PROYECTO DE TRABAJO DE GRADO

PROTOCOLOS PARA LA MITIGACION DE CIBERATAQUES EN EL HOGAR. CASO DE ESTUDIO: ESTRATOS 3 Y 4 DE LA CIUDAD DE BOGOTÁ

CAMILO ALFONSO GUZMAN FLOREZ

CRISTIAN ANDRES ANGARITA PINZON

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C. NOVIEMBRE DE 2017

TABLA DE CONTENIDO

Introducción.....7

1 Generalidades.....9

1.1 Línea de Investigación.....9

1.2 Planteamiento del Problema.....9

1.2.1 Antecedentes del problema.....11

1.2.2 Pregunta de investigación.....13

1.3 Justificación.....14

1.4 Objetivos.....15

1.4.1 Objetivo general.....15

1.5 Cronograma.....16

1.6 Presupuesto.....16

2 Marcos de referencia.....22

2.1 Marco conceptual.....22

2.2 Marco teórico.....26

2.3 Marco jurídico.....33

2.4 Estado del arte.....34

3 Metodología 36

3.1 Fases del trabajo de grado 36

3.2 Instrumentos o herramientas utilizadas 37

3.3 Población y muestra 37

3.4 Alcances y limitaciones 38

4 Levantamiento de vulnerabilidades 39

5. Evaluación de riesgos 59

6. Desarrollo de protocolos 63

7. Validación de protocolo 66

8. Estrategia de comunicación 75

9. Bibliografía 76

LISTA DE FIGURAS

Pág.

FIGURA 1.LÍNEA DE TIEMPO DE ATAQUES QUE EXPLOTAN LA VULNERABILIDAD CVE-2015-2545 12

FIGURA 2.CRONOGRAMA DE TRABAJO. FUENTE: ELABORACIÓN PROPIA 16

FIGURA 3.USO DE ANTIVIRUS EN EQUIPOS DE CÓMPUTO. FUENTE: ELABORACIÓN PROPIA 39

FIGURA 4.RESULTADOS FRECUENCIA ACTUALIZACIÓN DE ANTIVIRUS. FUENTE: ELABORACIÓN PROPIA 40

FIGURA 5.RESULTADOS FRECUENCIA ESCANEO DE ANTIVIRUS. FUENTE: ELABORACIÓN PROPIA 41

FIGURA 6.RESULTADOS ACTUALIZACIÓN SISTEMA OPERATIVO Y PROGRAMAS. FUENTE: ELABORACIÓN PROPIA 41

FIGURA 7.RESULTADOS ACTIVIDADES REALIZADAS DESDE EL HOGAR. FUENTE: ELABORACIÓN PROPIA 42

FIGURA 8.RESULTADOS CONOCIMIENTO DE AMENAZAS. FUENTE: ELABORACIÓN PROPIA 43

FIGURA 9.RESULTADOS HERRAMIENTAS CONOCIDAS O UTILIZADAS EN EL HOGAR. FUENTE: ELABORACIÓN PROPIA 44

FIGURA 10.RESULTADOS FRECUENCIA DEL CAMBIO DE CONTRASEÑAS. FUENTE: ELABORACIÓN PROPIA 45

FIGURA 11.RESULTADOS SOBRE ANUNCIOS QUE NO CONOZCA AL ANUNCIANTE. FUENTE: ELABORACIÓN PROPIA 45

FIGURA 12.RESULTADOS DE ANÁLISIS CON ANTIVIRUS, MANUAL O AUTOMÁTICOS DE ARCHIVOS DESCARGADOS. 46

FIGURA 13.RESULTADOS SOBRE DESCARGA DE ARCHIVOS DE FUENTES FIABLES. FUENTE: ELABORACIÓN PROPIA 47

FIGURA 14.RESULTADOS SOBRE ARCHIVOS ANALIZADOS MANUAL O AUTOMÁTICAMENTE POR ANTIVIRUS. 48

FIGURA 15.RESULTADOS SOBRE DESCARGA Y APERTURA DE FICHEROS ADJUNTOS EN CORREOS DESCONOCIDOS. FUENTE: ELABORACIÓN PROPIA. 49

