ANÁLISIS, EVALUACIÓN DE RIESGOS Y ASESORAMIENTO DE LA SEGURIDAD INFORMÁTICA EN EL ÁREA DE REDES Y SISTEMAS DE LA ALCALDÍA DE PAMPLONA - NORTE DE SANTANDER

JORGE ENRIQUE RAMIREZ MONTAÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PAMPLONA
2015

ANÁLISIS, EVALUACIÓN DE RIESGOS Y ASESORAMIENTO DE LA SEGURIDAD INFORMÁTICA EN EL ÁREA DE REDES Y SISTEMAS DE LA ALCALDÍA DE PAMPLONA - NORTE DE SANTANDER

JORGE ENRIQUE RAMIREZ MONTAÑEZ

Trabajo de grado para optar el título de Especialista en Seguridad informática

Director
John Freddy Quintero MS (c)

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PAMPLONA
2015

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Pamplona marzo de 2015

DEDICATORIA

Dedico mi trabajo a nuestro Dios ser superior que me ha brindado la fortaleza física, mental y espiritual para desarrollar este trabajo.

De la misma manera dedico este logro a mis padres, mi hija y mi esposa quienes me han dado su apoyo, cariño y comprensión para que mis metas se llevaran a cabo.

AGRADECIMIENTOS

Agradezco a Dios por siempre por permitirme llegar hasta estas instancias de mi formación, gracias porque siempre que he orado para que me ayude y me ilumine y he recibidos sus bendiciones.

Sinceros agradecimientos a mis padres, mi esposa y mi hija, por apoyarme para alcanzar estos logros.

Sinceros agradecimientos a las funcionarios de la Alcaldía Municipal de Pamplona en especial al señor Carlos bustos alcalde municipal, Omar Alfonzo Pérez jefe de talento humano y al ingeniero de sistemas José Gelvez ingeniero de soporte, por permitirme realizar la labor de investigar, prestándome su atención y su apoyo para alcanzar los objetivos propuestos.

Gracias a los docentes tutores, líderes de la escuela y el programa, quienes me han brindado su apoyo, asesoría y acompañamiento para llevar a cabo el presente trabajo.

Ing. Jorge Enrique Ramírez Montañez

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

INTRODUCCIÓN

Las organizaciones a través de la historia han tenido entre sus prioridades las protección de sus bienes documentales, con el avance de la tecnología la información revoluciono la forma de pensar y tomar el control del mundo de una manera intangible que se procesa se guarda y viaja a todas partes utilizando medios fabricados para servir a la información, el recurso más valioso para muchas personas y todas las organizaciones con la cual el mundo se integra a partir de sus servicios, aprovechando las bondades de la tecnología y las comunicaciones. Al ser tan valioso e importante recurso surgieron poco a poco tantas formas, técnicas y herramientas para vulnerarla, robarla y destruirla, se convirtió desde entonces en un objetivo para quienes comprendieron su verdadero valor en la dinámica del mundo, abarcando tanto aspectos, económicos, sociales y gubernamentales, con fines comerciales, destructivos; en la medida que la información se expandió gracias a internet también se expandieron las oportunidades y los beneficios para el desarrollo de la humanidad, pero con ellos también se inició una lucha cibernética entre quienes atacan la información de otros que la han conseguido con autoría propia, la compraron, la administran o simplemente la gestionan, en esta lucha se crearon muy rápido armas para atacar y otras defenderse lo que ha sido una evolución constante que ha generado que se perfeccionen de forma exponencial.

Con este trabajo se aborda el análisis de riesgos de una entidad pública que usa la información como materia prima para su gestión mediante herramientas informáticas y *hardware* que sirven de conexión entre los funcionarios. Con el análisis de riesgos se presenta un panorama real de la seguridad informática de la información en la entidad; el proceso conlleva un proceso de investigación aplicando técnicas interdisciplinares y otras aplicadas a la disciplina de la

seguridad informática, con el fin de encontrar la información suficiente para determinar el estado de vulnerabilidad que presenta la información en la entidad, es decir realizando diversas pruebas a los bienes informáticos dentro de un marco legal constituido en la ley 1273 del año 2009 que contempla los delitos informáticos y dentro del concepto y el actuar del investigador con pruebas de Ethical Hacking. Con el análisis de riesgos se pretende llegar a determinar los factores que amenazan la información y los bienes del entorno informático y formular una serie de controles de acuerdo a los bienes en riesgo, teniendo en cuenta normas referentes al tratamiento de los riesgos y su administración como los son la norma ISO 27001 y ISO 27002 dentro de un plan del gestión de la seguridad de la información. Finalmente la asesoría está dirigida a la aplicación de controles y su sostenibilidad que permitirá que la entidad este en el espectro seguro para el manejo de la información.

1. PLANTEAMIENTO DEL PROBLEMA

La Alcaldía del municipio de Pamplona, es una entidad del estado, compuesta administrativamente por el señor alcalde municipal, órganos de control (Personería, contraloría y procuraduría) secretarias, y otras entidades (consejo municipal, entidades descentralizadas, salud y educación). La labor del alcalde está basada en las funciones otorgadas por la constitución nacional, la ley, las instrucciones y órdenes que reciba del Presidente de la República y del respectivo gobernador.[1]

Ante la globalización de la tecnología y la aparición de diversas herramientas informáticas, el gobierno nacional ha venido creando diversos proyectos de implementación de tecnología para mantener en línea las entidades e instituciones del estado bajo marco de la estrategia de Gobierno en Línea del orden Territorial (GELT) que implementa el Programa Gobierno en Línea del Ministerio de Tecnologías de la Información y las Comunicaciones, sin embargo este desarrollo solo se ha aplicado al uso de servicios a nivel de portales *Web* y servicios en línea y no ha sido implementado para adecuar la infraestructura tecnológica y en general la parte informática de los despachos del gobierno municipal en tanto que desde allí mismo se generan volúmenes de información producto de las labores administrativas, siendo necesario la utilización algunas herramientas como apoyo tecnológico para llevar procesos administrativos que conducen a mejorar el manejo de la actividad en donde la labor se ejecuta sobre programas ofimáticos, contables, servicios financieros, mensajería en línea, operaciones interinstitucionales, correo electrónico, de vigilancia y otras aplicaciones basadas en internet para realizar comunicaciones; todo esto contemplado para facilitar y

[1] Alcaldía de Pamplona. (20 de Marzo de 2015). *Nuestra alcaldia*. Obtenido de http://pamplona-nortedesantander.gov.co/quienes_somos.shtml

generar una gestión más eficiente y oportuna a la población en general pero no es visible una seguridad informática y un Sistema de Gestión de la Seguridad de la informática que reserve la información, los recursos y los medios que se manejan ya sea porque al área soporte tecnológico el tema de seguridad informática no lo considera indispensable o ignoran los riesgos que se corren al no tener claridad sobre el valor de la información y las amenazas que la rodean.

Es evidente que se presenta una estructura de redes y sistemas administrados deficientemente sin la aplicación de un Sistema de Gestión de la Seguridad de la información ni alguna norma o control que regulen el correcto funcionamiento de los equipos en cuanto a la configuración, buenas prácticas y optimización de recursos. Este panorama de escasa protección a los bienes informáticos es causado por la deficiencia de las políticas de seguridad informática y los controles que permitan detectar y sanear las vulnerabilidades para evitar que posibles amenazas generen riesgo a la integridad de los bienes informáticos de la entidad.

Al continuar el desconocimiento de la seguridad de la información y el desconocimiento de las normas del Sistema de Gestión de la Seguridad de la informática por parte de la administración Área de redes y sistemas de la Alcaldía de Pamplona - Norte Santander, aumentarán las probabilidades de posibles delitos informáticos ante las vulnerabilidades y amenazas que comprometen procesos de gestión pública, acceso filtración de datos claves de funcionarios y población. Todo esto desfavorecerá la integridad, confidencialidad y disponibilidad de la información, lo cual se puede generar una crisis dentro de la entidad con repercusiones de la gestión hacia la población.

1.1 FORMULACIÓN DEL PROBLEMA

Ante el uso de las Tecnologías de la Información y la comunicación Tics como herramientas, administrativas, comunicación y de gestión ¿Cómo identificar los factores que amenazan la seguridad informática en el área de redes y sistemas de la Alcaldía municipal de Pamplona - Norte Santander, mediante el análisis y evaluación de riesgos?

2. JUSTIFICACIÓN DEL PROYECTO

La evolución de las diferentes relaciones humanas incluyó ineludiblemente la tecnología como elemento predominante para facilitar las diversas tareas y necesidades de una sociedad que cada vez es más cibernética. Las organizaciones sin importar su razón de ser requieren almacenar, tratar y transformar la información como un recurso valioso y predominante en el desarrollo, es así que ésta se convierte en atractivo sensible de ser vulnerado y atacado por quienes buscan un beneficio económico estratégico o simplemente de sabotaje, sin embargo ante estas circunstancias algunas organizaciones que mueven grandes y pequeños volúmenes de información, prestan poca atención al tema de seguridad y protección de sus datos en tal medida que no se invierten los recursos suficientes para establecer políticas que fortalezcan la protección de los sistemas; en este contexto de la inseguridad de la información en pymes, el robo y fuga de datos aumentó en un 42 por ciento desde el 2011 y el 2012 a nivel mundial. En Colombia este flagelo es más grave que en el promedio de empresas en el mundo. La 'Encuesta Global Sobre Fraude 2012' realizado por MaTTica,[2] laboratorio forense digital mexicano, encontró que el 19 por ciento de las compañías colombianas fueron víctimas del hurto de información, las pequeñas y medianas empresas son ahora el blanco del 31 por ciento de todos los ataques (estudio de Symantec, publicado por el periódico el tiempo 23 abril del 2013).[3] Los negocios que hasta ahora están implementando la sistematización como herramienta para su actividad, necesitan herramientas que complementen con las demás aplicaciones de administración el óptimo manejo y procesamiento de la información, en la medida que las configuraciones y equipos estén en buen estado

[2] Mattica. (26 de Marzo de 2013). *El perfil del ciber delincuente en las empresas*. Obtenido de mattica.com/el-perfil-del-ciberdelincuente-en-las-empresas/

[3] Redacción Tecnologia, P. e. (23 de Abril de 2013). *Dos de cada 10 empresas, víctimas de robo de datos* . Obtenido de http://www.eltiempo.com/archivo/documento/CMS-12758292

para su funcionamiento, es así que la sistematización es requerida con todo el soporte de seguridad.

Preservar la información y la integridad de un sistema informático es algo muy importante para una empresa o una entidad, ya que en pérdidas económicas, sin dejar a un lado el peligro que podría llevar el acceso al sistema de un usuario no autorizado. Con el análisis y evaluación de riesgos en el área de redes y sistemas de la Alcaldía municipal de Pamplona - Norte Santander se pretende obtener la información sobre amenazas y vulnerabilidades que constituyen los riesgos de perdida de información haciendo necesario ejecutar un plan de mejora dentro del marco del Sistema Gestión de la Seguridad Informática que permita formular procedimientos y políticas que garanticen un manejo y una dinámica la información de forma segura. Con los resultados y la información obtenida en la investigación se genera un estudio suficiente, del cual se deriva un nivel de apropiación del panorama y responsabilidad que administra área de redes y sistemas, en donde el asesoramiento constituye la concientización y puesta en marcha de buenas prácticas se seguridad informática del personal encargado sobre el tratamiento de los recursos y su óptimo funcionamiento soportado en conocimientos para identificar las posibles futuras vulnerabilidades y ataques a los que está expuesto el área de redes y sistemas y se asimile y se comprenda que la seguridad informática se encuentra articulada dentro del marco de la ley 1273 del año 2009, en donde se contemplan todos los delitos informáticos en Colombia.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un análisis y evaluación de riesgos para asesorar e implementar mejoras en la seguridad informática el área de redes y sistemas de la Alcaldía de Pamplona - Norte Santander.

3.2 OBJETIVOS ESPECÍFICOS

- Efectuar un diagnostico general sobre la red de datos identificando falencias de seguridad informática presentes el área de redes y sistemas de la Alcaldía de Pamplona - Norte Santander.

- Realizar un proceso de análisis para encontrar vulnerabilidades que generen amenazas y pongan en riesgo los bienes que comprende el área de redes y sistemas de la Alcaldía de Pamplona - Norte Santander.

- Plantear un Sistema Gestión para tratar eficientemente las vulnerabilidades halladas en el área de redes y sistemas de la Alcaldía de Pamplona - Norte Santander para reducir las amenazas y mitigar los riesgos.

- Formular una política de seguridad informática para reducir los niveles de vulnerabilidad existentes en el área de redes y sistemas de la Alcaldía de Pamplona - Norte Santander.

4. MARCO DE REFERENCIA

4.1 ANTECEDENTES DE LA INVESTIGACIÓN

La alcaldía del municipio de Pamplona Norte de Santander ha ejercido sus funciones mediante procesos y herramientas informáticas tradicionales desde las cuales se ha generado información administrativa y financiera la cual se llevaba mediante medios impresos y en algunos casos en discos duros y medios portátiles; estos aspectos fueron necesarios para la administración y contabilidad en donde la información estática en libros y dispositivos de almacenamiento era analizada para llevar procesos sobre impuestos, usuarios de los entidades descentralizadas y otras como planeación, tránsito y transporte, instrumentos públicos, pero no se pensó en la seguridad y protección de los datos como un componente dentro de un plan de administración y gestión. Con la aparición del internet , la implementación de redes locales, el uso de dispositivos móviles, redes inalámbricas y el uso de servicios como el correo electrónico, redes sociales y en general la *Web* 2.0, la entidad visualizo formas más prácticas y útiles para las funciones del despacho, adquiriendo y reemplazando equipos informáticos con el fin de facilitar la tarea de la administración municipal, en los equipos se trabajan aspectos administrativos, financieros, bases de datos como también se navega en internet en diferentes sitios institucionales, gubernamentales, redes sociales y de uso común. En este sentido se han desarrollado varias investigaciones y proyectos en entidades de la misma índole mencionadas a continuación:

- Estrategia de Ciberseguridad para enfrentar ciberdelitos y amenazas contra el Distrito Capital.[4]Estrategia implementada para proteger la información de los sistemas del distrito y la Registraduría luego de acceso no permitidos registrados.

- Política de seguridad de la información para la alcaldía mayor de Tunja,[5] estrategia de preparación por parte del Gobierno para soportar al Sistema de Administración de Seguridad de la Información de Gobierno en Línea (SASIGEL) como modelo sostenible, y cubre desde la preparación de entidad para comenzar la implementación del Modelo, la definición de las brechas, la alineación y la implementación del SGSI como modelo sostenible.

- Política de Seguridad Informática, "Alcaldía la Tebaida Quindío", plan de mejora con el propósito de implementar u sistema de gestión para efectuar u tratamiento adecuado de los riesgos con un sistemas de controles definidos por una política de seguridad que compromete a todos los funcionarios.[6]

- Dentro de los planes de modernización de las entidades del estado se ha venido implementando profundos cambios en cuanto a la infraestructura tecnológica de las entidades con el fin de realizar una atención más oportuna y cercana al ciudadano, haciendo uso de la tecnologías de la información y la comunicación las cuales requieren estandarización y planes para su

[4] Secretaría General de la Alcaldía Mayor de Bogotá D.C. (2013). *http://www.alcaldiabogota.gov.co.* Recuperado el 29 de Septiembre de 2014, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51661

[5]Alcaldía Mayor de Tunja. (enero de 2013). *Tunja-Boyaca.gov.co.* Recuperado el 29 de Septiembre de 2014, de http://tunja-boyaca.gov.co/apc-aa-files/495052435f494e464f524d4547454c54/politica-seguridad-alctunja.pdf

[6]Alcaldia La Tebaida Quindio - Quindio. (2013). *http://alcaldia724.com.* Recuperado el 30 de sep de 2014, de http://alcaldia724.com/politicadeseguridadlatebaida.pdf

implementación, como ejemplo de este modelo este modelo se puede mencionar el proceso de modernización de la Alcaldía de Medellín.[7]

4.2 MARCO CONTEXTUAL

El municipio de Pamplona Norte de Santander fue fundado el 01 de noviembre de 1549 por Pedro de Ursúa y el capitán Ortún Velázquez de Velasco, ciudad Enmarcada Pamplona sobre la Cordillera Oriental. Los primeros alcaldes de Pamplona fueron Alonso de Escobar y Juan Vasques; y los primeros regidores Juan de Alvear, Andrés de Acevedo, Hernando de Mescua, Juan de Tolosa, Sancho de Villanueva, Juan Andrés, Juan Rodríguez Suárez, Pedro Alonso, Juan de Torres y Beltrán de Unsueta: "Genealogías de Ocáriz" .Desde allí partieron las expediciones que fundaron, entre otras, las poblaciones de Mérida, San Cristóbal y La Grita, en la hermana República Bolivariana de Venezuela, y Ocaña, Salazar de Las Palmas, Chinácota, San Faustino, Bucaramanga y San José de Cúcuta en Colombia. Pamplona ha sido desde su fundación cuna de importantes personalidades del arte y la cultura, reconocida por ser la “ciudad del saber” ya que alberga estudiantes de todo el país y de la hermana república de Venezuela.

4.2.1 Planeación y estructura estratégica.

4.2.1.1 Misión. Buscar el bienestar general y el mejoramiento de la calidad de vida de los pamploneses, prestando los servicios públicos determinados por la ley,

[7]MINTRABAJO. (11 de Septiembre de 2012). *Proceso de modernizacion de la Alcaldia de Medellin*. Recuperado el 29 de Octubre de 2014, de http://www.mintrabajo.gov.co/medios-septiembre-2012/1008-asi-sera-proceso-de-modernizacion-de-la-alcaldia-de-medellin.html

construir las obras que demande el progreso local, ordenar el desarrollo territorial, promover la participación comunitaria, el mejoramiento cultural y social de sus habitantes, articulando los sectores productivos, económicos, sociales, políticos, culturales y ambientales.

4.2.1.2 Visión. En el año 2049 Pamplona será un municipio competitivo, planificado a partir de sus potencialidades, territorialmente arraigado en la cultura, socialmente amigable, equitativo e incluyente, ambientalmente sostenible, seguro y en paz.

4.2.1.3 Funciones de la Alcaldía del Municipio. Son competencias del Despacho del Alcalde Municipal, además de las dispuestas por la Constitución y las Leyes; entre otras, las siguientes:

- Atender los servicios que demande el ejercicio de las funciones y atribuciones constitucionales legales.

- Las ordenanzas y los acuerdos municipales que corresponda cumplir de conformidad con el Artículo 315 de la Constitución Política de Colombia.

- Conservar el orden público en el Municipio, de conformidad con la Ley, las instrucciones y las órdenes impartidas por el Presidente de la República y el Gobernador del Departamento Norte de Santander.

- Fijar políticas, dirigir, orientar, proponer los Acuerdos ante el Concejo en cuanto a la formulación de los planes, programas, presupuestos y demás iniciativas ejecutivas necesarias para la buena marcha del municipio,

asegurando que éstos contengan las reales demandas y ofertas de la población a través de la efectiva participación ciudadana, comunal y comunitaria; sancionar, promulgar y reglamentar los actos administrativos que de éstos se deriven y sean considerados convenientes y con sujeción a las normas, reglamentos y actos de delegación que le sean atribuidos expresamente.

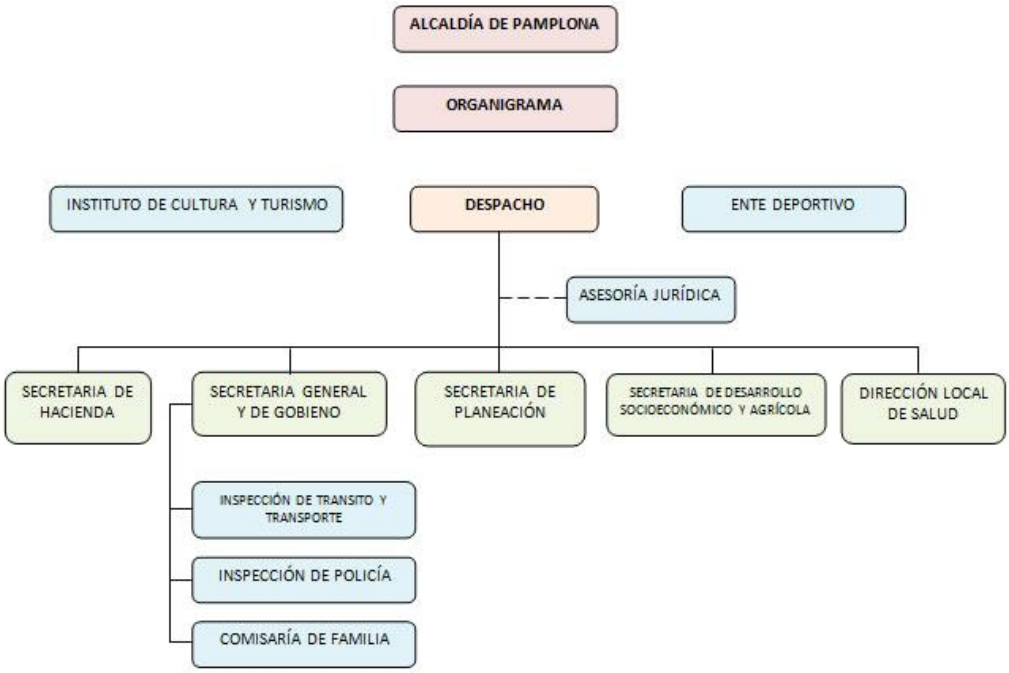
Dirigir, presidir, coordinar, articular y controlar la acción y gestión administrativa del municipio, apoyando y velando por el cumplimiento de la misión, objetivos, planes, programas y proyectos de cada una de las dependencias que conforman la administración central, asegurando el cumplimiento de las funciones y la presentación de los servicios municipales.

Fortalecer la organización administrativa, adecuándola oportunamente a las necesidades del servicio y a sus realidades socioeconómicas y tecnológicas.

4.2.1.4 Objetivos de la Alcaldía de Pamplona. Planear, programar, proyectar, coordinar y ejecutar acciones tendientes al desarrollo municipal y subregional, que permitan canalizar el apoyo interinstitucional y la eficiente y eficaz ejecución de los recursos.

4.2.1.5 Organigrama de la Alcaldía de Pamplona. La administración municipal cuenta con una estructura establecida de acuerdo a los lineamientos de la administración pública y debe contar con todos los órganos administrativos y de control, en la figura 1 se detalla el organigrama de la entidad.

Figura 1. Organigrama



Fuente: Documento oficina del despacho de la alcaldía**.**

4.3 MARCO TEÓRICO

4.3.1 Avance y evolución tecnológica. Desde los inicios de las generaciones de los computadores, que son el inicio de los desarrollos tecnológicos aplicados al manejo de información, se han producido inventos y aplicaciones sorprendentes cada día a tal punto que se sigue cumpliendo con la ley de Moore (La ley de Moore fue planteada en los años 50 y decía que: "Aproximadamente cada 18 meses la tecnología se duplica") también se puede plantear en términos electrónicos en los cuales se deduce que cada 18 meses la velocidad de los microprocesadores se duplica y el costo disminuye en la misma proporción.[8] La

[8] LEER, A. (2001). *Visión de los Lideres en la Era Digital.* Mexico: Mexico.

informática llego a las organizaciones y entidades, realizando funciones no solo para tareas ofimáticas, sino también de herramientas para almacenar datos, calcular costos, gestionar documentos, llevar control de la organización, etcétera. Logrando integrar todos los procesos que constituyen un sistema posible acorde a la realidad, con todos los datos e información actualizada. Proteger el sistema informático es una tarea que conlleva métodos y estrategias y herramientas con el fin de detener todas las amenazas potenciales para la organización.[9]

4.3.2 Seguridad Informática. Comprende las características, condiciones y parámetros de los sistemas de procesamiento de información para su almacenamiento administración y gestión, garantizando su confidencialidad, integridad y disponibilidad. Considerar las características de seguridad informática significa conocer el peligro, clasificarlo y protegerse de los ataques y daños de la mejor forma posible. Esto quiere decir que solamente cuando se conocen las potenciales amenazas, agresores y sus diferentes intenciones dañinas que pueden ser directas o indirectas en contra de un sistema o una organización, se puede adoptar las medidas de protección adecuadas, para que no se vulneren los recursos de información valiosos. En otros conceptos Representa el conjunto de medios y técnicas implementados para asegurar la integridad y que no se difundan involuntariamente los datos que recorren el sistema de información.[10] En un sentido contextual, la Seguridad Informática surgió para la protección de la información, en contra de amenazas y peligros, para evitar ataques y minimizar riesgos. La historia de la protección de la información y de los datos, hasta los últimos avances y desarrollos tecnológicos se evidencian tendencias en la protección con herramientas como: *Firewall*s,

[9] ROYER, J.-M. (2004). *Seguridad en la informatica de empresa.* Barcelona: Ediciones ENI.
[10] RAULT, A. -M.-S.-N.-R.-F.-J.-S.-D.-R. (2010). *Seguridad Informatica - Ethcal Hacking.* Ediciones ENI.

filtros, antivirus, sistemas de cifrado para los datos que son almacenados o se transmiten.

4.3.3 Pilares de la seguridad Informática. Se busca proteger en la información, son los cuatro pilares importantes que conlleva a que la información sea resguardada a gran escala. A continuación se especifican en su orden:

4.3.3.1 Confidencialidad. La información sólo puede y debe ser accedida, utilizada y gestionada por el personal de la empresa que ha obtenido la autorización para hacerlo. Se considera que este tipo de información no debe ser revelada a personal ajeno, ni debe ser pública, por lo tanto debe ser protegida por su razón de ser y sus características.

4.3.3.2 Integridad. Se refiere al momento en que la información de ninguna forma ha sido borrada, copiada o modificada, es decir, cuando se conserva tal como fue creada o enviada desde cualquier medio desde su origen hacia su destino. Un ataque a la integridad de la información se puede presentar en archivos planos de bases de datos, información documental, registros de datos, etc.

4.3.3.3 Disponibilidad. Tiene que ver con que la información facilitada en cualquier medio digital o *software* se encuentre a disposición de un usuario autorizado para el procesamiento de los datos, para el correcto funcionamiento de una organización, así como de sus clientes o personal requerido sin que estos sean afectados.

4.3.3.4 Autenticidad. Este pilar se define aquella información legítima, que al ser interceptada, puede ser copiada de su formato original a pesar de que la información sea idéntica.[11]

4.3.4 Normativas de Seguridad. Existen cantidades diferentes normas de seguridad que las empresas actualmente implementan para la seguridad de la información. Todas estas normativas persiguen los mismos objetivos, ya que están diseñadas para incluir a todas las unidades o departamentos que estructura a la empresa para obtener una seguridad mínima de la información procesada y transferida por el personal que hace parte de ella. Las normativas de seguridad, tienen la finalidad de presentar los lineamientos necesarios para que las empresas puedan implantar un sistema de gestión de la seguridad de la información.

4.3.5 Sistema de Gestión de la Seguridad de la información. Este sistema encierra todo lo pertinente al conjunto de normas, controles y políticas que conforman el contexto de la administración y gestión de la información dentro de un marco donde se construyen normas como la ISO/IEC 27001 y 27002 entre otras**.** Las normas que componen el Sistema Gestión Seguridad de la Información se basan en, normas que incluyen las buenas prácticas para la seguridad de la información, en las cuales se encuentran los códigos de las buenas prácticas que guían a las empresas para que las utilicen para mejorar la seguridad de su información incluyendo normativas que involucran las especificaciones del Sistema de Gestión de la Seguridad de la Información, que sería la documentación que deben tener las empresas que pretendan certificarse.[12]

[11] SIERRA, L. P. (2013). *Sistema de Gestion de la Seguridad de la Informacion.* Bogota: UNAD.
[12] UNAD. (Julio de 2013). *datateca.unad.edu.co/contenidos/modulo-SGSI-233003_listo.pdf.* Recuperado el 29 de Octubre de 2014, de http://datateca.unad.edu.co/contenidos/233003/

La norma ISO 27000 internacional está diseñada y emitida por la Organización Internacional de Normalización y describe cómo gestionar la seguridad de la información en una organización. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el saber y proporciona una metodología para implementar la gestión de la seguridad de la información en cualquier organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.[13]

La norma ISO 27002 fue publicada originalmente como un cambio de nombre de la norma ISO 17799 vigente, es un manual de prácticas para la seguridad de la información. Describe los controles y mecanismos, que pueden ser implementados, en base a la orientación proporcionada en la norma ISO 27001. Los controles que figuran en esta norma están destinados a suplir las necesidades específicas identificadas a través de una evaluación formal de riesgos. La norma también tiene por objeto proporcionar una guía para el desarrollo de "normas de seguridad de la organización y las prácticas eficaces de gestión de la seguridad y para ayudar a construir la confianza en las actividades inter-organizacionales". En 2013 se publicó la versión actual. ISO 27002: 2013 contiene 114 controles, en comparación con el 133 documentado dentro de la versión 2005.[14]

[13] Leal, R. (Enero de 2014). *Qué es norma ISO 27001.* Recuperado el 29 de Octubre de 2014, de Qué es norma ISO 27001: http://www.iso27001standard.com/es/acerca-de/

[14] ISO 27000 Directory 2013. (2013). *The ISO 27000 Directory*. Recuperado el 29 de Octubre de 2014, de The ISO 27000 Directory: http://www.27000.org/iso-27002.htm

La norma ISO 27003: Guía de implantación de un Sistema de Gestión de la Seguridad de la Información publicado el 1 de Febrero de 2010. Esta norma no se certifica, es una guía que contiene todos los aspectos necesarios para el diseño e implementación con la norma certificable ISO/IEC 27001:2005.

