UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

JUNIO –SEPTIEMBRE 2020

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO(A) EN SISTEMAS

TEMA:

ANÁLISIS DE VULNERABILIDADES PARA PREVENIR POSIBLES INSEGURIDADES INFORMÁTICAS EN LA RED INALÁMBRICA DE LA EMPRESA MOCALGRA C.A DE LA CIUDAD DE GUAYAQUIL.

EGRESADA(O):

DIEGO ANDRÈS RIZO FRANCO

TUTOR:

ING. HARRY ADOLFO SALTOS VITERI

AÑO 2020

INTRODUCCION

En las Organizaciones dentro del país se ve reflejado un aumento masivo de las Redes inalámbricas Wireless Fidelito (Wi-Fi). ya que esta conectividad inalámbrica simplifica el trabajo en movilidad, mejora la comunicación entre los empleados y el rendimiento de la transmisión de datos.

Hablar de este tipo de redes no sólo implica hablar de comunicación, sino de políticas de seguridad, configuraciones y de características técnicas, motivo por el que se ha hecho esencial la seguridad de las redes inalámbricas en las Organizaciones con el fin de tener resguardados los datos, sistemas y servicios, pero debido a que esta información viaja por el aire se vuelve un blanco de distintos tipos de amenazas.

La seguridad informática es de gran importancia dentro de las empresas, ya que esta otorga resguardo a la confidencialidad de los datos, información dentro de ella, privacidad e integridad.

Muchas de las empresas del País están siendo perjudicadas por no tomar las medidas correctas, no le brindan importancia a la seguridad informática. Piensan que no va a suceder algo de suma gravedad, pero en el momento menos esperado, se ven afectados por Amenazas informáticas que asechan a la información y los equipos de estas organizaciones.

Por tal motivo el objetivo de este trabajo de investigación es proporcionar un análisis de las vulnerabilidades de la red inalámbricas de la empresa Mocalgra C.A de la ciudad de Guayaquil el cual se encuentra ubicado Vélez 616 entre García avilés y rumi chaca, aplicando teorías, metodología, métodos e instrumentos de investigación.

Este análisis se llevó a cabo para verificar los riesgos a los cuales se encontraría expuesta la empresa Mocalgra C.A al no poseer una seguridad de software y hardware. Este caso de estudio utilizo la metodología de investigación cualitativa para poder llegar a obtener un conocimiento simplificado de la problemática a resolver, mediante las técnicas de observación directa y entrevista, usando herramientas de listado de preguntas y guion de observación, para obtener toda la información posible del estado en que se mantiene la red inalámbrica y así tener todas las vulnerabilidades para posteriormente buscar las posibles soluciones.

Se utilizaron 3 software orientado a redes: Advanced IP Scanner para verificar posibles intrusos en la red mediante verificación de dirección ip a través de un cálculo aproximado de dispositivos conectados a la red inalámbrica de la empresa. El programa Acrylic Wi-Fi home para ver rangos de frecuencia en el que emite el Router y el canal que utiliza para evitar el solapamiento de la señal, y Nessus para escanear las vulnerabilidades y así prevenir posibles ataques informáticos.

Este caso de estudio está orientado a la línea de investigación: Sistemas de información y comunicación, emprendimiento e innovación y la respectiva sublinea: Redes y tecnologías inteligentes de software y hardware a través de un análisis de amenazas y vulnerabilidades de la red inalámbrica Mocalgra C.A de la ciudad de Guayaquil.

DESARROLLO

El presente estudio se realizó en la Empresa Mocalgra C.A de la Ciudad de Guayaquil, ubicado en Vélez 616 entre García avilés y rumi chaca, inicio sus actividades comerciales 08/08/2017, se encuentra bajo la administración del Ing. Janio sudario López, quien asume el Cargo desde el mes de julio del 2019. La Empresa Mocalgra C.A se dedica al Diseño de Sistemas Computacionales Contables, en la actualidad la empresa está pasando por un cambio en su infraestructura y se evidencia un mal uso de los equipos de red y del cableado, también el Gerente dio a conocer que la red inalámbrica a presentado sinnúmeros de fallas en cuanto lentitud y caída de señal , en dicha red no se utilizan los debidos métodos de seguridad en cuanto al control de acceso a la red y Control del alcance de los datos que viajan por aire, haciéndola vulnerable a diversos ataques informáticos, problemas que afectan el funcionamiento de las diversas tareas de desarrollo, administrativas y comunicación que se manejan dentro de la Empresa.

La Empresa cuenta con 2 Departamentos: Desarrollo y Administración, cuanta con una velocidad de internet de 20 Mb con un router que abastece estas áreas donde laboran 6 personas que hacen uso de las red inalámbrica. En una Red inalámbrica no se utilizan cables y mediante ondas cumple su función de trasmitir datos. (Dordoigne, 2020)

Ventajas de las Redes inalámbricas:

- No se utiliza mucho cableado.
- Instalación de facilidad, se evita el traslado de cableado por techos o pisos.
- Movilidad, poder conectarse en cualquier lugar.

Desventajas:

- Velocidad disminuida en comparación a conexión por cable de red.