FIGURA 16.RESULTADOS SOBRE ANÁLISIS DE RESPUESTA O VISITA ENLACES DE CORREOS ELECTRÓNICOS SOSPECHOSOS.FUENTE:ELABORACIÓN PROPIA 49

FIGURA 17.RESULTADOS SOBRE EL INGRESO A REDES SOCIALES. FUENTE: ELABORACIÓN PROPIA 50

FIGURA 18.RESULTADOS SOBRE ENTREGA DE DATOS PERSONALES. FUENTE: ELABORACIÓN PROPIA 51

FIGURA 19.RESULTADOS SOBRE RECHAZO DE INVITACIONES A USUARIOS DESCONOCIDOS. FUENTE: ELABORACIÓN PROPIA 51

FIGURA 20.RESULTADOS SOBRE EL CIERRE DE SESIÓN AL REALIZAR PAGOS EN LÍNEA. FUENTE: ELABORACIÓN PROPIA. 52

FIGURA 21.RESULTADOS TECLEO DE LA DIRECCIÓN WEB DEL BANCO O TIENDA ONLINE. FUENTE: ELABORACIÓN PROPIA 53

FIGURA 22.RESULTADOS SOBRE LA CERTEZA QUE EXISTE SOBRE DESCARGAS DE ARCHIVOS ANALIZADOS MANUAL O AUTOMÁTICAMENTE. FUENTE: ELABORACIÓN PROPIA 54

FIGURA 23.HERRAMIENTA KALI LINUX 56

FIGURA 24.HERRAMIENTA PARA VULNERAR REDES INALÁMBRICAS WPA2 56

FIGURA 25.CAPTURA DE .CAP PARA UTILIZAR EL DICCIONARIO Y ROMPER LA CLAVE DE LA RED INALÁMBRICA. 57

FIGURA 26.RESULTADO ANÁLISIS RECONOCIMIENTO INGENIERÍA SOCIAL. FUENTE: ELABORACIÓN PROPIA 67

FIGURA 27.RESULTADOS ANÁLISIS DE USO DE HERRAMIENTAS DE MEJORA DE LA SEGURIDAD. FUENTE: ELABORACIÓN PROPIA..... 68
FIGURA 28.RESULTADO ANÁLISIS DE RIESGOS SOBREINFORMACIÓN SENSIBLE. FUENTE: ELABORACIÓN PROPIA 68
FIGURA 29.RESULTADO ANÁLISIS DE LA IMPORTANCIA DE MANTENER ANTIVIRUS Y SISTEMA OPERATIVO ACTUALIZADO. FUENTE: ELABORACIÓN PROPIA 69
FIGURA 30.RESULTADO ANÁLISIS DE CONTAR CON BACKUPS. FUENTE: ELABORACIÓN PROPIA 70
FIGURA 31.RESULTADO ANÁLISIS DE PROTOCOLOS CON CONTRASEÑAS SEGURAS. FUENTE: ELABORACIÓN PROPIA 70
FIGURA 32. RESULTADO DE LOS PROTOCOLOS MÁS SENCILLOS DE IMPLEMENTAR. FUENTE: ELABORACIÓN PROPIA 71
FIGURA 33. RESULTADO DE LOS PROTOCOLOS MÁS SENCILLOS DE IMPLEMENTAR. FUENTE: ELABORACIÓN PROPIA 72
FIGURA 34.RESULTADOS DE BENEFICIOS ADQUIRIDOS. FUENTE: ELABORACIÓN PROPIA..... 73

LISTA DE TABLAS

Pág.

