BUENAS PRÁCTICAS PARA AUDITAR LA RED INALÁMBRICA DE UNA COMPAÑÍA

García Rozo, Juan Martín
juan.garcia16@hotmail.com
Universidad Piloto de Colombia

Resumen— La red inalámbrica es una facilidad que tienen muchas compañías para la prestación de servicios de red que entrega el área de TI, que ha venido creciendo exponencialmente, a esta red se conectan tanto personal interno como externo de manera permanente o temporal, brindándoles servicios de acceso a internet y conectividad de las aplicaciones de producción para la realización de las distintas tareas en la organización, al igual que una red alambrada corporativa el buen uso que se dé a ésta es muy importante y se debe instalar con la infraestructura y la seguridad apropiada.

Adicionalmente hoy en día se ve más la tendencia de BYOD (bring your own device) en la que las empresas permiten a los trabajadores conectar a la red corporativa los dispositivos personales para llevar a cabo tareas de trabajo.

Debido al creciente uso de las redes inalámbricas, surgen nuevos riesgos, vulnerabilidades y amenazas que pueden ser aprovechadas por un atacante y afectar la seguridad de la información en cuanto a la integridad, confidencialidad y disponibilidad.

Abstract **-** The wireless network is a facility with many companies to provide network service that delivers the IT area, which has grown exponentially, this network can connect internal and external staff, permanent or temporary basis, providing services Internet access and production applications to carry out their various tasks, as well as a good corporate wired network use to which this network is very important and must be implemented with appropriate infrastructure and security.

In addition, today is a trend of BYOD (bring your own device) in which companies allow workers to connect their personal devices to the corporate network to carry out work tasks.

Due to the increased use of wireless networks, new risks, threats and vulnerabilities that can be exploited by an attacker and affect the security of information as to the integrity, confidentiality and availability arise.

Índice de Términos - access point (AP), cifrado, DoS, EAP, firewall, PEAP, PSK, radius, sniffer, SSID, TLS, VPN, WAN, WAP, WLAN, WIFI, WEP.

I. INTRODUCCIÓN

El presente artículo pretende mostrar algunos de los riesgos, vulnerabilidades y ataques, y plantear una guía de buenas prácticas para verificar el estado de salud de una red inalámbrica, que sirva a un auditor de apoyo, para ir más allá de realizar un monitoreo de los canales de emisión, niveles de las señales y el tipo de clave. Para ello se propone plantear una guía de buenas prácticas para auditar las redes inalámbricas, planteando dominios, actividades a seguir, herramientas y checklist, que ayuden a mejorar los procesos de auditoría para facilitar el trabajo y de este modo optimizar los tiempos de una auditoría de la red inalámbrica.

II. CONCEPTOS PREVIOS

A. Definición de red de área local inalámbrica

Una red inalámbrica es un sistema de comunicaciones de datos que proporciona conexión inalámbrica entre equipos situados dentro de la misma área (interior o exterior). En lugar de utilizar cableado físico de par trenzado, coaxial o la fibra óptica, utilizado en las redes LAN convencionales, las redes inalámbricas transmiten y reciben datos a través de ondas electromagnéticas.

La velocidad de transmisión se sitúa entre 10 Mbit/s, 20 Mbit/s y 50 Mbit/s, frente a 100 Mbit/s y 1000 Mbit/s que ofrece una red cableada convencional, las redes inalámbricas son la alternativa ideal para hacer llegar una red tradicional a lugares donde el cableado no lo permite, y en general se utilizan como un complemento de las redes fijas.

B. Características

Una red inalámbrica ofrece; movilidad, simplicidad, rapidez, escalabilidad, flexibilidad y costo reducido de instalación, sin embargo, esta facilidad de conexión exige poner los controles adecuados para evitar un posible ataque a nuestra red, que pueda poner en riesgo la confiabilidad, disponibilidad, e integridad de la información de la organización.