- Puede presentarse interferencias.
- Vulnerable a diversos tipos de ataques por usuarios ajenos . (François, 2016)

Este tipo de redes son de suma importancia para la optimización de actividades de los empleados de esta organización, sin embargo, se evidencia en la ilustración 1 que los equipos se encuentran un poco olvidados y en desorden.

Ilustración 1: *Ubicación de los equipos de red*

Elaborado por: Diego Rizo Franco.

Se evidencia en la ilustracion1 que los equipos se encuentran en un lugar no adecuado, con descuido del polvo y de fácil manipulación de todo el personal que ahí labora, y con poco cuidado en el cableado de la Red.

También se evidencio que alrededor de la Empresa están ubicadas viviendas y edificios con redes inalámbricas, lo que produce interferencia en la señal y por ende esta se debilita.

A continuación, se detalla los equipos informáticos que se encuentran en la red de la empresa:

Tabla 1: *Equipos de la red*

Equipos	**Cantidad**	**Características**
Router TP-Link	1	TP-Link TL-WR941ND 300Mbps Wireless 3 antenas
Switch Tp-link	2	TP-Link TL-SF1008D 8 puertos RJ45 a 10/100 Mbps
HP (Escritorio)	4	800Gb HDD. 8Gb Ram, I3 2.5 GHz
Dell(Laptop)	1	1 TB HDD . 8Gb Ram, i5 3.5 GHz
Impresora Canon E402	L355	Tinta continua , wifi

Elaborado por: *Diego Rizo Franco*

Wi-Fi es un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11 es un estándar para redes inalámbricas definido por el Institute of Electrical and Electronics Engineers (IEEE)., robusto, maduro y bien establecido que continúa creciendo y evolucionando. (Kurose, 2017)

Tabla 2. *Estándares 802.11*

802.11	Año	Velocidad	Compatibilidad	Frecuencia
A	1999	54 Mbps	No	5 GHz
B	1999	11 Mbps	No	2,4 GHz
G	2003	54 Mbps	802.11b	2,4 GHz
N	2009	600 Mbps	802.11a/b/g	2,4 GHz o 5 GHz
AC	2012	1Gbps 1000 Mbps	802.11a/n	2,4 GHz y 5 GHz
AD	2014	7 Gbps 7000 Mbps	802.11a/b/g/n/ac	2,4 GHz , 5 GHz y 60 GHz

Elaborado por Diego Rizo

Se utiliza el cifrado de redes inalámbricas para obtener seguridad por medio del protocolo de autenticación, que pide una contraseña cuando un usuario intenta conectarse.

Tabla 3. Tipos de cifrados inalámbricos**.**

	WEP	WPA	WPA 2
Duración de clave	24-bit IV	48-bit IV	48-bit IV
Integridad de cabecera	CRC-32	Michael	CCM
Cifrado	RC4	RC4	AES

Control de claves	Ninguna	EAP	EAP
Longitud de clave	40 bits	128 bits enc. 64 bits auth.	128 bits
Integridad de datos	CRC-32	Michael	CCM

Elaborado por: *Diego Rizo Franco*

Los Ataques Informáticos a la red inalámbrica Son métodos que se utilizan con el fin de crear un desequilibrio y tener el dominio de la red y de los datos de la misma. (Aguirre, 2018)

Tabla 4. *Tipos de Ataques a Redes Inalámbricas*

Man in the middle	**Denegación de Servicio (DoS)**	**Sniffing**	***MAC SPOOFING:***
Consiste en que el atacante se ubica en el centro de la conexión entre 2 equipos en comunicación con el fin de dirigir, separar, interferir o introducir el mensaje, obteniendo del equipo cliente todos los datos. (Astudillo, 2017)	La finalidad de este ataque es cargar al extremo la red mediante la saturación de peticiones al AP (Access point) lo cual hace que la red colapse de manera que se deniega a los usuarios el servicio. (Torres, 2018)	Este tipo de ataques consiste en mediante la tarjeta de red del equipo del atacante obtener le tráfico, paquetes que viaja mediante el aire, con el fin de usar la información de mala forma.	Consiste en el uso de programas para clonar la Dirección Mac de un equipo de la red hacia otro del atacante y así tener los beneficios de la Dirección clonada.

Elaborado por: *Diego Rizo Franco*

La red inalámbrica de MOCALGRA CA puede clasificarse como insegura porque no regula el rango de señales enviadas por la red más allá del área del edificio Por consiguiente no se puede eludir la interceptación de la información que se trasmite por el aire y la señal se puede detectar a amplia distancia e ingresar a la red como un usuario no autorizado .Hay inconsciencia de los usuarios de dicha red sobre los actuales técnicas herramientas de seguridad y métodos que hoy en día existen motivos por los cuales la información se va a encontrar en riesgo debido a que este tipo de redes poseen una gran desventaja que es la trasmisión de los datos por medio del aire ya que esta queda comprometida a la sustracción de terceras personas

Se propuso realizar un diagnóstico de todas las debilidades posibles a tener, de la estructura de la red inalámbrica de la empresa, debido a que es de suma importancia tener en conciencia los conocimientos de la seguridad informática como lo son la autenticidad, la confidencialidad, y la integridad, ya que por este tipo de redes se trasmite información de gran importancia, del mismo modo es necesario mejorar la calidad de la seguridad para evadir los diversos tipos de ataques. los beneficiados principalmente serán los usuarios que disponen de la red de la empresa, ya que se brindará una calidad de conexión con muchas más seguridades, amenorando y aportando a la reducción de vulnerabilidades.