4.3.6 Buenas prácticas en Seguridad Informática. Teniendo en cuenta la definición que dá acerca de las Buenas prácticas el European Microfinance network: Las buenas prácticas comprenden las estrategias, formas, tácticas, procesos, pruebas, metodologías, actividades y enfoques que se documentan, y están accesibles, son eficaces, pertinentes y aceptados, desarrollados por organizaciones y profesionales idóneos e implementados por un personal eficientemente preparado.[15]Entre las buenas prácticas de seguridad informática se describen:

- Configurar el sistema operativo con todas sus normas de seguridad.
- Mantener actualizado el sistema operativo y las aplicaciones.
- Protección en el correo electrónico, configuración de protección antispam.
- Conocimiento y protocolos para ingresar a aplicaciones externas que puedan ser objeto de Pishing.
- Seguridad en la navegación, configuración de *Firewall*, proxys, tiempos de navegación, bloqueo a ciertas aplicaciones que se consideren riesgosas.

[15] BORBÓN Sanabria, J. (2011). Buenas prácticas, estándares y normas. *REVISTA .SEGURIDAD, DEFENSA DIGITAL*, http://revista.seguridad.unam.mx/numero-11/buenas-pr%C3%A1cticas-est%C3%A1ndares-y-normas.

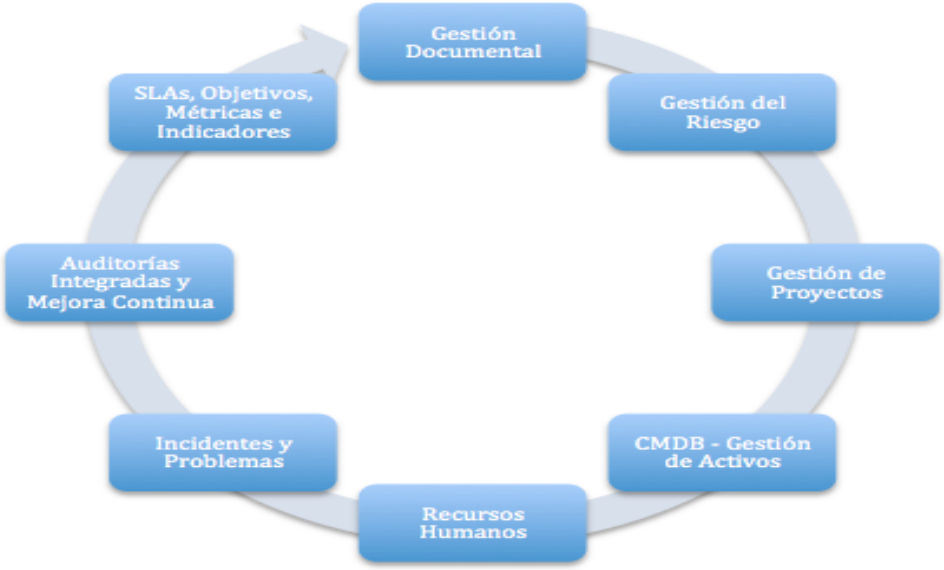
- Configuración de dispositivos de red sin dejar configuraciones por defecto.

- Protección física de los equipos de acuerdo a las políticas de seguridad.

4.3.7 Plan de gestión de un Sistema de Gestión de la Seguridad de la Información. La ISO 27001, manifiesta que un Sistema de Gestión de la Seguridad de la información, comprende un sistema de gestión que contempla básicamente la política, y la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implementar la gestión de la seguridad de la información. Este sistema es la herramienta que sirve a la Dirección de las organizaciones establecer las políticas y los objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidades, autenticación, etc.). La figura 2[16] muestra el ciclo de implementación que sigue el Sistema de Gestión de la Seguridad de la Información mediante la norma ISO 27001; Como se observa el ciclo comprende una serie de procesos enfocados en alcanzar ciertos objetivos parciales para avanzar al siguiente proceso que contempla cumplir el ciclo y alcanzar el equilibrio diseñando también planes de sostenibilidad.

[16] GESICONSULTOR. (2015). *Sistema de Gestión de la Seguridad de la Información*.

Figura 2. ISO 27001 SGSI



Fuente: GESlCONSULTOR. (2015). *Sistema de Gestión de la Seguridad de la Información*.

4.4 MARCO CONCEPTUAL

En esta sección se realiza la conceptualización de la terminología, procesos, procedimientos, programas, amenazas, vulnerabilidades, estados y técnicas utilizadas para documentar el proyecto.

4.4.1 Análisis de riesgos. El proceso de análisis y gestión de riesgos es una de los elementos más importantes constituidos dentro del Sistema de Gestión de la Seguridad de la información por cuanto este análisis constituye una metodología para obtener la información sobre las vulnerabilidades, amenazas y los riesgos que forman el conjuntos de elementos que crean el campo de falencias de la seguridad de la informática y la formación, haciendo evidentes la necesidades de

tomar decisiones y medidas con el fin evitar desastres en la información. La Organización Internacional define riesgo tecnológico como “La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole pérdidas o daños”. Es una herramienta para el diagnóstico que permite establecer los riesgos en una organización. Este análisis tiene como objetivos la identificación de los riesgos (mediante la identificación de sus elementos), lograr establecer el riesgo total y las implicaciones a que conduzca.[17]

4.4.1.1 Probabilidad. Para determinar la probabilidad de ocurrencia es posible de la forma cualitativa o cuantitativamente, considerando que la medida no debe contemplar la existencia de acciones de control.

4.4.1.2 Amenazas. Son acciones que pueden generar consecuencias negativas en la operación de la organización. Se referencian como amenazas a las fallas, los ingresos no autorizados, los virus, los desastres ocasionados por fenómenos naturales o ambientales, etc.

4.4.1.3 Vulnerabilidades. Son ciertas condiciones a las que se exponen los activos, están presentes en su entorno, facilitan que las amenazas se materialicen y se conviertan en vulnerabilidad.

[17] Universidad nacional abierta y a distancia, Mirian del Carmen Benavides, Francisco Solarte. (2012). *Módulo riesgos y control informático.* Bogota: Datateca UNAD.

4.4.1.4 Activos. Los activos en tecnología, es todos lo relacionado con los sistemas de información, las redes las, comunicaciones y la información en sí misma.

4.4.1.5 Impactos. Son las consecuencias de la materialización de las distintas amenazas y los daños que éstas puedan causar. Las pérdidas generadas pueden ser financieras, tecnológicas, físicas, entre otras.

4.4.2 Diagnostico e identificación de los riesgos. Este proceso surge de la utilización de las herramientas o las metodologías apropiadas en las cuales se pueden encontrar la forma metódica para efectuar el análisis en base a la organización en la que se pretenda análisis en este sentido se tienen en cuenta tres variables fundamentales sobre las cuales se basa la operación de análisis: activos, las amenazas y las vulnerabilidades son el objeto para identificar los riesgos, dado que una brecha no detectada permite la entrada al sistema de posibles amenazas .[18]En la figura 3, se ilustra el proceso a seguir en la gestión de riesgos.

- El hallazgo del peligro consiste en especificar el acontecimiento adverso que genera motivo de preocupación.

- Para la evaluación del riesgo hay que tener en cuenta la probabilidad (real y no sólo la posibilidad) de que se genere el peligro, las consecuencias si se materializa y el grado de incertidumbre

[18] GOMEZ, R. D. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de Ingeniería*.

- La gestión del riesgo consiste en la definición y aplicación del mejor control para reducir o eliminar la probabilidad de que se genere el peligro.

- La comunicación del riesgo es el intercambio franco de información y asesorías aclaratorias que generan una mejor comprensión y adopción de medidas.[19]

Figura 3. Gestión de Riesgos

Fuente: ISO27000.es. (2005). *El portal de ISO 27001 en Español*.

4.4.3 Análisis de vulnerabilidades. El análisis de vulnerabilidades se complementa el proceso de análisis de riesgo, es una actividad fundamental con el fin de orientarnos hacia un sistema de gestión de la seguridad de la información**.** Una vulnerabilidad, se puede definir como un estado de un sistema que puede:

- Permitir a un atacante acceder a información confidencial.

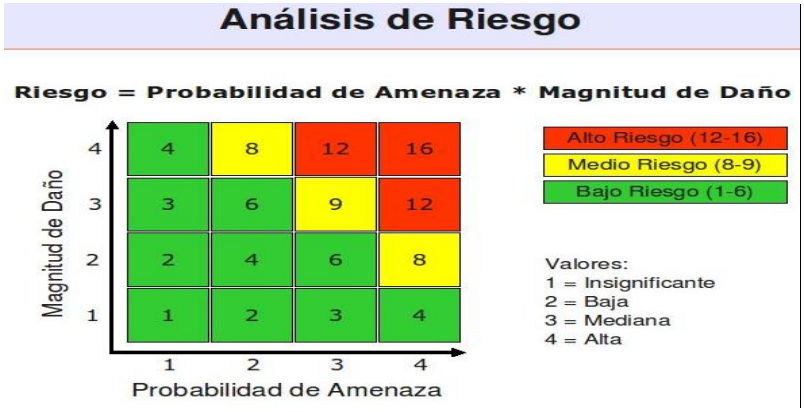
- Permitir a un atacante modificar información.

[19] ISO27000.es. (2005). *El portal de ISO 27001 en Español*.

- Permitir a un atacante negar un servicio.

4.4.4 Matriz para el análisis de riesgo. La Probabilidad de Amenaza y Magnitud de Daño pueden tomar los valores y condiciones respectivamente, por lo tanto la valoración de los riesgos se realiza teniendo en cuenta los siguientes valores, los cuales se distribuyen en la matriz de análisis de riesgo en la figura 4.[20]

Figura 4. Matriz de análisis de riesgo



Fuente: ERB, M. (2008). *Gestión de Riesgo en la Seguridad Informática*.

El Riesgo, que es el producto de la multiplicación Probabilidad de Amenaza por Magnitud de daño, está agrupado en tres rangos, contemplando la siguiente escala de valores:

- Bajo Riesgo = 1 – 6 (verde)

[20] ERB, M. (2008). *Gestión de Riesgo en la Seguridad Informática*.

- Medio Riesgo = 8 – 9 (amarillo)

- Alto Riesgo = 12 – 16 (rojo)

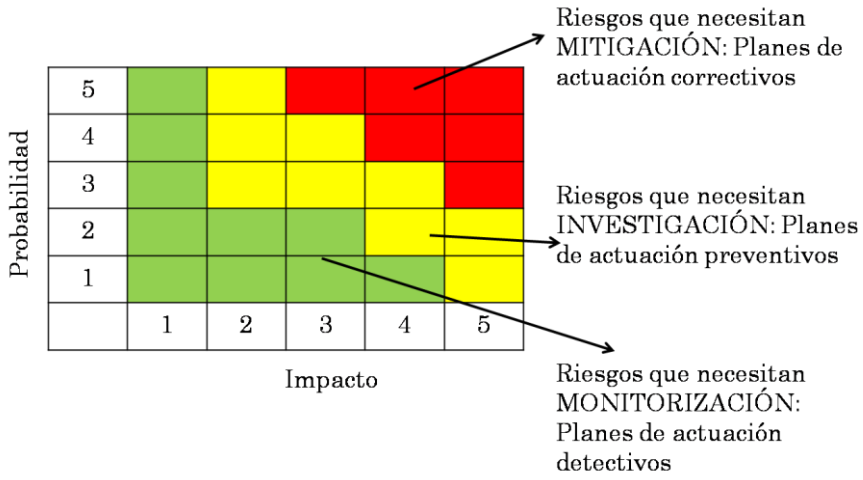
Valor total (Riesgo) = Probabilidad de Amenaza X Magnitud de Daño o
RT (riesgo total) = probabilidad x impacto.

Para calcular el riesgo es preciso identificar primero la magnitud del daño de cada uno de los elementos de información y también se debe identificar las probabilidades que ocurran las amenazas, basta con multiplicar de manera individual cada probabilidad con su respectiva magnitud de daño; de esta forma se identifica el índice de riesgo que se obtiene en la escala de 1-16 de acuerdo a lo mencionado anteriormente; es importante saber la probabilidad que tiene cada recurso de ser vulnerable porque no todos poseen la misma ya que dependiendo de la función y el entorno de los recursos que sirven a la información, algunos se encuentran más expuestos a ser vulnerables por la importancia en el proceso de gestión de la información por tal motivo necesitan mayor protección.

En la figura 5 se distribuye por colores los valores para su interpretación mediante la matriz.[21]

[21] ARJONA, K. (4 de Febrero de 2014). *Actuar sobre los riesgos*.

Figura 5. Interpretación de los valores



Fuente: ARJONA, K. (4 de Febrero de 2014). *Actuar sobre los riesgos*.

4.4.5 Amenazas a la seguridad con posibilidad de ser explotadas. Cuando existen vulnerabilidades en cualquier sistema informático esta constituye la posibilidad de que una amenaza la detecte la explote y genere un riesgo para la información y los demás bienes de una organización.

4.4.5.1 Códigos maliciosos. Los códigos maliciosos, o *malware*, están entre las principales amenazas de seguridad para cualquier entidad u Organización. Esta amenaza la conforman programas que causan algún daño o anomalía en el sistema informático. Dentro de esta categoría se incluyen los programas troyanos, gusanos, virus informáticos, spyware, Backdoor, rootkits, keyloggers, etc. En la actualidad, en promedio el 80% de los ataques informáticos son llevados a cabo mediante códigos maliciosos, programas troyanos estos pueden ser cualquier tipo, desde instrucciones diseñadas para destruir algún sector del disco duro, por lo general la MBR, eliminar archivos, registrar las pulsaciones del teclado, monitorear el tráfico de la red, etc.

4.4.5.2 Factor Insiders. Varios estudios han evidenciado que la mayoría de las violaciones de seguridad son cometidos por el factor humano de una empresa, es decir, por los mismos empleados desde dentro de la Institución u Organización. Una de las formas más eficaces que posee un atacante para romper los esquemas de seguridad, es desde el interior de la organización.

4.4.5.3 Ingeniería Social. Es una técnica de ataque que se basa en el engaño y que está orientada a explotar las debilidades del factor humano. Es una metodología que usan los atacantes para utilizar el factor Humano como herramienta de penetración a un sistema. Si bien esta técnica es utilizada en cualquier ámbito, en lo que a informática se refiere, consiste en la obtención de información sensible y/o confidencial de un usuario cercano a un sistema u organización explotando ciertas características que son propias del ser humano.[22]

4.4.6 Programas y procedimientos para Ethical Hacking y Pentesting. Son programas especializados para realizar las pruebas pertinentes para la búsqueda de vulnerabilidades.

4.4.6.1 Network Scanner*:* Multiescáner IPv4 / IPv6 con una interfaz moderna y muchas características avanzadas. Está dirigido a administradores de sistemas y usuarios en general interesados en la seguridad informática. Las computadoras pings programa, exploraciones para escuchar puertos TCP / UDP y descubre las carpetas compartidas, incluyendo el sistema y las ocultas. Además, se puede recuperar prácticamente cualquier información sobre los equipos de la red a través de WMI, SNMP, HTTP, *NetBIOS* y un montón de otras características. También

[22] SECURITY, e. (2010). *Debilidades de seguridad comúnmente explotadas.* Obtenido de https://www.evilfingers.com/

puede resolver nombres de host y detectar automáticamente el rango de direcciones IP local y externa. Para ayudar con la administración de la red, es compatible con el apagado remoto y Wake-On-LAN. Características principales:

- Pings ordenadores y pantallas los vivos.
- Totalmente compatible con IPv4 e IPv6 descubrimiento.
- Detecta *hardware* direcciones MAC, incluso a través de Routers.
- Detecta los directorios compartidos ocultos y los de escritura.
- Detecta las direcciones IP internas y externas.
- Exploraciones para escuchar los puertos TCP, algunos servicios UDP y SNMP.
- Recupera que ha iniciado sesión en usuarios, cuentas de usuario configuradas, el tiempo de actividad, etc.
- Monta y explora los recursos de red.
- Lanza aplicaciones externas de terceros.
- Exportaciones resultados a HTML, XML, CSV y TXT.
- Soporta Wake-On-LAN, apagado remoto y mensajes de la red de origen.
- Recupera cualquier información del sistema a través de WMI, registro remoto, sistema de archivos y gestor de servicios. Se puede obtener o descargar en:

https://www.softperfect.com/products/*Network Scanner*/ en la figura 6 se ilustra el logo de *Network Scanner* y las características acerca del programa.[23]

Figura 6. Network Scanner

Fuente: SOFTPERFECT. (16 de Marzo de 2015). *SoftPerfect Network Scanner* .

Los principales puertos usados en los equipos de uso común, son objeto de estudio porque constituyen en centro de análisis de la vulnerabilidades de entrada a un sistema mediante medios lógicos, siendo puertas para que las amenazas desplieguen sus ataques que tiene la posibilidad de poner en riesgo todo un sistema.

[23] SOFTPERFECT. (16 de Marzo de 2015). *SoftPerfect Network Scanner*.

Tabla 1. Listado de puertos analizados

Puerto	Protocolo	Descripción
11	sysstat	Es un servicio Unix que realiza un listado de todos los procesos que se generan en la máquina. Esto le proporciona al usuario, una gran cantidad de información con la que consigue conocer las vulnerabilidades de los programas que están instalados en la máquina o las cuentas del usuario.
13	daytime	Es un servicio que proporciona la fecha y hora del sistema.
15	netstat	Muestra las conexiones de TCP activas, los puertos en que el equipo escucha, las estadísticas de Ethernet, la tabla de enrutamiento IP, las estadísticas de IPv4 (para los protocolos IP, ICMP, TCP y UDP) y las estadísticas de IPv6 (para los protocolos IPv6, ICMPv6, TCP sobre IPv6 y UDP sobre IPv6).
21	FTP,	El ataque más común que realizan los hackers y crackers, que buscan servidores de FTP anónimos. Estos suelen ser servidores que disponen de directorios con permisos de escritura y lectura.
22	ssh	Está usado por PC Anywere. Hay veces que puede ser escaneado por gente que emplea esta herramienta y no sabe que está escaseando los puertos.
23	telnet	El intruso busca un login remoto. La mayoría de las veces de escaneo de intrusos desde este puerto, es para averiguar el sistema operativo que emplea el usuario.
25	smtp	Simple Mail Transfer Protocol, es el protocolo de salida del correo.
42	name	Con este servicio se consigue el nombre del servidor.
43	nicname	Who is. Con este servicio se obtiene la información sobre la red o el usuario.
49	tacasc	Login Host Protocol. Con este servicio se obtiene el protocolo de login del host.
53	DNS	Este servicio nos dice el nombre de la máquina remota. Los usuarios intentan acceder a zonas de transferencia (TCP) para engañar DNS (UDP) o incluso para ocultar el tráfico que desde el 53 no es reconocido por los Cortafuegos.
63	who is ++	Este servicio nos dice el nombre de propietario de dominio de segundo nivel.

Tabla 1. (Continuación)

Puerto	Protocolo	Descripción
69	TFTP	Algunos servidores soportan este protocolo en conjunto con BOOTP, con la intención de descargar código del sistema.
70	gopher	Buscador de información.
79	finger	Los usuarios le emplean para averiguar información del usuario, conseguir información impresa en pantalla o colgar el sistema.
80	http	Servidor *Web* con el que se puede acceder a páginas *Web*. Con este abierto, el usuario se puede conectar con programas de chat como el Messenger.
88	kerberos	Es un método seguro de autenticación de respuesta. Siempre que se requiera acceder a otro ordenador se necesita una respuesta de autenticación del servidor (AS).
107	rtelnet	Telnet remoto, es decir, con un telnet se accede a otra computadora a la que se supone hay un permiso.
109	pop2	Post Office Protocol, versión 2. Servidor de correo electrónico entrante.
110	pop3	Post Office Protocol, versión 3. Servidor de correo electrónico entrante. Un punto de presencia (pop) es un punto de acceso de Internet.
115	sftp	Simple File Transfer Protocol.
119	nntp	Este servicio proporciona grupos de noticias usenet.
133	statsrv	Servicio de estadísticas.
137	NetBIOS-ns	*NETBIOS* Name Service (*Windows*) *NetBIOS* es un programa que permite a las aplicaciones de diferentes ordenadores comunicarse sin una conexión de área local (LAN).
138	NetBIOS-dg	*NETBIOS* Datagram Service (*Windows*).
139	netvios-ssn	*NETBIOS* Session Service (*Windows*).
143	imap	Servicio de protocolo de mensajes de acceso de Internet (Internet Message Access Protocol).
161	snmp	Simple Network Management Protocolo (SNMP), es el protocolo de gestión de dispositivos de red y sus funciones.

Tabla 1. (Continuación)

Puerto	Protocolo	Descripción
194	Irc	Protocolo de Chat. Internet Relay Chat (IRC), es un sistema de comunicación instantánea que está envuelto en una serie de reglas cliente-servidor.
220	imap 3	Es un protocolo estándar cliente-servidor con el que puede acceder a nuestro correo desde el servidor local.
443	shttp	Servidor *Web* seguro.
513	login	Servicio que crea un login remoto al Telnet.
514	syslog	Syslog. Una lista de todas las peticiones que el usuario ha solicitado en un sitio *Web*.
520	router	Protocolo de información de routing.
529	irc-serv	IRC, chats.
530	RPC	Remote Procedure Call (RPC), es un protocolo que un programa puede usar para solicitar un servicio de un programa que se encuentra en otro ordenador.
1352	lotus notes	Desde este servicio se accede al servidor de correo de Lotus Notes.
1433	ms-spl-s	Microsoft SQL – server.
1527	tlisrv	Utilizado para acceder a Oracle.
5631	Pcanywhere data	Solución de control remoto que permite a los administradores que se conecten de forma segura, configuren y solucionen problemas a través de cualquier tipo de conexión.

Fuente: MIT.EDU. (2014). *Puertos comunes*.

En la tabla 1 a través de un listado se describen los principales puertos que en condiciones de uso normal y con aplicaciones para usuarios comunes se despliegan en un equipo de cómputo.[24] Para complementar aún más acerca de los puertos atacados por los troyanos consultar el ANEXO B disponible en https://www.dropbox.com/s/twtpdodhrr6iegj/ANEXO%20B.pdf?dl=0

[24] MIT.EDU. (2014). *Puertos comunes*.

4.5 MARCO LEGAL

En el mundo y en Colombia país la creciente exponencial del uso de la tecnologías de la información y la comunicación han generado un desarrollo en base al uso de la tecnología que fomenta el desarrollo social y nos permite hacer parte de una sociedad globalizada en donde las fronteras no existen en las relaciones cibernéticas, en este sentido surgen muchos beneficios y oportunidades, sin embargo también constituye una problemática social que hace un daño con las magnitudes de los delitos tradicionales incluso en mayores proporciones, ante este panorama la legislación de nuestro país Colombia realizo las leyes pertinentes para mitigar y establecer un marco jurídico que castigue y regule los delitos derivados del uso de la información sus componentes y la actuación de los ciudadanos frente a esta, en este sentido existe la ley 1273 del año 2009

5. DISEÑO METODOLÓGICO

5.1 PLANIFICACIÓN DEL ANÁLISIS, EVALUACIÓN DE RIESGOS Y ASESORAMIENTO DE LA SEGURIDAD INFORMÁTICA EN EL ÁREA DE REDES Y SISTEMAS DE LA ALCALDÍA DE PAMPLONA - NORTE DE SANTANDER

El análisis de riesgos de la seguridad informática está enfocado para aplicar en el ente objeto del estudio un análisis de vulnerabilidades con el fin de interpretar, explicar y asesorar las causas que generan el problema y la necesidad de implementar controles en el área de redes y sistemas de la Alcaldía municipal de Pamplona - Norte Santander para mitigar las amenazas que genera la desatención al tema. El trabajo se realiza en las instalaciones de área de redes y sistemas de la Alcaldía municipal de Pamplona por ser la fuente de datos para ser analizados y evidenciar el entorno de afectación. El análisis se centra en encontrar la información sobre vulnerabilidades, amenazas y los riesgos que están presentes en los sistemas donde opera en el objeto de estudio, con el propósito de obtener las evidencias que muestren el panorama general de la seguridad informática en la alcaldía del municipio de Pamplona.

5.1.1 Alcance del Proyecto. La alcaldía municipal es una de las entidades de gobierno presentes en la ciudad de Pamplona y desde varios las distintas dependencias cambiaron la forma de llevar sus proceso por eso dentro del presupuesto del municipio se encuentran los rubros para el sostenimiento y soporte de infraestructura tecnológica entre estos la contratación de servicios de internet con el proveedor que opera en la ciudad.

La alcaldía dispone de una infraestructura tecnológica dividida en tres plantas desde donde operan las oficinas que sirven a la administración municipal, funcionan permanentemente entre 40 y 65 computadores haciendo uso de recursos, como el internet recursos compartidos, impresoras, programa ofimáticos y aplicaciones en línea. El municipio tiene contratados tres servicios de internet banda ancha de 8, 4 y 6 megas con los cuales se suplen la necesidad de conectividad hacia internet del usuario de la red. Conociendo esta información y la que arrojan los resultados de la investigación se busca llegar a las finalidades de la misma de una forma descriptiva de los proceso para llevar a cabo en análisis de riesgos, ya que los estudios causales se realizan a partir de las correlaciones en donde se evalúan los recursos, los servicios, los medios y usuarios. La configuración del sistema se analizará para buscar posibles vulnerabilidades que generen amenazas a la seguridad y así sugerir los controles específicos para llevar los riesgos a un nivel mínimo de afectación.

5.1.2 Métodos para la búsqueda de información. En este proceso de encontrar los datos suficientes para realizar el análisis de riesgos y cumplir los objetivos se implementaron técnicas comunes para este tipo de procesos.

5.1.2.1 Observación directa. Mediante esta técnica se lograra evidenciar diversas vulnerabilidades presentes en los medios tangibles que conforman los bienes informáticos de la entidad; se lleva un registro fotográfico.

5.1.2.2 Entrevista. A través de una serie de preguntas a los funcionarios usuarios de los servicios informáticos de la entidad se lograron distinguir vulnerabilidades presentes en la entidad.

5.1.2.3 Ethical Hacking y Pentesting (Pruebas de penetración) Mediante el uso de programas especializados se realizaron diversas pruebas con el propósito de encontrar vulnerabilidades y brechas de seguridad en los equipos y la red; estas pruebas fueron realizadas con consentimiento y teniendo en cuenta los artículos de la ley 1273 del 2009.

Con la utilización de las anteriores técnicas se ha logrado encontrar información suficiente para aplicar los procedimientos de análisis de riesgos mediante una matriz, para realizar su valoración en base a las vulnerabilidades y amenazas determinando la probabilidad del riesgo y el impacto y conocer su valor total, el cual se registra en una matriz representado en un valor cuantitativo que por la posición y el color de la jerarquía deduce un valor cualitativo generando un concepto, en base al valor obtenido por cada ítem estipulado de acuerdo al recurso informático y su función se clasifica el determinante del riesgo para plantear el control.

5.1.3 Población y Muestra. Para llevar a cabo la investigación se logró determinar la población de elementos que componen las redes y sistemas que conforman el entorno informático de la alcaldía del municipio de Pamplona. La población objeto de la investigación distingue: Población de equipos de cómputo, población de equipos de red, población de usuarios finales. En la población mencionada, se tomaron muestra de equipos de cómputo, muestra de equipos de red, muestra de usuarios finales. El conjunto de operaciones que se realizan para estudiar la distribución de la población en base a sus características se efectuarán mediante Muestreo Aleatorio Simple es decir todos los elementos tienen la misma probabilidad de ser seleccionados. En este sentido en cada dependencia de la alcaldía se seleccionó como elemento de la población de usuarios al auxiliar administrativo quien hace uso del sistema informático, a esta persona se aplicó

una entrevista mediante la lista de chequeo ilustrada en la tabla 2. Los resultados revelados se registraron análisis en la matriz de riesgos con el fin de terminar vulnerabilidades presentes en el factor humano.

