido a que los controles se han implementado de forma empírica, lo que puede significar que no se toma en cuenta a otros controles relacionados a este dominio.

Por último, el dominio, Seguridad en la WLAN alcanza un valor de 1.73, resultado que denota falta de controles y efectividad de los mismos, por lo que es indispensable, al menos en este dominio por tratarse de la seguridad inalámbrica, efectuar una revisión integral de los documentos de seguridad y estrategias implementadas.

Gráfico 5: Evaluación de los dominios del mecanismo.



Fuente: Elaborado por el autor

Desde otra perspectiva, se analizó las frecuencias de cada variable ordinal, en los 141 controles evaluados en el Instituto, para agrupar las respuestas de los niveles de madurez según cada dominio de evaluación. Los resultados provienen de la evaluación de cada uno de los controles pertenecientes al dominio, como muestra la Tabla 5. Se encontró, que la mayor parte de los controles verificados se encuentran en los últimos niveles, de lo que se deduce que la organización debe implementar o mejorar un total de 63 controles, equivalente al 49% del total de los controles verificados, donde se evidencia que la organización se encuentra en riesgo de sufrir algún tipo de ataque a la seguridad en la red inalámbrica.

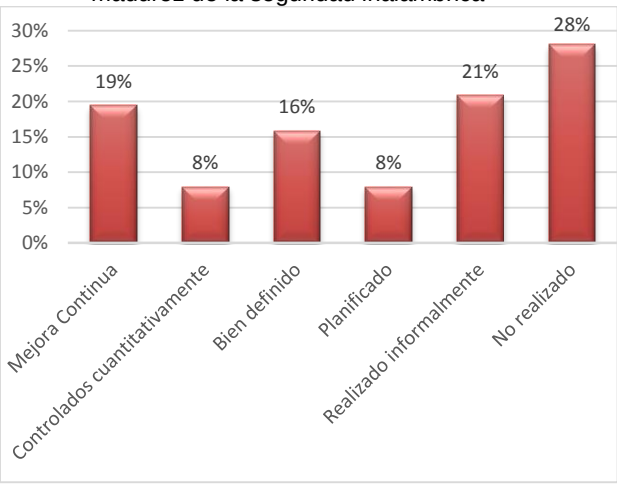
Tabla 5: Frecuencias de los niveles de madurez agrupados por dominio

Diseño WLAN	Administración WLAN	Seguridad WLAN	Dominio / Madurez
8	7	10	(5) Mejorar continuamente
10	1		(4) Cuantitativamente controlado
13	9		(3) Bien definido
5	6	5	(2) Planificado
3	17	4	(1) Realizado informalmente
11	12	16	(0) No realizado

Fuente: Elaborado por el autor.

Además, en el Grafico 6, se observa el porcentaje de los niveles de madurez que se han señalado para indicar el nivel de cumplimiento de cada control evaluado. Es evidente que el porcentaje más alto (28%) corresponden a controles inexistentes en el instituto y el 21% de los controles se han implementado informalmente lo que demuestra que no se ha planificado para implementar este grupo controles y carecen de un respectivo monitoreo o seguimiento, por lo que se puede afirmar que no se han considerado muchos aspectos relacionados con la seguridad en la red inalámbrica.

Gráfico 6: Grado del cumplimiento de los niveles de madurez de la seguridad inalámbrica



Fuente: Elaborado por el autor.

Finalmente, para cumplir con el objetivo planteado para la presente investigación, se determinó el estado de madurez de la seguridad inalámbrica del Instituto, esto de forma integral, para el efecto se calculó el promedio de los tres dominios evaluados, donde se obtuvo un valor de 2.06, que respecto al valor máximo que es 5 (Mejora continua), corresponde a un nivel de madurez de: Planificado. Además, el porcentaje equivalente por el cumplimiento de los controles evaluados es de 41%, que aunque es un resultado aceptable deja notar que existen algunos controles que no se han realizados hasta el momento, por lo que al implementarlos incrementaría el porcentaje de cumplimiento y, por lo tanto, a la seguridad en la red.