Permanentemente la información sencible de una compañia viaja por el aire mediante las señales transmitidas por las redes inalámbricas, de este modo la información esta expuesta a posibles incidentes de seguridad, por esta razón surgen ciertas contramedidas que ayudan a controlar el acceso a las redes inalámbricas tales como; cifrado WEP, WPA, WPA2 basados en el estándar IEEE 802.11i, AES, TKPI, 802.1x, autenticación *radius*, EAP, PEAP y portales cautivos, todas estas medidas

ofrecen ciertos niveles de seguridad de un menor a mayor grado, pero pueden presentarse ciertas amenazas como se revisará más adelante.

Los estándares IEEE 802.11b, IEEE 802.11g y 802.11n disfrutan de una aceptación internacional debido a que opera en la banda de 2,4 GHz que está disponible casi universalmente, es una banda no licenciada, con una velocidad de 11 Mbit/s, 54 Mbit/s y hasta 300 Mbit/s.

El estándar IEEE 802.11ac, conocido como WIFI-5, opera en la banda de 5 GHz y disfruta de una operatividad con canales relativamente limpios. Su alcance es algo menor que los estándares que trabajan a 2,4 GHz , debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance).

Existen otras tecnologías inalámbricas como bluetooth que también operan en la frecuencia de 2,4 GHz, y pueden interferir con la tecnología WIFI.

Debido a esto, en la versión 1.2 del estándar bluetooth se actualizó para que no halla interferencia con la utilización simultánea de ambas tecnologías.

III. HARDWARE DE LA RED INALÁMBRICA

Las redes inalámbricas utilizan componentes similares a las redes cableadas. Estos componentes comprenden dos diferentes clases de dispositivos:

- Dispositivos de acceso al medio como tarjetas inalámbricas y estaciones base (puntos de acceso, enrutadores inalámbricos).
- Dispositivos de usuario final como computadores personales, portátiles, agendas digitales, cámaras web, impresoras, teléfonos, tabletas.

A. Tarjeta de red inalámbrica

La tarjeta de red inalámbrica también conocida como NIC (*network interface card*) provee la interfase y el radio que comunica el dispositivo de usuario final con la infraestructura de red inalámbrica. Algunas NIC inalámbricas van en el interior de los dispositivos como computadores de escritorio o portátiles, otras se conectan exteriormente a través de puertos USB o ranuras PCMCIA.

B. Access point o punto de acceso

Es un equipo que asume las funciones de repetidor de señales y permite la conectividad de los dispositivos inalámbricos. Se comporta de manera similar a la de un concentrador de cableado (*hub* o *switch*) y maneja un ancho de banda por equipo que disminuye en la medida en que más dispositivos se comuniquen a través de él, opera en las capas 1 y 2 del modelo de referencia OSI. En grandes instalaciones, la funcionalidad de *roaming* proporcionada por múltiples puntos de acceso permiten a los usuarios inalámbricos desplazarse libremente a través de las instalaciones, a la vez que se mantiene un acceso sin fisuras e interrupciones.

C. Bridges

Los *bridges* están diseñados para conectar dos o más redes ubicadas en general en diferentes edificios. Los *bridges* conectan sitios difíciles de cablear, pisos no continuos, pueden configurarse para aplicaciones punto a punto o punto multipunto.

D. Switch

Un *Switch* se describe a veces como un *bridge* multipuerto. Mientras que un *bridge* típico puede tener sólo dos puertos que enlaza dos segmentos de red, el *switch* puede tener varios puertos, según la cantidad de segmentos de red que sea necesario conectar. Al igual que los *bridges*, el *switch* aprenden determinada información sobre los paquetes de datos que se reciben de los distintos computadores de la red. Los *switches* utilizan esa información para crear tablas de envío y determinar el destino de los datos que se están mandando de un computador a otro en la red.

E. Router

Los router son los responsables de enrutar paquetes de datos desde su origen hasta su destino en la LAN, y de proveer conectividad a la WAN. Además de comportarse como puntos de acceso (con funciones de concentración, amplificación y repetición) son dispositivos más inteligentes tienen la función primaria de permitir que los equipos cableados e inalámbricos en una red accedan a otra red.

A diferencia de los puntos de acceso, los enrutadores inalámbricos permiten entre otras las siguientes funciones:

- Permiten o niegan la conexión de los dispositivos de usuario final a las redes.
- Facilitan la conexión a la red tanto a dispositivos inalámbricos como a dispositivos cableados.
- Servicios de DHCP, DNS y firewall
- Proveen funciones de calidad de servicio para mejorar las comunicaciones.