Tabla 2. Lista de chequeo

Pruebas de Checklists al área de redes y sistemas de la Alcaldía de Pamplona – Norte de Santander para determinar los riesgos mediante la observación			
Pregunta	Si	No	N/A
1. ¿Se han adoptado medidas de seguridad en el área de redes y sistemas?			
2. ¿Existe una persona responsable de la seguridad para el área de redes y sistemas?			
3. ¿Existe personal de vigilancia en la entidad?			
4. ¿Existe una clara definición de funciones entre los puestos clave?			
5. ¿Existe vigilancia en la entidad las 24 horas?			
6. ¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?			
7. ¿Se registra el acceso al área de redes y sistemas de personas ajenas a la persona de soporte?			
8. ¿Se ha adiestrado el personal en el manejo de los extintores?			
9. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?			
10. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego?			
11. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?			
12. ¿Saben qué hacer en el área de redes y sistemas, en caso de que ocurra una emergencia ocasionado por fuego?			

Tabla 2. (Continuación)

Pruebas de Checklists al área de redes y sistemas de la Alcaldía de Pamplona – Norte de Santander para determinar los riesgos mediante la observación			
Pregunta	Si	No	N/A
13. ¿El personal ajeno a operación sabe qué hacer en el caso de una emergencia (incendio)?			
14. ¿Existen salidas de emergencia en la entidad?			
15. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?			
16. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?			
17. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior área de redes y sistemas para evitar daños al equipo?			
18. ¿Se limpia con frecuencia el polvo acumulado en los equipos?			
19. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?			
20. ¿Se tienen establecidos procedimientos de actualización a estas copias?			
21. ¿Existe departamento de auditoria interna en la institución?			
22. ¿Este departamento de auditoria interna conoce todos los aspectos de los sistemas?			
23. ¿Se cumplen?			
24. ¿Se auditan los sistemas en operación?			

Fuente: Autor

5.1.3.1 Diseño de la muestra. Mediante el esquema de muestreo aleatorio simple se determina el tamaño de la muestra donde.

- N = tamaño de la muestra

- p = población

- m = media de la población

- Formula: $n = {}^{p}/_{m}$

Se analizaran los entes individuales bajo los criterios para determinar las variables de estructura y configuración de sus sistemas informáticos y así de terminar, vulnerabilidades y estado del sistema ante un prospecto de seguridad informática. Este esquema se repite en cada muestra partiendo de patrones comunes.

Dentro de la población objeto de estudio se encuentra el recurso humano como variable en el proceso de manejo de la información y administración de los equipos. Las personas estudiadas se estipulan de acuerdo al rol que tengan frente a la parte informática de la entidad es decir determinar qué tipo de usuario es, con el fin de establecer los privilegios que tiene frente a la información. Como parte importante se evaluarán cada equipo de cómputo como ente fundamental del proceso informático y comunicacional, de igual forma se tomarán cada uno de los dispositivos finales de red. En cada equipo y dispositivo se analizará su configuración y las aplicaciones que tiene instaladas y la manera como se comunica con la red y hacia la WAN o red de área Mundial. Con este procedimiento a nivel individual se obtendrá una muestra de las posibles vulnerabilidades comunes en los demás equipos de la red.

Las Variables del proyecto definen las características que posee cada dispositivo tanto a nivel de *hardware* como de *software* como también los elementos de conectividad que componen la red.

En los equipos de cómputo se tienen en cuenta características de *hardware*, disco duro, memoria RAM, procesador y tarjetas de red. Respecto al *software* se consulta el sistema operativo, antivirus, aplicaciones que utilizan la red y *Firewall* configuración global. En los dispositivos de red se consultan los router, *switch* (Marca, modelo y configuración). Respecto al factor humano se indaga sobre las personas midiendo el nivel de conocimiento en el manejo y uso de los dispositivos computacionales tanto *hardware* como *software*.

5.1.4 Metodología para el análisis y evaluación de riesgos. Como se mencionó en el aporte teórico sobre el análisis de riesgos para obtener la información sobre las vulnerabilidades, amenazas y los riesgos que forman los conjuntos de elementos que crean el campo de falencias de la seguridad de la informática y la formación en área de redes y sistemas de la Alcaldía de Pamplona, se utilizó la matriz de riesgos.

5.1.4.1 Inventario de los Activos. En el inventario realizado a cada dependencia, se verificó mediante la observación cada uno de los equipos informáticos registrando sus características y afinidades con los recursos de red presentes.
El resultado total del inventario en mención de registran en el ANEXO A disponible en https://www.dropbox.com/s/xnsp7qv0xvv9kk3/ANEXO%20A.pdf?dl=0.

El inventario de la red informática se registró también de forma lógica en cuanto a los equipos de que se conectar a la red, los cuales se registraron mediante las herramientas escaneo *Network Scanner* y Nmap.

5.1.4.2 Valoración de los Activos. Para determinar el valor de cada activo y clasificarlos se tuvieron en cuenta los siguientes criterios estipulados en la Tabla 4. Valoración de activos en donde se verifica el ítem, el valor y la descripción.

Tabla 3. Valoración de activos

Ítem	Valor	Descripción
Mb: muy bajo	1	No es indispensable
B: bajo	2	Indispensable, alguna tarea.
M: medio	3	Importante para varias tareas
A: Alto	4	Muy importante,
Ma: muy alto	5	Su falta genera parálisis en la operación.

Fuente: Autor.

5.1.4.3 Análisis de vulnerabilidades a los sistemas operativos. En este apartado del trabajo se describen las pruebas de penetración (Pentesting), escaneo de la red, escaneo de puertos y pruebas de vulnerabilidades realizadas y en el área de redes y sistemas de la Alcaldía de Pamplona - Norte de Santander. Pruebas de penetración, escaneo de la red y de puertos (Ethical Hacking)todo el proceso se realiza teniendo en cuenta el marco legal que regula el uso de los sistemas informáticos, amparado en todos los artículos de la ley 1273 del 2009.

En la tabla 4 se realiza la descripción de los equipos a analizar, mostrando la cantidad y el tipo de máquina que se analiza, en este sentido analizar las máquinas representa un gran avance para encontrar las vulnerabilidades que están presentes en el sistema informático en donde se concentra la gestión de la entidad y por ende es uno de los recursos informáticos con mayores probabilidades de estar ante determinada amenaza.

Tabla 4. Activos Informáticos a analizar

Descripción		Sistema Operativo		
Equipo	Cantidad	*Windows* XP	*Windows* 7	*Windows* 8.1
Escritorio	41	16	25	0
Equipo Portatil	9	0	6	3
ALL IN ONE	13	0	9	4
Servidor	1	1	0	0
Router	4	N/A	N/A	N/A
Switch X 24	3	N/A	N/A	N/A
Gabinete de Pared	2	N/A	N/A	N/A
Modem ADSL	3	N/A	N/A	N/A
UPS	1	N/A	N/A	N/A

Fuente. Propia

Las Pruebas de *NetBIOS* se realizaron con la aplicación *Network Scanner,* dirigidas a la red de equipos informáticos de la Alcaldía de Pamplona Norte de Santander teniendo en cuenta el soporte jurídico de la legislación Colombia. Ley 1273 de 2009.

Para conocer al fondo el objetivo del escaneo es preciso saber el concepto de *NetBIOS* “Network Basic Input/output System sobre lo cual se puede decir que se dio inicio en 1984 con IBM, con colaboración con Microsoft, donde anunciaron el desarrollo del Network Basic Input/Output System (*NETBIOS*), un código catalizador inicio el desarrollo de redes de comunicación. *NetBIOS* sobre TCP/IP, se conoce también como NBT o NetBT, es el protocolo que ha sido utilizado por Microsoft para la transmisión de bloques de mensajes de servidores, o SMBs por

sus siglas en Ingles, y es esta instalado en todos los sistemas operativos *Windows*.[25]

Para los sistemas operativos *Windows NetBIOS* sobre TCP/IP se entiende como el componente de red que resuelve y asigna los nombres de equipo a dirección IP (NETBT.SYS en *Windows* NT, y VNBT.VXD en *Windows* para Trabajo en Grupo y *Windows* 95). Por lo general utiliza los puertos del 135 al 139 el servicio *NetBIOS* que se encarga de compartir ficheros del computador, en la red interna.[26]

Entre las Características de *NetBIOS* se conoce que provee los servicios de sesión mencionados en la capa número 5 del modelo OSI. Es un protocolo para compartir recursos en la red. Establecer la sesión y mantiene las conexiones. Sin embargo este protocolo debe transportarse en las máquinas mediante otros protocolos; debido a que el mismo no puede transportar los datos en redes LAN como WAN, en necesario usar otra forma de transporte.

El Ataque por *NetBIOS* en una vulnerabilidad presente en los sistemas de *Windows* ha sido objeto de estudio por cuanto constituye una falla de seguridad en proceso de compartir la información en una red de datos el ataque a *NetBIOS* es una de las formas de intrusión más conocidas, es necesario escanear segmentos de red con sus rango de IP's para encontrar muchos ordenadores que, por desconocimiento, descuido o falta de sensibilización tienen compartidas partes

[25] Blogs, T. (23 de Junio de 2009). *NetBIOS sobre TCP/IP y resolución de nombres cortos* . Obtenido de http://blogs.technet.com/b/latam/archive/2009/01/23/netbios-sobre-tcp-ip-y-resoluci-n-de-nombres-cortos.aspx

[26] MICROSOFT. (2014). *Resolución de nombres de NetBIOS sobre TCP/IP y WINS*. Obtenido de : https://support.microsoft.com/es-es/kb/119493/es

muy importantes de sus discos duros, ignorando que no son accesibles desde internet.[27]

El área de redes y sistemas se compone de varias subredes conectadas a internet mediante la tecnología ADSL (*Asimétrica Digital Subscriber Line*) utilizando un modem que conecta la red de área local con el ISP (*Internet Service Provider)*. Las redes LAN se concentran en el Rack principal ubicado en el primer piso del edificio; en el Rack se encuentran los dispositivos de red que conectan la red computadores hacia internet; la red cableada se distribuye desde el modem hacia los *switch* los cuales son tres dispositivos de 24 puertos que interconectan las diferentes dependencias de la entidad pública. Las pruebas realizadas a esta red tienen como fin investigar fallas de seguridad en cuanto al uso de los recursos compartidos es decir, encontrar en la red de datos, unidades de almacenamiento como discos duros y carpetas compartidas que estén en riesgo de ser objeto de intrusiones y posible robo, modificación y eliminación de información, teniendo en cuenta que los datos procesados en las diferentes dependencias dentro del proceso de gestión, generan información sensible la cual debe estar dentro de los parámetros de la confidencialidad, integridad y la disponibilidad.

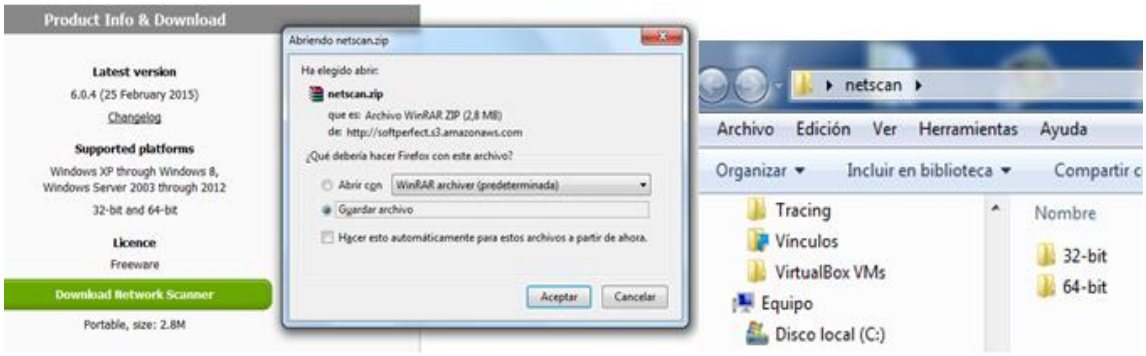
La práctica Implementación del escaneo a la red de datos pretende poner en evidencia los equipos con las unidades que se encuentren compartidas sin profundizar en la consulta de documentos que contengan.

[27] Sistemas, L. (12 de Marzo de 2014). *NetBIOS, Sistema de Entrada Salida Básica de Red* . Obtenido de http://www.investigacion.frc.utn.edu.ar/labsis/Publicaciones/InvesDes/Protocolos-NBI/doc/netbios.html

Para realizar las pruebas se utilizaron Herramientas de *Software* como Sistema operativo *Windows* XP y *Windows* 7 *ultímate*, máquina desde la cual se genera el escaneo a la red., con el programa *Network Scanner* se ejecutó el escaneo.

Respecto al *Hardware* se utilizó un Equipo portatil con elementos adicionales como cables de red UTP y tarjetas de red inalámbricas para establecer conexión con la red. Para el procedimiento de escaneo se realizó la descarga del *Network Scanner* de la página https://www.softperfect.com/products/*Network Scanner*/ como se ilustra en la figura 7.

Figura 7. Descarga Network Scanner

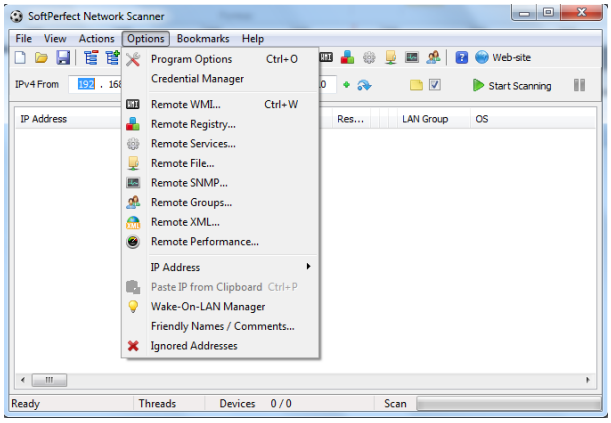


Fuente: Autor.

Se realiza la descarga se descomprime el archivo en una carpeta con el mismo nombre al abrir la carpeta nestcan se encuentran dos carpetas más que disponen la aplicación para sistemas operativos de 32 Bits o 64 Bits, en cada una se encuentra un archivo con el icono representativo en cual al ser ejecutado abre inmediatamente la interfaz de controles de la aplicación, esto quiere decir que la aplicación es portable, no necesita ser instalada en el sistema operativo

Para iniciar se abre la carpeta contenedora del archivo y Se ejecuta la aplicación, inmediatamente abre la interfaz inicial como lo muestra la Figura 8.

Figura 8. Interfaz Network Scanner

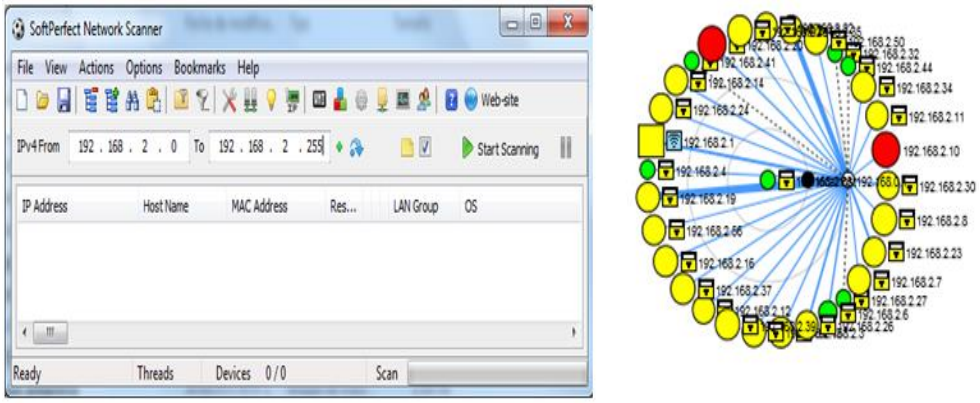


Fuente: Autor.

Se conecta el equipo con el cual se realiza el escaneo al *switch* de la red de datos, se utiliza un cable de conexión (patch cord) UTP, sigla que significa *Unshielded Twisted Pair* (Par trenzado no blindado) y se ejecutan los siguientes pasos:

- Obtener una dirección IP de la misma red a la cual se va a escanear.
- Verificar el rango de IPs de la subred a la que pertenece la máquina
- conectada, se deduce su tamaño y el segmento para indicar el rango en las casillas “IPv4 from” de la aplicación.
- Se configura el rango de IPs en las casillas correspondientes como lo indica la figura 9 en donde se aprecian los equipos conectados.

Figura 9. Red en Network Scanner

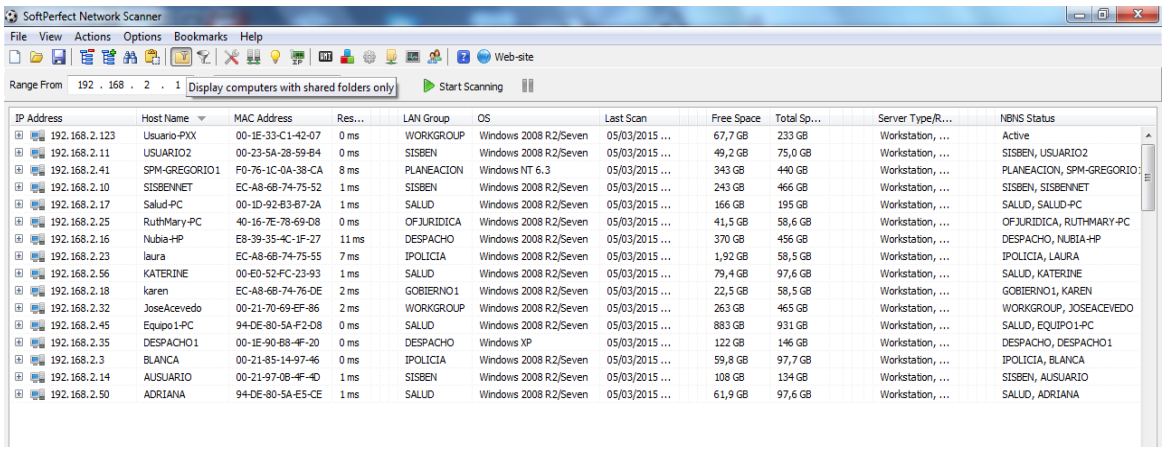


Fuente: Autor

- Se inicia el escáner de la red dando click en el botón Start Scanning y se obtienen los siguientes resultados con respecto al inventario de equipos de la red de datos.

- Se obtiene la lista de equipos escaneados como los deja ver la figura 10.

Figura 10. Equipos en Network Scanner



Fuente: Autor.

En la ventana de resultados se encuentra la lista de 16 equipos conectados sobre los cuales se obtiene la siguiente información de cada uno:

- Dirección Ip, nombre del equipo, dirección física o MAC, tiempo de respuesta, grupo de trabajo al que pertenece.

- Sistema operativo, espacio total y disponible de cada unidad de disco duro y estado de los puertos *NetBIOS*.

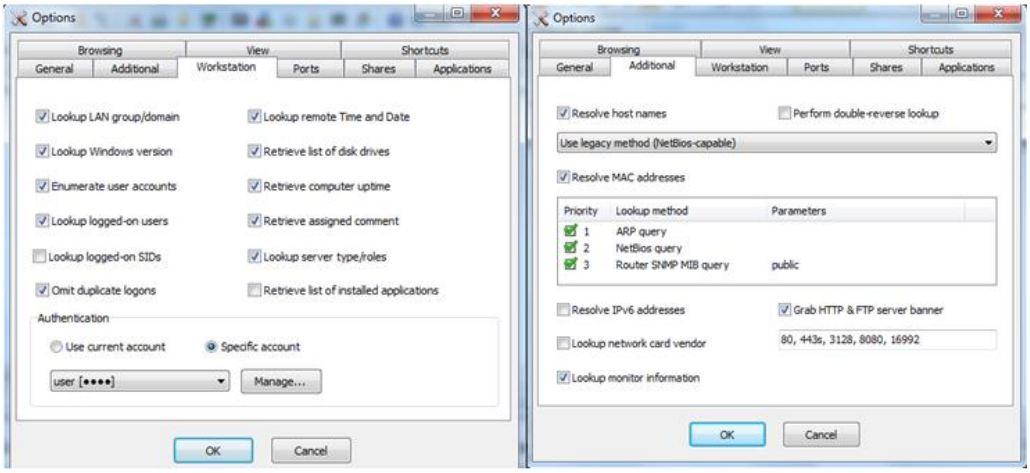
La información obtenida de cada equipo es posible configurarla mediante el menú *Options*, en donde se encuentran las pestañas de *Network Scanner* como se muestra en la figura 11:

- Pestaña *Workstation* mediante la cual se selecciona las características sobre las cuales se desea información del equipo escaneado.

- Pestaña *Additional* mediante la cual se selecciona la forma como la aplicación recupera parámetros y usa métodos para obtener información de los equipos escaneados.

- La configuración de los datos se realiza en base a una configuración personalizada con el propósito de obtener suficiente información de un equipo, esto quiere decir que de acuerdo a los datos que se necesiten se configura la búsqueda.

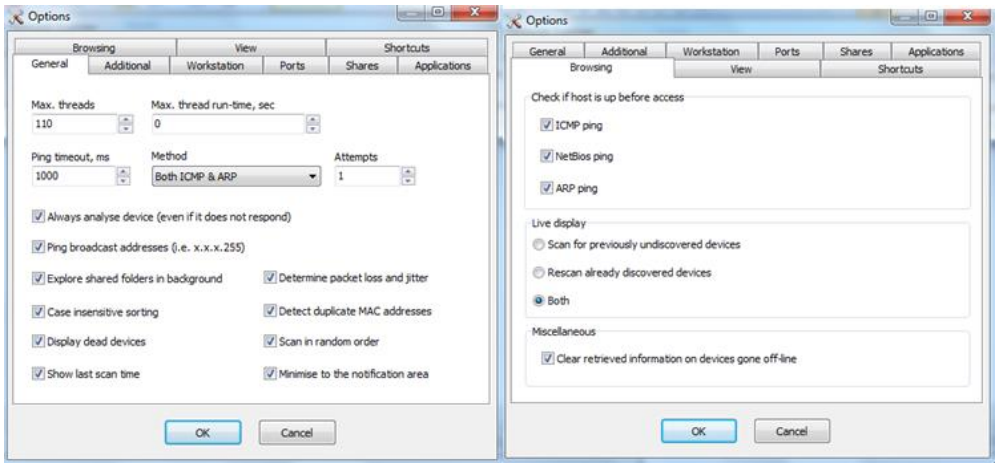
Figura 11. Pestañas Network Scanner



Fuente: Autor

Por medio de la pestaña General se indica la forma de realizar el escaneo configurando los parámetros con el fin de optimizar los resultados. Como se muestra en la figura 12 la pestaña Browsing se configura la búsqueda de los equipos en la red y el uso de los protocolos para ello.

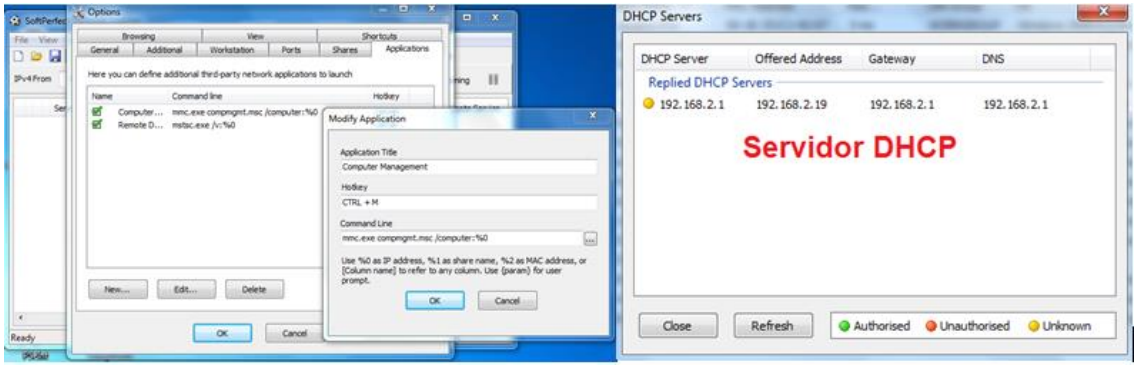
Figura 12. Pestañas2 Network Scanner



Fuente: Autor

La prueba se realiza utilizando las funciones básicas de la aplicación no se profundiza en el proceso de implementación de otras funcionalidades dado que esta acción puede afectar algunas acciones del uso compartido como por ejemplo es posible lanzar una aplicación desde la pestaña aplicaciones configurando o modificando los parámetros de la misma como se puede apreciar en la figura 13.

Figura 13. Funciones Network Scanner



Fuente: Autor.

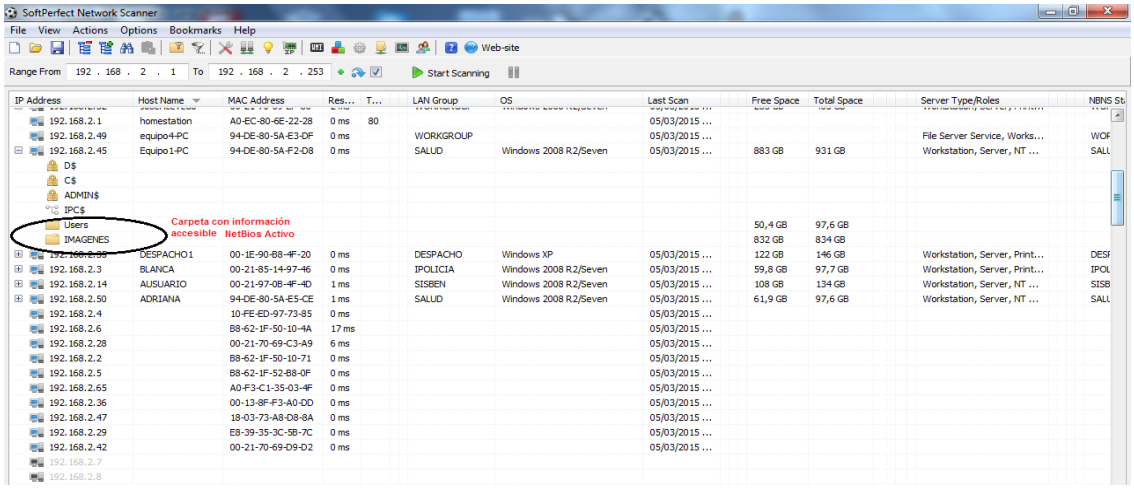
Como Resultados del proceso de escaneo en la red seleccionada se identifican los servidores DHCP (protocolo de configuración dinámica de host) se registran dos servidores (192.168.2.1 y 192.168.2.19) se deduce que además del modem ADSL el cual se verifica visualmente ingresando a la ventana de configuración del mismo como se ilustra en la figura 14, el otro servidor se determina como un router ubicado en la segunda planta del edificio para ampliar el espectro de la red inalámbrica.

Figura 14. Interfaz Modem ADSL

Fuente: Autor.

EL resultado del análisis y despliegue de cada equipo analizado se muestra y evidencia que en la red hay equipos que tienen carpetas compartidas lo cual evidencia en la figura 15.

Figura 15. Resultado Escaneo NS

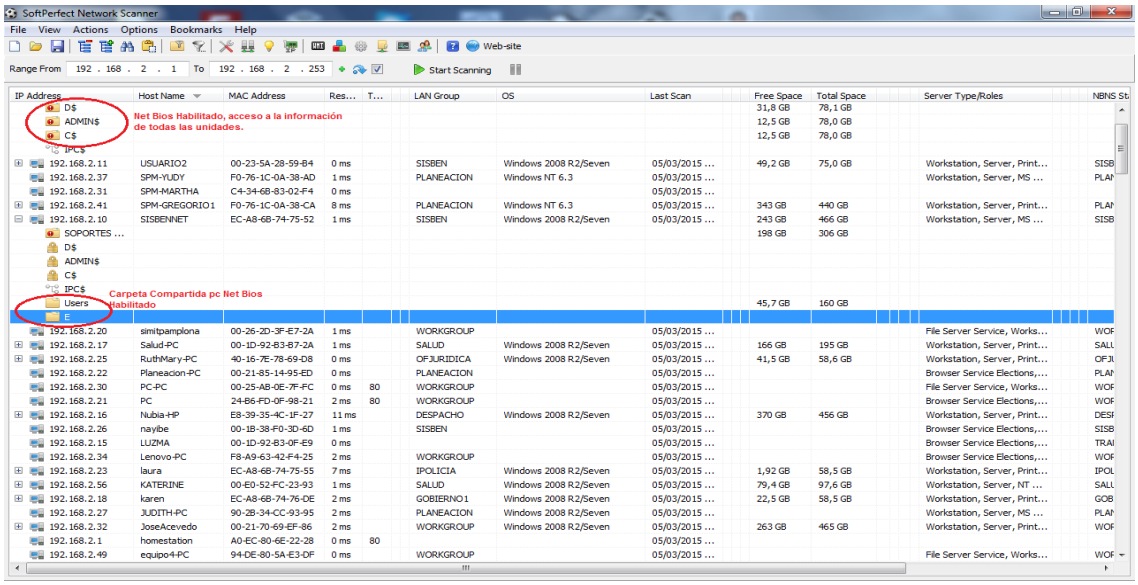


Fuente: Autor.

