Visión Antataura
Vol.2, No.2: 33-48
Diciembre 2018 - Mayo 2019
Panamá
ISSN 2520-9892

Modelo de estimación del nivel de seguridad en redes inalámbricas que utilizan tecnología Wi-Fi

Security level estimation model for wireless networks using Wi-Fi technology

Edwin J. Cedeño Herrera[1], Óscar E. Rodríguez C.[2], Gloris M. Batista de Cedeño.[3]

[1]Ph.D en Ingeniería de Sistemas Telemáticos; Docente, Universidad de Panamá, Centro Regional Universitario de Veraguas; edwin.cedenoh@up.ac.pa
[2]Magister en Sistemas Computacionales; Docente, Universidad de Panamá, Centro Regional Universitario de Veraguas; oseroca.rodriguez@up.ac.pa
[3]Magister en Administración de Negocios; Docente, Universidad de Panamá, Centro Regional Universitario de Veraguas; gloris.batista@up.ac.pa

Resumen: Con el propósito de estimar los niveles de seguridad en las redes inalámbricas que utilizan tecnología Wi-Fi, se realizó un recorrido por las principales avenidas del distrito de Santiago de Veraguas, aplicando la técnica de *WarDriving* y la herramienta *NetStumbler*, para escanear las redes inalámbricas. Esta exploración fue realizada durante 4 semanas, entre los meses de enero a marzo de 2017. Para el análisis de los puntos de acceso (AP), se propone un modelo de estimación de los niveles de seguridad, el cual está basado en los siguientes criterios: confidencialidad, autentificación, integridad, disponibilidad y no repudio. Estos criterios presentan indicadores que permiten cuantificarlos. Los resultados de la estimación de los niveles de seguridad en redes W-Fi analizados con el modelo propuesto, muestran que el 33% está en un nivel "muy bajo", un 64% tienen un nivel "bajo" y el 3% observan un nivel "muy alto".

Palabras clave: redes de área local, tecnología Wi-Fi, modelo de evaluación, punto de acceso, seguridad.

Abstract: In order to estimate the security levels in wireless networks which use Wi-Fi technology, a tour by the main avenues in Santiago, Veraguas was made. The inspection was carried out using the WarDriving technique and the NetStumbler tool with the purpose of scanning wireless networks. This was done during 4 weeks, from January to March of 2017. For the analysis of the access points (AP), a security level estimation model is proposed based on the following criteria: Confidentiality, Authentication, Integrity, Availability, and Non-repudiation. These criteria present indicators that allow quantifying them. The results of the estimation of security levels in the W-Fi networks analyzed with the proposed model show that 33% of them are at a "very low" level, 64% are at a "low" level, and 3% show a "very high" level.

Key words: local area networks, Wi-Fi technology, evaluation model, access point, security.

Fecha de recepción: 28 de septiembre de 2018 *Fecha de aceptación: 27 de noviembre de 2018*

1. Introducción

La movilidad hacia cualquier sitio dentro de su cobertura, su fácil instalación, rapidez, simplicidad en la utilización, la flexibilidad, el acceso, la facilidad de incorporar redes en cualquier lugar sin necesidad de extender el cableado, la adaptabilidad a los frecuentes cambios de la topología de la red y la escalabilidad, son algunos de los principales factores que actualmente hacen de la tecnología inalámbrica una de las opciones que ofrecen un sinnúmero de ventajas en el proceso de transmisión de datos. Sin embargo, estas facilidades han llevado a empresarios, ingenieros y demás personas a pensar que no es necesario ser un especialista para instalar, configurar y poner en marcha redes con tecnología Wi-Fi, lo que resulta ser uno de sus grandes inconvenientes, puesto que estas utilizan la radio-frecuencia como medio de difusión a través del aire (Reid y Seide, 2004).

Esto propicia que cualquier persona, con un mínimo de conocimiento en redes, pueda capturar y escuchar los paquetes de datos que se transmiten a través del medio (Academia de Networking de CISCO Systems, 2006). Esta característica particular hace que, cuando se utilice tecnología Wi-Fi en las redes de áreas locales, la seguridad sea considerada como su talón de Aquiles (Pérez, 2003).