IV. AMENAZAS Y VULNERABILIDADES DE LA RED INALÁMBRICA

Por las características en que se propagan las ondas de radio de las redes WIFI, están expuestas a las siguientes amenazas y vulnerabilidades.

A. Pérdida de señal

Se entiende por perdida de señal cuando las ondas de radio atraviesan un medio que la señal se desvanezca.

B. Cracking de contraseña

Los puntos de acceso inalámbricos que todavía utilizan protocolos de seguridad antiguos, como WEP, son blancos fáciles porque las contraseñas son muy fácil de adivinar.

C. Hotspots falsos

Puntos de acceso que parecen ser legitimos, son instalados por los cibercriminales con el proposito de que los usuarios se contecten para sustraer información confidencial que posterioemente es usada para llevar acabo fraudes informáticos. Los usuarios que son víctimas de un *hostpot* falso son susceptibles de verse afectados por códigos maliciosos, que a menudo pasan desapercibidos.

D. Colocación de malware

Los usuarios que se unen a una red inalámbrica de visitantes son susceptibles, sin saberlo, de llevarse malware no deseado de algún vecino con malas intenciones. Una táctica común utilizada por los *hackers*, es colocar una puerta trasera en la red, lo que les permite regresar más tarde para robar datos confidenciales.

E. Espionaje

Los usuarios corren el riesgo de que sus comunicaciones privadas sean interceptadas por ciber espías mientras están conectados a una red inalámbrica sin protección.

F. Robo de datos

Unirse a una red inalámbrica expone a los usuarios a la pérdida de documentos privados que caen en manos de los cibercriminales, que están pendientes de escuchar las transmisiones para interceptar la información que se está transmitiendo.

G. Uso inapropiado e ilegal

Las empresas que ofrecen WIFI de invitados se enfrentan al riesgo de un uso indebido por parte de los usuarios, ya sea por acceder a contenidos de adultos o extremistas, descargas ilegales, o ataques contra otras empresas. La empresa podría enfrentarse a demandas judiciales.

H. Los malos vecinos

A medida que el número de usuarios de la red inalámbrica crece, también lo hace el riesgo de que un dispositivo previamente infectado entre en la red. Los ataques móviles, tales como *stagefright* de android, se propagan de un usuario a otro, incluso sin que la víctima lo sepa.

I. Vulnerabilidades en portales cautivos

Debido a las características de las zonas abiertas en los sistemas que implantan este sistema de portales, se permite la asociación al punto de acceso a cualquier cliente y el tráfico entre los clientes y el punto de acceso pasa, por este motivo se puede capturar el tráfico de las conexiones en las zonas privadas. Por otra parte es posible implementar ataques de tipo *spoofing* o *hijacking* mientras el token que emplea el usuario sea válido.

V. ATAQUES DE LA RED INALÁMBRICA

Se pueden encontrar entre otros los siguientes ataques a la red inalámbrica.

A. Eavesdropping

Las ondas de RF viaja a través del aire, un atacante puede analizar el tráfico y capturar información privilegiada, como claves para acceder a más información sin que nadie se entere.

B. Spoofing

Consiste en el uso de técnicas de suplantación de identidad generalmente con fines maliciosos.

C. Wardriving

Búsqueda de redes WIFI desde un vehículo en movimiento para conocer su posición.

D. Ataque denegación de dervicio (DoS)

El objetivo de este ataque implementado en una red inalámbrica consiste en impedir una comunicación entre la terminal y un punto de acceso. Para lograr esto, solo debemos hacernos pasar por el punto de acceso poniéndonos su dirección MAC (obtenida mediante un simple *sniffer*) y negarle la comunicación al terminal o terminales elegidas mediante el envío continuo de notificaciones de des-asociación.