Se determina que la maquina Equipo1-PC del grupo LAN Group Salud con *Windows* 7 comparte 2 carpetas. Equipo con *NetBIOS* Activo. Las carpetas compartidas registran los siguientes atributos:

<folder attributes="readonly" sharesec="" readers="" writers="" freespace="50,4 GB" diskspace="97,6 GB">Users</folder>
<folder attributes="readonly" sharesec="" readers="" writers="" freespace="832 GB" diskspace="834 GB">IMAGENES</folder>

Figura 16. Evidencia Escaneo



Fuente: Autor

En un Nuevo escaneo se evidencian dos equipos con *NetBIOS* activo ilustrado en la figura 16, se evidencia una carpeta compartida llamada “E”.

*<ip-address>**192.168.2.123**</ip-address><folders>*

<folder attributes="writable" sharesec="" readers="No DACL" writers="No DACL" freespace="23,5 GB" diskspace="76,6 GB">E$</folder>

<folder attributes="writable" sharesec="Everyone: RWF" readers="BUILTIN\Administradores, Todos" writers="BUILTIN\Administradores, Todos" freespace="12,5 GB" diskspace="78,0 GB">Users</folder>

<folder attributes="writable" sharesec="" readers="No DACL" writers="No DACL" freespace="31,8 GB" diskspace="78,1 GB">D$</folder>

<folder attributes="writable" sharesec="" readers="No DACL" writers="No DACL" freespace="12,5 GB" diskspace="78,0 GB">ADMIN$</folder>

<folder attributes="writable" sharesec="" readers="No DACL" writers="No DACL" freespace="12,5 GB" diskspace="78,0 GB">C$</folder>

<folder attributes="ipc" sharesec="" readers="" writers="" freespace="" diskspace="">IPC$</folder>

*<Hostname>**Usuario-PXX**</hostname><langroup>WORKGROUP</langroup>*

<os>Windows 2008 R2/Seven</os> <sharesec>Everyone: RWF</sharesec> <readers>BUILTIN\Administradores,NoDACL,Todos</readers>

<writers>BUILTIN\Administradores, No DACL, Todos</writers>

<users>Administrador, HomeGroupUser$, Invitado, Usuario, VUSR_USUARIO-PXX</users>

<roles>Workstation, Server, NT Workstation/Server, Potential Browser, Master Browser</roles>

<nbns>Active</nbns><monitor/><httpbanner>80:Apache/2.2.16(Win32)PHP/5.2.14</httpbanner> <item>Running</item>

El equipo Usuario-PXX se convierte en el equipo encontrado con mayor vulnerabilidad ya que registra varias carpetas compartidas con atributos de lectura y escritura, además registra una vulnerabilidad aun mayor ya que es un servidor *WEB* tiene instalado un servidor Apache/2.2.16(Win32) y PHP/5.2.14 los dos se

encuentran corriendo; según las indagaciones el equipo se utiliza para procesos generadores de contenidos de una de las dependencias. Ante la vulnerabilidades encontradas, el servidor está expuesto a un ataque potencial a la base de datos que contenga, de igual forma la información en cada una de las carpetas compartidas están expuesta a ser extraída, borrada, modificada, los contenidos o páginas *Web* almacenadas están expuestas a cualquier tipo de ataque relacionado con las formas de manipular información de forma ilegal.

<ip-address>192.168.2.10</ip-address><folders>
<folder attributes="writable" sharesec="" readers="" writers="" freespace="198 GB" diskspace="306 GB">SOPORTES FICHAS</folder>
<folder attributes="password" sharesec="" readers="" writers="" freespace="" diskspace="">D$</folder>
<folder attributes="password" sharesec="" readers="" writers="" freespace="" diskspace="">ADMIN$</folder>
<folder attributes="password" sharesec="" readers="" writers="" freespace="" diskspace="">C$</folder>
<folder attributes="ipc" sharesec="" readers="" writers="" freespace="" diskspace="">IPC$</folder>
<folder attributes="readonly" sharesec="" readers="" writers="" freespace="45,7 GB" diskspace="160 GB">Users</folder>
<folder attributes="readonly" sharesec="" readers="" writers="" freespace="" diskspace="">E</folder></folders>
<Hostname>SISBENNET</hostname>
<Langroup>SISBEN</langroup> <os>Windows 2008 R2/Seven</os
<Roles>Workstation, Server, MS SQL server, NT Workstation/Server, Potential Browser</roles>

La información del escaneo registra que el equipo tiene instalado un servidor SQL en un sistema *Windows* Server, la aplicación del servidor guarda información de los usuarios de un sistema que registra a los beneficiarios de un programa de subsidio. Ante la vulnerabilidades encontradas, el equipo está expuesto a un ataque potencial a la base de datos que contenga, de igual forma la información en cada una de las carpetas compartidas están expuesta a ser extraída, borrada, modificada, los contenidos o páginas *Web* almacenadas están expuestas a cualquier tipo de ataque relacionado con las formas de manipular información de forma ilegal.

Ante las evidencias encontradas se sugiere implementar las siguientes soluciones para prevenir ataques por *NetBIOS* lo que se conoce como deshabilitar *NetBIOS* en el servidor DHCP:

- Haga clic en Inicio, seleccione programas, seleccione herramientas administrativas y, a continuación, haga clic en DHCP.

- En el panel de navegación, expanda el server name, expanda Ámbito, haga clic en Opciones de ámbito y, a continuación, haga clic en Configurar opciones. Nota En este paso, el marcador de posición nombre_servidor especifica el nombre del servidor DHCP.

- Haga clic en la ficha opciones avanzadas y, a continuación, haga clic en Opciones de Microsoft *Windows* 2000 en la lista de clase de proveedor. Asegúrese de que se selecciona la clase de usuario predeterminado en la lista de clase de usuario.

- Haga clic para seleccionar la casilla de verificación opción 001 Microsoft deshabilitar *NetBIOS*, en la columna opciones disponibles.

- En el área de entrada de datos, tipo 0x2 en la caja larga, y luego haga clic en Aceptar.

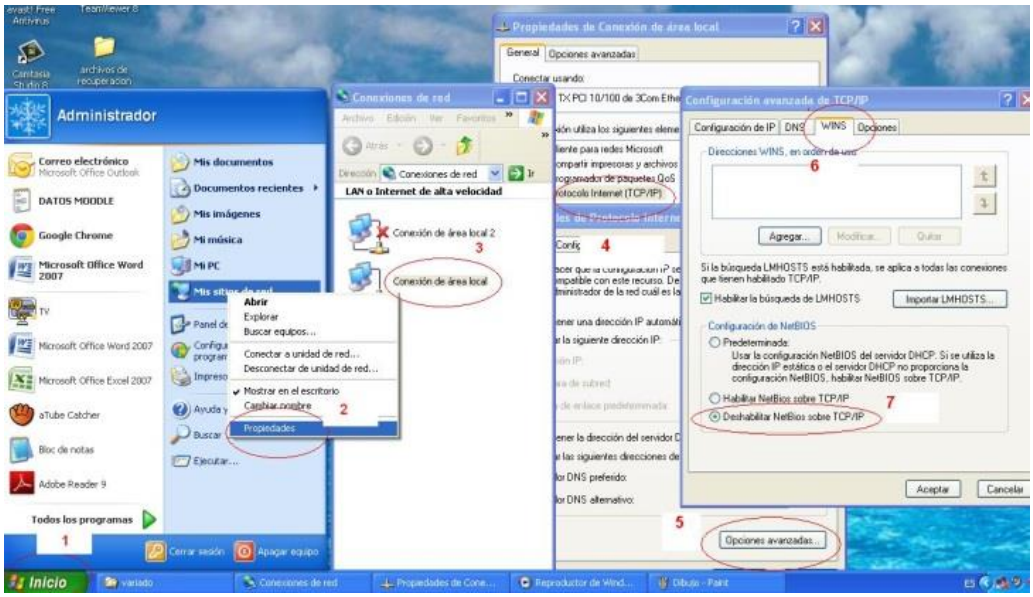
- Configure el cliente DHCP para que el servidor DHCP para determinar el comportamiento de *NetBIOS*.

Para *Windows* XP, *Windows* Server 2003 y *Windows* 2000: En el escritorio, haga clic en mis sitios de red y, a continuación, haga clic en propiedades siguiendo los siguientes pasos:

- Haga clic derecho en Conexión de área local y a continuación, haga clic en Propiedades: En los componentes seleccionados son utilizados por esta lista de conexiones, haga doble clic en protocolo Internet (TCP / IP), haga clic en opciones avanzadas y a continuación, haga clic en la ficha WINS. En *Windows* XP y en *Windows* Server 2003, debe hacer doble clic en Protocolo Internet (TCP / IP) en el Esta conexión utiliza los siguientes elementos de la lista.

- Haga clic en configuración de uso de *NetBIOS* del servidor DHCP y, a continuación, haga clic en Aceptar tres veces. Los pasos se resumen en la figura 17.

Figura 17. Desactivar NetBIOS en XP



Fuente: Autor

En *Windows* Vista En el escritorio, haga clic en Red y, a continuación, haga clic en Propiedades. En Tareas, haga clic en Administrar conexiones de red, se siguen los siguientes pasos:

- Haga clic derecho en Conexión de área local y, a continuación, haga clic en Propiedades. En Esta conexión utiliza la lista siguientes elementos, haga doble clic en Protocolo de Internet versión 4 (TCP / IPv4), haga clic en Opciones avanzadas y, a continuación, haga clic en la ficha WINS.

- Haga clic en configuración de uso de *NetBIOS* del servidor DHCP y, a continuación, haga clic en Aceptar tres veces.

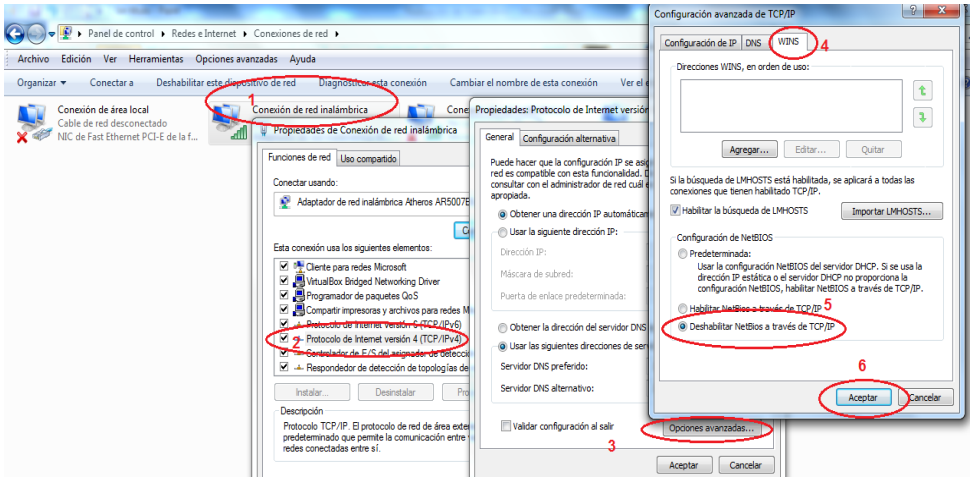
En *Windows* 7 haga clic en Inicio y, a continuación, haga clic en Panel de control. En Red e Internet, haga clic en Ver estado de la red y las tareas.

- Haga clic en Cambiar configuración del adaptador.

- Haga clic en Conexión de área local y a continuación, haga clic en Propiedades. En Esta conexión utiliza la lista siguientes elementos, haga doble clic en Protocolo de Internet versión 4 (TCP / IPv4), haga clic en Opciones avanzadas y, a continuación, haga clic en la ficha WINS.

- Haga clic en configuración de uso de *NetBIOS* del servidor DHCP y, a continuación, haga clic en Aceptar tres veces,[28] en la figura 18 se ilustran la secuencia de pasos para desactivar *NetBIOS*.

Figura 18. Desact_NetBIOS_Win_7



Fuente: Autor

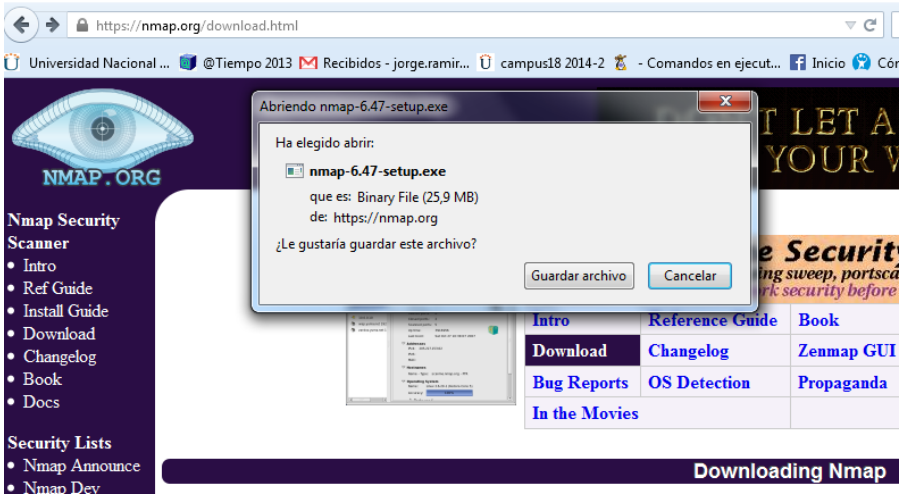
[28] MICROSOFT. (21 de Agosto de 2009). */support.microsoft*. Obtenido de How to disable NetBIOS over TCP/IP by using DHCP server options Consultado en : http://support.microsoft.com/en-us/kb/313314

Se advierte que Las anteriores pruebas fueron desarrolladas con autorización de la entidad en el marco del permiso para realizar el trabajo. Se advierte que realizar este tipo de actividades de forma maliciosa sin autorización incurre en la violación de los artículos: 269 A. Acceso abusivo a un sistema informático, de la ley 1273 del año 2009.

Luego de analizar el puerto de *NetBIOS*, se continúan las pruebas de análisis de puertos con el programa Nmap**;** para abordar esta esta etapa del análisis de la red de datos es necesario conocer las variables y parámetros sobre los cuales se obtendrá resultados por medio de las aplicaciones.

Para ejecuta el Procedimiento de escaneo: se realiza la descarga del programa Nmap de la página: https://nmap.org/dist/nmap-6.47-setup.exe como se muestra en la figura 19 y se inicia la instalación de Nmap.

Figura 19. Instalación Nmap



Fuente: Autor

El programa necesita ser instalado en el equipo desde el cual se realizara el escaneo, se instalada como cualquier otro programa en *Windows* siguiendo intuitivamente los pasos y luego ejecutando el acceso directo que el instalador ubica en el escritorio del sistema operativo. Luego de la instalación se ejecuta el programa desde el acceso directo creado en el escritorio de la maquina; inmediatamente abre la interfaz principal del programa mediante la cual se ejecutan todas las acciones y eventos que conlleva la realización del escaneo a la red; antes de iniciar es preciso configurar o ingresar los parámetros las casillas disponibles en la interfaz del programa:

- Se conecta la máquina al *switch* de la red de datos.

- Se utiliza un Cable de conexión (*patch cord*) UTP.

- Obtener una dirección IP de la misma red a la cual se va a escanear.

- Verificando el rango de IPs de la subred a la que pertenece la máquina conectada, se deduce su tamaño y el segmento para indicar el rango en las casillas "*Target*" de la aplicación.

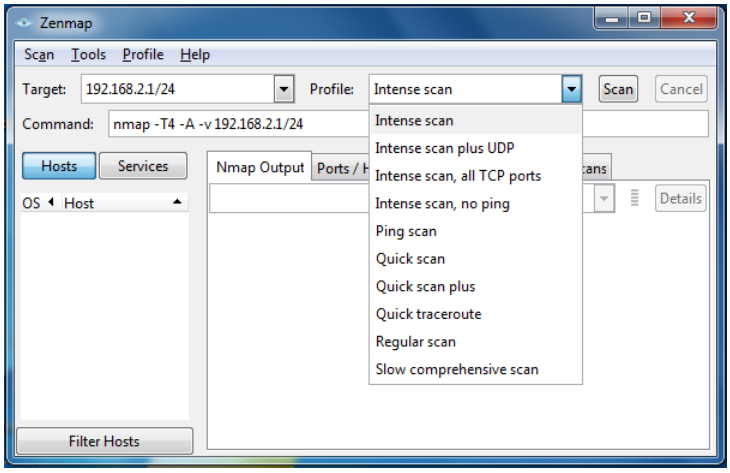
- Se indica al programa el tipo de escaneo en la casilla *Command* "nmap -T4 -A –v" con este parámetro se indica al programa que realice un mapeo de forma agresiva con una plantilla de tiempos y que imprime la versión de Nmap y finalice la ejecución.

- En la casilla Profile, seleccionar el nivel y las variable que se van a usar para el mapeo de la red, dependiendo del perfil el programa gasta un tiempo determinado. Se dispone de un listado completo de comandos, de acuerdo a lo

que se pretenda conseguir con el escaneo se combinan los comandos para obtener los resultados.[29]

En esta instancia se analiza la Red 192.168.2.0 como indica en la figura 20, esta red se origina en el Rack Principal Primer Piso.

Figura 20. Interfaz de Nmap



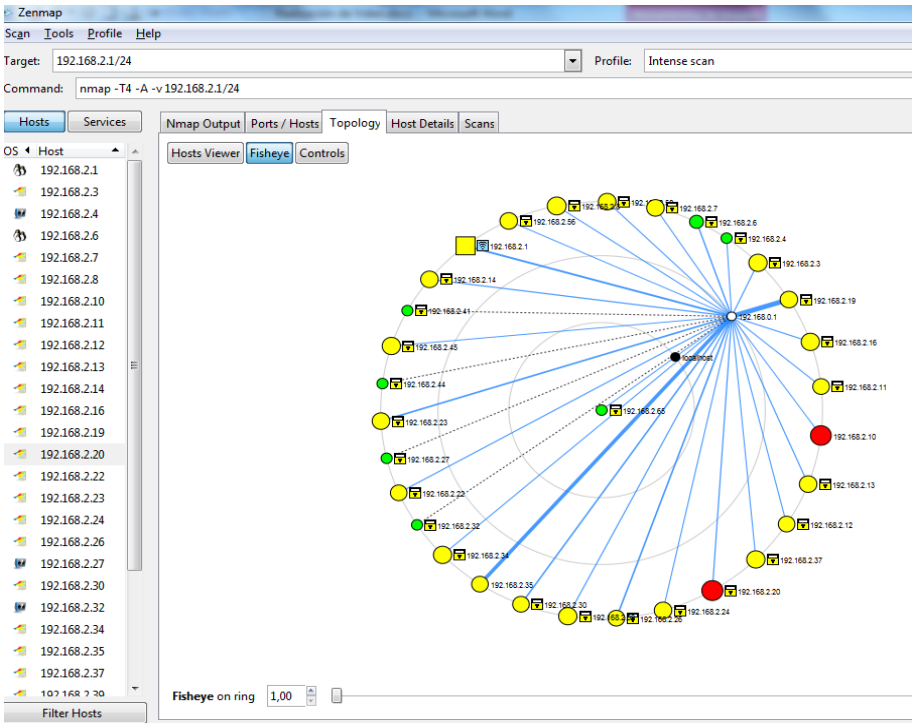
Fuente: Autor

Con el escaneo configurado se procede a iniciar dando click con el botón “Scan”, de acuerdo al tamaño de la red y la cantidad de equipos es el tiempo que demorara en dar los resultados finales.

[29]CSIRT. (21 de agosto de 2014). *CSIRT-cv.* Obtenido de NMAP 6: Listado de comandos: http://www.csirtcv.gva.es/sites/all/files/downloads/NMAP%206_%20Listado%20de%20comandos.pdf

En la figura 21 se ilustra el complejo de la red que el programa Nmap analiza, para cada equipo se ejecutara el mismo comando para recuperar la información que imprime Nmap[30].

Figura 21. Topología para análisis Nmap

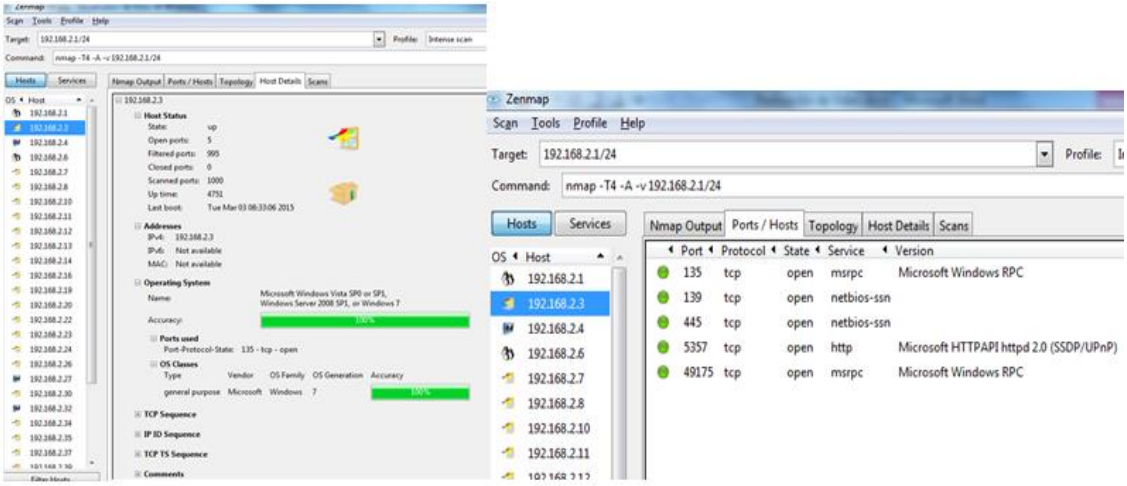


Fuente: Autor

Para los Resultados del análisis y despliegue de Nmap en cada equipo se muestran las siguientes ventanas.

[30] GORDON, L. (2015). *ZenMap Screen shots*. Obtenido de http://nmap.org/zenmap/images/zenmap-hd-648x700.png

Figura 22. Resultado 1 análisis Nmap



Fuente: Autor

En el informe muestra la IP y el equipo que la está utilizando, mostrando el sistema operativo, como se aprecia en la figura 22, en este caso se puede verificar que en el equipo *NetBIOS Computer name* BLANCA (IP 192.168.2.3) muestra la siguiente información:

PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open NetBIOS-ssn
445/tcp open NetBIOS-ssn
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49175/tcp open msrpc Microsoft Windows RPC
Host script results:
nbstat:
NetBIOS name: BLANCA, NetBIOS user: <unknown>, NetBIOS MAC: 00:21:85:14:97:46 (Micro-star Int'l Co.)
BLANCA<00> Flags: <unique><active>

BLANCA<20> Flags: <unique><active>

IPOLICIA<00> Flags: <group><active>

IPOLICIA<1e> Flags: <group><active>

IPOLICIA<1d> Flags: <unique><active>

Smb-os-discovery:

OS: Windows 7 Professional 7600 (Windows 7 Professional 6.1)

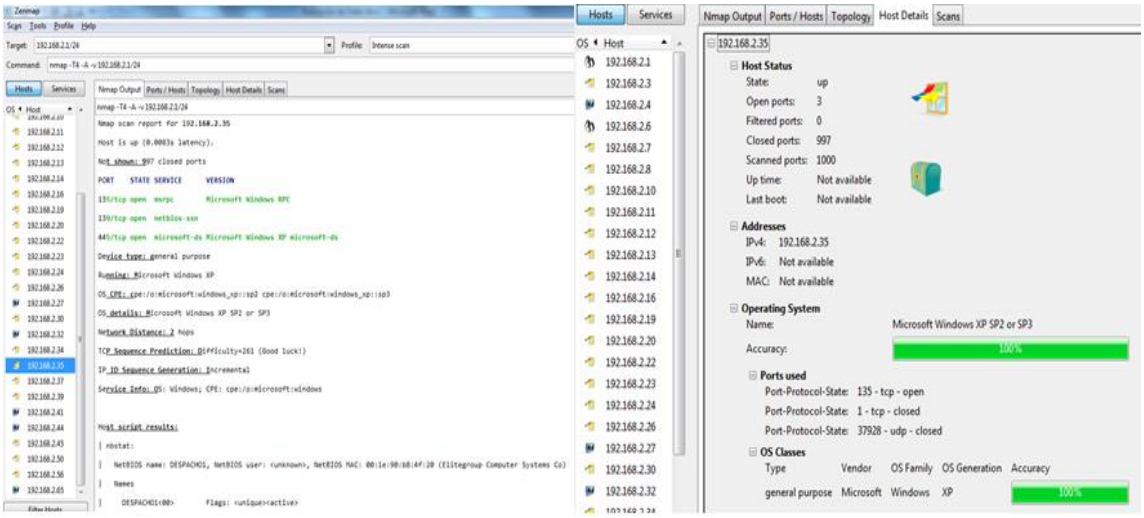
OS CPE: cpe:/o:microsoft:Windows_7::-:professional

Computer name: BLANCA

NetBIOS Computer name: BLANCA

Según el reporte de Nmap se verifica los puertos *NetBIOS* abiertos 135, 139, 445; constituye una falla de seguridad ya que es posible un ataque por *NetBIOS*; se conoce el nombre del equipo, se distingue el sistema operativo y las características.

Figura 23. Resultado 2 análisis Nmap



Fuente: Autor

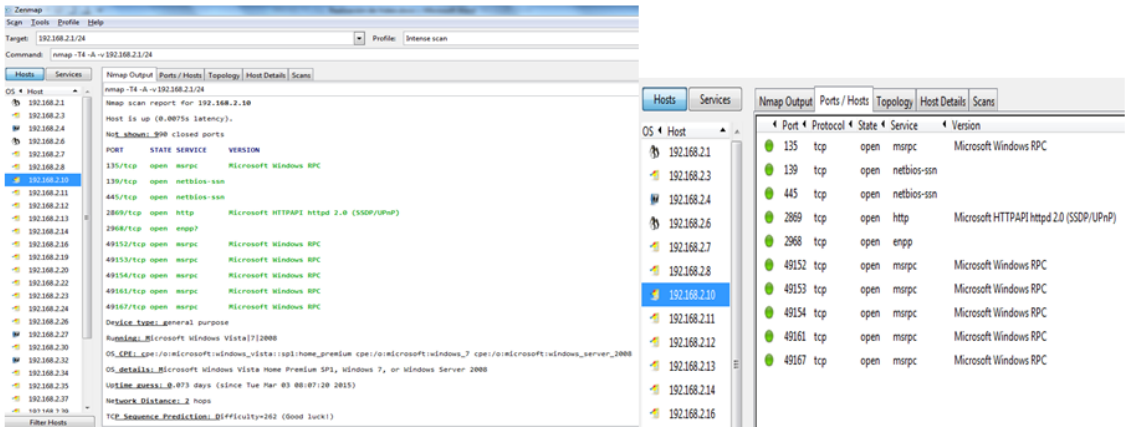
En este informe se evidencia que la maquina DESPACHO1 con IP 192.168.2.35 y *Windows* XP tiene abiertos los puertos como se ilustra en la figura 23:

PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open NetBIOS-ssn
445/tcp open Microsoft-ds Microsoft Windows XP Microsoft-ds
Device type: general purpose.
OS: Windows XP (Windows 2000 LAN Manager)
OS CPE: cpe:/o:microsoft:Windows_xp::-
Computer name: Despacho1
NetBIOS Computer name: DESPACHO1
Workgroup: DESPACHO

Según el reporte de Nmap se verifica los puertos *NetBIOS* abiertos 135, 139, 445; constituye una falla de seguridad ya que es posible un ataque por *NetBIOS*; se conoce el nombre del equipo, se distingue el sistema operativo y las características.

En la figura 24 se distingue la operación de un servidor *Windows* identificado como *server name*: SISBENNET

Figura 24. Resultado 3 análisis Nmap



Fuente: Autor

Nmap scan report for 192.168.2.10

Host script results:

Ms-sql-info:

Windows server name: SISBENNET

[192.168.2.10\MSSQLSISBEN]

Instance name: MSSQLSISBEN

Version: Microsoft SQL Server 2005 RTM

Version number: 9.00.1399.00

Product: Microsoft SQL Server 2005

Service pack level: RTM

Post-SP patches applied: No

TCP port: 53164

Named pipe: \\192.168.2.10\pipe\MSSQL$MSSQLSISBEN\sql\query

Clustered: No

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open NetBIOS-ssn

445/tcp open NetBIOS-ssn

2869/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
2968/tcp open enpp?
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49161/tcp open msrpc Microsoft Windows RPC
49167/tcp open msrpc Microsoft Windows RPC

Según el reporte de Nmap se verifica los puertos *NetBIOS* abiertos 135, 139, 445; constituye una falla de seguridad ya que es posible un ataque por *NetBIOS*; se conoce el nombre del equipo, se distingue el sistema operativo y las características, además se revelan puertos tcp abiertos: 2869, 2968, 49152, 49153, 49154, 49161, 49167. Con el reporte se determina que el HOST SISBENNET se encuentra en peligro de ser atacado sin mayores obstáculos ya que se verifican puertos abiertos *NetBIOS*; el servidor instalado en la maquina se encuentra en estado de vulnerabilidad.