Para la elaboración de este estudio se usó la metodología de investigación Cualitativa , se utilizó dos de sus técnicas , la observación de campo y la entrevista , para así hacer un diagnóstico de la condición actual sobre la problemática que se ha establecido , estas se realizaron en el departamento de administración , y la entrevista se le realizo al Gerente de la empresa Mocalgra C.A el Ing. , Janio Sudario, así mismo se procedió a la verificación de todos los dispositivos que conforman la red inalámbrica con la debida autorización , con los diferentes tipos de técnicas que se adaptaron se adjuntó gran información y de esa manera se dio a conocer los distintos problemas que posee

la red inalámbrica de la empresa en la actualidad .De la técnica entrevista se utilizó de herramienta una guía de entrevista estructurada , y de la técnica observación fueron registro anecdóticos y guía de observación .

El Poco control de acceso a la red inalámbrica se debe a la baja importancia de seguridad del cambio de clave por tiempo establecido, a la verificación de los distintos dispositivos conectados, para así conocer la existencia de intrusos en la red y proceder a hacer la restricción de acceso por filtrado Mac, de la misma manera la computadora central del área administrativa no posee un sistema detector de intrusos, que hoy en día existen y se pueden descargar gratuitamente en internet.

La caída de señal de la red inalámbrica se puede deber a diversos factores uno de ellos y el más frecuente es el solapamiento de la señal, ya que alrededor de la empresa se encuentran funcionando un sinnúmero de redes inalámbricas y algunas usan los mismos canales del rango de frecuencia , otro factor que conlleva a la caída de la señal es el ataque por Denegación de Servicio (DoS) .El control y verificación del buen funcionamiento del router, como la mala ubicación y que no haya otros aparatos electrónicos encima o alrededor de este ayudan a que siempre la señal sea más estable en la Empresa.

Este tipo de redes puedes ser afectadas por interferencias de otros dispositivos que están en funcionamiento de una frecuencia igual, eso podría bajar el rendimiento de la velocidad de trasmisión de datos. (Stallings, 2016)

El Nivel bajo de métodos seguridad en la red inalámbrica, las empresas han descuidado la seguridad a nivel de software en los ordenadores para evitar ataques, como un antivirus original y actualizado, Firewall, Software de detection de Malware, Software de Detención de Spyware. (Cano, 2018)

El Gerente dio a conocer que se encuentra en construcción otra área de trabajo en la parte baja del edificio, por lo cual se despliega como otra problemática la poca cobertura wifi de la red , que se puede solucionar con el cambio de dispositivo, a uno de mejor características, hoy en día existen dispositivos de más calidad y fuerza de señal, otro método para empresas de gran infraestructura es el de añadir una subred a los diversos departamentos donde la fuerza de la señal es muy baja, pero utilizando los canales adecuados y por ultimo una buena ubicación del dispositivo inalámbrico también ayuda de gran manera a la potencia de la señal.

El router puede emitir la señal wifi a través de 2 bandas de frecuencias, 2,4 y 5 GHz estas bandas se dividen en varios canales de trasmisión wifi que el router utiliza para brindar la señal . (Urbina, 2016) La mayoría de dispositivos actuales operan, por defecto, en la franja de frecuencias cercana a 2.4 GHz.

Los router de gama media alta cuentas con un sistema que analizan el espectro electromagnético para configurar automáticamente el mejor canal optimo entre estos 3 canales en función de los usados entre router vecinos. Para la frecuencia de 2, 4 GHz se habla de 14 canal que tienen 22mhz de ancho cada uno la calidad de conexión depende mucho del canal usado, por lo tanto, a mayor cantidad de dispositivos que emitan en el mismo canal mayor interferencia.

Para esta investigación del análisis de vulnerabilidades de la red inalámbrica y pensando en la búsqueda de los mejores tipos de herramientas para encontrar las posibles soluciones, en este caso se utilizaron 3 programas de uso Gratuito enlazados a este tipo de redes que son los siguientes:

- Advanced IP Scanner
- Acrylic Wi-Fi Home
- Nessus

Advanced IP Scanner es un programa el cual nos permite escanear nuestra red de internet y verificar cuantos dispositivos están conectados a ella, nos brinda información de que direcciones ip están tomando y que dirección Mac poseen cada dispositivo y así posteriormente detectar los dispositivos conectados a la red que no están verificados ni considerados pertenecientes al personal de la empresa.