E. Descubrimiento SSID ocultos

En casi todos los puntos de acceso podemos encontrar la opción de deshabilitar el envío del SSID en los paquetes o desactivar *beason frames.* Ante esta medida de seguridad, un presunto atacante tendría dos opciones:

- Hacer *sniffer* de la red durante un tiempo indeterminado a la espera de una nueva conexión con el objetivo de conseguir el SSID presente en las tramas *prove request* del cliente (en ausencia de *beason frames*) o en las tramas *prove response*.
- Provocar la desconexión de un cliente mediante el mismo método que empleamos en el ataque DoS pero sin mantener al cliente desconectado.

F. Ataque man in the middle

Este ataque apareció en escena a raíz de la aparición de los *switches* que dificultaban el empleo de *sniffer* para obtener los datos que viajan por la red. Mediante el ataque *man in the middle* se hace creer al cliente víctima que el atacante es el punto de acceso, y al mismo tiempo convencer al punto de acceso que el atacante es el cliente.

Para llevar a cabo un ataque de este tipo es necesario obtener los siguientes datos mediante el uso de un *sniffer*:

- El SSID de la red.
- La dirección MAC del punto de acceso.
- La dirección MAC de la víctima.

Una vez obtenidas estos datos se emplea la misma metodología que en el ataque de tipo DoS para romper la conexión entre el cliente y el punto de acceso. Tras esta ruptura, la tarjeta del cliente comenzará a buscar un nuevo punto de acceso en los diferentes canales, momento que aprovechará el atacante para suplantar al punto de acceso empleando su MAC y SSID en un canal distinto. Para ello el atacante pondrá su propia tarjeta en modo maestro.

De forma paralela el atacante logra suplantar la identidad del cliente con el punto de acceso real empleando para ello su dirección MAC, de esta forma el atacante logra colocarse entre ambos dispositivos de forma transparente.

G. Ataque WPA- PSK

El único ataque conocido contra WPA – PSK es el de tipo fuerza bruta o diccionario, pese a la existencia de este ataque la realidad es que el rendimiento es tan bajo y la longitud de la *passphrase* puede ser tan larga, que implementarlo de forma efectiva es prácticamente imposible. Los requisitos para llevar a cabo el ataque son:

- Un archivo con la captura del establecimiento de conexión entre el cliente y el AP.
- El nombre de SSID.
- Un archivo de diccionario.

Se puede auditar la fortaleza de las contraseñas empleadas en un sistema realizando ataques de diccionario o de fuerza bruta, en este último caso empleando herramientas usadas para crear todas las combinaciones de caracteres posibles.

H. Rogue AP

Es un punto de acceso no autorizado, este tipo de ataque consiste a nivel básico; en colocar un punto de acceso bajo control del atacante cerca de las instalaciones de la víctima de forma que los clientes asociados o por asociar a esa red se conecten a dicho punto de acceso en lugar de conectarse al legítimo de la víctima debido a la mayor señal que este entrega.

Una vez conseguida la asociación al rogue AP, el atacante puede provocar ataques de tipo DoS, robar datos de los clientes como usuarios y contraseñas de diversos sitios web o monitorear las acciones del cliente.

Este tipo de ataques se ha empleado tradicionalmente para; crear puertas traseras corporativas, o para espionaje industrial.

VI. TIPOS DE SEGURIDAD

A. WEP

Es el algoritmo de seguridad empleado para brindar protección a las redes inalámbricas incluido en la primera versión del estándar IEEE 802.11 se ha mantenido sin cambios en 802.11a y 802.11b, con el fin de garantizar la compatibilidad entre los distintos fabricantes. Este sistema emplea el algoritmo simétrico *RC4*, para cifrar emplea llaves que pueden ser de 64 o 128 bits teóricos, puesto que en realidad son 40 o 104 y el resto (24 bits) se emplean como vector de inicialización.

La seguridad ofrecida tiene como pilar central una clave secreta compartida por todas las estaciones de los clientes y los puntos de acceso, y que se emplea para cifrar los datos enviados, WEP es un sistema muy débil ya que se puede conseguir la clave de cifrado monitoriando las tramas y procesándolas.

La integridad se consigue utilizando técnicas de detección de errores (CRC) que no son eficientes para garantizar la integridad.

La autenticación es inexistente ya que incluso permite hallar la clave usada por WEP de forma muy sencilla. Algunos fabricantes proporcionan autenticación del equipo a partir de la dirección MAC de la estación.