En la figura 25 se muestran los resultados del escaneo al equipo SIMITPAMPLONA, según el siguiente reporte de Nmap el equipo presenta los puertos *NetBIOS* abierto, 135, 139, 445, registrando también otros puerto TCP abiertos.

Nmap scan report for 192.168.2.20
Host is up (0.0069s latency).
Not shown: 989 filtered ports
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC

139/tcp open NetBIOS-ssn

445/tcp open NetBIOS-ssn

3389/tcp open ms-wbt-server Microsoft Terminal Service

5800/tcp open vnc-http Ultr@VNC (Name simitpamplona; resolution: 1440x932; VNC TCP port: 5900)

_http-title: [simitpamplona]

5900/tcp open vnc VNC (protocol 3.8)

Vnc-info: Protocol version: 3.8 Security types: Ultra_ VNC Authentication

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

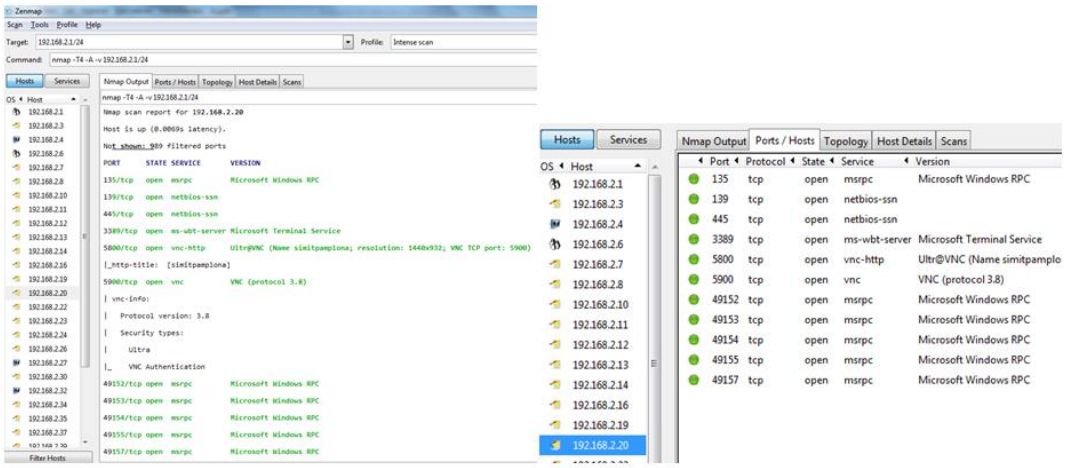
49157/tcp open msrpc Microsoft Windows RPC

Host script results:

Nbstat:

NetBIOS name: SIMITPAMPLONA, NetBIOS user: <unknown>, NetBIOS MAC: 00:26:2d:3f:e7:2a (Wistron) Names SIMITPAMPLONA<00> Flags: <unique><active> WORKGROUP<00> Flags: <group><active>SIMITPAMPLONA<20> Flags: <unique><active>

Figura 25. Resultado 4 análisis Nmap

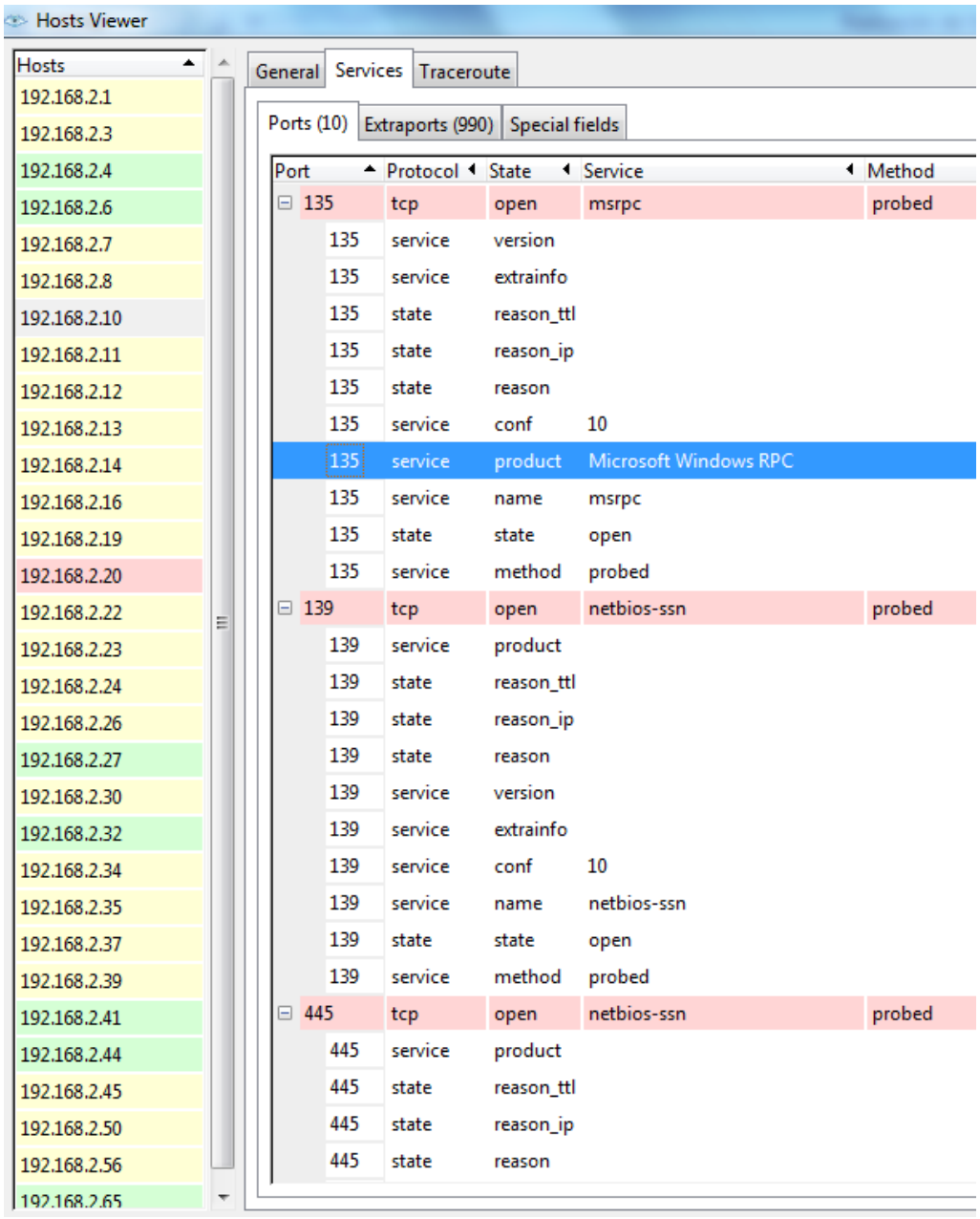


Fuente: Autor

Según el reporte de Nmap se verifica los puertos *NetBIOS* abiertos 135, 139, 445; constituye una falla de seguridad ya que es posible un ataque por *NetBIOS*; se conoce el nombre del equipo, se distingue el sistema operativo y las características, además se revelan puertos tcp abiertos: 2869, 2968, 49152, 49153, 49154, 49157, 49161, 49167.

El Resumen de los puertos *NetBIOS* abiertos en la red se muestra en la figura 26 en donde se resume el número de puerto el estado en el que se encuentra, la IPs y los equipos involucrados

Figura 26. Resultado 5 análisis Nmap

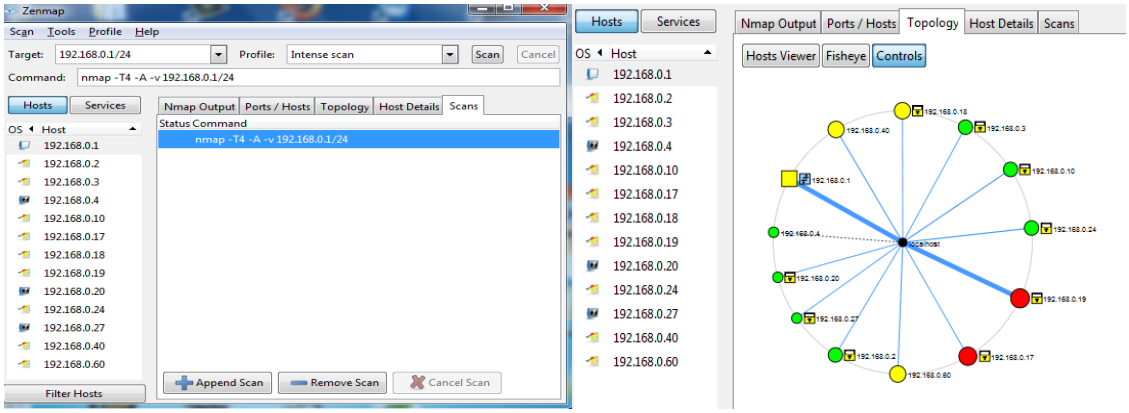


Fuente: Autor

En desarrollo de la búsqueda de vulnerabilidades se procede a realizar el análisis de la red 192.168.0.0 Ubicada en el Rack principal primer piso, con el escaneo

configurado se procede a iniciar dando click con el botón “Scan” como se ilustra en la figura 27 en la cual se aprecia la Topología de la red objeto del análisis**.**

Figura 27. Resultado 6 análisis Nmap

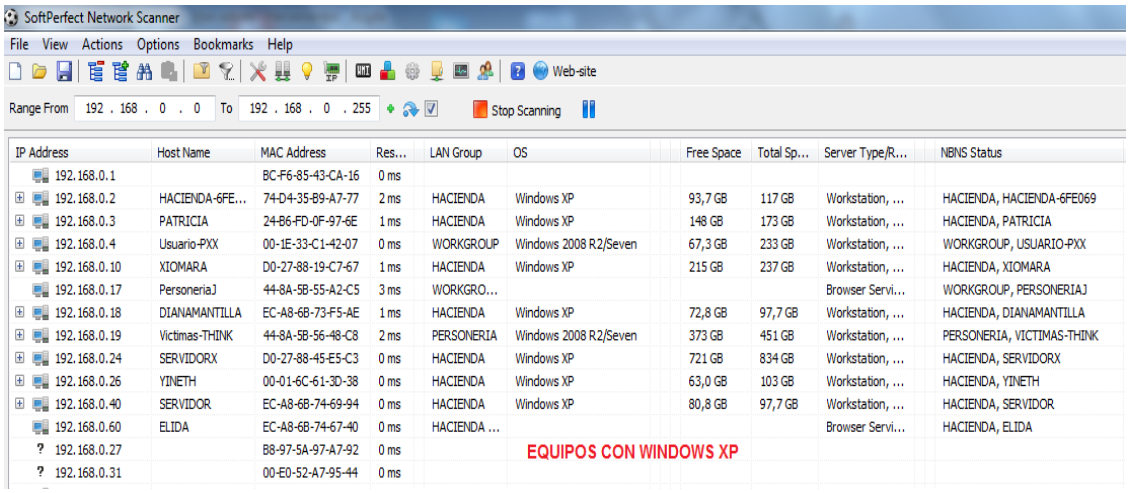


Fuente: Autor

Lo resultados del análisis y despliegue de Nmap en cada equipo analizado se muestra en las siguientes ventanas. Como se ha mostrado en los anteriormente el objetivo de Nmap es realizar un sondeo profundo de los puertos que se encuentran desplegados como servicios en cada una de las máquina para determinar su estado y función al sistema que soportan, conociendo mediante el análisis si se constituye una vulnerabilidad y su nivel de probabilidad.

En la figura 28 se muestra como se hace uso de la herramienta *Network Scanner* como apoyo para obtener información de los equipos y visualizar 8 equipos con *Windows* XP.

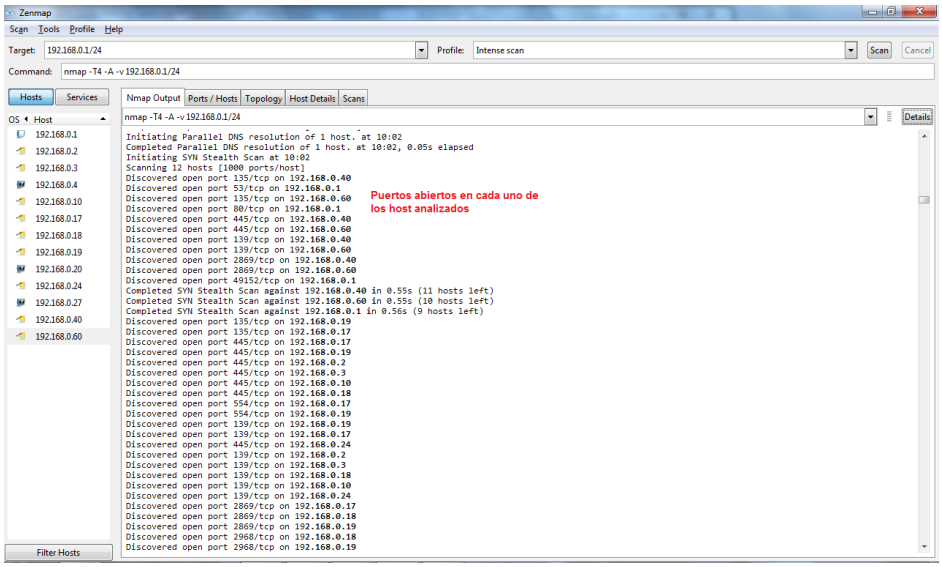
Figura 28. Resultado 7 análisis NS



Fuente: Autor

En la figura 29 se observa la lista de puertos que abiertos que Nmap recupero de cada máquina.

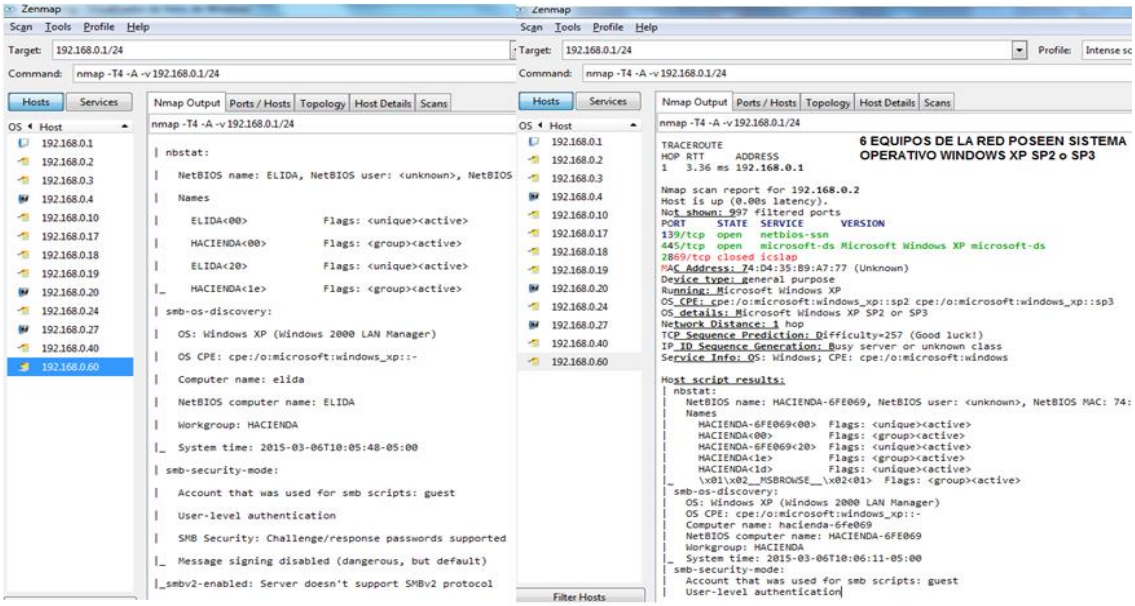
Figura 29. Resultado 8 análisis Nmap



Fuente: Autor

En la figura 30 se evidencian con el reporte de Nmap los diferentes puertos descubiertos en la red y se detalla la implicación de cada máquina con cada uno de ellos.

Figura 30. Resultado 9 análisis Nmap



Fuente: Autor

Según el reporte de Nmap se verifica los puertos *NetBIOS* abiertos 135, 139, 445; constituye una falla de seguridad ya que es posible un ataque por *NetBIOS*; se conoce el nombre del equipo, se distingue el sistema operativo y las características, además se revelan puertos tcp abiertos: 2869, 2968, 49152, 49153, 49154, 49157, 49161, 49167. Con el reporte se determina que los equipos ELIDA, HACIENDA y *NetBIOS* name: SERVIDORX se encuentra en peligro de ser atacado sin mayores obstáculos, como se demuestra en el siguiente fragmento del reporte:

NetBIOS name: SERVIDORX

Host script results: ms-sql-info: [\\192.168.0.24\pipe\MSSQL$SQLEXPRESS\sql\query]

Version: Microsoft SQL Server 2008 R2 RTM

Version number: 10.50.1600.00

Product: Microsoft SQL Server 2008 R2, Service pack level: RTM Post-SP patches applied: No Named pipe: \\192.168.0.24\pipe\MSSQL$SQLEXPRESS\sql\query

Nbstat: NetBIOS name: SERVIDORX, NetBIOS user: <unknown>

NetBIOS MAC: d0:27:88:45:e5:c3 (Hon Hai Precision Ind.Co.Ltd)

Names SERVIDORX<00> Flags: <unique><active>

SERVIDORX<20> Flags: <unique><active>

HACIENDA<00> Flags: <group><active>

OS: Windows XP (Windows 2000 LAN Manager)

OS CPE: cpe: /o: Microsoft: Windows_xp::-

Computer name: SERVIDORX

NetBIOS Computer name: SERVIDORX

Workgroup: HACIENDA

Con el reporte de Nmap se verifica que existe un servidor una base de datos donde se almacenan los datos del sistema de Hacienda en decir impuestos del municipio, ante los puertos abiertos encontrados , el sistema operativo que lo soporta , se deduce que la información sensible que procesa gestiona y genera se encuentra en un riesgo muy alto. En la figura 31 se aprecia el análisis que Nmap desplego sobre en el servidor. En el siguiente reporte se detallan las algunas características del sistema instalado en el servidor.

Host script results: ms-sql-info: [\\192.168.0.24\pipe\MSSQL$SQLEXPRESS\sql\query]

Version: Microsoft SQL Server 2008 R2 RTM

Version number: 10.50.1600.00

Product: Microsoft SQL Server 2008 R2

Service pack level: RTM

Post-SP patches applied: No

Named pipe: \\192.168.0.24\pipe\MSSQL$SQLEXPRESS\sql\query

Nbstat: NetBIOS name: SERVIDORX, NetBIOS user: <unknown>, NetBIOS MAC: d0:27:88:45:e5:c3 (Hon Hai Precision Ind.Co.Ltd)

Names SERVIDORX<00> Flags: <unique><active>

SERVIDORX<20> Flags: <unique><active>

HACIENDA<00> Flags: <group><active>

OS: Windows XP (Windows 2000 LAN Manager)

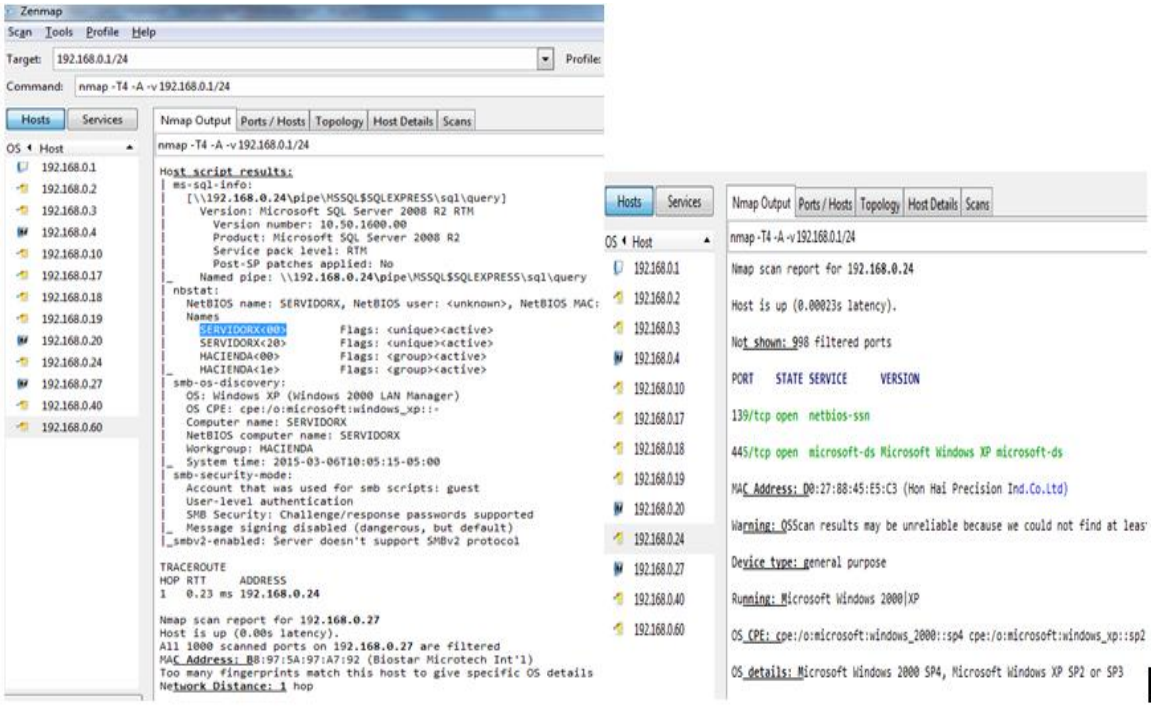
OS CPE: cpe: /o: Microsoft: Windows_xp::-

Computer name: SERVIDORX

NetBIOS computer name: SERVIDORX

Workgroup: HACIENDA

Figura 31. Resultado 10 análisis Nmap

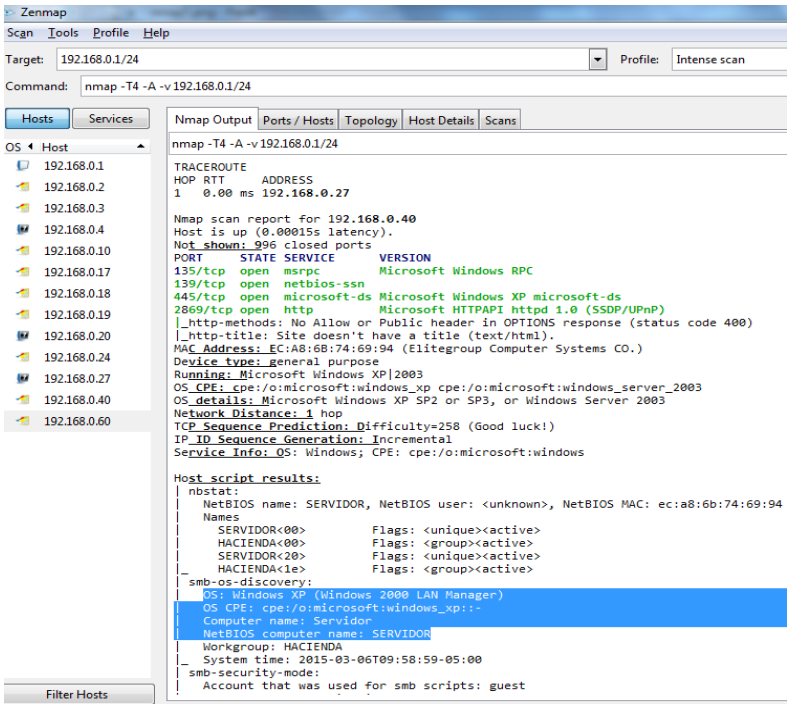


Fuente: Autor

La mayoría de los equipos que procesan la información referente al sistema de impuestos y rentas del municipio son soportados por el sistema operativo *Windows* XP, con lo que se concluye como una red insegura que tiene en riesgo el funcionamiento de una de las dependencias de la entidad.

Con el reporte de Nmap se verifica que existe un servidor una base de datos donde se almacenan los datos del sistema de Hacienda en decir impuestos del municipio, ante los puertos abiertos encontrados, el sistema operativo que lo soporta, se deduce que la información sensible que procesa gestiona y genera se encuentra en un riesgo muy alto ya que como ilustra la figura 32 el sistema operativo *Windows* XP revela en los puertos *NetBIOS* a la red.

Figura 32. Resultado 11 análisis Nmap



Fuente: Autor

La mayoría de los equipos que procesan la información referente al sistema de impuestos y rentas del municipio son soportados por el sistema operativo *Windows* XP, con lo que se concluye como una red insegura que tiene en riesgo el funcionamiento de una de las dependencias de la entidad.

Se advierte que las anteriores pruebas fueron desarrolladas con autorización de la entidad en el marco del permiso para realizar la investigación. Se advierte que realizar este tipo de actividades de forma maliciosa sin autorización incurre en la violación de los artículos: 269 A. Acceso abusivo a un sistema informático, de la ley 1273 del año 2009.

5.1.4.4 Análisis de vulnerabilidades al recurso humano. Para este proceso se realiza un análisis utilizando técnicas inherentes a la persuasión de los usuarios de un sistema informático para conseguir información.

Se Implementa la técnica *Trashing* como práctica de ingeniera social a una dependencia de la Alcaldía del Municipio de Pamplona – Norte de Santander Para abordar esta práctica es preciso conocer la conceptualización de las técnicas implementadas para tal fin.

Como se ha descrito *Trashing* consiste en una técnica de ingeniería social presencial no agresiva, que tiene como propósito escudriñar o buscar en las papeleras o en cestas de basura de las oficinas de una organización con el fin de encontrar documentos importantes, privados, datos personales, extractos bancarios, facturas de servicios y demás información que sirva al atacante obtener información para documentar e implementar otro tipo de ataque.[31]

El Procedimiento para el implementar la técnica de ingeniería social para extraer información en una de las oficinas de la alcaldía municipal es el siguiente:

- Encontrar una papelera en una oficina importante.

- Se escoge una de las oficinas con más importancia en cuanto a la gestión y el manejo de información importante.

[31] SEGURIDAD, e. (Octubre de 2014). *Debilidades de seguridad comúnmente explotadas.* Obtenido de https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

- Se solicita permiso de ingreso a la persona que se encuentra presente indicándole que se está llevando a cabo una campaña de reciclaje del papel y por ende que si es posible le permita tomar los papeles desechos en la cesta, cuando el funcionario accede se pasa la basura de la cesta a una bolsa como se aprecia en la figura 33 y se lleva a otro sitio para ser analizada.

Figura 33. Practica Trashing.

Fuente: Autor

- En otro lugar se saca la basura de la bolsa y se clasifica entre hojas completas, hojas cortadas y papeles de notas como se observa en la figura 34.

- Las hojas rotas se intentan unir para darle forma original y visualizar su contenido.

- Se Clasifican los papeles, ordenando los documentos encontrados.

Figura 34. Practica Trashing

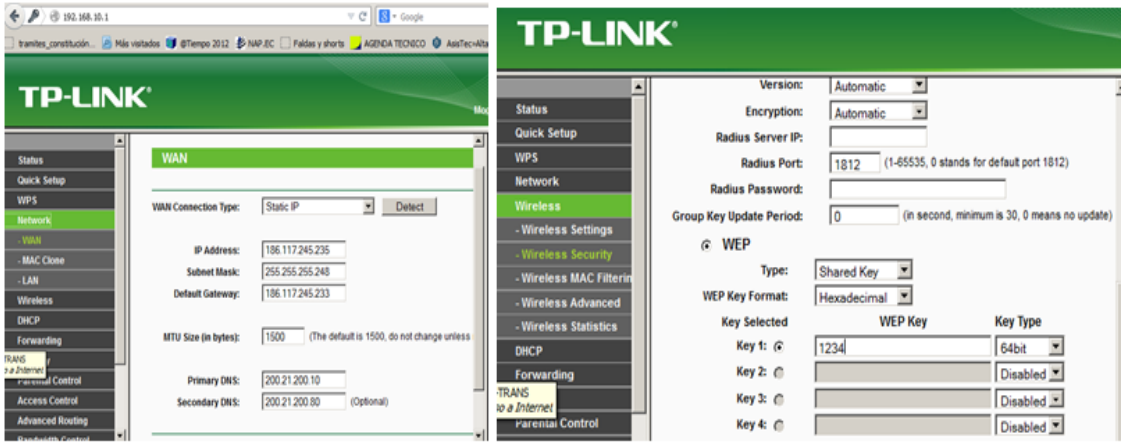
Fuente: Autor

Analizando los resultados se encontró que entre los documentos, se encuentra la liquidación de un contrato que seguro se imprimió en una hoja que ya tenía una cara usada y por eso imprimieron una nueva y desecharon la anterior, en el documento aparecen los datos de contratista número de documento o NIT, valor a pagar, ítems, número de cuenta que gira el dinero, número de cheque, etc. Esta información en manos criminales pude ser usada para realizar diversos ataques al contratista por ejemplo una extorsión, suplantación, etc y para la entidad genera riesgos ya que se revelan datos de cuentas bancarias que pueden constituir avances en la búsqueda de más información por parte de los criminales para llevar ataques mayores. También el atacante luego puede suplantar de alguna forma al contratista, haciendo contacto con el personal que líquido el contrato para obtener información. Se encontró una lista de personas con número de documento nombres completos y fecha de nacimiento; esta información puede ser usada por un atacante para simular o suplantar alguna de las personas en la lista.