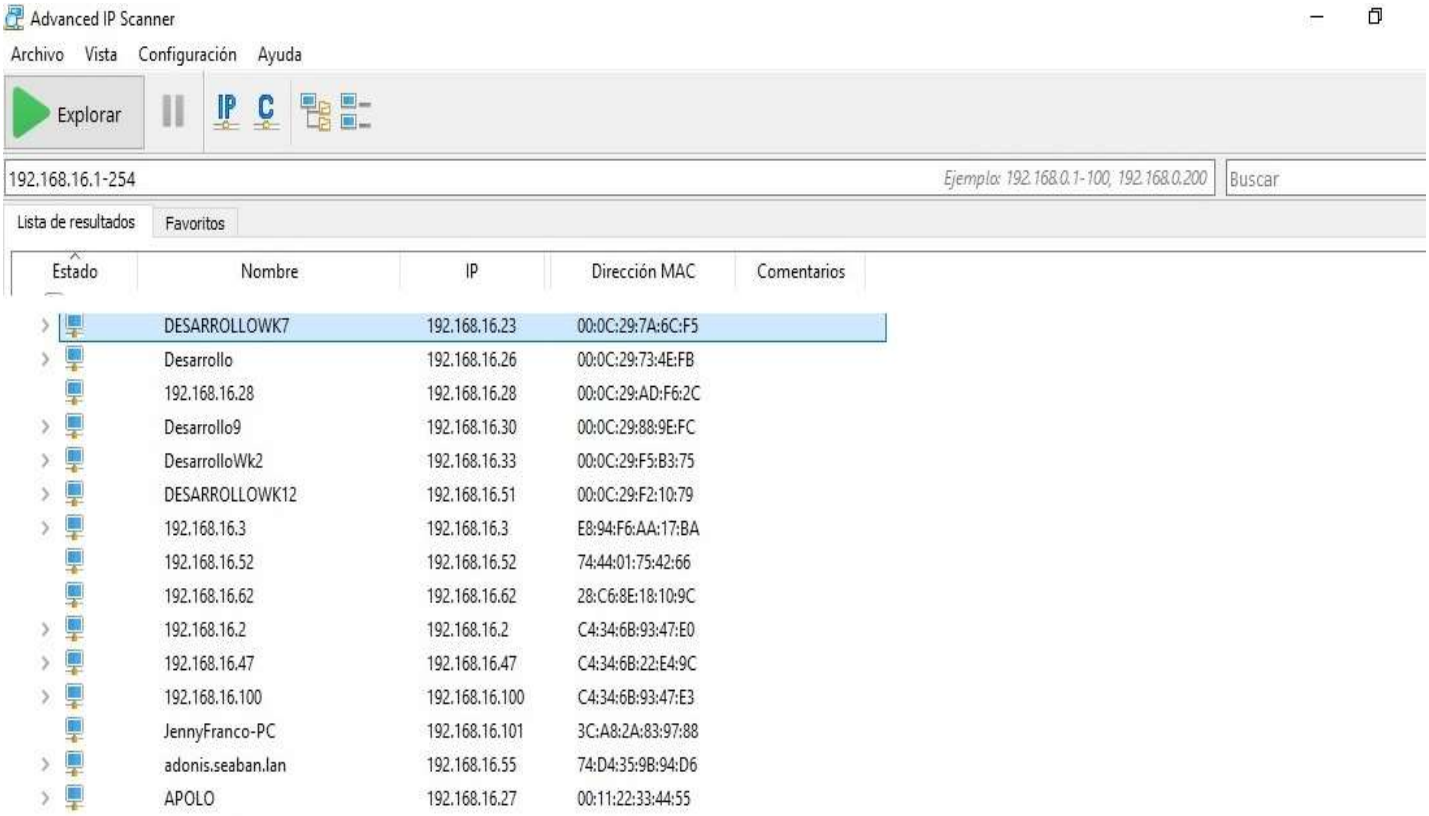
Mediante este programa se realizó un escáner de los dispositivos conectados a la red wifi, y se encontró alrededor de 15 dispositivos conectado con su marca e ip de la empresa, de tal manera se hizo un conteo de cálculo estimado de los dispositivos que deberían estar en ese momento conectados y dieron en total 10 dispositivos incluyendo los celulares del personal de la empresa que en ese momento laboraban.

De esa forma se demostró que 5 dispositivos conectados estaban fuera del rango del cálculo estimado que se verificaron en ese momento en la red, estos eran posiblemente ajenos a la empresa. Una solución sería negar el acceso mediante su dirección Mac, que es posible teniendo acceso a las configuraciones del router e ingresando a las opciones de filtrado de direcciones Mac bloqueando los dispositivos que no queremos que accedan a nuestra red inalámbrica, como un método de control de acceso.

Este tipo de sistemas es un método de gran importancia que un administrador necesita, para tener mejor comprendimiento y visibilidad de lo que en la red está ocurriendo, mostrando todos los dispositivos que circulan en ella. (Lederkremer, 2020)

De esta manera una persona encargada de la empresa tendría ventaja con esta técnica y así mantener la red en optima condiciones en cuanto a acceso y conexión.

Ilustración 2: *scanner dispositivos conectados.*



Elaborado por: *Diego Rizo Franco*

Acrylic Wi-Fi Home es un programa de escaneo de redes inalámbricas que nos brinda toda la información a fondo de cada una de ellas como los es el: SSID la potencia de la señal, el rango de frecuencia, el canal en el que trasmite, la velocidad y el tipo de seguridad. El uso de este programa en esta investigación conlleva a que existe mucha interferencia en la señal por la gran cantidad de dispositivos conectado cerca a el edificio de la empresa Mocalgra C.A , que se puede evidenciar en la siguiente imagen.