CONCLUSIONES

En base a la información revisada y analizada para el presente estudio, implantar y mantener una arquitectura AAA resulta considerablemente costoso, y algunas empresas no disponen de presupuesto suficiente. Por lo tanto, las auditorías a la red inalámbrica, el monitoreo constante de los controles de protección, como son los IDS/IPS, contar con una política de seguridad informática bien definida, así como las capacitaciones periódicas a los usuarios y disponer del equipamiento mínimo de firewall y sistemas robustos de autenticación, autorización y registro de actividades, disminuye notablemente las posibilidad de sufrir un ataque en la red inalámbrica. Además, se reconoce el crecimiento de los diferentes tipos ataques informáticos que se han detectado en estos últimos años.

Por ello, es indispensable que el encargado de la seguridad cuente con los conocimientos y herramientas adecuadas, para que logre analizar los grandes volúmenes de información que generan los procesos de autenticación y autorización por cada conexión que se realiza. Tener conocimiento en Big Data, contribuye a identificar posibles amenazas mediante el análisis de los registro y el reconocimiento de patrones y predecir ataques por medio de la explotación de alguna vulnerabilidad.

Por lo tanto, el mecanismo ágil de auditoría cumplió con las expectativas esperadas. La integración de la metodología OSSTMM y la norma ISO 27002, con sus mejores prácticas hacen del mecanismo una herramienta efectiva y eficiente, puesto que permitió identificar 39 controles que no están implementados y 24 controles que se han implementado informalmente, resultados que, en términos porcentuales, alcanzan un 49% de los controles verificados, los mismos que necesitan atención inmediata. Además, el subdominio que corresponde al componente de pruebas de penetración inalámbrica permitió determinar que la organización era susceptible a ataques MITM, utilizando la herramienta AIRSSL para el secuestro de sesión. Asimismo, otra prueba realizada fue la creación de un punto de acceso no autorizado el mismo que no tuvo mayor efecto en el Instituto.

Por consiguiente, los resultados obtenidos en el caso de estudio demostraron un nivel de seguridad poco satisfactorio. Por lo que es necesario que se realice un monitoreo constante a la red inalámbrica. Además, el modelo de madurez seleccionado, es similar a otros modelos mundialmente reconocidos como por ejemplo Cobit y el NIST, por lo que se incrementa la confianza en la eficacia del mecanismo ágil de auditoría.

La única limitación que surgió en la presente investigación tiene que ver con la falta de recursos de hardware puesto que se requería para ejecutar pruebas de penetración en un ambiente controlado previo al caso de estudio, por tal motivo solo se incluyó, en el subdominio Pruebas, 6 pruebas penetración a la red inalámbrica.

Por último, como una futura investigación, en base al mecanismo diseñado, se podría desarrollar un mecanismo similar para evaluar el grado de cumplimiento del plan de continuidad del negocio, para determinar si se han identificado y ordenado las amenazas internas y externas, el impacto en la organización y la eficiencia del plan de respuesta y recuperación.

REFERENCIAS BIBLIOGRÁFICAS

Martínez, A., & Gómez, M. (2009). Control de acceso a Redes Inalámbricas. Revista Técnica de la Empresa de Telecomunicaciones de Cuba S.A., 83-88.

Alabady, J. S. (2008). Diseño e Implementación de un modelo de seguridad de red con VLAN estática y servidor AAA. IEEE Xplore.

Ali, S., & Heriyanto, T. (2011). BackTrack 4 Assuring Security by Penetration Testing : Assuring Security by Penetration Testing. Olton: Packt Publishing.

Barchini, G. E., Sosa, M., & Herrera, S. (2004). La informática como disciplina científica. Ensayo de mapeo disciplinar. Revista de Informática Educativa y Medios Audiovisuales.

Bautts, T., Dawson, T., & Purdy, G. N. (2005). Linux. Guía para administradores de redes. España: ANAYA MULTIMEDIA.

Beggs, R. W. (2014). Mastering Kali Linux for Advanced Penetration Testing. BIRMINGHAM - MUMBAI: PACKT.

Bellido, W. J. (2013). Ethical Hacking: Hacking de Red Inalámbrica Wifi. Revista de Información, Tecnología y Sociedad.

Buritica, A. (2016). 802.11ax - High Efficiency Wireless. Microwave Journal, 62-72.

Bustamante, M. G., & Osorio, C. J. (2014). Metodología de la seguridad de la información como medida de protección en pequeñas empresas. Cuaderno Activa, 71-77.