5.1.4.5 Análisis de vulnerabilidades a dispositivos inalámbricos. Las siguientes pruebas son dirigidas a las redes WIFI ubicadas en el edificio de la

Alcaldía de Pamplona – Norte de Santander, se pudo evidenciar fallas de configuración en algunos dispositivos que sirven como soporte a la conectividad de forma inalámbrica, lo que constituye otra forma de exponer los recursos de la información que se gestiona de forma individual y organizativa en la entidad. Se revisa la configuración de los routers WIFI como se aprecia en la figura 35.

Figura 35. Estado WIFI.

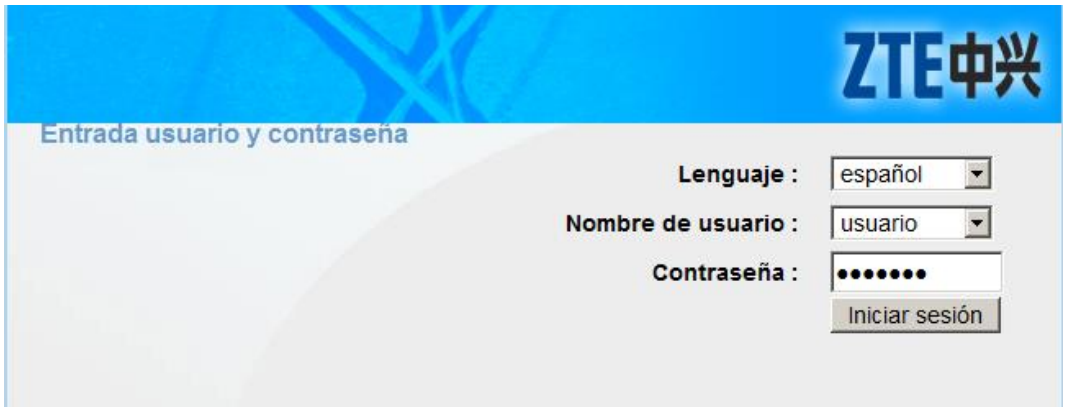


Fuente: Autor

Se evidencia una configuración Inalámbrica con un sistema de protección muy débil se hace necesario cambiar el tipo de seguridad de la red inalámbrica.

En la figura 36 se evidencia la Red Inalámbrica principal primer piso tiene una configuración por defecto para el ingreso al modem ADSL del ISP; se hace necesario deshabilitar el ingreso por el puerto 80 al modem o configurar clave personaliza para ingreso a la configuración.

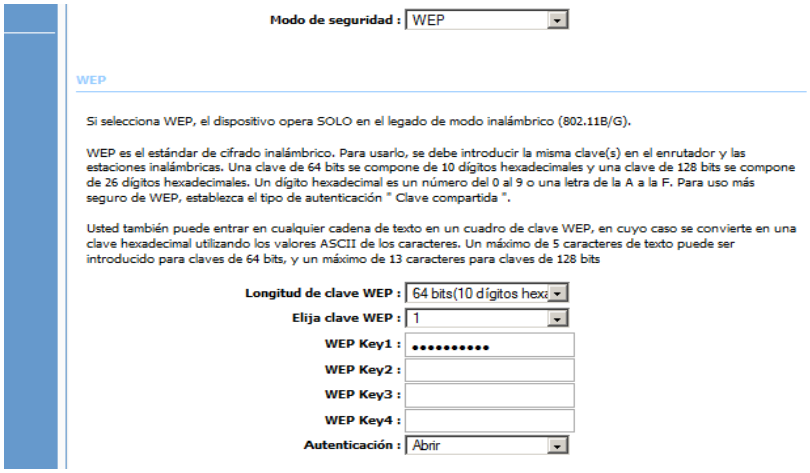
Figura 36. Modem ADSL.



Fuente: Autor

Se evidencia una configuración Inalámbrica con un sistema de protección muy débil se hace necesario cambiar el tipo de seguridad de la red inalámbrica. En la figura 37 se muestra que el tipo de seguridad implementado es wep el cual es un estándar comúnmente vulnerado por los atacantes, quienes al realizar un leve rastreo se notaran la vulnerabilidad.

Figura 37. Modem ADSL- WIFI.



Fuente: Autor

5.1.4.6 Análisis de vulnerabilidades a los bienes informáticos físicos. Usando la técnica de la observación para verificar el estado físico de los bienes que soportan la operatividad de la red informática que por defectos de instalación y no aplicación de una normatividad adecuada en el diseño e implementación de cableado estructurado y circuito eléctrico regulado, está generando una baja protección física de los equipos informáticos que sirven a la diferentes oficinas que trabajan para la gestión de la administración municipal; esta situación genera riesgo a la integridad de los equipos y a la misma información ante un posible fallo eléctrico. En el estado actual se pudieron evidenciar los siguientes aspectos:

- No se cuenta con un cuarto de comunicaciones y de energía adecuado ni soporte técnico inmediato.

- UPS Netion 20 CP 20KVA, buen estado, falta mantenimiento limpieza, posee demasiado polvo en el interior genera recalentamiento.

- Tablero regulado con algunos disyuntores automáticos en estado Off (circuito abierto, apagado)

- Algunos tomacorrientes de voltaje regulado sin corriente eléctrica, es necesario hacer uso de los tomacorrientes normales como se observa en la figura 38.

Figura 38. Vulnerabilidades-bienes

Fuente: Autor

Se observa regleta multitomas conectada a un tomacorriente regulado, además existe información en carpetas que no han sido archivadas y se encuentran en el piso o sobre los equipos como se observa en la figura 38, además se verifica sobrecarga a los tomacorrientes de voltaje regulado.

Figura 39. Vulnerabilidades-bienes-ups.

Fuente: Autor

- UPS Netion 20 CP 20KVA está expuesta a diversas fuentes de entrada de polvo y no posee sistema ventilación artificial desde el exterior como se aprecia en la figura 39.

- En la instalación no se planificaron el posible número de equipos por oficina, ha sido necesario que instalen multitomas conectados a un único tomacorriente regulado ante la demanda y necesidad de conectar equipos informáticos y accesorios. En la figura 40 se observan multitomas conectados a la red de corriente normal para multiplicar las salidas y conectar otros equipos.

Figura 40. Vulnerabilidades-bienes-Tomas

Fuente: Autor

Como consecuencia de los anteriores factores se derivan posibles amenazas que se mencionan a continuación.

- Debido a la falta de ventilación adecuada y factores como la acumulación de polvo en su interior, es posible un sobrecalentamiento de los circuitos y daños en los dispositivos de la UPS por ende los equipos informáticos conectados a esta quedarían sin servicio eléctrico.

- La falta de suficientes tomacorrientes regulados ha generado la necesidad de conectar los equipos directamente a la red corriente normal poniendo en riesgo los equipos ante fallas por variaciones de voltaje de la red comercial. El uso de multitomas genera sobrecarga a un circuito eléctrico calculado para dar servicio a determinada carga, ante una sobrecarga el disyuntor desconecta el circuito automáticamente, los equipos se apagarán inmediatamente.

Figura 41. Vulnerabilidades-bienes-acceso.

Fuente: Autor

- Como se aprecia en la figura 41 la entrada a los equipos no tiene protección, es posible accesos no autorizados y abusivos por falta de protección a los equipos que soportan la red estructurada de datos y energía, existe el riesgo que se generan ataques a la integridad de los equipos, robos, daños a los dispositivos y medios de transmisión, baja del servicio de energía y datos.

- Segmentación de la red no está normalizada ni documentada.

- Distribución de la carga entre los dispositivos inequitativa.

- No existe inventario de los recursos físicos ni lógicos de la red, como se aprecia en la figura 42 no se visualizan planillas ni documentos de registro.

- Acceso libre a internet.

Figura 42. Cuarto de comunicaciones.

Fuente: Autor

Como consecuencias de las vulnerabilidades mencionadas y el desconocimiento del riesgo de exponer toda la red a internet sin protección eficaz es posible que se generen amenazas de ataques y otros problemas relacionados con la conectividad como cuellos de botella en dispositivos y canales sobrecargados, conflictos de IPs. Posibles negaciones del servicio por malas prácticas de mantenimiento o escalamiento de la red, ataques, intrusiones y robo o pérdida de información, quejas constante de los usuarios ante las fallas de conectividad en la red interna.

5.1.4.7 Análisis de vulnerabilidades relacionadas con el uso del sistema operativo Windows XP. En algunos equipos de la Alcaldía de Pamplona – Norte de Santander según la investigación realizada en las diferentes dependencias mediante observación, acceso a las características de cada equipo (previa autorización del usuario) y escaneo con herramientas informáticas (*Network Scanner* y Nmap) se pudo comprobar lo siguiente:

- Se localizaron 64 equipos informáticos de diferentes marcas, aplicaciones y propósitos, relacionados en la Tabla 5.

Tabla 5. Sistemas operativos usados

Sistema Operativo	Cantidad	Porcentaje
Windows XP	17	27%
Windows 7 Profesional	17	27%
Windows 7 Ultimate	16	24%
Windows 7 Started	7	11%
Windows 8.1	7	11%
Total	64	100%

Fuente: el autor

Como se puede apreciar en la tabla todos los equipos trabajan bajo *Windows* en donde el escalamiento o renovación de versión se evidencia en que solo el 11% de los equipos poseen la última versión de *Windows* (*Windows* 8.1), el 62% en una Versión intermedia (*Windows* 7 Lanzado al mercado en el 2009 primeras versiones) con un promedio de 6 años de uso; el 27% comprende la versión más obsoleta de *Windows* (*Windows* XP Lanzado al mercado en el 2001 primeras versiones) con un promedio de 13 años de uso y el soporte de Microsoft está descontinuado. Con los datos anteriores se afirma que existe un 27% de los equipos de la red en estado de vulnerabilidad por cuanto se soportan con *Windows* XP.

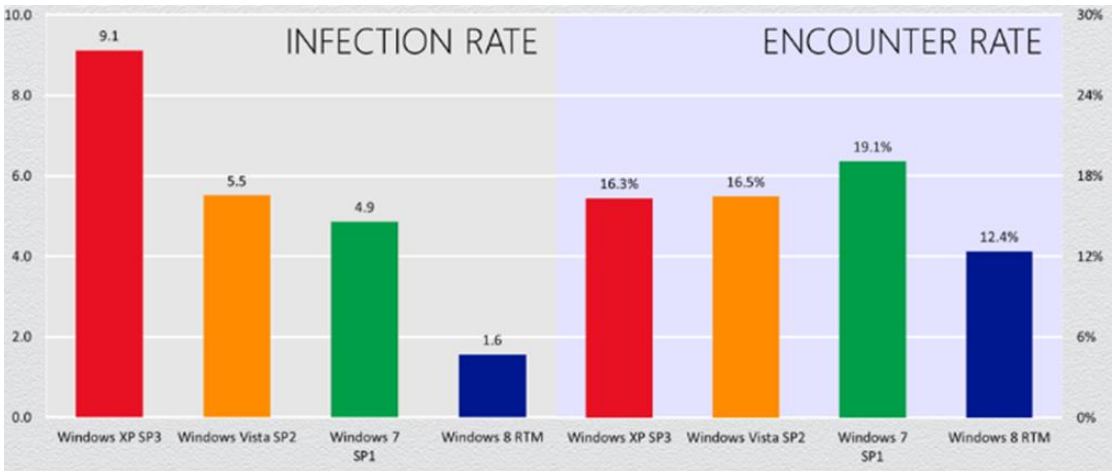
En el año 2014 Microsoft la empresa diseñadora de *Windows* XP dejo de dar soporte al sistema operativo en segundo lugar de popularidad a nivel Mundial, esto

quiere decir que no se han venido creando más parches de seguridad a las vulnerabilidades que explotan los cibercriminales al quedar al descubierto cierta vulnerabilidad del sistema operativo queda expuesta la integridad, disponibilidad, confidencialidad de la información que este soporta, a pesar esta situación miles de *Webs* y millones de equipos domésticos y empresariales siguen utilizando *Windows* XP como herramienta fundamental para la operación y las tareas personales. Los autores de *malware* conocen que las empresas y los otros usuarios aún usan *Windows* XP, estos sistemas quedan vulnerables desde el 8 de abril del 2014. El día cero los creadores de *malware* no liberaran código malicioso, lo harán después del 8 de abril; selectivamente con códigos de explotación (Incluyendo ataques dirigidos) y gradualmente (Durante varios años).[32]

En la figura 43 se realiza la comparación de la tasa de infección de las diferentes versiones de *Windows*, se verifica que la tasa de infección para *Windows* XP es significativamente más alta que la tasa de infección de las dos versiones más nuevas de *Windows*. Las diferencias de tipo de encuentro entre los sistemas operativos son significativamente más pequeñas.

[32] ESTANDARIT, C. (1 de Mayo de 2014). *Un Windows XP sin soporte, será full vulnerable 'Por Siempre' - CIOAL The Standard IT*. Obtenido de http://www.cioal.com/2014/05/01/ya-pusieron-descansar-windows-xp-las-vulnerabilidades-se-mantendran-sin-parches-por-siempre/

Figura 43. Comparación Windows.



Fuente: MICROSOFT, C. T. (15 de Agosto de 2013). *The Risk of Running Windows XP After Support Ends April 2014*.

Existe riesgo de ejecución de *Windows* XP Después de la finalización del soporte Abril del 2014esto quiere decir que las vulnerabilidades en *Windows* XP después de su "fin de la vida" ya no se abordarán en las nuevas actualizaciones de seguridad de Microsoft. ¿Cuál es el riesgo de seguir usando *Windows* XP después de su fecha de fin de soporte? Uno de los riesgos es que los atacantes tendrán la ventaja sobre los defensores de los que optan por ejecutar *Windows* XP porque los atacantes probablemente tendrán más información sobre vulnerabilidades en *Windows* XP que quienes defienden el sistema.[33]

En lo que respecta a los equipos con sistema operativo *Windows* XP en el área de redes y sistemas de la Alcaldía de Pamplona – Norte de Santander, la información anterior acerca del panorama del sistema operativo *Windows* XP revela que es

[33] MICROSOFT. (15 de Agosto de 2013). Obtenido de The Risk of Running Windows XP after Support Ends April 2014: http://blogs.microsoft.com/cybertrust/2013/08/15/the-risk-of-running-windows-xp-after-support-ends-april-2014/

uno de los sistema operativos más inseguros para el tratamiento y la gestión de información; también queda demostrado en las pruebas de testeo realizado, en donde los puertos *NetBIOS* abiertos en los equipos que ejecutan *Windows* XP y las carpetas compartidas en la red tienen en riesgo la información contenida y procesada en las dependencias que usan este sistema operativo y más grave aún el servidor de una importante gestión como lo es la secretaria de hacienda esta soportado con *Windows* XP y sirve a una base de datos con información muy importante. Ante el poco o nulo soporte que Microsoft brinda para el sistema operativo *Windows* XP, la falta de mantenimiento del *software* de los equipos: actualización de parches de seguridad, el uso libre del internet y descargas inapropiadas de herramientas facilitadoras de tareas de dudosa procedencia cargadas de adware y *malware*, contribuyen al complejo de inseguridad.

5.1.4.8 Ataques, herramientas y amenazas para la seguridad informática.

Con la siguiente documentación se busca demostrar en primera instancia con el uso del troyano *LittleWitch* unas de las formas de atacar un sistema operativo con *Windows* XP, luego se mostraran dos herramientas de ataque a los pilares de la seguridad de la información, que son comercializadas en el exterior. Cabe indicar que con las siguientes indicaciones no se está incitando al uso ni mucho menos malicioso, solo se pretende ilustrar la forma como operan y los riesgos que generan, con el fin de sensibilizar son sobre cómo prevenir para no ser víctimas de este tipo de herramientas y amenazas. Las ilustraciones y las pruebas se realizan teniendo en cuenta la ley 1273 del 2009 que contempla los delitos informáticos.

Ataque con el troyano *LittleWitch*, desde un sistema operativo *Windows* XP en ambiente controlado (Máquina Virtual) dirigido a una máquina de la red que es controlada por el sistema operativo *Windows* XP propiedad de la persona que realiza las pruebas.

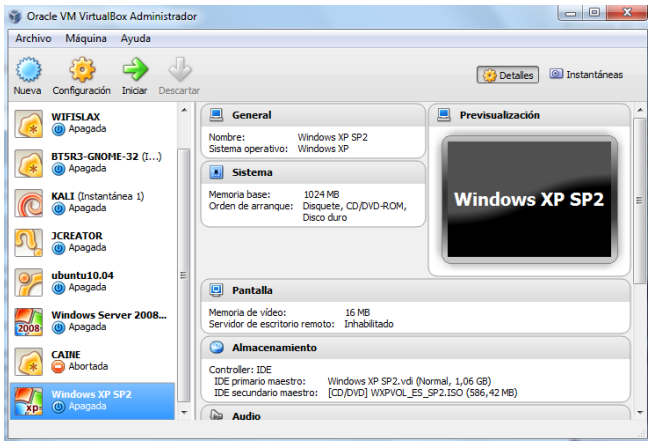
El presente tutorial tiene como fin demostrar una de las formas posibles de realizar un ataque para implementar un troyano en un equipo de cómputo de uso común. Para realizar la práctica Herramientas se utilizan las siguientes herramientas:

- Sistema atacante: Equipo anfitrión: *Windows* 7 profesional, sistema Operativo virtualizado *Windows* XP**,** máquina Virtual: Oracle VM Virtual Box**,** Troyano Little Witch**.**

- Sistema Victima Sistema Operativo *Windows* XP, *Hardware* Equipo escritorio. A continuación se describe el método de ejecución del ataque:

Un troyano se activa al ser ejecutado con la ayuda de un usuario de un sistema informático. La implantación del *LWSERVER* se puede llevar a cabo mediante diversos métodos dado las diferentes formas de interacción que existen entre los usuarios, la red y la información; en este caso la implementación se va a realizar con ayuda de otras herramientas de *software* y la ingeniería social para hacer que el *LWSERVER* sea ejecutado por parte del usuario sin que él lo note. Para iniciar con el ataque primero que todo se debe contar y tener listas las herramientas mencionadas teniendo en cuenta la puesta en marcha de cada una en su momento; en este orden de ideas como se ilustra en la figura 44 se crea la nueva máquina Virtual con el sistema operativo *Windows* XP.

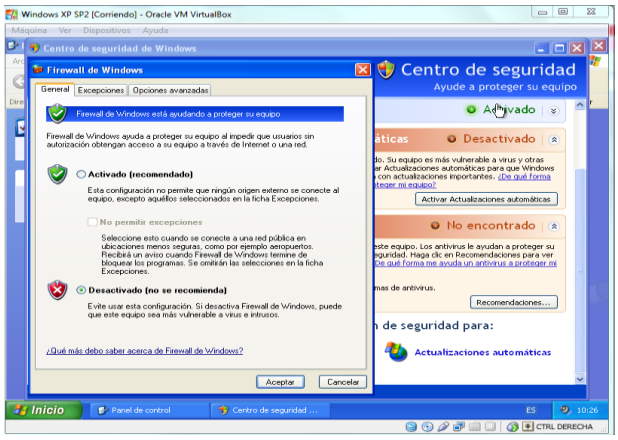
Figura 44. Windows XP Virtualizado.



Fuente: Autor

Se inicia el sistema operativo virtualizado, luego se verifica que tenga conexión a la red de área local mediante el equipo anfitrión, luego se reúne las herramientas de *software* en el escritorio de sistema operativo virtualizado el cual se prepara como se muestra en la figura 45 desactivando los mecanismos de defensa como antivirus y cortafuego con el fin de que no intervengan en el proceso de manipulación de los archivos del troyano.

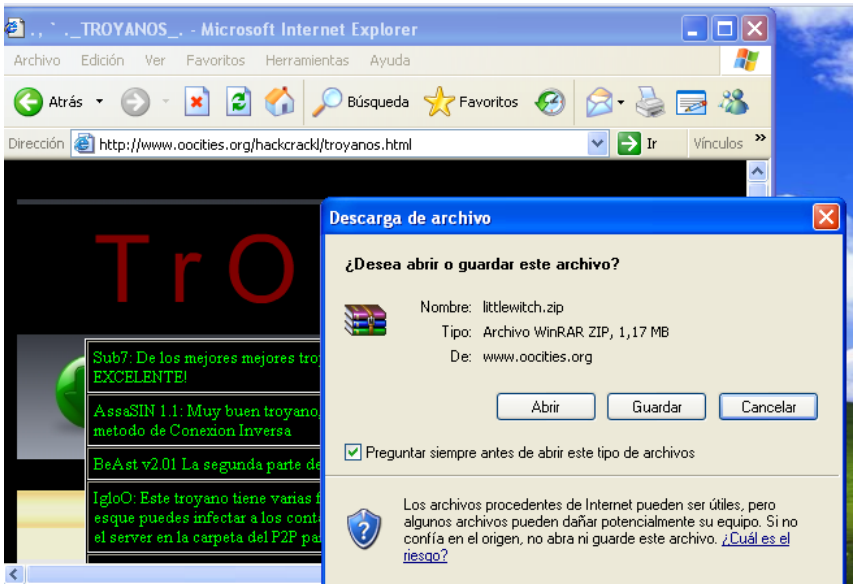
Figura 45. Firewall Windows XP desactivado.



Fuente: Autor

En la figura 46 se observa como parte del alistamiento de herramientas de *software* es realizar la descarga del troyano en el mismo sistema operativo virtualizado, se realiza de la página *Web* http://www.oocities.org/hackcrackl/troyanos.html

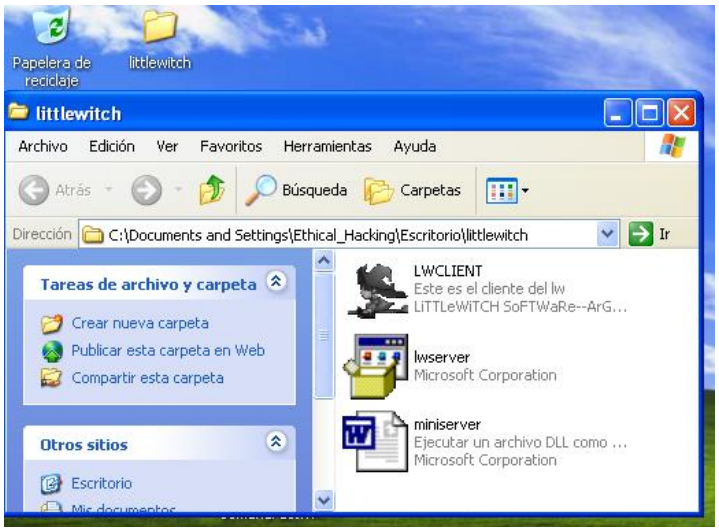
Figura 46. Descarga de LittleWitch.



Fuente: Autor

En la figura 47 se muestra como se obtiene un archivo comprimido el cual se extrae en una carpeta que contiene el *LWSERVER y LWCLIENTE.*del troyano, el cual se debe manipular con precaución y evitar la ejecución del servidor en nuestra maquina

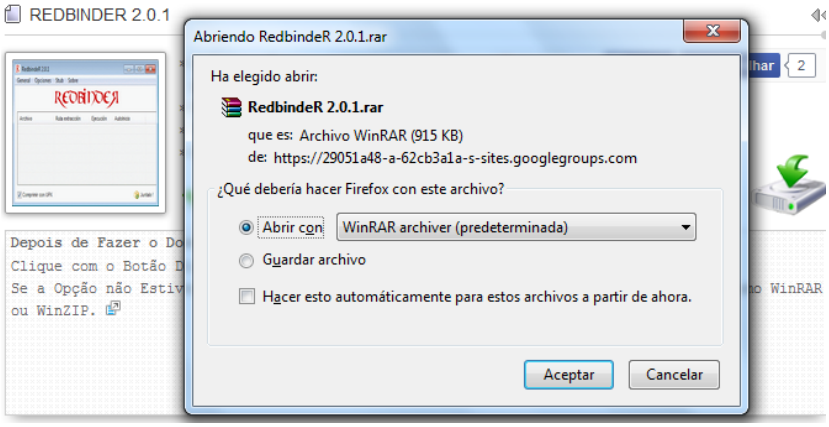
Figura 47. Carpeta _LittleWitch.



Fuente: Autor

Con el objetivo de atacar un equipo con alguna vulnerabilidad en la red se realiza un escaneo con la herramienta *Network Scanner* mediante la cual se encuentra un objetivo atractivo ya que comparte una carpeta con documentos, se accede a la misma y se comprueba que los documentos que contiene, poseen atributos de lectura y escritura, esto constituye el centro del ataque ya que uno de los archivo contiene una base de datos en formato Microsoft Excel; se toma el archivo como elemento para el propósito del ataque, el cual consiste en hacer que el usuario ejecute el servidor del troyano; para esta labor se inicia el proceso de esconder el programa *LWSERVER* junto con el documento extraído de la carpeta compartida; es necesario contar con una herramienta para juntar archivos bajo cierta apariencia conservando la independencia funcional de cada aplicación que contenga; se descarga la aplicación RedBinder la cual juntara el programa *LWSERVER* y el documento .xls. En la figura 48 se muestra como Se realiza la descarga del programa juntador de la página *Web* *http://connect-trojan.blogspot.com/2014/04/redbinder-201.html*.

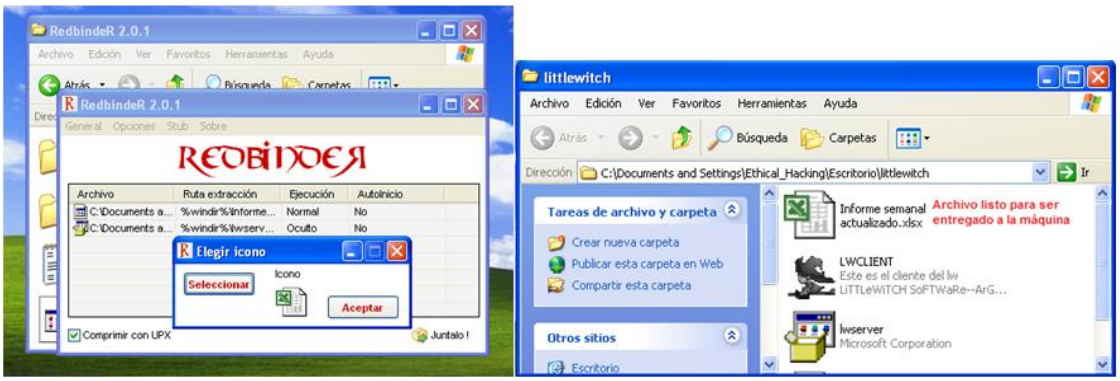
Figura 48. Descarga_RedBinder.



Fuente: Autor

Se obtiene un archivo comprimido el cual se extrae en una carpeta que contiene la aplicación; se ejecuta al archivo con el icono representativo se inicia una interfaz sencilla que contiene un breve menú de opciones en la parte superior; para añadir el programa *LWSERVER* y el documento es necesario dar click derecho en la ventana de la interfaz inicial eligiendo la opción añadir ítem, la cual inserta cada documento independientemente; ya con los archivos montados nuevamente se da click derecho en la misma ventana y se escoge un icono representativo del archivo resultante, para este ataque el preciso escoger el icono del programa que el usuario va ejecutar en formato xls, es decir el icono de Microsoft Excel, para terminar se ejecuta la opción júntalo como se muestra en la figura 49 y se realiza el proceso de unión de los dos archivos solicitando guardar con un nombre el cual se asigna siendo el mismo que nombra el archivo original en la carpeta compartida y en base a la naturaleza del archivo que el usuario crea que va abrir lo cual es verdadero pues al contener una archivo de Microsoft Excel en el nuevo paquete este abrirá el programa y los datos del archivo que contiene, sin embargo al mismo tiempo se habrá ejecutado el programa *LWSERVER* de forma transparente a la vista del usuario.