Ilustración 3: *Escaneo de redes inalámbricas cercanas.*

Elaborado por: *Diego Rizo Franco*

Los canales que no se cruzan o superponen son el 1, 5 ,11 que son los más recomendados. Nuestra red se llama R Suarez, de esta manera se pudo visualizar el inmenso listado de redes inalámbricas cercanas alrededor de más de 30 redes , el objetivo del uso de esta herramienta fue analizar los canales de trasmisión que usaban todos los dispositivos y buscar el canal más adecuado y con menos uso de toda la lista, para así poder liberar un poco el solapamiento de la señal inalámbrica, de tal manera con toda esta información el canal más adecuado sería el número 1.

En cuanto al RSSI que es el indicador de la fuerza de la señal recibida, muestra -55 que puede mejorar buscando la mejor ubicación y altura del router. Ya que esa cantidad reflejada no es tan óptima para ser un dispositivo que está funcionando dentro de la empresa.

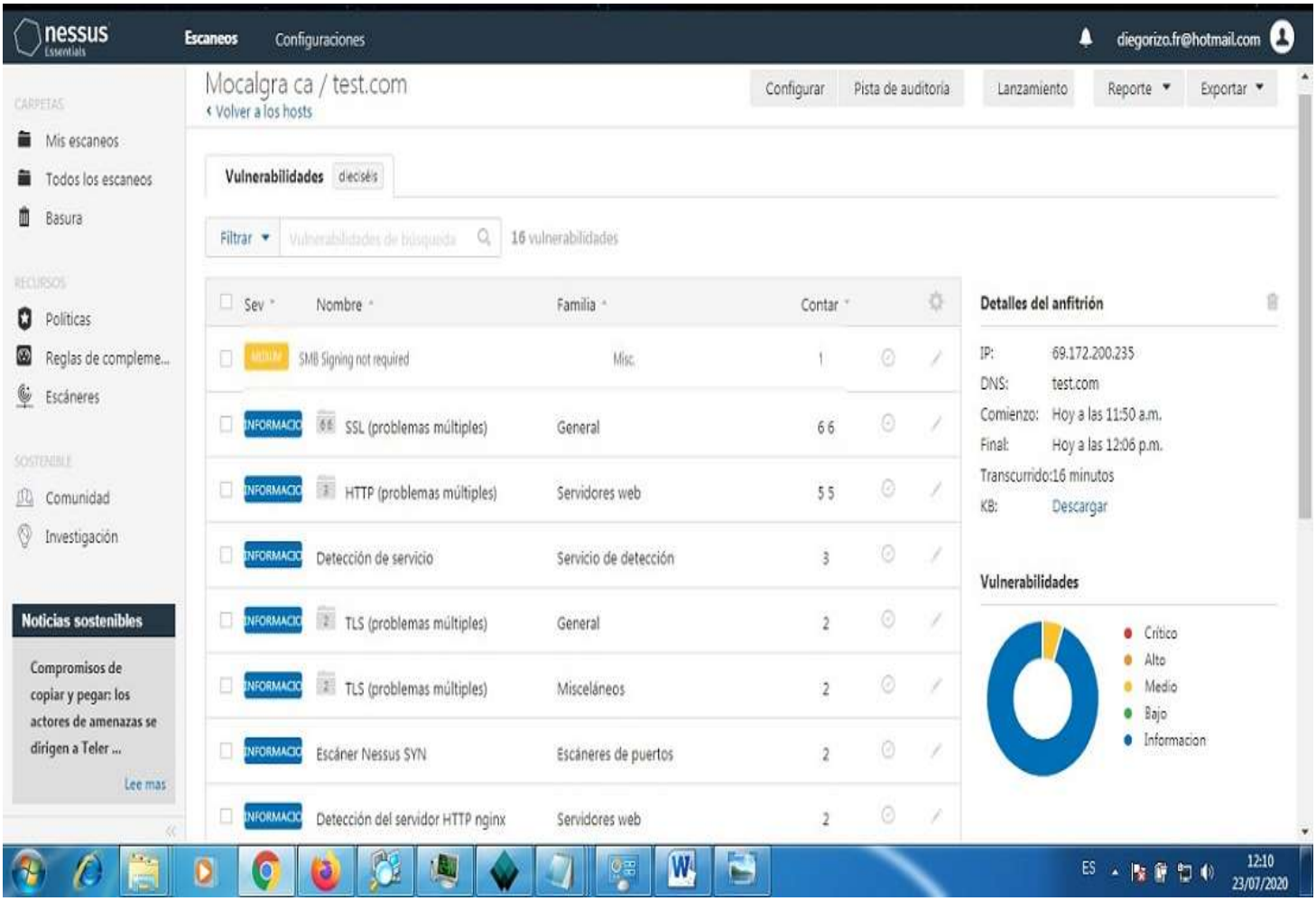
Como ultima herramienta se utilizó Nessus que es un software que sirve para escanear vulnerabilidades de red, es uno de los programas más utilizados en el mundo empresarial para este tipo de propósitos, permite bridar Información precisa y detallada de estas vulnerabilidades.

Las vulnerabilidades se pueden encontrar en sistemas ya que estos pueden poseer huecos de seguridad desconocidos y conocidos, estas tienen configuraciones por default o tienen errores de configuración como resultado. (JAEN, 2020)

De esta manera se instaló esta herramienta en la maquina principal del departamento de administración de la Empresa ya que es la que tiene más actividad a los distintos procesos que la empresa lleva a cabo a diario.