TABLA 1.DESCRIPCIÓN DE LOS EQUIPOS QUE SE PLANEA ADQUIRIR (EN MILES DE $)..... 16
TABLA 2.DESCRIPCIÓN SALIDAS DE CAMPO..... 17
TABLA 3.DESCRIPCIÓN DE LOS MATERIALES, INSUMOS Y SERVICIOS TÉCNICOS (EN MILES DE $) 17
TABLA 4.DESCRIPCIÓN PUBLICACIONES Y PATENTES (EN MILES DE $) 18
TABLA 5.DESCRIPCIÓN MATERIAL BIBLIOGRÁFICO (EN MILES DE $)..... 18
TABLA 6. PRESUPUESTO GLOBAL DE LA PROPUESTA POR FUENTES DE FINANCIACIÓN (EN MILES DE $)..... 19
TABLA 7. DESCRIPCIÓN DE LOS GASTOS DE PERSONAL (EN MILES DE $). 19
TABLA 8. DESCRIPCIÓN DE LOS EQUIPOS QUE SE PLANEA ADQUIRIR (EN MILES DE $)..... 20
TABLA 10. DESCRIPCIÓN Y CUANTIFICACIÓN DE LOS EQUIPOS DE USO PROPIO (EN MILES DE $) 20
TABLA 11. DESCRIPCIÓN DEL SOFTWARE QUE SE PLANEA ADQUIRIR (EN MILES DE $). 20
TABLA 12. DESCRIPCIÓN Y JUSTIFICACIÓN DE LOS VIAJES (EN MILES DE $)..... 20
TABLA 13. VALORACIÓN DE LAS SALIDAS DE CAMPO (EN MILES DE $). 21
TABLA 14. MATERIALES Y SUMINISTROS (EN MILES DE $)..... 21
TABLA 15. BIBLIOGRAFÍA (EN MILES DE $). 21
TABLA 16.SERVICIOS TÉCNICOS (EN MILES DE $)..... 21
TABLA 17.IDENTIFICACIÓN DE ACTIVOS.FUENTE:ELABORACIÓN PROPIA 61

INTRODUCCIÓN

En la actualidad, dado el crecimiento y adquisición de componentes con acceso a internet, la tecnología ha presentado un auge rápido y continúo debido a la demanda focalizada en la compra de artículos o uso de servicios en la Internet lo que genera a su vez un aumento en la demanda del mercado tecnológico. Lo anteriormente dicho y teniendo en cuenta los múltiples servicios que se ofrecen a través de la red de internet, lo consolidan más que en una exclusividad en una necesidad de primer nivel (PANDA SECURITY, 2008) y requiere contar con una identificación de incidencias a las que se encuentra expuesto y no se dimensionan en la utilización de estos servicios, como por ejemplo: pagos a través de internet, Phishing, Malware tales como (Troyanos, Ramsomware en portales financieros, Rootkids, Gusanos, Spam, Spyware, Adware, y Scam) Botnets. (Periodico El Tiempo, 2017)

Por estas vulnerabilidades se proposu un documento que contenga protocolos permitiendo preparar a una persona del común para mitigar la probabilidad de un ciberataque en su hogar identificando herramientas y brindando conocimientos para su protección (Antivirus, anti espías, cortafuegos, control parental, anti Phishing, protección web, analizador de Url) y así minimizar los vectores de ataque. (PANDA SECURITY, 2008)

1 GENERALIDADES

1.1 LÍNEA DE INVESTIGACIÓN

Por el contexto en el que se desarrolla este trabajo de investigación suscrito alrededor de la necesidad de conocer las conductas que desarrollan en el ámbito del hogar en nivel de seguridad en los últimos dos años debido al aumento en cobertura de acceso a internet en los años en estratos 3 y 4 de la ciudad de Bogotá compete esta temática en la línea de "Software inteligente y convergencia tecnológica" avalada por la Universidad Católica de Colombia", logando identificar las vulnerabilidades y riesgos a los que se encuentran expuestos, brindando información, contramedidas de protección posibilitando tomar las acciones preventivas y correctivas en el ambiente técnico y tecnológico buscando un proceso de mejora de la seguridad de los hogares.

1.2 PLANTEAMIENTO DEL PROBLEMA

En la actualidad no es difícil determinar la confianza que cada persona pretende tener cuando accede a servicios de tecnología desde la comodidad del hogar, se podría decir que se debe gracias a que el entorno que que lo rodea es conocido y con ello se determina que las actividades normales como: consulta de correo, acceso a redes sociales o por citar otro ejemplo realizar pagos de servicios financieros; son actividades sin ningún peligro o se precisa que tantas noticias de brechas de inseguridad se presentan en empresas con gran envergadura, indudablemente son los más buscados, pero a nivel del hogar se han evidenciado un alto crecimiento en el consumo de la Internet y adquisición de dispositivos para conectarse a él, datos que se pueden evidenciar en los enlaces que se relacionan con información respecto a situaciones que se han presentado en el ámbito de los hogares.