El estudio realizado por la empresa Panda Software International, en el año 2005, cuyo alcance fue de 12 ciudades pertenecientes a 9 países europeos y americanos, tuvo como objetivo comprobar el nivel de concienciación de empresas y entidades particulares con relación a la seguridad de sus redes de áreas locales con tecnología Wi-Fi (Software, Panda, 2005). Citando los resultados de este estudio, en términos generales, la seguridad es pobre, ya que la mitad de las redes no contaban entre otros aspectos, con sistemas de cifrado adecuados para evitar la intrusión de usuarios en el sistema inalámbrico. De un total de 905 redes analizadas, 374 (41.33%) disponían de algún sistema de cifrado, mientras que 531, lo que representó un sorprendente 58,37%, carecía de este.

El caso se agrava cuando se analiza que, dentro de las redes desprovistas de sistema de cifrado, se conserva el identificador y el fabricante de la red por defecto, lo cual representó el 3.75% de las redes, lo que puede ser indicativo de una configuración también

por defecto, y que provee la coyuntura para que haya una alta probabilidad de ataque contra estas, con sus consecuentes repercusiones.

Un aspecto muy importante que se vincula como referente principal, y que sirve de base técnica para la investigación en nuestro contexto, son las publicaciones digitales emitidas por el diario "Martes Financiero", en el año 2015, en donde los estudios realizados por la compañía independiente y especializada en consultorías, en cuanto a seguridad de la información, riesgos tecnológicos y auditorías internas RISCCO (RISCCO, 2017), señalan la poca confianza en la forma cómo las organizaciones están protegiendo los datos personales (Revista Digital Martes Financiero, 2015).

Durante ese mismo año, la consultora publicó los resultados del sondeo realizado durante los meses de marzo y abril sobre el cibercrimen en Panamá, en el cual participaron 133 ejecutivos de organizaciones privadas e instituciones del Estado. Se buscaba detectar y demostrar si las empresas en Panamá están preparadas para prevenir y afrontar un ataque cibernético (Revista Digital El Financiero, 2015).

Los resultados fueron alarmantes, puesto que el 92% de los participantes consideraron que pueden ser blanco de cibercrímenes; sin embargo, solo el 24% dijo estar preparado para resistirlo de forma exitosa.

En el año 2017, la consultora realizó el mismo sondeo y se determinó que el 94% de los participantes consideraron que pueden ser blanco de ciberataques; sin embargo, solo el 32% dijo estar preparado para resistirlos de forma exitosa (Diario Digital Panamá24Horas, 2017). Los datos resultantes de estos sondeos, ameritan reflexión, ya que, al compararlos con los resultados del año 2015, pareciera que, en materia de seguridad de información, el tiempo no pasa en Panamá (Ayala, 2017). Lo expuesto pone de manifiesto aspectos de suma importancia en el contexto de la seguridad de la tecnología Wi-Fi y del desarrollo de las operaciones administrativas y comerciales de las empresas en Panamá.

El objetivo principal del estudio es definir un modelo de estimación de los niveles de seguridad en las redes de área local que utilizan tecnología Wi-Fi. Es por ello que se realiza

un diagnóstico en la ciudad de Santiago, provincia de Veraguas, aplicando el modelo de estimación propuesto.

2. Materiales y métodos

Se elaboró una encuesta que contenía 10 preguntas de tipo selectivas (opción múltiple), la cual se aplicó a 15 profesores especialistas en el área de redes de computadoras, quienes laboran en las 3 universidades estatales ubicadas en el distrito de Santiago, provincia de Veraguas. Su finalidad era la de establecer los pesos de los criterios para ponderar los niveles de la seguridad en las redes de área local que utilizan tecnología Wi-Fi. Estos se definen conceptualmente de la siguiente manera (Association for Progressive Communications (APC), 2015):

Confidencialidad: Asegurar que la información no sea divulgada a personas no autorizadas en cuanto a procesos o dispositivos.