Se procedió a el escaneo de red como se muestra en la siguiente ilustración a continuación y se evidencio las distintas vulnerabilidades de tipo información y de nivel medio.

Ilustración 3:*Escaneo de vulnerabilidades con Nessus.*

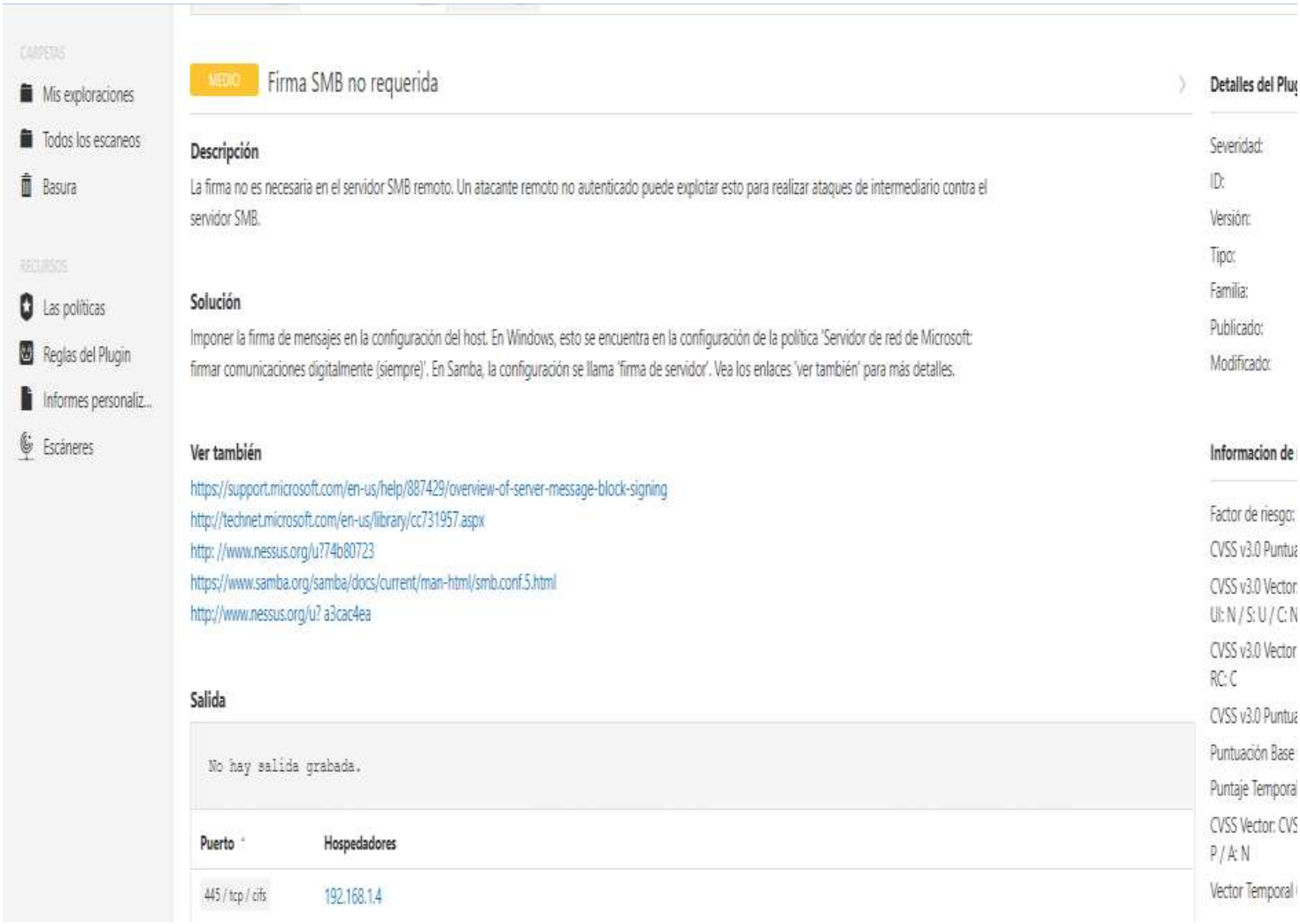


Elaborado por: *Diego Rizo Franco*

Luego de realizarse el escaneo de las vulnerabilidades con el software nessus se realizó una comparación de los resultados obtenidos y se realiza un análisis de los niveles de gravedad que se muestran por colores.

La mayoría eran de nivel de información, luego se evidencio uno de nivel medio que se refleja en la siguiente imagen.

Ilustración 4: *Vulnerabilidad nivel medio*



Elaborado por: *Diego Rizo Franco*

Se evidencio una de vulnerabilidad de nivel medio “Firma SMB no requerida” . Un atacante remoto no identificado puede abusar de esto y realizar ataques de man-in-the-middle (hombre en medio) contra el SMB servidor. Indicando que un atacante con la capacidad de interceptar el tráfico del servidor RDP puede establecer el cifrado con el cliente y el servidor sin ser detectado permitiendo tener cualquier información confidencial transmitida incluida las credenciales de autenticación.