B. WAP

A diferencia de WEP, utiliza un vector de inicialización de 48 bits y una clave de cifrado de 128 bits. Lo más importante es que WPA, utiliza lo que se llama el protocolo de integridad de clave temporal (TKIP). Considerando que WEP usa la misma clave para cifrar todos los paquetes que fluyen a través de la red, WPA con (TKIP), cambia la clave de cifrado cada vez que un paquete se transmite. Lo anterior, combinado con el uso de claves más largas, impide que un router sea fácilmente accedido solo a través de la observación de un conjunto de transmisión de paquetes.

C. WAP2

Es simplemente la versión certificada del estándar de la IEEE de WPA con algunas actualizaciones como el uso de cifrado AES.

D. TKIP

Significa “Protocolo de integridad de clave temporal”. Fue un protocolo de cifrado provisional introducido con WPA para reemplazar el cifrado WEP, el cual se veía muy afectado por la inseguridad en el momento, aunque TKIP es en realidad muy similar a WEP.

E. AES

Es un protocolo de cifrado más seguro introducido con WPA2, que reemplazó el estándar WPA. AES no es una norma creada específicamente para redes WIFI, es un estándar de cifrado usado globalmente, incluso ha sido

adoptado por el gobierno de Estados Unidos. AES se considera generalmente muy seguro, y la principal debilidad sería un ataque de fuerza bruta, el cual se puede impedir usando una contraseña muy segura.

F. PSK

Significa "llave pre-compartida", que es generalmente la frase de cifrado. Esto lo distingue de WPA-enterprise, que utiliza un servidor *radius*, que crea de forma aleatoria claves únicas en redes corporativas o gubernamentales.

G. Autenticación 802.1X/EAP

El estándar 802.11x consiste es encapsular los protocolos de autenticación sobre los protocolos de la capa de enlace de datos y permite emplear el protocolo de autenticación extensible (EAP) para autentificar al usuario de varias maneras.

IEEE 802.1x define 3 entidades:

- El solicitante (*suplicant*), reside en la estación inalámbrica.
- El autenticador (*authenticator*), reside en el AP.
- El servidor de autenticación, reside en un servidor AAA (*authentication, authoization, accounting*) como *radius*.

EAP comprende 4 tipos de mensajes:

- Petición; empleado para enviar mensajes desde el AP al cliente.
- Respuesta; empleado para enviar mensajes desde el cliente al AP.
- Éxito; emitido por el AP, significa que el acceso está permitido.
- Fallo; enviado por el AP para indicarle al solicitate que se deniega la conexión.

Proceso de autenticación, tras la asociación:

Se envía el AP-request/identity desde el autenticador al solicitante.

- El suplicante responde con EAP *response/identity* al autenticador, el cual lo pasa al servidor de autenticación.
- Se tuneliza el *challenge/response* y si resulta acertado el autenticador permite al suplicante acceso a la red condicionando por las directrices del servidor de autenticación.

El funcionamiento base del estándar 802.11x se centra en la negación de cualquier tráfico que no sea hacia el servidor de autenticación hasta que el cliente no se haya autenticado correctamente. Para ello el autenticador crea un puerto por cliente que define dos caminos, uno autorizado y otro no, manteniendo el primero cerrado hasta que el servidor de autenticación le comunique que el cliente tiene acceso al camino autorizado.

H. EAP-TLS

Requiere de la poseer certificados digitales por parte del cliente y el servidor de autenticación; el proceso de autenticación comienza con el envío de su identificación (nombre de usuario) por parte del solicitante hacia el servidor de autenticación, tras esto el servidor envía su certificado al solicitante que, tras validarlo, responde con el suyo propio. Si el certificado del solicitante es válido, el servidor responde con el nombre de usuario antes enviado y se comienza la generación de la clave de cifrado, la cual es enviada al AP por el servidor de autenticación para que pueda comenzar la comunicación segura.