Autenticación: Su objetivo en cuanto al diseño es establecer la validez de una transmisión, mensaje o remitente, o un medio para verificar la autorización de un individuo para recibir categorías específicas de información.

Integridad: La calidad de un sistema de información refleja el correcto funcionamiento y confiabilidad del sistema operativo, la coherencia del hardware y del software que implementan los sistemas de protección y la consistencia de las estructuras de datos de la información almacenada. En otras palabras, la integridad consiste en la capacidad de un protocolo inalámbrico para determinar si la información transmitida ha sido alterada por personas no autorizadas.

Disponibilidad: Acceso oportuno y confiable a datos y servicios de información para usuarios autorizados.

No Repudio: Asegurar que el remitente de la información posee evidencia del envío y que el receptor posee evidencia de la identidad del remitente, de manera que ninguna de las partes pueda negar el proceso de dicha información.

Los indicadores representan las acciones que denotan la presencia o ausencia, en alguna medida, de los criterios de seguridad antes señalados (Common Criteria for Information Technology Security Evaluation, 2016).

Para operacionalizar estos criterios mediante indicadores, se realizaron acciones para cada uno de los mismos; estos dependían del diseño, de las políticas de seguridad que se deseaban y del contexto que marcaba la implementación. Los indicadores para cada uno de los criterios que se presentan a continuación, han sido extraídos del informe del proyecto capacity building for wireless connectivity in LAC region (TRICALCAR), el cual pertenece a la Association for Progressive Communications (APC), cuyos recursos están disponibles en el sitio web itrainonline, específicamente en la sección de Wireless Security (Escudero Pascual, 2008).

Confidencialidad:

- Verificar el algoritmo de cifrado
- Monitorear o medir el SNR (Signal Noise Ratio)
- Verificar si se está publicando el SSID (Service Set IDentifier)
- Monitorear la dirección Mac de su conexión (Domenico Aime, Calanrtiello, & Lioy, 2007)

Autenticación:

- Verificar la autenticación: abierta o cerrada
- Verificar si se está publicando el SSID (Domenico Aime, Calanrtiello y Lioy, 2007)
- Utilizar filtrado de MAC's (Media Access Control)
- Implementar portales cautivos
- Control de acceso implementado en el IEEE 802.1X (Jyh-Cheng, Ming-Chia y Yi-Wen, 2005)

Integridad:

- Aplicar cifrado a las comunicaciones (capas superiores)
- Utilizar cifrado en capa de enlace

Disponibilidad:

- Rastrear periódicamente las frecuencias de radio (Domenico Aime, Calanrtiello y Lioy, 2007)
- Monitorear las retransmisiones de los AP (Access Point)
- Monitorear los tráficos ICMP (Internet Control Message Protocol) y UDP (User Datagram Protocol)

No Repudio:

- Implementar la red inalámbrica fuera del *firewall*
- Implementar VPN (Virtual Private Network)
- Controlar el acceso en el protocolo IEEE 802.1X
- Implementar portal cautivo
- Implementaciones de firmas digitales

Para realizar las ponderaciones, se aplicó un modelo matemático y de escala, el cual permitió establecer las siguientes relaciones entre los Indicadores de Seguridad Wi-Fi ($\boldsymbol{ISW}$) y las siguientes variables:

- $\boldsymbol{PCS}$ = Valor porcentual del criterio
- $\boldsymbol{CS}$ = Criterio de seguridad
- $\boldsymbol{P}$ = Peso total de la unidad de análisis

Considerando que la presencia de cada indicador es ponderada con base en su importancia, según el criterio, entonces tenemos la siguiente expresión:

$$CS_k = \left(\left(\sum_{i=1}^{n} ISW_i \right) * PCS_k \right) / 100$$

En donde:

$[\boldsymbol{k}]$ = {Confidencialidad, autenticación, integridad, disponibilidad, no repudio}

$[\boldsymbol{i}]$ = {Cifrado, no publicar SSID, filtrado de Mac, portales cautivos, monitoreo de Mac, monitoreo del SNR, monitoreo de frecuencias, monitoreo de retransmisiones, monitoreo ICMP/UDP, red Wi-Fi fuera del firewall, VPN, firmas digitales}.