El siguiente articulo indica como reconocer un perfil falso indicándonos “Por eso, muchas redes están **utilizando mecanismos de verificación**” (Natour, 2017) no dar click en enlaces de redes sociales de desconocidos, evitar abrir enlaces enviados al correo electrónico por remitentes sospechosos, o aceptar la entrada a sitios emergentes que aparecen en páginas web que no se navegan frecuentemente. (ELTIEMPO.COM, 2017) Con ello debemos preguntarnos ¿Cuáles son los riesgos a los que me encuentro expuesto al realizar estas actividades?, la respuesta a esta pregunta puede causar confusión pero es la clave, ya que la mayor causa de exposición a estas actividades son los eventos asociados debido a conductas inadecuadas; al final las personas seguimos siendo el eslabón más débil. Se podrán implementar controles y desplegar herramientas con la más alta tecnología siendo conocedores en el tema, pero si en el entorno no siempre somos quienes usan el acceso a la red de internet ese conocimiento queda aún lado si las conductas que nosotros aplicamos no son retroalimentadas a toda persona que conviva en nuestro mismo entorno.

Dados estos casos se evidencia que una persona del común puede ser atacada en su hogar a raíz de esto se ha generado la necesidad de ayudar a un sector de personas en un inicio, pero con la gran certeza que podría ser difundida para que la seguridad sea parte de todos impactando de buena manera cualquier nicho poblacional.

Los antecedentes del desarrollo actual coincide con los acontecimientos de la sociedad de la información, las redes entre computadoras y el fenómeno “Internet”, cuya expansión ha configurado la quinta dimensión de la guerra moderna y ha afectado sensiblemente la vida cotidiana de los diversos actores en el mundo global. De hecho, su estudio se convierte en una

tarea obligada para la conducción político-estratégica de la defensa de las naciones. (Armadas, 2017)

También se toma la siguiente referencia, en primer lugar estudiamos el nacimiento de un nuevo espacio delictivo el "ciberespacio" y todas sus amenazas, en una segunda parte se ve la reacción que este fenómeno ha provocado en las naciones y organizaciones internacionales en dirección a determinar y estudiar todos estos delitos, sus causas, métodos y reacciones, para poder combatirlos desde el aspecto legal (legislación española, europea e internacional) y a partir de aquí finalizar mostrando la visión estratégica de defensa de los estados, estudiando como ejemplos las líneas de actuación que utiliza España y Europa para contrarrestar su efecto destructivo en la sociedad actual. ((España)), 2017)

1.2.1 Antecedentes del problema

Las investigaciones acerca de la delincuencia cibernética y las amenazas a la ciberseguridad se centran en gran medida en mecanismos de defensa de la cooperación y las infraestructuras nacionales, dejando de lado en gran medida uno de los eslabones más débiles en este sistema el cual proviene de los dispositivos utilizados en las hogares conectados a la web, por tal motivo al realizar una revisión literaria al respecto, se evidenció que a nivel nacional son prácticamente nulos los trabajos investigativos realizados acerca de esta temática; sin embargo a nivel internacional ya se han adelantado algunos estudios con este propósito destacando la publicación de (Arabo, 2015) quien adelantó una revisión acerca de los retos a los cuales se enfrentan los hogares frente a la seguridad cibernética puesto que, así como los dispositivos

ofrecen más características y funcionalidad, también introducen nuevos riesgos. Por otra parte, (Noam Ben-Asher, 2015) establecieron los efectos del conocimiento de la seguridad cibernética en la detección de ataques.

Se respaldan estos antecedentes con los siguientes resultados dados por Kaspersky en el 2016.