I. PEAP Y EAP – TTLS

El mayor inconveniente que tiene el uso de *EAP – TLS* es que tanto el servidor de autenticación como los clientes deben poseer su propio certificado digital, y la distribución entre un gran número ellos puede ser difícil y costosa. Para corregir este defecto se crearon *PEAP* (protected *EAP*) y *EAP - tunneled TLS* que únicamente requieren certificado en el servidor.

La idea base de estos sistemas es que, empleando el certificado del servidor previamente validado, el cliente pueda enviar sus datos de autenticación cifrados a través de un túnel seguro. A partir de ese momento, y tras validar el servidor al solicitante, ambos pueden generar una clave de sesión.

VII. METODOLOGÍA A SEGUIR PARA AUDITAR UNA RED WIFI

Después de hacer un barrido por las amenazas y vulnerabilidades más reconocidas y los distintos métodos de seguridad implementados sobre la red inalámbrica se mostrará una guía a utilizar para auditarla. En la auditoría se recomienda seguir las metodologías internacionalmente reconocidas tales COBIT 4.1, ISO IEC 27001, IEC 27002, OSSTMM Wireless 2.9, como parte de las buenas prácticas se encuentra, los dominios de diseño, administración y seguridad, cada una presenta sus buenas prácticas , sus objetivo, actividades o tareas, herramientas de apoyo y checklist para auditar una red inalámbrica.

A. Plan de auditoría

En la auditoría se deberá seguir los siguientes pasos:

1) Planeación general

- Objetivos.
- Alcance.
- Metodología a utilizar.

2) Plan de la auditoría

- Objetivos del examen; son los resultados que se esperan alcanzar.
- Alcance del examen; es el grado de extensión de las labores de auditoría.
- Descripciones de las actividades de la compañía.
- Normas aplicables a la compañía.
- Informes a emitir y fecha de entrega.
- Identificación de las áreas críticas.
- Nombre del personal y categoría de los auditores.
- Funcionarios de la entidad a examinar.
- Presupuesto de tiempo.
- Participación de otros profesionales.
- Papeles de trabajo.
- Herramientas a utilizar.

2) Ejecución

- Comunicación de hallazgos.
- Borrador del informe.

4) Hallazgo: Condición, criterio, causa y efecto.

5) Formulación del informe

- Elaboración del informe.
- Emisión del informe.
- Supervisión de la estructura y contenido del borrador del informe administrativo y el debido respaldo en papeles de trabajo.
- Evaluación de los comentarios de la entidad y supervisión del informe administrativo final.
- Supervisión de las observaciones, conclusiones, recomendaciones, proceso de determinación de las responsabilidades, administrativas, civiles o penales.
- Supervisión del informe especial de ser el caso.
- Revisión final y suscripción de los informes.
- Trámite de aprobación y remisión del informe a la entidad.

6) Contenido del informe

- Estructura del informe.
- Origen del examen.
- Naturaleza y objetivos del examen.
- Alcance del examen.
- Antecedentes, base legal de la entidad.
- Comunicación de hallazgos.
- Memorando de control interno.
- Otros aspectos de importancia.
- Observaciones.
- Conclusiones de las observaciones.
- Recomendaciones y conclusiones.
- Anexo.
- Firma.
- Síntesis gerencial.

B. Dominios de las buenas prácticas

Los escenarios que contemplan las buenas prácticas para auditar redes inalámbricas deberán tener en cuenta los tres dominios que cubran en la totalidad la red inalámbrica, que son el diseño, la administración y la seguridad de la red inalámbrica de la empresa. Los aspectos a contemplar en cada uno de estos dominios serán:

1) Dominio diseño

Para este dominio se deberá realizar un análisis de las metodologías orientadas al diseño, infraestructura y hardware de la red inalámbrica, alineadas a la verificación de planes, normas, fuentes de diseño, implementación, migración, infraestructura, ubicación, temperatura, límites de señal de la red y equipos de comunicaciones adecuados que permitan el funcionamiento óptimo de la red en la empresa, examinar que los equipos de la red inalámbrica sean soportados, adecuados para el funcionamiento de la misma, acordes con las necesidades, y finalmente un marco de trabajo de auditoría de diseño de la red inalámbrica.

Determinar objetivos de control orientados a:

- Análisis de la empresa.
- Análisis tecnológico de la empresa.
- Diseño físico de la red
- Diseño lógico de la red.
- Planes de implementación.