$[\boldsymbol{n}]$ = cantidad de indicadores de seguridad Wi-Fi.

La sumatoria de los porcentajes de peso para cada criterio de seguridad, determinará el peso total de la unidad de análisis o informante; expresado en términos matemáticos, tendríamos la siguiente expresión:

$$P = \sum_{k=1}^{m} CS_k$$

Donde $\boldsymbol{m}$, corresponde a la cantidad total de criterios de seguridad evaluados.

Para comparar el valor obtenido, se establece una matriz de rangos, basada en una distribución normal de la población (Stuffelebeam y Coryn, 2014), en una escala de cero hasta cien. Se establecieron cuatro niveles de seguridad, determinados a través de la relación general: $\boldsymbol{Distribución} = \frac{\textbf{Escala de Valor Propuesta}}{\boldsymbol{Cantidad\ de\ Niveles}}$, la cual dio como resultado el valor nominal de 25; lo que representa la media de referencia para determinar los rangos de los Niveles de Seguridad buscados. De esta forma, se obtienen cuatro intervalos o rangos que expresan la distribución normal teórica del comportamiento de la población.

Se asignó la letra $[\boldsymbol{P}]$ para establecer el calificativo del peso, en función de:

$$\forall\ [\boldsymbol{P}] \in\ \mathbb{R}, en\ donde\ 0\ \leq [\boldsymbol{P}] \leq 100$$

El valor $[\boldsymbol{P}]$ puede obtener una ponderación de la siguiente manera:

- Si $[\boldsymbol{P}]$ es menor a 25%, se considerará un Nivel de Seguridad **MUY BAJO**.
- Si $[\boldsymbol{P}]$ es mayor o igual a 25%, pero menor o igual a 50%, se considerará un Nivel de Seguridad **BAJO**.
- Si $[\boldsymbol{P}]$ es mayor a 50%, pero menor o igual a 75%, se considerará un Nivel de Seguridad **ALTO**.
- Si $[\boldsymbol{P}]$ es mayor a 75%, se considerará un Nivel de Seguridad **MUY ALTO**.

3. Resultados y discusión

El modelo propuesto, ha sido utilizado para evaluar el nivel de seguridad en las redes de área local con tecnología Wi-Fi en un área geográfica de Panamá; específicamente en la

provincia de Veraguas, distrito cabecera de Santiago. En la figura 1, se muestra el recorrido del rastreo de redes que utilizan tecnología Wi-Fi, que inició desde la Avenida Héctor Alejandro Santacoloma (vía principal), Ave. Central, Intersección Calle 3ra, Avenida Sur, Calle 9na y la Ave. Polidoro Pinzón (Calle 10ma).

Se aplicó la técnica *WarDriving* para el rastreo e identificación de redes con tecnología Wi-Fi, la cual consiste en la búsqueda de redes inalámbricas a través de la detección de los puntos de acceso en un área determinada, tras el recorrido en un vehículo en marcha, y con la ayuda de equipos informáticos y de un software especializado (Ch. Sai, Syed y Siricha T., 2013).

Estas áreas constituyen las zonas de mayor concentración y presencia de la tecnología sujetas de estudio, determinadas por la aplicación de la técnica de *WarDriving* como herramienta para la determinación de las zonas de concentración de redes (Jones y Ling, 2007).

Figura 1. Recorrido en el rastreo de redes de área local que utilizan tecnología Wi-Fi.

Fuente: Elaborada por los autores.

Para recolectar los datos que servirían de estadísticas, se aplicó el escaneo de redes a través del software *NetStumbler* (Hwagm, 2016). Este software es utilizado para el registro de las redes, el cual permite la verificación de la configuración de la red, el análisis de cobertura, la detección de interferencias entre redes, la orientación de antenas direccionales y la localización de puntos de acceso no autorizados, entre otras (Netstumbler, 2014).