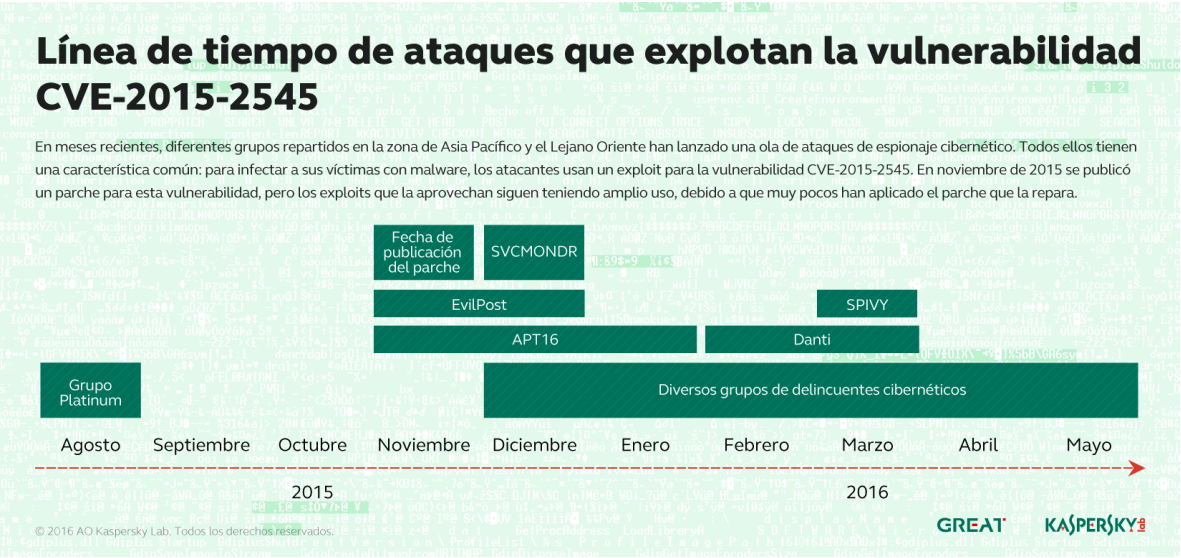

Figura 1.Línea de tiempo de ataques que explotan la vulnerabilidad CVE-2015-2545

Una de las formas más directas que los ciberpiratas usan para ganar dinero son los ataques selectivos contra los clientes de bancos. Por lo general, los atacantes utilizan la ingeniería social para engañar a sus víctimas e inducirlas a revelar su información personal o a instalar programas maliciosos que recopilan información personal (como contraseñas) que la víctima usa para acceder a su cuenta bancaria. En 2016, las soluciones de Kaspersky Lab bloquearon los intentos de implementar programas maliciosos capaces de robar el dinero a través de la banca en línea en 2 871 965 dispositivos; un aumento del 46% en 2015 (1 966 324).

La siguiente URL permite identificar el estudio realizado de un experto de la empresa Kaspersky lo cual fue realizar el ataque a su propio hogar para probar el nivel de seguridad https://securelist.lat/iot-el-da-que-ataqu-mi-propia-casa/72452/.

Se nombran algunas consecuencias que se evidenciaron a causa de la práctica ejecutada.

- Acceder al dispositivo; por ejemplo, acceder a los archivos en los dispositivos de almacenamiento en red.
- Lograr acceso administrativo al dispositivo, no sólo en la interfaz administrativa, sino también a nivel del sistema operativo.
- Poder transformar/modificar el dispositivo para mis intereses personales (puerta trasera, trampolín, etc.).

Puerta trasera, también conocida como backdoor, es una manera de ingresar a un programa, al servicio en línea o a un equipo informático entero, lo cual es permitir o dejar una entrada en la programación de una aplicación lo cual permitirá al atacante tener acceso al quipo infectado.

1.2.2 Pregunta de investigación

¿Cómo mitigar riesgos asociados a ciberataques en el hogar para estratos 3 y 4 de la ciudad de Bogotá?

1.3 JUSTIFICACIÓN

La presente investigación expone la información que actualmente se desconoce con los ciberataques en el ámbito del hogar, con el objetivo de concientizar a las personas en estrato 3 y 4 de la ciudad de Bogotá de las amenazas como son (Scam logrando provocar una estafa realizando pagos a través de internet, Spyware, Adware, Botnets, familia de Malware tales como Ramsomware, gusanos, Rootkids) como también brindar el conocimiento básico para ser aplicados los controles que son esenciales.