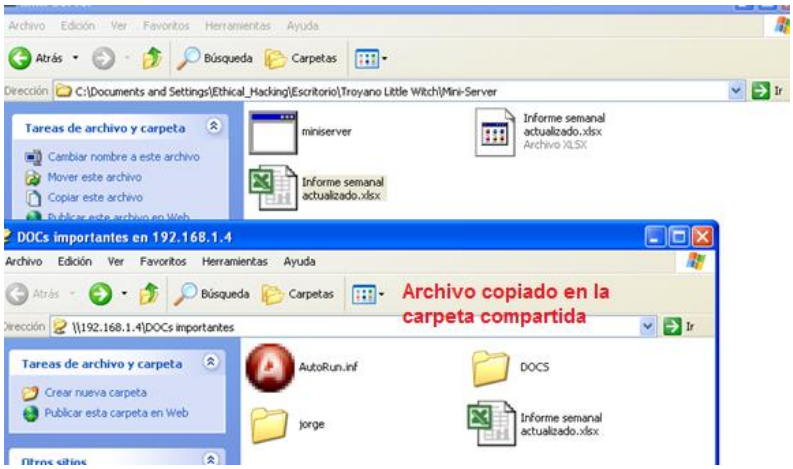
Figura 49. Unión de dos archivos.



Fuente: Autor

Con el archivo terminado se copia en la carpeta compartida reemplazando el original como se ilustra es la figura 50.

Figura 50. Archivo Entregado.



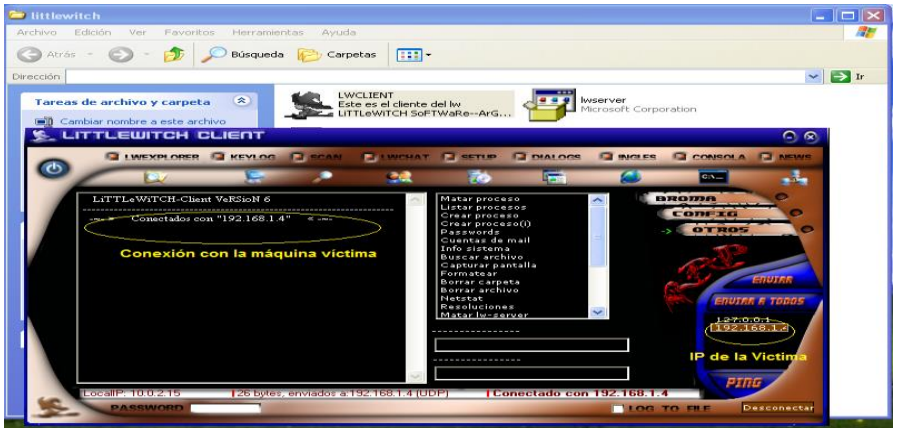
Fuente: Autor

En el momento que el usuario de la máquina infectada recurra al archivo reemplazado y lo ejecute el programa *LWSERVER* comienza su proceso de

ocultamiento y despliegue de su código quedando a la escucha para comunicarse con el cliente. En la máquina atacante ejecuta el programa LWCLIENTE, inicia la consola de comando, desde allí se requieren los siguientes pasos para encontrar al programa *LWSERVER* y sincronizar la escucha:

Si se conoce la Ip de la víctima se introduce en la parte inferior derecha, si no se conoce la Ip de la víctima se realiza un escaneo con la opción “Scan” ubicada en la parte superior de la consola la cual abre un interfaz en donde se indica la posible red a la que se encuentra conectada la víctima. Localizada la víctima se procede a establecer conexión con el botón conectar ubicado en la parte inferior derecha, establecida la conexión como se observa en la figura 51, el cliente muestra el estado en la ventana de información.

Figura 51. Cliente LittleWitch.



Fuente: Autor

Para realizar la labor que facilita un troyano *LittleWitch* tiene las Opciones disponibles en el *LWCLIENTE*.

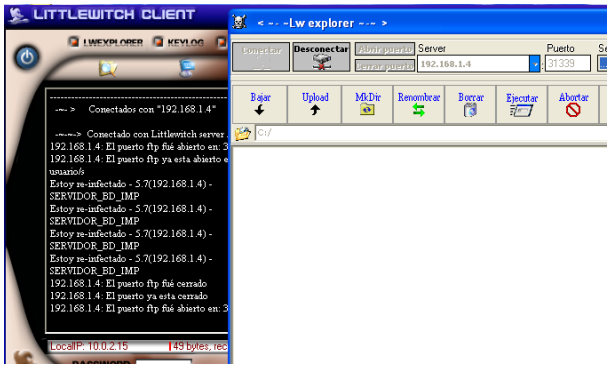
Como se aprecia en la figura 52 En la opción *Setup* se encuentra una ventana mediante la cual se configura el servidor para ser enviado a una posible victima por alguno de los diversos medios para compartir información.

Figura 52. Setup Cliente LittleWitch.

Fuente: Autor

Como se observa en la figura 53 la opción *LWExplorer* es para acceder al sistema de archivos de la víctima mediante el protocolo ftp, ejecutar comandos, crear, eliminar, subir y bajar carpetas y archivos.

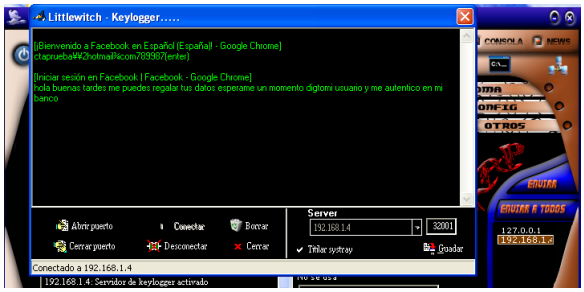
Figura 53. LWExplorer Cliente LittleWitch



Fuente: Autor

Como lo muestra la figura 54 la Opción *Keylog* captura toda la actividad del teclado de la víctima.

Figura 54. Keylog Cliente LittleWitch.



Fuente: Autor

La figura 55 muestra como con la opción *LWCHAT* se establece comunicación con el usuario del equipo víctima de forma síncrona.

Figura 55. LWchat Cliente LittleWitch.

Fuente: Autor

La opción dialogo como se observa en la figura 56 permite enviar una ventana de dialogo al equipo victima simulando determinado mensaje de alerta, etc.

Figura 56. LWdialogo Cliente LittleWitch

Fuente: Autor

La figura 57 muestra la opción broma, una serie de eventos que pueden generar molestia al usuario del equipo victima entre ellos: abrir la unidad de CDRom, ocultar la barra de tareas, bloquear el mouse y el teclado, cambiar el fondo del escritorio, reproducir sonidos, ocultar archivos, etc. Dentro de la opción otros: se encuentran eventos relacionados con el funcionamiento del sistema por ejemplo se interviene para terminar procesos, crear otros, obtener password guardadas, etc.

Figura 57. LWbroma LWotros cliente.

Fuente: Autor

Las Consecuencias causadas por el troyano *LittleWitch* son diversas entre ellas se encuentran:

El *LWSERVER* infecta al proceso Rundll.exe donde almacena la clave de registro**:** HKEY_LOCAL_MACHINE*SOFTWARE*\Microsoft*Windows*\CurrentVersion\Run. Simultáneamente se reproduce en %System%\Rundll.exe, genera un archivo %windir%\Usr.dat en donde se almacenan contraseñas cifradas, además se copia en C:*Windows*\System32. Cabe aclarar que este troyano afecta sistemas de *Windows* basados en *Windows* 95/98/Me/NT/2000/XP. Las consecuencias al usar estos sistemas operativos y estar infectado por el troyano constituyen una exposición a la información y la confidencialidad lo cual puede incurrir en un desastre informático como robo de información, modificación de la información, robo de contraseñas y violación a la privacidad, borrado de información, bloqueo o daño al sistema informático.

Para prevenir el ataque infección el troyano es preciso usar un antivirus confiable y mantenerlo actualizado analizar las unidades extraíbles cada vez que se utilicen desde fuentes externas al equipo, no descargar ni ejecutar archivos sospechosos provenientes de correo electrónico o desde carpetas compartidas, ante un mensaje sospechoso en pantalla no aceptar y consultar con el administrador del sistema, evitar compartir archivos de uso frecuente y con información de uso común e importante en carpetas de red, evitar descargar programas facilitadores de tareas desde paginas no seguras o de dudosa reputación. En el ANEXO C se documenta mediante un video tutorial el proceso de implementación del troyano LittleWitch. El video se encuentra disponible en https://www.dropbox.com/s/57fywtkp31rmrws/ANEXO%20C%20.mp4?dl=0

Se advierte que realizar este tipo de actividades de forma maliciosa sin autorización incurre en la violación de los artículos: 269 A. Acceso abusivo a un sistema informático, Artículo 269 C. Interceptación de datos informáticos, Artículo 269 E: Uso de *software* malicioso, Artículo 269 F. Violación de datos personales. Entre otros de la ley 1273 del año 2009.

En el proceso de investigación de herramientas que son considerablemente peligrosas a la seguridad de la información se hace a *Ruber ducky*, este dispositivo es un teclado programado en forma de USB que al momento de conectarse escribe en el equipo de forma automática, lanzando programas y herramientas que pueden estar en el equipo de la víctima o cargados en la memoria Micro SD que lleva incluida. En pocos segundos tendría acceso a información que podría subir automáticamente a un servidor FTP u otro sitio.[34]

La ingeniería Social continúa al siguiente nivel con una poco visible "unidad flash" escondida dentro de una USB *Rubber Ducky*. Todas las fijaciones incluidas.

Desde 2010 el USB *Rubber Ducky* ha sido un favorito para pruebas de penetración entre los hackers y profesionales de TI. Con orígenes en el concepto de la automatización de TI con sencillas pruebas utilizando un procesador incrustado, se ha convertido en una plataforma de Ataque de inyección tecleo de comandos con pleno derecho comercial. El *Rubber Ducky* USB ha capturado la imaginación de los piratas con su sencillo lenguaje de programación, *hardware* formidable, y el diseño encubierto. Casi todos los equipos incluyendo equipos de escritorio, portátiles, tabletas y Smartphone toman las entradas de los seres humanos a través de teclados. Es por eso que hay una especificación con el estándar USB ubicua conocida como HID (Human Interface Device) o dispositivo de interfaz humana. En pocas palabras, cualquier dispositivo USB que dice ser un teclado se detectará automáticamente y aceptado por la mayoría de los sistemas

[34] Maligno. (26 de Mayo de 2014). *USB Rubber Ducky: Un teclado malicioso como un pendrive*. Obtenido de http://www.elladodelmal.com/2014/05/usb-rubber-ducky-un-teclado-malicioso.html

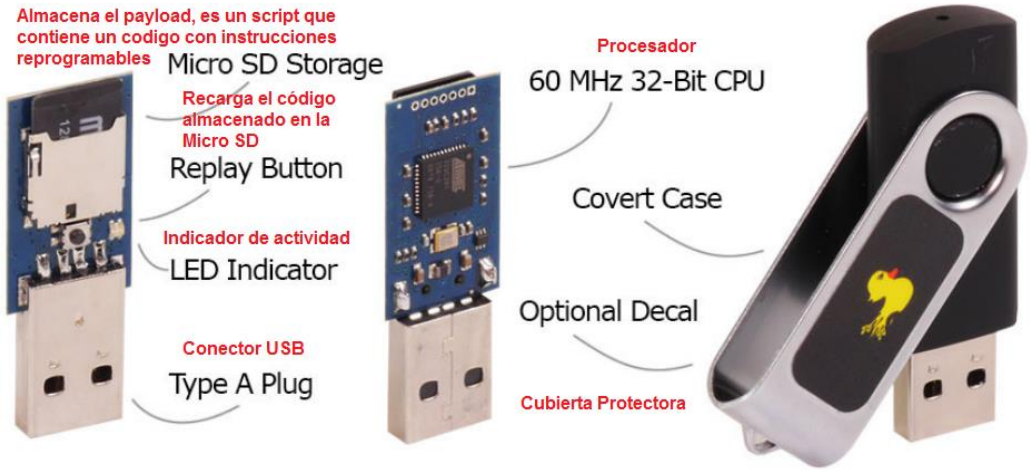
operativos modernos. Ya se trate de un dispositivo con *Windows*, Mac, Linux o Android.

Al tomar ventaja de esta confianza inherente con las pulsaciones de teclado con guion a velocidades más allá de 1000 palabras por minuto contra las medidas tradicionales, pueden ser dejados de lado por este nuevo dispositivo. El lenguaje de scripting de él USB *Rubber Ducky* se centra en la facilidad de uso. Escribir Payload es tan simple como escribir un archivo de texto en el bloc de notas. En este sentido se puede hablar también de sus características, entre ellas:

- Rendimiento incomparable, simplicidad y valor.
- Magnitud mayor capacidad de procesamiento y versatilidad. 60 MHz procesador rápido de 32 bits.
- Conector A USB.
- Memoria ampliable mediante Micro SD con un botón de repetición (Payload) de la carga.[35]
- La memoria USB simulada encierra todo un sistema de ataque contra los pilares de la seguridad informática y de la información. Todas sus características físicas se observan en la figura 58.

[35] HAKSHOP. (2015). *USB Rubber Ducky Deluxe*.

Figura 58. Partes Rubber Ducky.



Fuente: HAKSHOP. (2015). *USB Rubber Ducky Deluxe*.

Rubber Ducky es soportado por cualquier sistema operativo que reconozca la interfaz Humana a través de USB, es decir: *Windows*, Linux, Android, Mac, etc.

Un ataque se produce en el momento que se conecta el USB *Rubber Ducky* y se pulsa el botón, se descarga el Payload en la máquina y en modo comparativo es como si el atacante tuviera el teclado del equipo desde el cual puede escribir un código y ejecutarlo en el equipo. Esto quiere decir que si el usuario legítimo de una maquina descuida por un momento su equipo un atacante con la USB *Rubber Ducky* fácilmente la inserta y en cuestión de menos de 10 segundos habrá alguno o varios de los siguientes posibles ataques:

- Recolección de información del sistema operativo.

- Robar información importante de los navegadores de Internet.

- Robar y usar las cookies de las sesiones abiertas.
- Hacer capturas de pantalla del escritorio y carpetas importantes del sistema.
- Robar y utilizar las contraseñas de las conexiones WiFi de la víctima.
- Subir la información a través un servidor FTP.
- Agregar usuarios con permisos administrativos al equipo de la víctima.
- Borrar usuarios del sistema.
- Hacer Pharming de DNS.
- Infección del sistema descargando y ejecutando un binario de Internet.
- Crackear passwords del administrador en el sistema.
- Crear un Backdoor WiFi.
- Bloquear programas en el sistema operativo de forma sigilosa.

Luego de conocer estos ataque posibles desde la USB *Rubber Ducky* vale la pena pensar donde es posible cualquiera de los ataques mencionados, en ese sentido todo el tiempo se visitan oficinas en donde la computadora tiene expuestos los puertos USB, en bancos, oficinas del estado, oficinas de ventas y servicios y aun así no estén al frente de una persona con solo un momento que el usuario del

equipo lo abandone existe la posibilidad de ejecutar la conexión de la USB *Rubber Ducky* al equipo.

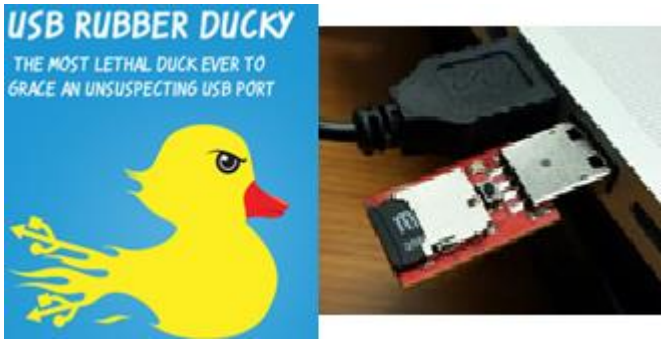
Para programar *Payload* la página *Web* que promociona y aloja todo el soporte técnico y comercial de USB *Rubber Ducky* ofrece también la herramienta o *Toolkit* para diseñar las cargas que se grabaran en la memoria micro SD de USB *Rubber Ducky* entre otras cosas: Se visita: http://duck*Toolkit*-411.rhcloud.com/Home.jsp
Este sitio *Web* le permite crear cargas útiles personalizadas para el USB *Rubber Ducky*. El sitio contiene 25 secuencias de comandos que puede seleccionar individualmente o combinar para hacer cualquier Payload.

- Scripts requieren:
- Acceso Administrativo.
- PowerShell para ser instalado.
- Símbolo del sistema para ser habilitado.
- Algunos Scripts requieren acceso a Internet.

Solo basta seguir las instrucciones que se dan en el sitio, que entre otras solicita en que forma quiere y donde almacenar el script. Luego de descargar el script y almacenarlo en la memoria micro SD de USB *Rubber Ducky* se conecta al equipo

víctima como se muestra en la figura 59 e inmediatamente con el botón se lanzara el script.[36]

Figura 59. Insertar Rubber Ducky.



Fuente: DUCKTOOLKIT. (2015). *Welcome to DuckTolkit*.

Para toma medidas y evitar un ataque de USB *Rubber Ducky* se debe saber que el ataque no se lleva a cabo vía USB de almacenamiento, se hace como si alguien estuviera escribiendo en un teclado USB, por eso no sirve desactivar el "autoplay" de las unidades USB. La forma que se puede utilizar para saber que un USB es realmente un HID (dispositivo de interfaz humana) USB, es realizando un script en PowerShell que enumere la lista de dispositivos HID para que alerte cuando uno nuevo dispositivo se haya conectado y se bloquee.[37]

Para Adquirir o comprar USB *Rubber Ducky* la oferta del producto se encuentra en la página http://hakshop.myshopify.com/products/usb-rubber-ducky deluxe?variant=353378649 alojada en el servidor de http://hakshop.myshopify.com localizada en Ottawa Canadá. Desde este sitio se

[36] DUCKTOOLKIT. (2015). *Welcome to DuckTolkit*.

[37] Prey, P. &. (2014). *Malicious USB devices*. Obtenido de http://www.irongeek.com

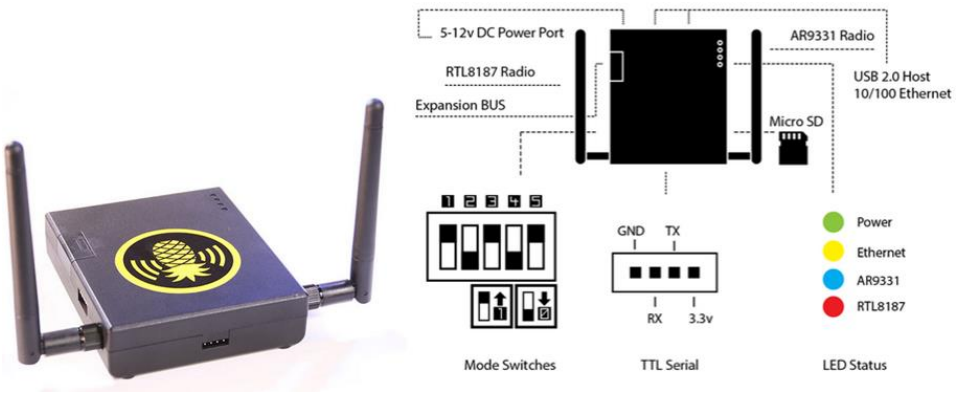
realiza todo el despliegue para comercialización del producto; en la página no se ofrece venta para Colombia, para comprar se deben registrar las direcciones de tarjetas de crédito, que son las mismas a donde se envía el dispositivo, el valor del dispositivo es de 43 dólares.

Entre otras herramientas que se son grandes amenazas para la seguridad informática se encuentra *WiFi Pineapple* equipo de escaneo de redes inalámbricas de gran potencia y despliegue de espectro, diseñado para penetrar en la infraestructura de las redes WiFi escaneadas y lograr tener acceso a los equipos que se encuentran conectados realizando diversos ataques que contemplan infiltraciones que ponen en riesgo la integridad, confidencialidad y disponibilidad de la información. Es un dispositivo único desarrollado por Hak5 con el objetivo de la auditoría en redes WiFi y pruebas de penetración. Desde 2008, *WiFi Pineapple* ha crecido hasta abarcar las mejores características de punto de acceso dudoso, *hardware* con único propósito, construido en interfaces *Web* intuitivas, opciones de despliegue versátiles, *software* poderoso y ayudas de desarrollo de *hardware* en un ecosistema de aplicaciones modulares y una creciente comunidad de Pentesting**.**

Por su Diseño y desempeño *WiFi Pineapple* es el único *hardware* inalámbrico con radios duales integrados a la medida para ataques inalámbricos avanzados. La generación Mark V se basa en un sistema de Atheros AR9331 eficiente en un chip (SoC), que integra un procesador MIPS 400 MHz, 16 MB de ROM y 64 MB de memoria RAM. Como lo muestra la figura 60 *WiFi Pineapple* Tiene instalado un radio Realtek RTL8187 con capacidad de monitoreo e inyección, un puerto de

expansión para memoria Micro SD, un banco de interruptores de modo auto-ataque configurables, un puerto host USB 2.0 y puerto Ethernet 10/100 .[38]

Figura 60. Estructura WiFi Pineapple.

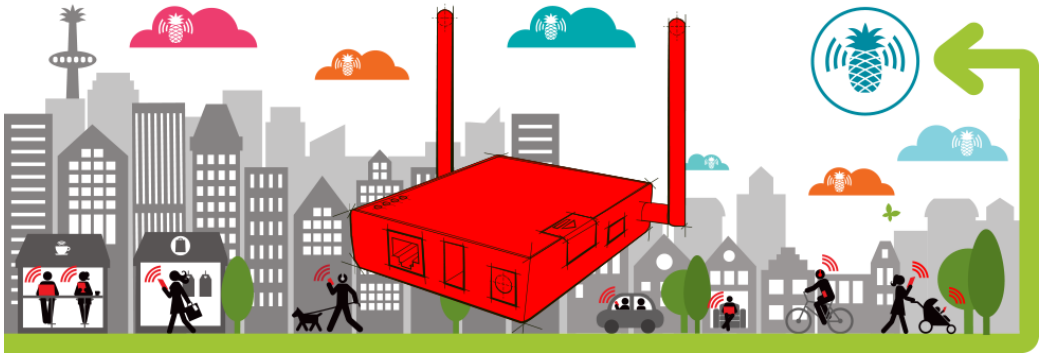


Fuente: HAK5. (2015). *WiFiPineapple.com*.

En el núcleo de *WiFi Pineapple* es una interfaz *Web* modular diseñada para simplificar la gestión y ejecución de ataques avanzados. Un conjunto de módulos proporcionan convenientes interfaces gráficas para aplicaciones de línea de comandos populares. Además, las intrusiones pueden ser desarrolladas directamente en el dispositivo mediante la interfaz de programación de aplicaciones (API) abierta. Una vez presentado para su revisión, la intrusión se incluirá en el portal en línea para todos los usuarios de *WiFi Pineapple*. En la figura 61 se muestra el despliegue de espectro de *WiFi Pineapple.*

[38] HAK5. (2015). *WiFiPineapple.com*.

Figura 61. Espectro WiFi Pineapple.



Fuente: Fuente: HAK5. (2015). *WiFiPineapple.com*.

En este sentido es preciso mencionar las características, el componente tecnológico del dispositivo y las especificaciones, entre ellas:

- *CPU: 400 MHz MIPS Atheros AR9331 SoC.*
- *Memory: 16 MB ROM, 64 MB DDR2 RAM.*
- *Disk: Micro SD support up to 32 GB, FAT or EXT, 2 GB Included.*
- *Mode Select: 5 DIP Switches - 2 System, 3 User configurable.*
- *Wireless: Atheros AR9331 IEEE 802.11 b/g/n + Realtek RTL8187 IEEE 802.11 b/g.*
- *Ports: (2) SMA Antenna, 10/100 Ethernet, USB 2.0, Micro SD, TTL Serial, Expansion Bus.*

- *Power: DC in Variable 5-12v, ~1A, 5.5mm*2.1mm connector, International Power Supply.*

- *Status Indicators: Power LED, Ethernet LED, Wireless 1 LED, Wireless 2 LED*

WiFi Pineapple es Un *hardware* muy potente que implementa diversos ataques en el espectro WIFI: La técnica más usada con este dispositivo es *MitM, Man in the Middle* (Hombre en el medio) *WiFi Pineapple*, monta una red inalámbrica y tiene varias herramientas para atacar a sus huéspedes como se observa en el diagrama de la figura 62.

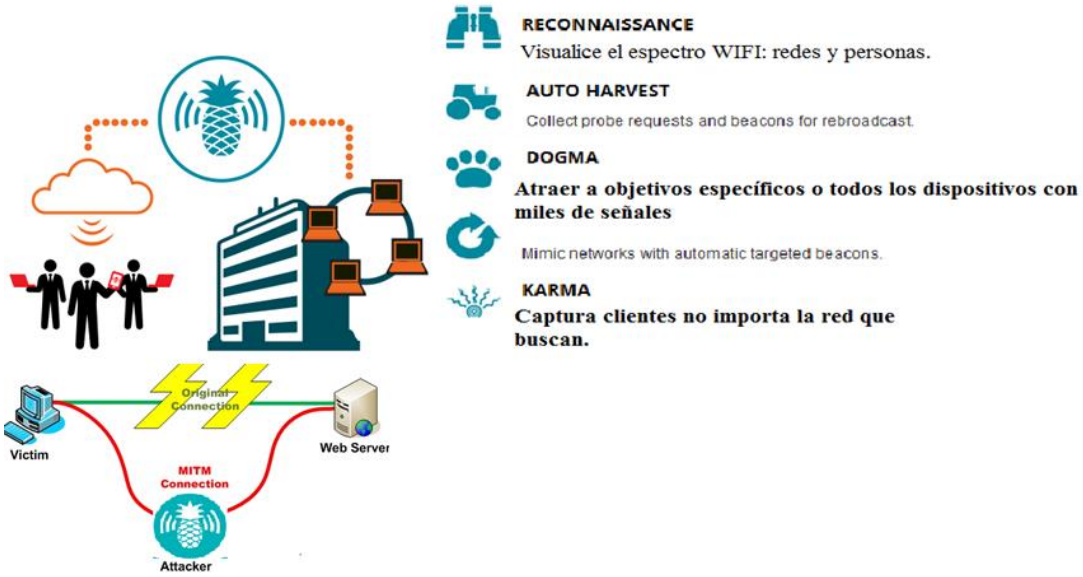
- Eavesdropping: o interceptación de los mensajes transmitidos.

- Ataques de sustitución.

- Ataque de modificación de paquetes.

- Ataque de denegación de servicios.

Figura 62. Man in the Middle Pineapple.



Fuente**:** Fuente: HAK5. (2015). *WiFiPineapple.com*.

A través PineAP. Al imitar completamente las redes preferidas, la suite **Rogue** Access Point avanzado y conecta los dispositivos inteligentes modernos en la conexión a la red *WiFi Pineapple*. Capaz de suplantar los puntos de acceso WIFI públicos y con garantía real y precisión el dispositivo, PineAP ofrece el probador de penetración con capacidades de adquisición de clientes objetivo.

En este escenario, el atacante puede controlar todo el tráfico de red que fluye entre una puerta de enlace de Internet y los clientes conectados, así como manipular estos datos en tránsito, como a través de los portales cautivos, spoofing DNS, re direccionamiento IP e incluso la sustitución de ejecutables en tránsito.

Entre las Medidas Para evitar un ataque de *WiFi Pineapple* seguir la recomendación más segura y precisa para todos los usuarios de redes

inalámbricas o WiFi, es conectarse siempre a una red segura protegida con contraseñas robustas con estándares WPA o WPA2 e encriptación AES y filtrado MAC; para las organizaciones a parte de la anterior recomendación es aconsejable implementar un servidor Radius**.**

Para Adquirir o comprar *WiFi Pineapple,* la oferta del producto se encuentra en la página http://hakshop.myshopify.com/collections/wifi-pineapple-kits alojada en el servidor de *http://hakshop.myshopify.com* localizada en Ottawa Canadá. Desde sitio se realiza todo el despliegue para comercialización del producto; en la página no se ofrece venta para Colombia, para comprar se deben registrar las direcciones de tarjetas de crédito, que son las mismas a donde se envía el dispositivo, el valor del dispositivo es de 100 dólares.

5.1.4.9 Tratamiento de las vulnerabilidades y amenazas detectadas. Mediante las pruebas de penetración (Pentesting), escaneo de la red, escaneo de puertos y pruebas de vulnerabilidades realizadas en el área de redes y sistemas de la Alcaldía de Pamplona - Norte de Santander, se realiza la identificación de los riesgos y su valor total mediante la matriz de riesgos. En el análisis se evidenciaran y se identificaron las vulnerabilidades y las amenazas, las cuales conforman la matriz de riesgos en donde se clasifican los recursos estudiados, los cuales están conformados por los activos analizados de donde se derivan las vulnerabilidades.