De las redes existentes en las áreas en estudio, hay un porcentaje mínimo que quedarían fuera, ya que existen condiciones específicas no controladas, como, por ejemplo, que, al momento del rastreo, las mismas estén apagadas o que no funcionen correctamente.

La tabla 1 presenta los valores de la distribución de los resultados obtenidos de los niveles de seguridad y su relación con los intervalos calculados.

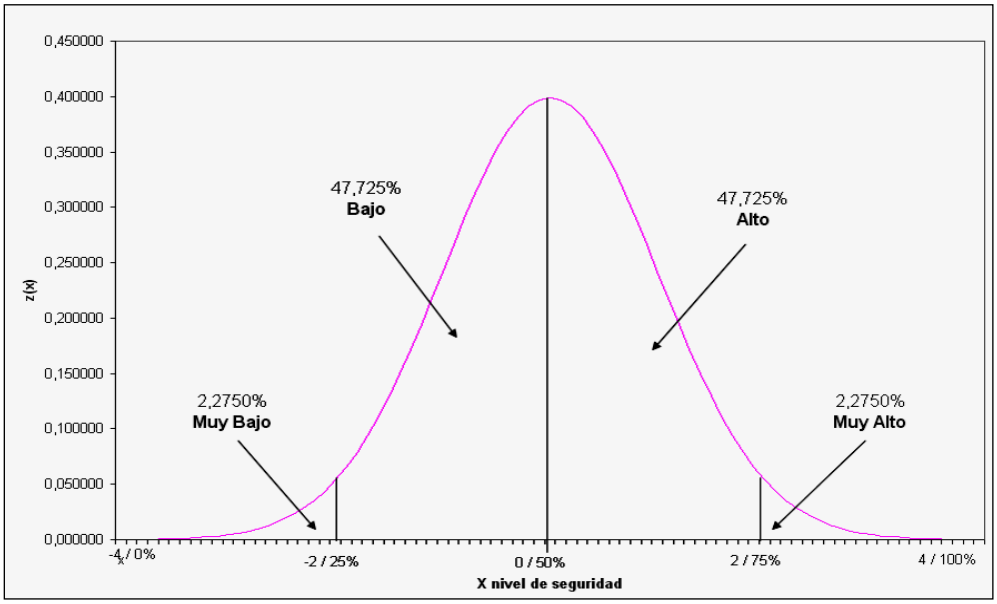
Tabla 1. Ponderación de los niveles de configuración de la seguridad

Valor de [P]	Unidades de desviación estándar	Nivel de configuración
P ≤ 25%	-4 σ	Muy bajo
25% ≤ P ≤ 50%	-2 σ	Bajo
50% < P ≤ 75%	2 σ	Alto
P > 75%	4 σ	Muy alto

Fuente: Elaborada por los autores.

La figura 2, muestra la distribución normal utilizada para el cálculo de los intervalos del nivel de seguridad y las unidades de desviación estándar propuestas entre $\pm \mathbf{4}\ \boldsymbol{\sigma}$.

Figura 2. Distribución normal para ± 4 errores



Fuente: Elaborada por los autores.

La tabla 2, muestra el resumen de la asociación de los indicadores para cada criterio de seguridad en redes de área local que utilizan tecnología Wi-Fi.

Tabla 2. Distribución de indicadores según criterio

Indicador \ Criterio	C	A	I	D	N.R
Cifrado	X	X	X		X
No publicar SSID	X	X			
Filtrado de Mac		X			
Portales cautivos		X			X
Monitoreo de Mac	X				
Monitoreo del SNR	X				
Monitoreo de frecuencias				X	
Monitoreo de retransmisiones				X	
Monitoreo ICMP/UDP				X	
Red wi-fi fuera del firewall					X
VPN					X
Firmas digitales					X

Fuente: Escudero Pascual, 2008.