Se desarrolló un protocolo que brinda pasos para la mitigación de un ciberataque en el hogar, dirigido a los estratos 3 y 4 de la ciudad de Bogotá donde se encuentra el mayor incremento en la cobertura y utilización de acceso a internet. (Secretaria Distrital De Planeacion) (Periodico El Tiempo, 2017).

Dando a conocer por medio del documento, protocolos que permitan mejorar la seguridad de los hogares colombianos en la ciudad de Bogotá entre los estratos 3 y 4 culturizando a las personas de las vulnerabilidades y herramientas para aplicar controles que mitigaran los riesgos.

Por esta razón, con la información recolectada se estima que el desarrollo de la guía para su entrega será de 7 meses corriendo desde la recopilación de información mediante encuestas realizada a los estratos 3 y 4 para determinar el uso del internet en el hogar, esto también aporta a la documentación ya que en la actualidad no se encuentra mucha información a nivel nacional, por ello la importancia del desarrollo de la investigación que permite la entrega de información desarrollada con estándares que son aplicables en el entorno empresarial pero se han adoptado

para que sean implementados en el ámbito del hogar, logrando demostrar las conductas inapropiadas en el uso de la tecnología pero controladas con protocolos que mitigan las vulnerabilidades, para lograr beneficios a las personas del entorno tales como; conocimientos en seguridad, importancia de la divulgación de las políticas para su correcta implementación, uso responsable de la tecnología, herramientas de libre uso para su protección, importancia de contar con copias de respaldo, etc.

1.4 OBJETIVOS

1.4.1 Objetivo general

Proponer un protocolo para la mitigación de ciberataques en el hogar de estratos 3 y 4 de la ciudad de Bogotá.

Objetivos específicos

- Realizar un levantamiento de vulnerabilidades en el hogar a la población en estrato 3 y 4 de la ciudad de Bogotá a través de una encuesta y de un laboratorio hacking.

- Elaborar una evaluación de los riesgos tomando como base las vulnerabilidades y amenazas encontradas.

- Desarrollar protocolos que mitiguen los riesgos evaluados .

- Validar el protocolo a través de una encuesta.