Server Message Block (SMB), trabaja como un protocolo de red de capa de aplicación empleado principalmente para dar acceso compartido a archivos, impresoras y puertos serie y comunicaciones misceláneas entre nodos en una red **.** (Rascagneres, 2016)

El programa nos brinda la descripción de solución de Aplicar la firma de mensajes en la configuración del host. SMB se ejecuta a través de TCP / IP utilizando el puerto 445 específicamente. De tal manera tomamos esa referencia de información para una solución óptima del problema encontrado. (Mitnick, 2017)

CONCLUSIONES

Por medio de esta investigación se evidencio la falta de métodos de seguridad de la red inalámbrica en la empresa Mocalgra C.A de la ciudad de Guayaquil Clasificándola como insegura.

Se demostró la carencia de nivel de seguridad en cuanto al acceso de usuarios no identificados a la red mediante el uso de la herramienta Advanced IP Scanner, dando como resultado que 5 dispositivos conectados a la red inalámbrica eran ajenos a la empresa , como posible medida de solución se recomienda el bloqueo de estos dispositivos mediante Filtrado Mac del router , y el uso un sistema de detección de Intruso (IDS) para el control de acceso a Red en tiempo real como por ejemplo el programa snort que tiene ganado el puesto como uno de los principales programas usado en el mundo para estas tareas y es gratuito , otra recomendación es el cambio de contraseña en tiempos establecidos.

Se evidencio a través del programa *Acrylic wifi* home el solapamiento de la señal a gran escala por el sinnúmero de redes inalámbricas alrededor de la empresa como solución en base a este estudio de la red, se recomienda cambiar el canal de trasmisión del router al número 1 que es el menos usado y con menos interferencia en cuanto a todas las redes escaneadas. La fuerza de la señal fue de -55 poco potente para un router inalámbrico que este emitiendo señal dentro de una misma área de cercanía. La mejor ubicación del router a un área elevada, la prevención del polvo y el cambio de tecnología son posibles soluciones para mejorar la calidad de la señal.

En cuanto a la seguridad a nivel de Software de la red mediante la herramienta Nessus se encontró la vulnerabilidad de nivel medio “Firma SMB no requerida”. Un atacante remoto no identificado puede abusar de esto y realizar ataques de man-in-the-middle (hombre en medio). la manera de arreglar esa vulnerabilidad es poner la firma de mensajes en la configuración del host.

REFERENCIAS

Aguirre, L. A. (2018). *Hacking y Cracking Redes Inalàmbircas wifi.* Lima, Perù: MACRO.

Astudillo, K. (2017). *Como Hackear Redes Inalàmbricas facilmente.* BESTSELLER.

Cano, G. S. (2018). *Seguridad cibernètica. Hackeo èticoco y programación defensiva.* Mèxico: Alfaomega Grupo Editor.

Dordoigne, J. (2020). *Redes Informáticas - Nociones fundamentales.* ENI.

François, J. (2016). *La seguridad informática en la PYME.* eni.

JAEN, F. S. (2020). *DIRECCION DE SEGURIDAD Y GESTION DEL CIBERRIESGO.* RA-MA.

Kurose, J. (2017). *Redes de com putadoras. Un enfoque descendente.* Madrid, España: PEARSON EDUCACIÓN, S. A.

Lederkremer, M. (2020). *Redes Informàticas Avanzado.* Buenos Aires, Argentina: SIXEDICIONES.

Mitnick, K. (2017). *UN FANTASMA EN EL SISTEMA.* CAPITAN SWING.

Rascagneres, P. (2016). *Seguridad informática. Hacking Ético. Conocer el ataque para una mejor defensa.* Barcelona: Eni.

Stallings, W. (2016). *COMUNICACIONES Y REDES DE COMPUTADORES.* PEARSON.

Torres, D. P. (2018). *Redes CISCO.* Alfaomega.

Urbina, G. B. (2016). *Introducción a la Seguridad Informàtica.* Mexico: Grupo Editorial PATRIA.

ANEXOS

Entrevista con el Gerente

Realizando las pruebas

Área de desarrollo

Área de Administrativa

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

LUGAR A ENTREVISTAR: Mocalgra C.A de la ciudad de Guayaquil

ENTREVISTADO: Gerente de la Empresa: Ing. Janio Sudario

Entrevista

¿Qué velocidad de internet tiene contratada la empresa?

20 megas se tiene Contratado

¿Cree usted que la red inalámbrica de la Empresa presenta alguna vulnerabilidad?

La verdad si lo creo porque en ocasiones el internet se pone demasiado lento que no se pueden abrir páginas y en ocasiones caídas de señal, no creo que con la velocidad que se cuenta se ponga tan inestable.

¿Con que frecuencia cambian las contraseñas del /los Router's?

No sé a cambiado desde que se contrató el servicio.

Con que frecuencia actualizan o cambian los dispositivos de conexión inalámbrica.

La empresa no ha hecho ningún cambio de router desde que instalaron el servicio**.**

¿Usted tiene conocimiento acerca de la seguridad informática?

No lo tengo.

Considera usted que el personal de la empresa está debidamente capacitado para dar mantenimiento a los dispositivos de conexión inalámbrica.

Los empleados si tienen conocimientos de informática, pero nadie lo ha hecho por descuido, incluido el mío.

¿Los equipos informáticos se mantienen en un cuarto con un ambiente adecuado?