En donde: $[\boldsymbol{C}]$ Confidencialidad, $[\boldsymbol{A}]$ Autenticación, $[\boldsymbol{I}]$ Integridad, $[\boldsymbol{D}]$ Disponibilidad y $[\boldsymbol{N}.\boldsymbol{R}]$ No Repudio.

De los resultados obtenidos al aplicar el instrumento a los especialistas, se calcula el promedio para cada criterio propuesto; además, se promedia el peso por indicador del criterio. Los resultados para los indicadores se muestran en la tabla 3, y los pesos para valorar los criterios son los siguientes: Confidencialidad (26%), Autenticación (24%), Integridad (20%), Disponibilidad (20%) y No Repudio (10%).

Los indicadores están distribuidos entre los cinco criterios considerados en el modelo. Estos se ponderan con dicho valor cuando el indicador está presente en el equipo evaluado; en caso contrario, estos tendrán un valor igual a cero.

Tabla 3. Ponderación para los criterios propuestos

Indicador \ Criterio	C	A	I	D	N.R.
Cifrado	34	35	100		23
No publicar SSID	25	21			
Filtrado de Mac		26			
Portales cautivos		18			18
Monitoreo de Mac	23				
Monitoreo del SNR	18				
Monitoreo de frecuencias				34	
Monitoreo de retransmisiones				26	
Monitoreo ICMP/UDP				40	
Red wi-fi fuera del firewall					20
VPN					19
Firmas digitales					20

Fuente: Elaborada por los autores.

Con una población total que asciende a 140 redes con tecnología Wi-Fi, la muestra es probabilística simple, y como había que seleccionar los sitios para la aplicación de las encuestas, se recurrió a la elección por números aleatorios. Para calcular el tamaño de la muestra, se utilizó la siguiente ecuación (Hernández S, Fernández C y Baptista L, 2010):

$$n = \frac{n'}{1} + \left(\frac{n'}{N} \right)$$

Siendo el significado y valor de cada variable, el siguiente:

- **se** = 0,04 error estándar
- **V2** = 0,0016 varianza de la población
- **s2** = 0,09 varianza. p*(1-p) donde p = 0.9
- **n´** = 56,25 la muestra sin ajustar s2 / V2

- **N** = 140 tamaño de la población
- **n** = 40 tamaño de la muestra

Los resultados del análisis de los informantes, según el modelo que ha sido diseñado para la evaluación de los niveles de seguridad en redes de área local con tecnología Wi-Fi, se pueden observar en la tabla 4.

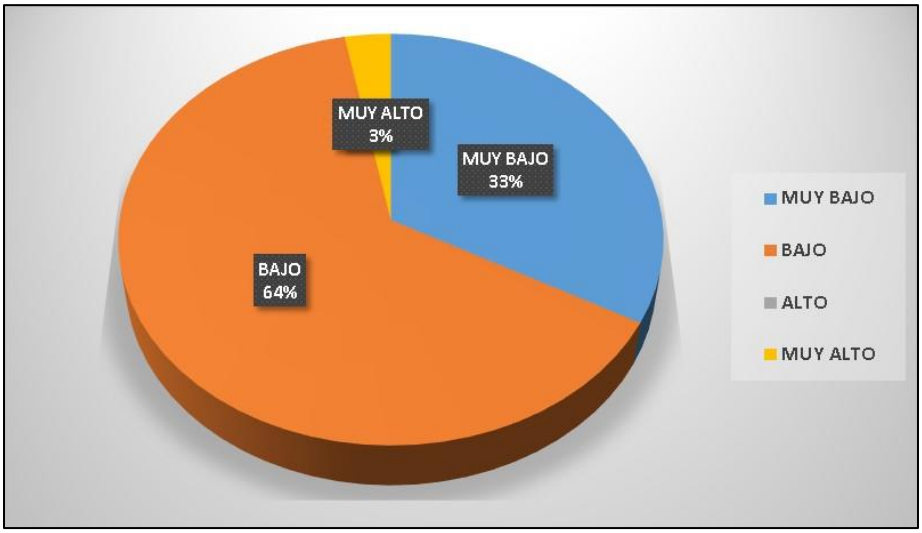
Tabla 1: Nivel de seguridad en las redes de área local con tecnología Wi-Fi

Nivel de Seguridad	Cantidad	Porcentaje
Muy Bajo	13	33
Bajo	26	64
Alto	0	0
Muy Alto	1	3

Fuente: Elaborada por los autores.