1.5 CRONOGRAMA

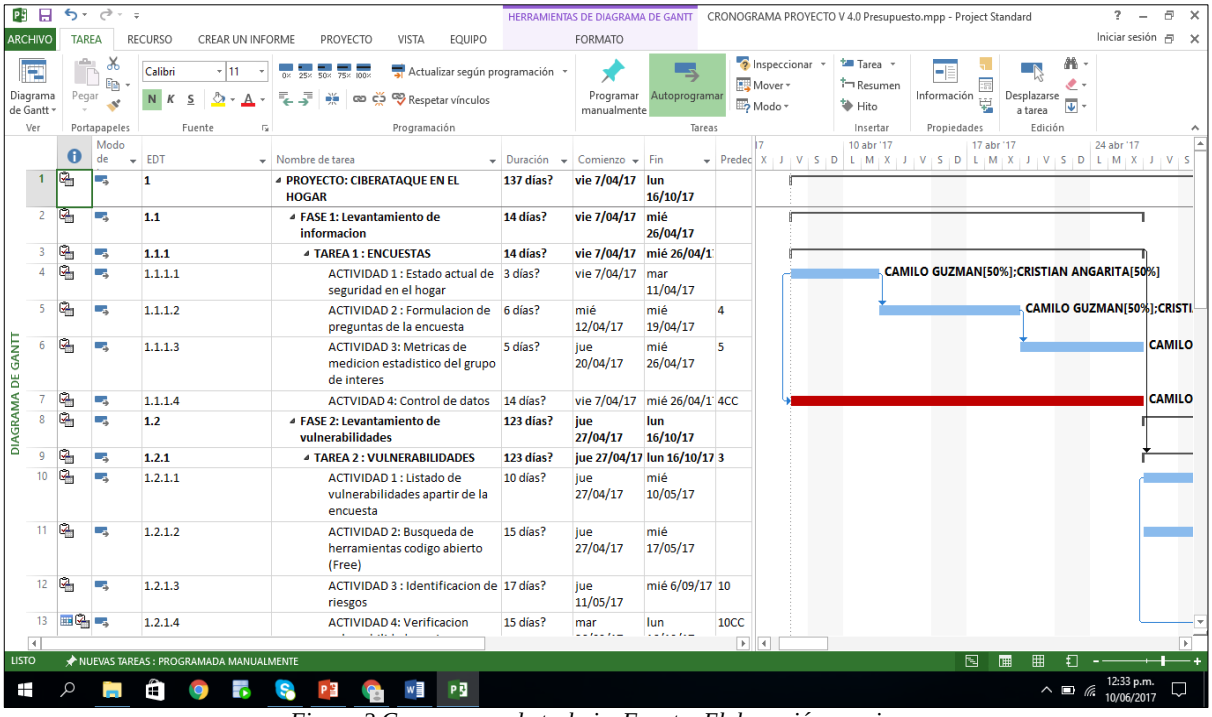

Figura 2.Cronograma de trabajo. Fuente: Elaboración propia

1.6 PRESUPUESTO

- **Equipos:**

UNIDADES	DESCRIPCIÓN	VALOR
1	Portátil	$ 700.000
1	Portátil	$ 700.000
1	Impresora	$ 550.000
TOTAL		**$ 1950.000**

Tabla 1.Descripción de los equipos que se planea adquirir (en miles de $)..

- **Viajes: N/A**

- **Salidas de campo:**

DESCRIPCIÓN	VALOR MENSUAL
Trasporte urbano Transmilenio	$66.000
Trasporte urbano SIPT	$60.000
Vale taxis	$32.000
TOTAL	**$ 158.000**

Tabla 2.Descripción salidas de campo

- Materiales, insumos y servicios técnicos:

SERVICIO MENSUAL	VALOR MENSUAL
Internet	$ 60.000
Papelería	$ 9.000
Insumos impresora	$ 35.000
TOTAL	**$ 104.000**

Tabla 3.Descripción de los materiales, insumos y servicios técnicos (en miles de $)

- Publicaciones y patentes:

DESCRIPCIÓN	VALOR
Publicación articulo revista indexada	$ 84.000
TOTAL	**$ 84.000**

Tabla 4.Descripción publicaciones y patentes (en miles de $)

- Material Bibliográfico:

DESCRIPCIÓN	VALOR
Suscripción revista tecnológica	$ 70.000
TOTAL	**$ 70.000**

Tabla 5.Descripción material bibliográfico (en miles de $)

RUBROS	VALOR UNITARIO	VALOR TOTAL
PERSONAL	$ 22.000	$ 22’176.000
EQUIPOS	$ 1.250.000	$ 1’950.000
SOFTWARE	N/A	N/A
MATERIALES	$ 104.000	$ 104.000
SALIDAS DE CAMPO	$ 12.200	$ 158.000
MATERIAL BIBLIOGRÁFICO	$ 70.000	$ 70.000
PUBLICACIONES Y PATENT	$ 84.000	$ 84.000
SERVICIOS TÉCNICOS	$ 129.000	$ 129.000
VIAJES	N/A	N/A

CONSTRUCCIONES	N/A	N/A
MANTENIMIENTO	N/A	N/A
ADMINISTRACION	N/A	N/A
TOTAL	**$ 1’671.200**	**$ 24’671.000**

Tabla 6. Presupuesto global de la propuesta por fuentes de financiación (en miles de $).

INVESTIGADOR EXPERTO/ AUXILIAR	**FORMACIÓN ACADÉMICA**	**FUNCIÓN DENTRO DEL PROYECTO**	**DEDICACIÓN Horas/semana**	**VALOR**
Investigador	Ingeniero de sistemas	Ejecutor/ consultor	30 horas / semana	$ 22.000
Investigador	Ingeniero de sistemas	Ejecutor/ Consultor	30 horas/ semana	$ 22.000
TOTAL				$ 660.000

Tabla 7. Descripción de los gastos de personal (en miles de $).