Para el proceso de determinación de la probabilidad de ocurrencia de las amenazas y el impacto con el objeto de establecer una priorización de las mismas, se debe implementar la siguiente metodología:

5.1.4.9.1 Matriz para el análisis de riesgo. La Probabilidad de Amenaza y la Magnitud del daño pueden tomar los valores y condiciones respectivamente, por lo tanto la valoración de los riesgos se realiza teniendo en cuenta los valores.

5.1.4.9.2 Probabilidad. Tiene una escala de 1 a 5, siendo 1 una probabilidad escasa de que se materialice la amenaza y 4 la máxima probabilidad.

5.1.4.9.3 Impacto. Tiene una escala de 1 a 5, siendo 1 un impacto menor con pocas consecuencias de afectación al recurso que lo recibió y 4 un impacto con consecuencias graves si la probabilidad también es alta.

5.1.4.9.4 Calculo del riesgo total. Para este proceso se debe identificar primero la magnitud del daño de cada uno de los elementos de información y también se debe identificar las probabilidades que ocurran las amenazas, se multiplica de manera individual cada probabilidad con la respectiva magnitud de impacto del daño, de esta manera se identifica el índice de riesgo que se obtiene en la escala de 1-16 de acuerdo a lo mencionado anteriormente.

En el proceso análisis del riesgo se usa la Matriz de asignación de los valores de acuerdo a cada vulnerabilidad encontrada relacionada con la amenaza y referente a los activos involucrados como se observa en el Cuadro 1, se determina el posible riesgo producto de la probabilidad que tiene de ocurrir por el posible impacto o consecuencia generada si se materializa la amenaza.

Cuadro 1. Valoración del riesgo

Recurso	Item	Vulnerabilidades	Amenaza	Riesgo	Probabilidad				Impacto				Valor Total
					1	2	3	4	1	2	3	4	
Software	1	Falta de seguridad en el sistema	Ataque a aplicaciones	Acceso a la información.	X						X		3
	2	Mal manejo de las políticas de Backup	Perdida de información	Perdida de información			X					X	**16**
	3	Usuarios con Privilegios inadecuados	Instalación de software sin permiso	Sanciones.		X				X			4
	4	Falta de instalación o actualización del software antivirus	Virus	Infección o ataque por virus	X						X		3
	5	Mala configuración o actualización de los sistemas de cortafuego y detección de software malicioso	Software Malicioso	Ataques informáticos, Publicidad no deseada.			X				X		**9**
	6	Forma inadecuada que generar y cifrar las contraseñas de los usuarios	Suplantación de Identidad	Robo de información.				X			X		**12**
	7	configuración inadecuada a las políticas de uso de internet	Acceso a páginas web prohibidas	Ataques informáticos, virus.				X			X		**12**

Cuadro 1. (Continuación)

Recurso	Item	Vulnerabilidades	Amenaza	Riesgo	Probabilidad				Impacto				Valor Total
Hardware	8	Falta de seguridad física e infraestructura	Acceso a personas no autorizadas	Robo de equipos				X				X	**16**
	9	Falla de equipos de refrigeración	Altas temperaturas	Daño de equipos críticos				X			X		4
	10	Mal uso de los recursos por parte de los operadores del sistema	Deterioro prematuro de hardware	Daño en periferia	X				X				1
	11	Escaso mantenimiento o equipos de mala calidad	Extrema suciedad, Altas temperaturas,	Daño de equipos críticos		X					X		6
	12	No existe un sistemas de respaldo de energía contra fallos	Fallas eléctricas	Daño de equipos críticos				X				X	**16**
	13	Mala gestión de incidentes	Fallas de equipos de cómputo	Ataques Informáticos			X				X		**9**

Cuadro 1. (Continuación)

Recurso	Item	Vulnerabilidades	Amenaza	Riesgo	Probabilidad				Impacto				Valor Total
Comunicaciones	14	Falta de mantenimiento del hardware de red	Deterioro de la conexión cableada	Perdida de las comunicaciones		X				X			4
	15	Mal manejo en la trasmisión de la información	Snifing	Robo de información			X				X		**9**
	16	Fallos en el cifrado de la información	Des encriptación de seguridad	Robo de información				X				X	**16**
	17	Falta de mantenimiento del hardware	Extrema suciedad, Altas temperaturas,	Falla de equipos de comunicaciones		X				X			4
	18	Red de datos abierta	Escucha de paquetes por terceros	Robo de información			X					X	**12**
	19	Interferencia electromagnética	Comunicación deficiente	Perdida en la transmisión de datos	X					X			2
	20	Falta de control de acceso	Acceso no autorizado al data center	Ataques a servidores				X				X	**16**

Cuadro 1. (Continuación)

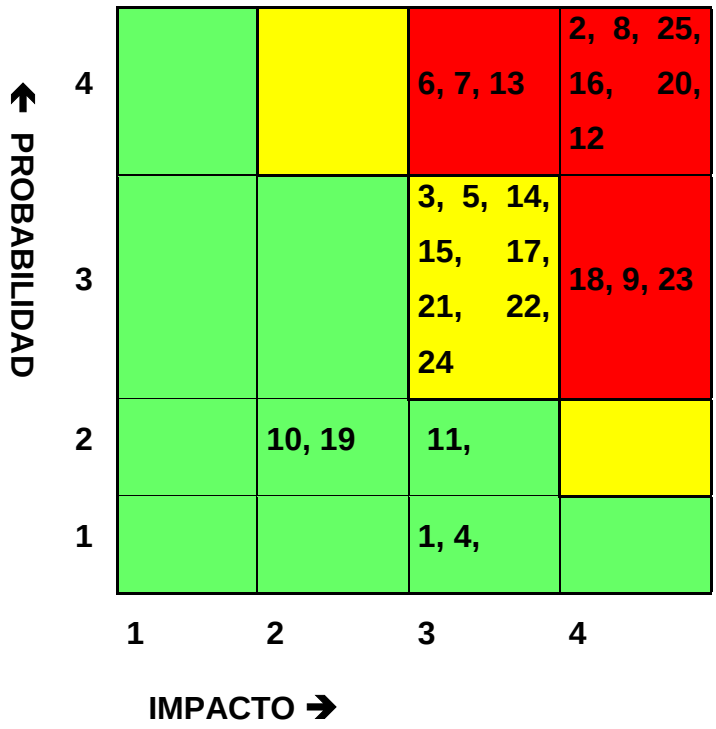
Recurso	Item	Vulnerabilidades	Amenaza	Riesgo	Probabilidad				Impacto				Valor Total
Seguridad Física	21	Falta de sprinklers	incendio	Daño de equipos críticos			X				X		**9**
	22	Falta de fijación de equipos	terremotos	Daño de equipos críticos		X			X				2
	23	Falta de piso falso	inundación	Daño de equipos críticos			X				X		**9**
	24	Bajos niveles de protección física en aéreas perimetrales	Saqueos	daños por vandalismo		X				X			4
	25	Falta de control de acceso	accesos no autorizados	Perdida de información o equipos				X				X	**16**

Fuente: el autor

5.1.4.9.5 Matriz de vulnerabilidades y amenazas de seguridad. En la tabla 6 como matriz se muestra el panorama del análisis de riesgos al área de redes y sistemas de la Alcaldía de Pamplona – Norte de Santander, donde los números dentro de los cuadro corresponde al número del ítem del cuadro 1, en el cual se definió el riesgo total al que se encuentran expuestos los recurso informáticos de la entidad.

Tabla 6. Matriz de Riesgos

MATRIZ DE RIESGOS



Fuente: ERB, M. (2008). *Gestión de Riesgo en la Seguridad Informática*.

5.1.4.9.6 Interpretación de los valores ubicados en la matriz. El Riesgo, se constituye como el producto de la multiplicación de la Probabilidad de la Amenaza de ser materializada por la Magnitud del daño que pueda causar esta amenaza; los valores están agrupados en tres rangos, contemplando la siguiente escala de valores:

- Bajo Riesgo = 1 – 6 (verde)
- Medio Riesgo = 8 – 9 (amarillo)
- Alto Riesgo = 12 – 16 (rojo)

Valor total (Riesgo) = Probabilidad de Amenaza X Magnitud de Daño o RT (riesgo total) = probabilidad x impacto

5.1.4.9.7 Determinación de la probabilidad. La probabilidad se deduce de todos los ítems que se encuentran ubicados en el área roja (Riesgo alto), son los riesgos que necesitan Mitigación y atención, mediante planes de mejoras; los ítems se representan en cuadro 2 muestra el filtrado el resultado con los ítems con riesgo alto, se verifica están involucrados activos de todos los recursos.

Cuadro 2. Valor total de cada riesgo

Recurso	**Ítem**	**Vulnerabilidades**	**Amenaza**	**Riesgo**	**Probabilidad**				**Impacto**				**Valor Total**
					1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	
Software	2	Mal manejo de las políticas de Backup.	Perdida de información	Perdida de información				**X**				**X**	**16**
	6	Forma inadecuada que generar y cifrar las contraseñas de los usuarios	Suplantación de Identidad	Robo de información.				**X**			**X**		**12**
	7	configuración inadecuada a las políticas de uso de internet	Acceso a páginas *Web* prohibidas	Ataques informáticos, virus.				**X**			**X**		**12**

Cuadro 2. (Continuación)

Recurso	Ítem	Vulnerabilidades	Amenaza	Riesgo	Probabilidad				Impacto				Valor Total
					1	2	3	4	1	2	3	4	
Hardware	8	Falta de seguridad física e infraestructura	Acceso a personas no autorizadas	Robo de equipos				**X**				**X**	**16**
	9	Falla de equipos de refrigeración	Altas temperaturas	Daño de equipos críticos			**X**					**X**	**12**
	12	No existe un sistemas de respaldo de energía contra fallos	Fallas eléctricas	Daño de equipos críticos				**X**				**X**	**16**
	13	Mala gestión de incidentes	Fallas de equipos de cómputo	Ataques Informáticos				**X**			**X**		**12**
Comunicaciones	16	Fallos en el cifrado de la información	Des encriptación de seguridad	Robo de información				**X**				**X**	**16**
	18	Red de datos abierta	Escucha de paquetes por terceros	Robo de información			**X**					**X**	**12**
	20	Falta de control de acceso	Acceso no autorizado al data center	Ataques a servidores				**X**				**X**	**16**
Seguridad Física	23	Falta de piso falso	inundación	Daño de equipos críticos			**X**					**X**	**12**
	25	Falta de control de acceso	accesos no autorizados	Perdida de información o equipos				**X**				**X**	**16**

Fuente: el autor

5.1.4.9.8 Lista de los controles definidos para los hallazgos encontrados. En la tabla 7 se encuentra los riesgos que necesitan Mitigación o Planes de actuación Correctivos, para tal fin se realiza una propuesta para cada uno; en este aspecto se tiene en cuenta el análisis que se ha realizado a cada recurso y el entorno en donde opera..

Tabla 7. Controles para el tratamiento

Recurso	Ítem	Vulnerabilidades	Amenaza	Riesgo	Control de Mitigación
Software	2	Mal manejo de las políticas de Backup	Perdida de informaci ón	Perdida de informac ión	Se hace necesario Instalar un servidor para almacenamiento del backup, establecido por medio de una política que contemple los periodos para realizarlo
	6	Forma inadecuada que generar y cifrar las contraseñas de los usuarios	Suplantac ión de Identidad	Robo de informac ión.	Implementar un proceso de cifrado de contraseñas utilizando herramientas de encriptación, almacenadas en un servidor protegido por medio de una política de seguridad.
	7	configuración inadecuada a las políticas de uso de internet	Acceso a páginas *Web* prohibida s	Ataques informáti cos, virus.	Se hace necesario Instalar un servidor proxy con el objetivo de filtrar el tráfico de información desde y hacia internet por medio de una política que contemple, los sitios *Web* restringidos y el filtrado de paquetes entrantes y salientes de la red

Tabla 8. (Continuación)

Recurso	Ítem	Vulnerabilidades	Amenaza	Riesgo	Control de Mitigación
Hardware	8	Falta de seguridad física e infraestructura	Acceso a personas no autorizadas	Robo de equipos, negación del servicio	Utilización de un sistema de vigilancia, monitoreado con cámaras de seguridad. Usar cerraduras seguras para evitar se abran los gabinetes que guardan los depósitos de red.
	9	Falla de equipos de refrigeración	Altas temperaturas	Daño de equipos críticos, inoperatividad de la Red	Construcción y adecuación del cuarto de comunicaciones por medio de una política que contemple las normas para la instalación y ubicación y operación de equipos de procesamiento de información, comunicación, energía.
	12	No existe un sistemas de respaldo de energía contra fallos	Fallas eléctricas	Daño de equipos críticos, inoperatividad de la Red	Corregir el acoplamiento del banco de baterías a la red de corriente regulada para tener disponibilidad de la UPS en caso de desconexión de la red comercial. Establecimiento de políticas de seguridad sobre el uso y conexión de equipos a la red eléctrica.
	13	Mala gestión de incidentes	Fallas de equipos de cómputo	Ataques Informáticos	Sensibilizar a todos los funcionarios y colaboradores sobre planes de documentación y llevado de formatos y reporte acerca de los incidentes que encierra el uso de bienes informáticos

Tabla 9. (Continuación)

Recurso	Ítem	Vulnerabilidades	Amenaza	Riesgo	Control de Mitigación
Comunica-ciones	16	Fallos en el cifrado de la información	Des encriptación de seguridad	Robo de información	Implementar un proceso de cifrado de contraseñas utilizando herramientas de encriptación, almacenadas en un servidor protegido por medio de una política de seguridad.
	18	Red de datos abierta	Escucha de paquetes por terceros	Robo de información	Implementar un proceso de configuración de equipos, estableciendo parámetros con un nivel alto: WPA2 algoritmo AES, clave compartida con números letras y caracteres. por medio de una política de seguridad para proteger la red de accesos no autorizados
	20	Falta de control de acceso	Acceso no autorizado al data center	Ataques a servidores	Construir e implementar una política de seguridad que contemple el proceso de autorización de ingreso y manipulación de bienes informáticos instalados en la entidad.
Seguridad	23	Falta de piso falso	inundación	Daño de equipos críticos	Construir e implementar una política de seguridad que contemple el plan para elevar los equipos instalados en el piso.
	25	Falta de control de acceso	accesos no autorizados	Perdida de información o equipos	Construir e implementar una política de seguridad que contemple los procesos de autorización de ingreso y manipulación de bienes informáticos.

Fuente: el autor

5.2 ASESORAMIENTO DE LA SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN EN EL ÁREA DE REDES Y SISTEMAS DE LA ALCALDÍA DEL MUNICIPIO DE PAMPLONA

Con las siguientes recomendaciones se busca sensibilizar y contribuir al saneamiento de las vulnerabilidades que están generando riesgo al óptimo funcionamiento y tratamiento de la información, asesorando sobre controles que disminuyan la probabilidad de los riesgos.

5.2.1 ISO 27002. Código de buenas prácticas. Publicado el 1 de julio de 2007. Esta norma no certificable, es una guía de buenas prácticas que detalla los objetivos de control y controles recomendables en los aspectos de seguridad de la información. En cuanto a seguridad de la información. La ISO 27002, contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Esta norma se encuentra publicada en Español a través de la empresa AENOR y en Colombia NTC-ISO IEC 27002), así mismo se pueden encontrar en Perú, chile, entre otros países latinoamericanos.[39]

Toda organización que desee resguardar la información debe implementar un Sistema de Gestión de seguridad de la Información (SGSI), que constantemente esté evaluando la organización en busca de soluciones de seguridad de la entidad tratando con esto la mejora continua en para los sistemas. Un SGSI basado en la Norma NTC/ISO 27001 brinda las pautas para implementar un sistema de esta calidad así como también busca dirigir a la organización hacia un clima general de seguridad en todos los niveles.

[39] español, E. p. (2012). *Gestión de Seguridad de la Información*. Obtenido de ISO27000.es: http://www.iso27000.es/sgsi.html

5.2.2 Riesgos que necesitan investigación y planes de prevención. Con el establecimiento de una política de seguridad informática y de la información y en base a la asesoría y recomendaciones para implementar las correcciones para Mitigar y corregir el factor d alto riesgo, colateralmente se mejora el panorama de los riesgo que están en un nivel intermedio de ocurrir por tanto el factor de riesgo disminuye considerablemente quedando al mismo nivel de los riesgos que necesitan Monitorización: Planes de actuación detectives.

5.2.3 Mejoramiento del panorama. Ante la cantidad de equipos con el sistema operativo *Windows* XP (27%) es urgente que la administración del área de redes y sistemas de la Alcaldía de Pamplona – Norte de Santander diseñe e implemente un plan de mejoramiento o escalamiento a nuevas versiones del sistema operativo sobre el cual se tenga soporte por parte de la casa diseñadora.

Con base en los resultados obtenidos en análisis de riesgos, se realizan las siguientes recomendaciones.

- Diseñar e implementar un plan para migrar a nuevas versiones el sistema operativo *Windows* XP; las nuevas versiones se deben configurar con todas las medidas de seguridad teniendo en cuenta la configuración más apropiada los cortafuegos, licencias de *software* y antivirus.

- Diseñar políticas de seguridad para mantener protegida la información almacenada y generada por causas de la gestión de cada dependencia.

- Implementar un servidor proxy configurado en base a las políticas de seguridad establecidas para el uso de los sistemas informáticos de la Alcaldía de Pamplona – Norte de Santander.

- Documentar cada proceso y procedimiento generado desde el área de soporte de la Alcaldía de Pamplona – Norte de Santander.

- Instalación y Configuración de un *Firewall* para diversos noveles de la entidad desactivando los puertos que no se utilicen.

- Implementar en la red un sistema de detección de intrusos IDS.

- Implementar políticas de gestión y creación de contraseñas seguras, mínimo de 8 caracteres, combinación de mayúsculas, minúsculas, números y caracteres especiales.

- Capacitar a los funcionarios sobre seguridad informática, hacer énfasis en la creación de claves seguras, política de seguridad sobre seguridad informática y de la información, Sensibilizar sobre cómo detectar ataque de ingeniera ingeniería social, como mantener el Antivirus actualizado.

- Adecuación del espacio donde se encuentran instalados los equipos de infraestructura tecnológica y energía.

- Mantenimiento correctivo y preventivo a la UPS en cuanto a limpieza de sus partes accesibles (solo personal calificado y autorizado)

- Revisión técnica de los circuitos eléctricos con el fin de restaurar aquellos que se encuentren desconectados y ampliar puntos nuevos para conectar los equipos que no se encuentran en la red de corriente regulada.

- Reestruración física y lógica de la red, cambiando o mejorando procedimientos y prácticas de administración de la red de datos optimizando el servicio.

- Usar el estándar de seguridad WPA2 claves compartidas en redes WiFi.

- Cambiar valores por defecto a valores con claves seguros.

6. CONCLUSIONES

Con los resultados obtenidos en el análisis de vulnerabilidades y el análisis de riesgos se lograron identificar las fallas de seguridad que tiene el área de redes y sistemas de la Alcaldía de Pamplona; ante las evidencias de las vulnerabilidades que conllevan amenazas fue posible identificar los controles para implementar y mitigar la situación de riesgo, En este sentido se concluye:

- Se realizó un diagnostico al área de redes y sistemas de la Alcaldía de Pamplona y fue posible identificar las vulnerabilidades que generan riesgo a los bienes informáticos.

- Mediante pruebas, testeo y análisis se lograron evidenciar vulnerabilidades presentes en la gestión de la información y en los bienes físicos que soportan la operatividad de área de redes y sistemas de la Alcaldía de Pamplona.

- Con la implementación, el uso de la matriz de riesgos y el análisis que genera para el tratamiento de los activos involucrados se determinó el riesgo total de cada uno de los ítems que conforman los recursos de área de redes y sistemas de la Alcaldía de Pamplona.

- Ante los resultados del análisis de riesgo fue posible recomendar y asesorar mediante los controles sugeridos y la formulación de una política de seguridad informática para remediar y prevenir las posibles amenazas derivadas de las vulnerabilidades encontradas y tratadas. Dentro de este ámbito también se sugiere mejorar continuamente las políticas de seguridad en la entidad con el fin de llevar un tratamiento continuo de los riesgos.

BIBLIOGRAFIA

ALCALDÍA DE PAMPLONA. (20 de Marzo de 2015). *Nuestra alcaldia*. Obtenido de http://pamplona-nortedesantander.gov.co/quienes_somos.shtml

ALCALDIA LA TEBAIDA QUINDIO - Quindio. (2013). *http://alcaldia724.com.* Recuperado el 30 de sep de 2014, de http://alcaldia724.com/politicadeseguridadlatebaida.pdf

ALCALDÍA MAYOR DE TUNJA. (enero de 2013). *Tunja-Boyaca.gov.co.* Recuperado el 29 de Septiembre de 2014, de http://tunja-boyaca.gov.co/apc-aa-files/495052435f494e464f524d4547454c54/politica-seguridad-alctunja.pdf

ARJONA, K. (4 de Febrero de 2014). *Actuar sobre los riesgos*.

BLOGS, T. (23 de Junio de 2009). *NetBIOS sobre TCP/IP y resolución de nombres cortos* . Obtenido de http://blogs.technet.com/b/latam/archive/2009/01/23/netbios-sobre-tcp-ip-y-resoluci-n-de-nombres-cortos.aspx

BORBÓN Sanabria, J. (2011). Buenas prácticas, estándares y normas. *REVISTA .SEGURIDAD, DEFENSA DIGITAL*, http://revista.seguridad.unam.mx/numero-11/buenas-pr%C3%A1cticas-est%C3%A1ndares-y-normas.

CSIRT. (21 de agosto de 2014). *Centro de Seguridad TIC de la Comunitat Valenciana.* Obtenido de NMAP 6: Listado de comandos: http://www.csirtcv.gva.es/sites/all/files/downloads/NMAP%206_%20Listado%20de%20comandos.pdf

DATOS, G. D. (Febrero de 2012). *Puertos Lógicos - GESTION DE REDES DE DATOS "SMT".* Obtenido de https://sites.google.com/site/gestionderedesdedatossmt/puertos-y-servicios/puertos-fisicos/puertos-fisicos

DUCKTOOLKIT. (2015). *Welcome to DuckTolkit*.

DURIVA. (1 de Marzo de 2015). *Diplomado de Informatica Forense Duriva.* Obtenido de Fuente: Penetration Test consultado de https://www.duriva.com/wp-content/uploads/2011/07/Diplomado-de-Informatica-Forense-Duriva.pdf

ERB, M. (2008). *Gestión de Riesgo en la Seguridad Informática*.

ESPAÑOL, E. p. (2012). *Gestión de Seguridad de la Información*. Obtenido de ISO27000.es: http://www.iso27000.es/sgsi.html

ESTANDARIT, C. (1 de Mayo de 2014). *Un Windows XP sin soporte, será full vulnerable 'Por Siempre' - CIOAL The Standard IT*. Obtenido de http://www.cioal.com/2014/05/01/ya-pusieron-descansar-windows-xp-las-vulnerabilidades-se-mantendran-sin-parches-por-siempre/

GESlCONSULTOR. (2015). *Sistema de Gestión de la Seguridad de la Información*.

GIDT, U. (21 de Noviembre de 2012). *Listado de Puertos usados por troyanos*. Obtenido de noticias de seguridad/78-puertos-troyanos: http://gidt.unad.edu.co/noticias-seguridad/78-puertos-troyanos

GOMEZ, R. D. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de Ingeniería*.

HAK5. (2015). *WiFiPineapple.com*.

HAKSHOP. (2015). *USB Rubber Ducky Deluxe*.

INSECURE org, N. (23 de Agosto de 2014). *Introducción al análisis de puertos*. Obtenido de http://nmap.org/man/es/man-port-scanning-basics.html

ISO 27000 Directory 2013. (2013). *The ISO 27000 Directory*. Recuperado el 29 de Octubre de 2014, de The ISO 27000 Directory: http://www.27000.org/iso-27002.htm

ISO27000.es. (2005). *El portal de ISO 27001 en Español*.

LEAL, R. (Enero de 2014). *Qué es norma ISO 27001.* Recuperado el 29 de Octubre de 2014, de Qué es norma ISO 27001: http://www.iso27001standard.com/es/acerca-de/

LEER, A. (2001). *Visión de los Lideres en la Era Digital.* Mexico: Mexico.

MALIGNO. (26 de Mayo de 2014). *USB Rubber Ducky: Un teclado malicioso como un pendrive*. Obtenido de http://www.elladodelmal.com/2014/05/usb-rubber-ducky-un-teclado-malicioso.html

MATTICA. (26 de Marzo de 2013). *El perfil del ciber delincuente en las empresas*. Obtenido de mattica.com/el-perfil-del-ciberdelincuente-en-las-empresas/

MICROSOFT. (21 de Agosto de 2009). */support.microsoft*. Obtenido de How to disable NetBIOS over TCP/IP by using DHCP server options Consultado en : http://support.microsoft.com/en-us/kb/313314

MICROSOFT. (15 de Agosto de 2013). Obtenido de The Risk of Running Windows XP after Support Ends April 2014: http://blogs.microsoft.com/cybertrust/2013/08/15/the-risk-of-running-windows-xp-after-support-ends-april-2014/

MICROSOFT. (2014). *Resolución de nombres de NetBIOS sobre TCP/IP y WINS*. Obtenido de https://support.microsoft.com/es-es/kb/119493/es

MICROSOFT, C. T. (15 de Agosto de 2013). *The Risk of Running Windows XP After Support Ends April 2014*.

MINTRABAJO. (11 de Septiembre de 2012). *Proceso de modernizacion de la Alcaldia de Medellin*. Recuperado el 29 de Octubre de 2014, de http://www.mintrabajo.gov.co/medios-septiembre-2012/1008-asi-sera-proceso-de-modernizacion-de-la-alcaldia-de-medellin.html

MIT.EDU. (2014). *Puertos comunes*.

Prey, P. &. (2014). *Malicious USB devices*. Obtenido de http://www.irongeek.com

RAULT, A. -M.-S.-N.-R.-F.-J.-S.-D.-R. (2010). *Seguridad Informatica - Ethcal Hacking.* Ediciones ENI.

REDACCION TECNOLOGIA, P. e. (23 de Abril de 2013). *Dos de cada 10 empresas, víctimas de robo de datos* . Obtenido de http://www.eltiempo.com/archivo/documento/CMS-12758292

REDIRIS, ©. (12 de Noviembre de 2008). *RedIRIS - Ataques remotos*. Obtenido de http://www.rediris.es/cert/doc/unixsec/node25.html

REPUBLICA, G. N. (5 de Enero de 2009). *Ley 1273 del 2009.* Obtenido de MinTic: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

ROYER, J.-M. (2004). *Seguridad en la informatica de empresa.* Barcelona: Ediciones ENI.

SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C. (2013). *http://www.alcaldiabogota.gov.co.* Recuperado el 29 de Septiembre de 2014, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51661

SECURITY, e. (2010). *Debilidades de seguridad comúnmente explotadas.* Obtenido de https://www.evilfingers.com/

SEGU, I. (28 de Octubre de 2014). *Seguridad Informática / Amenazas Lógicas - Tipos de Ataques*. Obtenido de http://www.segu-info.com.ar/ataques/ataques_monitorizacion.htm

SEGURIDAD, e. (Octubre de 2014). *Debilidades de seguridad comúnmente explotadas.* Obtenido de https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

SIERRA, L. P. (2013). *SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION.* BOGOTA: UNAD.

SISTEMAS, L. (12 de Marzo de 2014). *NetBIOS, Sistema de Entrada Salida Básica de Red* . Obtenido de http://www.investigacion.frc.utn.edu.ar/labsis/Publicaciones/InvesDes/Protocolos-NBI/doc/netbios.html

SOFTPERFECT. (16 de Marzo de 2015). *SoftPerfect Network Scanner*.

UNAD. (Julio de 2013). *datateca.unad.edu.co/contenidos/modulo-SGSI-233003_listo.pdf.* Recuperado el 29 de Octubre de 2014, de http://datateca.unad.edu.co/contenidos/233003/

UNAD. GONZALEZ, Y. C. (2013). *fundamentos de seguridad de la información.* Bogota: datateca UNAD.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, Mirian del Carmen Benavides, Francisco Solarte. (2012). *Módulo riesgos y control informático.* Bogota: Datateca UNAD.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. MORALES, J. (Diciembre de 2013). *Seguridad Avanzada en Redes de Datos.* Medellín: UNAD.

ANEXOS

ANEXO A. INVENTARIO DE ACTIVOS INFORMATICOS DE LA ALCALDIA PAMPLONA.

ANEXO B. LISTA DE PUERTOS EXPLOTADOS POR LOS TROYANOS

ANEXO C. VIDEO TUTORIAL IMPLEMENTACIÓN DEL TROYANO LITTLE WITCH