Byung-Gil, L., Doo-Ho, C., Hyun-Gon, K., Sohn, S.-W., & Parque, K.-H. (2003). IP móvil y WLAN con el protocolo de autenticación AAA utilizando la

criptografía basada en la identidad. IEEE Xplore, 597 - 603 vol.1.

Caicedo, O., De La Cruz, E., & Taimal, G. (2010). Middleware de seguridad para el interworking WLAN-IMS. Facultad de Ingeniería Universidad de Antioquia, 193-202.

Capano, D. d. (2015). Wireless intrusion detection and protection systems. Control Engineering, 62-80.

Cardwell, K. (2013). BackTrack : Testing Wireless Network Security. Olton: Packt Publishing.

Castillo, R. S. (2006). Detección de Intrusos mediante Técnicas de Minería de Datos. Clepsidra, 31-44.

Cheng, J., Hu, L., Liu, J., Zhang, Q., & Yan, C. (2014). A New Mechanism for Network Monitoring and Shielding in Wireless LAN . Mathematical Problems in Engineering.

Chui, S. H. (2009). Seguridad de la red inalámbrica 802.11. Ciens.

CISCO. (2012). BYOD: una perspectiva global. Internet Business Solutions Group [IBSG].

CISCO. (2015). Informe anual de seguridad de Cisco 2014.

CISCO. (2016). Informe anual de seguridad de Cisco 2016. San José.

Comunidad de Prácticas APS. (2012). ¿QUÉ ES UNA BUENA PRÁCTICA? Chile.

Cortés, M. E., & Iglesias, M. L. (2004). Generalidades sobre Metodología de la Investigación. México.

Díaz, O., Alzórriz, A., & Ruiz, I. S. (2014). Procesos y herramientas para la seguridad de redes. Madrid: UNED - Universidad Nacional de Educación a Distancia.

Earle, A. E. (2006). Wireless Security Handbook . New York: Auerbach Publications.

Erfani, S. (2003). Security Functional Architecture. Ingeniería Eléctrica y Computación. Ontario - Canada: University of Windsor.

ESET. (2015). ESET Security Report. Eset.

ESET. (2017). Informe de Tendencias 2017: La seguridad como rehén.

Ferreira, P. L., Petter, D. R., Maran, V., & Ellwanger, C. (2015). Um Método para Minimizar Falhas de Segurança em Redes WLAN 802.11b/g: Controlando Acessos Provenientes de Dispositivos Móveis . Anais do EATI, 39-46.

FORCEPOINT. (2017). 2016 Global Threat Report . España.

Fulgueira, C. M., Fuenteseca, H. V., & Hernández, D. O. (2015). Paralelización del Algoritmo Criptográfico GOST Empleando el Paradigma de Memoria Compartida. Lámpsakos, 18-24.

Gomes, R. &. (2008). The adoption of IT security standards in a healthcare environment. Studies In Health Technology And Informatics, 765-770.

Heru, S., Mohammad, N. A., & Yong, C. T. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences, 23-29.

Horváth, M., & Jakub, M. (2009). Implementation of security controls according to ISO/IEC 27002 in a small. Quality Innovation Prosperity, 48-54.

Hsu, C., Nat. Taiwan University, T. T., Wang, T., & Lu, A. (2016). El impacto de la norma ISO 27001 sobre los resultados empresariales. IEEE Xplore, 4842 - 4848.

Hurley , C., Baker , B., Barnes , C., Bautts , T., Bonawitz , D., Bruno , A., & Connelly , D. (2006). How to Cheat at Securing a Wireless Network . Rockland, Massachusetts: Syngress Publishing, Inc.

Intel. (2016). De la sala de computo a la sala directiva: Informe anual de desempeño de TI de Intel 2015-2016.

Iqbal, A., Horie, D., Goto, Y., & Cheng., J. (2009). A Database System for Effective Utilization of ISO/IEC. IEEE Computer Society, 607-612.

Jara, H., & Pacheco, F. (2012). Ethical Hacking 2.0. Buenos Aires.

Johns, A. (2015). Mastering Wireless Penetration Testing for Highly Secured Environments. Birmingham - Mumbai: Packt Publishing.

Joshi, J., McCabe, S. ,., Davie, B. S., Peterson, L. L., Farrel, A., Ramaswami, R., . . . Yu-Sung. (2008). Network Security Know It All. Estados Unidos: ELSERVIER.