La figura 3, indica que el 64% de las redes estudiadas han reflejado serias carencias en su seguridad, ya que, al ser evaluadas, les corresponde un nivel de seguridad bajo; sin embargo, existe un crítico 33% de las redes que han quedado evaluadas con niveles de seguridad muy bajo, lo que también representa un segmento muy pequeño, que corresponde al 3% con un nivel de seguridad muy alto.

Figura 3. Resultados del análisis del nivel de seguridad en redes Wi-Fi, según el modelo propuesto.



Fuente: Elaborada por los autores.

4. Conclusiones

- El modelo de evaluación de la seguridad propuesto, permite determinar el nivel de cultura de seguridad que se aplica a la administración de las redes de área local que utilizan tecnología Wi-Fi en las áreas estudiadas. Esta evaluación permite tener una referencia para futuras evaluaciones, permitiendo establecer los márgenes de mejoras con respecto al estudio realizado.
- Las ponderaciones asignadas a los criterios utilizados para construir el modelo están bastante balanceadas en cuatro de ellos: confidencialidad, autenticación, integridad y disponibilidad, teniendo de media un peso de 22% aproximadamente, exceptuando el no repudio que tiene un peso de 10%. El modelo expresa objetividad en sus valoraciones, si consideramos que el criterio de no repudio es el que menos influye en los resultados, puesto que es el más complejo de implementar.
- Es de vital importancia publicar los resultados obtenidos, ya que el 97% de los puntos de acceso detectados y analizados, cuentan con niveles deficientes de seguridad en sus redes Wi-Fi, lo que propicia que, en cualquier momento, se puedan efectuar ataques a la infraestructura de red de las empresas dentro del área de análisis, repercutiendo negativamente en el desarrollo de sus funciones y operaciones comerciales.
- Solo un 3% de los puntos de acceso de las redes detectadas, presentan niveles de configuración cónsonos con los estándares de seguridad para redes con tecnología Wi-Fi, lo que representa un aspecto positivo en el estudio realizado.
- Los estándares de la familia IEEE 802.11 han sido definidos en la capa física y la de enlace, por lo que es imperativos que los criterios de seguridad que no se proporcionan como servicios en los protocolos que operan en estas capas, deben ser implementados en las capas superiores.
- La diversidad de usos, configuraciones y de infraestructuras de redes Wi-Fi, impiden la definición de un estándar de seguridad para todas las redes inalámbricas. Es por ello que, en el diseño de soluciones de ingeniería de seguridad, se deben considerar los requisitos de seguridad y los contextos o ámbitos de su aplicación.

5. Recomendaciones

- Los profesionales encargados de la seguridad en las redes Wi-Fi deben ser personas idóneas, y no delegar esta responsabilidad en cualquier persona, teniendo en cuenta que, en muchos casos, estas redes son utilizadas para procesos muy críticos de las empresas, como la facturación.
- Actualmente, los proveedores de servicios de internet (ISP), proporcionan a los clientes equipos con tecnología Wi-Fi, cuyas configuraciones de seguridad están por defecto y, más grave aún, es que utilizan las mismas para todos los usuarios; por ello, los clientes deben exigir al proveedor de servicios que la configuración personalizada del equipo sea parte del servicio de instalación de los mismos.
- Es fundamental, basados en los resultados obtenidos de la evaluación de la seguridad en las redes Wi-Fi, que se desarrolle una campaña de concientización para los gerentes o encargados de las empresas en cuanto a la importancia que tiene la seguridad inalámbrica y en cuanto a los riesgos que tiene la utilización de la misma de forma inadecuada.
- Se deben realizar otros estudios en la misma zona bajo análisis, pero con otros modelos de caracterización de los niveles de seguridad, para evaluar si los resultados finales son análogos a los obtenidos con el modelo propuesto en esta investigación. Esto permitirá identificar las desviaciones que pueden estar incluidas en el diseño del modelo.
- Es importante en este tipo de investigaciones analizar cuáles son los equipos comerciales que brindan mejores prestaciones de seguridad, y cuál es la razón por la cual no han sido implementadas dichas medidas.