2) Dominio administración

Para este dominio se deberá realizar el análisis de metodologías orientadas a la administración de la red inalámbrica, alineadas a verificar, comprobar, analizar, examinar la continuidad de la operación constante de la red inalámbrica soportada en la empresa; obteniendo finalmente un marco de trabajo de auditoría de administración de la red inalámbrica. Se deberá determinar objetivos de control orientados a:

- La administración de recursos informáticos.
- La administración de recursos humanos.
- La administración de comunicaciones y operaciones.
- La administración de control de accesos.

3) Dominio seguridad

Para este dominio se deberá realizar el análisis de metodologías orientadas a la seguridad de la red inalámbrica, alineadas a verificar, comprobar, analizar, examinar la seguridad de las operaciones, transacciones de información constante de la red inalámbrica, abarcando pruebas de seguridad externa, que va de un ambiente no privilegiado a uno privilegiado, asimismo examinar que existan; controles, procedimientos y políticas de seguridad que permitan monitorear las operaciones, transacciones de información constante de la red inalámbrica, obteniendo finalmente un marco de trabajo de auditoría de hardware de

la red inalámbrica. Se deberá determinar objetivos de control orientados a:

- Política de seguridad de la información en la red inalámbrica de la compañía.
- Organización de la seguridad de la información en la red inalámbrica.
- Seguridad de la red inalámbrica.

C. Recomendaciones

Se propone realizar encuestas y entrevistas, para saber la situación actual de la red inalámbrica, periodo de auditorías y si se cuentan con buenas prácticas, como también información de nuestro interés para la elaboración de la guía de buenas prácticas para auditar la red inalámbrica.

Revisión de las metodologías, normas y buenas prácticas nacionales e internaciones para auditar de las redes inalámbricas que son utilizadas en la actualidad.

De acuerdo a los conceptos ya mencionados de las metodologías, estándares y normas nacionales e internacionales, las buenas prácticas propuestas, se proponen los dominios de diseño, administración y seguridad de la red inalámbrica, que permitan evaluar de forma completa cada uno. Para cada dominio se deberá determinar las buenas prácticas, proponiendo para cada uno su objetivo o propósito de las buenas prácticas, actividades o tareas a desarrollar, apoyándose de herramientas físicas y de software, cuestionarios y checklist, teniendo como resultado la propuesta siguiente:

En la parte del dominio diseño se propone 5 buenas prácticas, cada una con su respectivo checklist, incluidas herramientas de apoyo, con un total de 11 herramientas.

Item	Dominio Diseño	Checklist	Herramientas
1	Buena Práctica Dis001: Análisis de la empresa	✓	• Inventario de estaciones
2	Buena Práctica Dis002: Análisis tecnológico de la empresa.	✓	• MSIA 5.1 Analizador de Inventario de Software • Total Network Inventory 2.0.1 • Inventario de dispositivos inalámbricos • Inventario de estaciones
3	Buena Práctica DIS003: Diseño físico de la red	✓	• AirWave VisualRF Report • Network Event Viewer • AirWave Wireless Site Plan
4	Buena Práctica DIS004: Diseño lógico de la red	✓	• Secure Shell • Administración Remota EMCO • Comandos "Ping" y "Traceroute"
5	Buena Práctica DIS005: Planes de implementación	✓	

Tabla I
Dominio diseño y buenas prácticas
Arteaga,M.2009.Metodologíasde controlinterno,seguridad y auditoría informática. Artículo

En la parte del dominio administración se propone 4 buenas prácticas, cada una con su respectivos checklist, incluidos herramientas de apoyo, con un total de 9 herramientas.