Kaklauskas, L., & Rathosi, I. (2014). ŠIAULIŲ MIESTO BELAIDŽIŲ TINKLŲ SAUGOS TYRIMAS. Studies in Modern Society, 131-137.

Karygiannis, T., & Owens, L. (2002). NIST Special Publication 800-48: Wireless Network Security 802.11, Bluetooth and Handheld Devices . Gaithersburg, Maryland: National Institute of Standards and Technology.

Laudon, K., & Laudon, J. (1997). Essentials of Managment. US: Prentice Hall.

Lehembre, G. (2006). Seguridad Wi-Fi – WEP, WPA y WPA2. Hakin9, 12-26.

Li, X., Ma, J., & Yulong, S. (2012). Un protocolo de autenticación de acceso WLAN inicial eficiente. IEEE Xplore, 1035 - 1040.

Liang, W., & Wang, W. (2004). Un esquema de control de autenticación local basado en la arquitectura de AAA en las redes inalámbricas. IEEE Xplore, 5276 - 5280.

Lorincz, J. .., Udovicic, G. .., & Begušić, D. (2007). Arquitectura de bases de datos SQL para el control de acceso WLAN y contabilidad. IEEEE Xplore.

Macaulay, T. (2006). Securing Converged IP Networks. New York: Auerbach.

Martelo, R. J., Madera, J. E., & Betín, A. D. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). Información tecnológica , 129-134.

Martínez, A. A., & Gómez, M. C. (2009). Control de acceso en redes inalámbricas. Revista Técnica de la Empresa de Telecomunicaciones de Cuba, S.A., 83-88.

Mathews, M., & Hunt, R. (2007). EVOLUTION OF WIRELESS LAN SECURITY ARCHITECTURE TO IEEE 802.11i (WPA2). AsiaCSN '07 Proceedings of the Fourth IASTED Asian Conference on Communication Systems and Networks table of contents, 292-297.

McAfee. (2016). Informe de McAfee Labs sobre amenazas, septiembre de 2016.

Meb, C. (2009). Protocolos de la AAA: autenticación, autorización y contabilidad para Internet. IEEE Xplore, 75-79.

Méndez, W., Mosquera, D. J., & Trujillo, E. R. (2015). Vulnerabilidad de protocolos de encriptación WEP, WPA y WPA2 en redes inalámbricas con plataforma Linux. Tecnura, 79-87.

Mesquida, C. A. (2012). Un Modelo para Facilitar la Integración de Estándares de Gestión de TI en Entornos Maduros (Tesis Doctoral). Universitat de les Illes Balears, Palma.

Moeller, R. R. (2013). Executive's Guide to COSO Internal Controls : Understanding and Implementing the New Framework. Somerset, EE.UU: Wiley .

Montesino, P. R., Baluja, G. W., & Porvén, R. J. (2013). Gestión automatizada e integrada de controles de seguridad informática. Ingeniería Electrónica, Automática y Comunicaciones, 40-58.

Mookiah, P., Walsh, J. M., Greenstad, R., & Dandekar, K. R. (2013). Reconfigurable Antenna Assisted Intrusion Detection in Wireless Networks. International Journal of Distributed Sensor Networks.

Nakhjiri. (2005). AAA and network security for mobile access . England: John Wiley & Sons Ltd.

Navarro, J., & Ascencio, É. d. (2016). ANÁLISIS DE LOS MECANISMOS DE SEGURIDAD EN REDES INALÁMBRICAS DE ÁREA LOCAL (WLAN). RES NON VERBA, 47-54.

Ndaw, M., Mendy, G., & Ouya, S. (2016). Modeling the Impact of Controls on Information System Risks . Network, 13-17.

Noor, A. I., & Mohamad, N. K. (2010). Wireless Local Area Network (LAN) Security Guideline . Malasia: CyberSecurity Malaysia.

Ochoa Ovalle, S., & Cervantes Sánchez, O. (2012). SEGURIDAD INFORMÁTICA . Contribuciones a las Ciencias Sociales.

Organización Internacional para la Estandarización [ISO]. (2008). iso.org. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:21827:ed-2:v1:en

Perahia, E., & Stacey, R. (2013). Next Generation Wireless LANs: 802.11n and 802.11ac. Reino Unido: Cambridge University Press.

Poddar, V., & Choudhary, H. (2014). A COMPARITIVE ANALYSIS OF WIRELESS SECURITY PROTOCOLS (WEP and WPA2). International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 3.