Referencias bibliográficas

Academia de Networking de CISCO Systems. (2006). *Fundamentos de redes inalámbricas* (primera ed.). Madrid: Pearson Education, Inc.

Association for Progressive Communications (APC). (2015). *Asociación para el progreso de las comunicaciones*. Recuperado de http://www.apc.org/wireless/

Ayala, A. (25 de enero de 2017). VP Ejecutivo RISCCO.

Ch. Sai, P., Syed, U., & Siricha T. (2013). The impact of war driving on wireless networks. *LICSET, 3*(6), 230-235.

Common Criteria for Information Technology Security Evaluation. (2016). *Common criteria*. Recuperado de http://www.commoncriteriaportal.org

Diario Digital Panamá24Horas. (2017). *Panamá24Horas*. Recuperado de: http://www.panama24horas.com.pa/

Domenico Aime, C., Calanrtiello, G., & Lioy, A. (2007). Security & Privacy. *IEEE Computer Society, Enero-Febrero* (Digital Object Identifier 10.1109/MSP.2007.4.), 23.

Hernández S, R., Fernández C, C., & Baptista L, P. (2010). *Metodología de la investigación* (5ta ed.). México D.F.: McGraw-Hill.

Hwagm. (octubre de 2016). *Hwagm.* Recuperado de http://hwagm.elhacker.net/htm/netstumbler.htm

Jones, K., & Ling, L. (2007). What where Wi: An analysis of millions of Wi-Fi access points. *IEEE International Conference On* (Digital Object Identifier 10.1109/PORTABLE.2007.45), 6.

Jones, K., & Liu, L. (2007). What where Wi: An analysis of millions of Wi-Fi access points. *IEEE International Conference*(10.1109), 6.

Jyh-Cheng, C., Ming-Chia, J., & Yi-Wen, l. (2005). Wireless LAN security and IEEE 802.11i. *Wireless communications IEEE* (Digital Object Identifier 10.1109/MWC.2005.1404570), 10.

Netstumbler. (2014). *Netstumbler*. Recuperado de netstumbler: http://www.netstumbler.com/

Pascual Escudero, A. (2008). *Association for progressive communications (APC) - ITRAINONLINE*. Recuperado de wireless security handout: http://www.itrainonline.org/itrainonline/mmtk/wireless_en/15_Wireless_Security/15_en_mmtk_wireless_security_handout.pdf

Pérez, J. (Noviembre de 2003). *Grupo de análisis y prospectiva del sector de las telecomunicaciones (GAPTEL).* Recuperado de GAPTEL: http://aui.es/IMG/pdf_04_02_20_wifi.pdf

Reid, N., & Seide, R. (2004). *Manual de redes inalámbricas 802.11 (Wi-Fi)* (primera ed.). México: McGraw-Hill.

Revista Digital El Financiero. (2015). *Revista digital el financiero*. Recuperado de http://efpanama.com/

Revista Digital Martes Financiero. (2015). *Revista digital martes financiero*. Recuperado de http://www.martesfinanciero.com/

RISCCO. (2017). *Riscco it risk & security, internal audit*. Recuperado de https://www.riscco.com/riscco/publicacion/2015

Software, Panda. (2005). *www.pandasoftware.es*. Recuperado de http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/documentos/WP_wifi_PSE.pdf

Stuffelebeam, D., & Coryn, C. (2014). *Evaluation theory, models, y applications* (segunda ed.). San Francisco: CA:Jossey-Bass.

Trucos Windows. (2017). *Trucos windows.net*. Recuperado de https://www.trucoswindows.net/