Item	Dominio Administración	Checklist	Herramientas
1	Buena Práctica ADM001: Administración de recursos informáticos	✓	• Network event viewer • MSIA 5.1 analizador de inventario de software • Total network inventory 2.0.1 • Inventario de dispositivos inalámbricos • Inventario de estaciones
2	Buena Práctica ADM002: Administración de recursos humanos	✓	
3	Buena Práctica ADM003: Administración de comunicaciones y operaciones inalámbricas	✓	
4	Buena Práctica ADM004: Administración de control de accesos	✓	• Recomendaciones en relación a la gestión y establecimiento de contraseñas • MaxPassword • Password generator • Password strength analyser and generator

Tabla II
Dominio administración y buenas prácticas
Arteaga,M.2009.Metodologíasde controlinterno,seguridad y auditoría informática. Artículo

En la parte del dominio seguridad se propone 4 buenas prácticas, cada una con su respectivo checklist, incluidos herramientas de apoyo, con un total de 4 herramientas.

Item	Dominio Seguridad	Checklist	Herramientas
1	Buena Práctica SEG001: Política de seguridad de las TIC's	✓	• Recomendaciones para la concientización en seguridad de información
2	Buena Práctica SEG002: Organización de la seguridad inalámbrica	✓	
3	Buena Práctica SEG003: Implementación de la seguridad Inalámbrica	✓	• BackTrack • InSSIDER • Xirrus Wifi Inspector
4	Buena Práctica SEG004: Gestión de incidentes de seguridad inalámbrica	✓	

Tabla III
Dominio seguridad y buenas prácticas
Arteaga,M.2009.Metodologíasde controlinterno,seguridad y auditoría informática. Artículo

VIII. CONCLUSIONES

Una guía de buenas prácticas para auditar redes inalámbricas permitirá:

Al personal involucrado de TI realizar un estudio de la red WIFI de la organización, aplicando unas buenas prácticas, logrando hacer un análisis de las redes inalámbricas en su estado actual, permitiendo analizarla sobre la posición de los canales de emisión, el ancho de banda necesario para

tener una buena navegación y cobertura, permitiendo mejorar la disponibilidad, confiabilidad e integridad de la información, facilitando que las personas puedan realizar sus actividades de trabajo o entretenimiento de una manera continua y sin interrupciones.

Cotejar las metodologías, manuales y buenas prácticas nacionales e internacionales, tales como; ISO 27001, ISO 27002, y OSSTMM 2.9, identificar las buenas prácticas en promedio en los dominios de; diseño, administración y seguridad, para lograr mayor eficiencia y eficacia en el proceso de auditoría de las redes inalámbricas.

Utilizar las herramientas adecuadas y actualizadas para realizar el monitoreo de los canales de emisión, tipos de cifrado, nombres de los SSID, de manera detallada en cada buena práctica, herramientas como; *InSSIDER*, *Xirrus Wi-Fi monitor*, formatos y checklist que permita ayudar al auditor la ejecución de la auditoría a la red inalámbrica.

Con el desarrollo de las buenas prácticas mejorar el proceso de auditoría a la red inalámbrica, facilitando y apoyando la labor del auditor con experiencia para el desarrollo de la auditorías, además de reducir el tiempo de ejecución de una auditoría, logrando una importante disminución de tiempo, dinero y personal.

REFERENCIAS

[1] Arteaga, M. 2009. Metodologías de control interno, seguridad y auditoría informática. Artículo.
[2] IT Governance Institute. 2007. Cobit 4.1.
[3] ISO/IEC 27002:2013, [En línea]. Disponble: *http://www.iso27000.es/download/ControlesISO27002-2013.pdf*
[4] Plan de cinco pasos para la seguridad de wifi. [En línea]. Disponble: *http://www.fiercemarkets.tradepub.com/free/w_ai05/pf/w_ai05.pdf*
[5] OSSTMM 3 - The Open Source Security Testing Methodology Manual.
[6] Principales amenazas para la seguridad de las redes inalámbricas, [En línea]. Disponble: *http://www.networkworld.es/seguridad/principales-amenazas-para-la-seguridad-de-las-redes-inalambricas*

García Rozo, Juan Martín. Ingeniero Electrónico egresado de la Universidad Pontificia Bolivariana de Medellín, especialista en Telemática en la U.A de Medellín, certificado en CCNA labora como Coordinador de Telecomunicaciones de la red de Copa Airlines Colombia donde ha desarrollado en numerosos proyectos de infraestructura de adecuación de redes LAN, WAN y redes inalámbricas en diferentes sedes donde opera la red Copa Airlines.