Están encima de un escritorio en el área de desarrollo

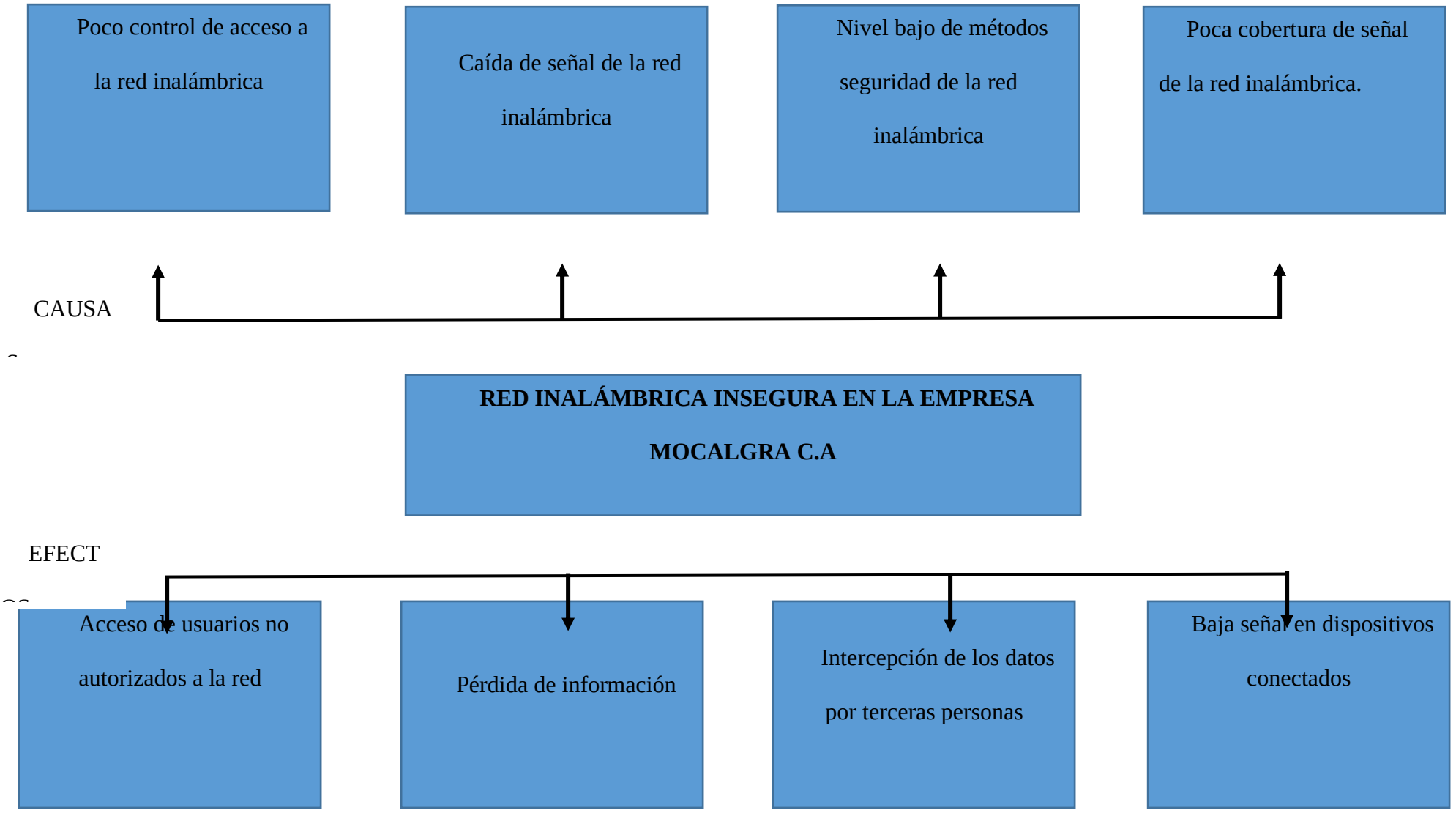
¿Conoce usted de los peligros que pueden ocurrir al no contar con una seguridad dentro dela red?

Muy poco

¿Cree usted que los datos e información que transitan dentro de la red están protegidos ante ataques informáticos?

No lo creo que este cien por ciento segura, porque la tecnología avanza y existen hackers

ÁRBOL DE PROBLEMAS



Análisis Foda

FORTALEZAS	OPORTUNIDADES
conexión Internet de alta velocidad. Buena infraestructura de los distintos departamentos de la empresa para mejor ubicación de cableado y posición del dispositivo de conexión inalámbrica.	Aplicación de charlas a los distintos empleados para fortalecer conocimientos sobre posibles inseguridades informática. Adquisición de nuevas tecnologías para mejor el rendimiento de la red inalámbrica. Cambio de los canales de emisión de la red inalámbrica para evitar solapamiento de la señal Bloqueo de dispositivos conectados ajenos al personal de la empresa mediante filtrado Mac.
DEBILIDADES	**AMENAZAS**
Falta de mantenimiento preventivos y correctivos a los equipos informáticos. Mala estructura del cableado de la red. Falta de un Sistema de Detección de Intrusos. Falta de conocimiento de los empleados sobre las distintas herramienta y métodos que en la actualidad existen para vulnerar las redes inalámbricas.	Aparición de nuevas herramientas y método de ataque a las redes inalámbricas Polvo acumulado en los Equipos Informáticos. Pocos recursos para la renovación de tecnológica de la empresa.