Preetham, V. (2002). Internet Security and Firewalls . Boston: Course Technology / Cengage Learning.

Prodanovic, R., & Simic, D. (2007). A Survey of Wireless Security. Journal of Computing and Information Technology - CIT 15, 237–255.

Quezada Reyes, C. (2015). Mecanismos de seguridad. Universidad Nacional Autónoma de México, Depto. de Ingeniería en Computación, México.

Quivy, R., & Campenhoudt, V. (2000). Manual de investigación en ciencias sociales. México.

RAE. (1 de Diciembre de 2016). Diccionario de la lengua española [DLE].

Ramachandran, V. (2011). BackTrack 5 Wireless Penetration Testing Beginners Guide . Olton: Packt.

Ramón, R. E. (2006). Historia y Evolución del Pensamiento Científico. México.

Red Hat. (2011). Red Hat Enterprise Linux 6 Guía de seguridad. redhat.

Sangkyun, K. (2011). Classification of ISO27002 Controls. Models and Methods in Applied Sciences, 62-65.

Shannon, C. E., & Weaver, W. (1949). Teoría matemática de la comunicación. España: Forja.

Shoemaker, D., & Sigler, K. (2015). Cybersecurity: Engineering a Secure Information Technology Organization . USA: CENGAGE Learning.

Silva, E., Machado, I., Oliveira, M., & Amorim, R. (2007). Metodologia Osstmm para Teste De Segurança em Ti . Edilms, 1-7.

Silva, F., & Ludwig, G. A. (2011). Desenvolvimento de uma Metodologia para Auditoría em Redes Sem Fio IEEE 802.11b/g. En: VIII Simpósio Brasileiro em Segurança, 337-346.

Syngress, Liu, D., & Miller, S. (2006). Firewall Policies and VPN Configurations . Rockland: Syngress.

Talib, M., Adel , K., & Barachi, M. (2011). "Estudio exploratorio Sobre el USO Innovador de las Normas ISO Para La Seguridad de TI en los EAU". IEEE Xplore.

Talib, M., Khelifi, A. .., & Ugurlu, T. (2012). Using ISO 27001 in teaching information security. IEEE Xplore, 3149 - 3153.

Tejvir, K., Vimmi, M., & Dheerendra, S. (2014). Comparison of network security tools-Firewall, Intrusion Detection System and Honeypot. International Journal of Enhanced Research in Science Technology & Engineering, 200-204.

Thomas, N., Willis, M., & Craig, K. (2006). Analysis of Co-Existence between IEEE 802.11 and IEEE 802.16 Systems. 3rd Sensor and Ad Hoc Communications and Networks, 2006. SECON , 615-620.

Touhill, Gregory, J., & Touhill, C. J. (2014). Cybersecurity for Executives : A Practical Guide . EE.UU: Wiley-AIChE.

USER. (2011). Hacking desde Cero. Buenos Aires.

Valdez, A. A. (2013). OSSTMM 3. Revista de Información, Tecnología y Sociedad.

Valencia Blanco, L. S. (2013). Metodologías Ethical Hacking. Revistas Bolivianas, 27-28.

Wagner, N., Lippmann, R., Winterrose, M., Riordan, J., Yu, T., & Streilein, W. W. (2015). Agent-based Simulation for Assessing Network Security Risk due to Unauthorized Hardware . Society for Modeling & Simulation International (SCS) , 18-26.

Wall, D. (2004). Managing and Securing a Cisco Structured Wireless-Aware Network. Rockland, US: Syngress.

Wilhelm, T. (2013). Professional Penetration Testing : Creating and Learning in a Hacking Lab (2) . Saint Louis, Estados Unidos: Syngress.

Yago, F. H. (2008). RADIUS / AAA / 802.1X. Sistemas basados en la autenticación para Windows y Linux. Madrid: Rama.

Zamora Márquez, M., & Plá Feria, P. J. (2007). Seguridad en redes inalámbricas. Revista Técnica de la Empresa de Telecomunicaciones de Cuba S.A, 98-104.

Zhou, J., Xin, Y., Nan , W., & Li, L. (2006). Una arquitectura de seguridad para redes inalámbricas IEEE 802.11 en gran escala las empresas multinacionales. IEEE Xplore, 846-849.