EQUIPO	JUSTIFICACIÓN	VALOR TOTAL
PC portátil	Para trabajar en casa y oficina	$ 700.000
Impresora	Imprimir documentación acerca proyecto	$ 550.000
TOTAL		**$ 1’250.000**

Tabla 8. Descripción de los equipos que se planea adquirir (en miles de $).

EQUIPO	VALOR TOTAL
2 PC Portátil	$ 1’400.000
Impresora	$ 550.000
TOTAL	**$ 1’950.000**

Tabla 9. Descripción y cuantificación de los equipos de uso propio (en miles de $)

SOFTWARE	JUSTIFICACIÓN	VALOR TOTAL
N/A	N/A	N/A

Tabla 10. Descripción del software que se planea adquirir (en miles de $).

LUGAR / NO. VIAJES	JUSTIFICACIÓN	PASAJES ($)	ESTADÍA ($)	TOTAL DÍAS	TOTAL
N/A	N/A	N/A	N/A	N/A	N/A

Tabla 11. Descripción y justificación de los viajes (en miles de $).

ITEM	COSTO UNITARIO	#	TOTAL
Pasaje Transmilenio	$ 2.200	140	$ 308.000
Pasaje SITP	$ 2.000	140	$ 280.000
Taxi	$ 8.000	1	$ 224.000
TOTAL			**$ 812.000**

Tabla 12. Valoración de las salidas de campo (en miles de $).

MATERIALES	JUSTIFICACIÓN	VALOR TOTAL
Resma papel	Impresión de documentos	$ 9000
Insumos impresora	Imprimir los documentos	$ 35.000
TOTAL		**$ 44.000**

Tabla 13. Materiales y suministros (en miles de $).

ÍTEM	JUSTIFICACIÓN	VALOR TOTAL
Suscripción revista	Información de nuevas tecnologías emergentes	$ 490.000
TOTAL		$ 490.000

Tabla 14. Bibliografía (en miles de $).

TIPO DE SERVICIOS	JUSTIFICACIÓN	VALOR TOTAL
Internet	Consultas, publicación y realización encuesta	$ 420.000
TOTAL		$ 420.000

Tabla 15.Servicios Técnicos (en miles de $).

2 MARCOS DE REFERENCIA

Los autores se hallan en libertad de incluir u omitir los marcos mostrados en esta plantilla de ejemplo.

2.1 MARCO CONCEPTUAL

Ramsomware: Es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados. El virus lanza una ventana emergente en la que nos pide el pago de un rescate, dicho pago se hace generalmente en moneda virtual (bitcoins, por ejemplo). (PANDASECURITY)

Phishing: Consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude. (PANDA SECURITY)

Spam: Se llama **spam** o **correo basura** a los mensajes no solicitados, no deseados o de remitente desconocido y que son sumamente molestosos. (seguridadpc., s.f.)

Troyanos: Aunque es menos "peligroso" que un virus, los troyanos deben tenerse muy encuentra, se puede definir de una persona que accede por un agujero en nuestro sistema (puerta trasera) por el cual acceden a nuestro ordenador, desde otro, en busca de información que

poseamos como claves de cuentas bancarias o inclusive pueden tomar el control de nuestro PC y eliminar archivos, cerrarnos programas, no pudiendo manejar el ratón, etc. (Dursula, s.f.)

Malware: Es la abreviatura de Malicious software y este término engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento; dentro del grupo de Malwares podemos encontrar términos como, por ejemplo, Virus, Troyanos, Gusanos (Worm), keyloggers, Botnets, Ransomwares, entre otros. (iiemd, s.f.)

Spyware/Anti espía: Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. (Masadelante)

Botnets: Es el nombre genérico que denomina a cualquier grupo de PC infectados y controlados por un atacante de forma remota. Generalmente, un hacker o un grupo de ellos crea un botnet usando un malware que infecta a una gran cantidad de máquinas. (Kaspersky)

Gusano: Un gusano es un programa que se reproduce por sí mismo, que puede viajar a través de redes utilizando los mecanismos de éstas y que no requiere respaldo de software o hardware (como un disco duro, un programa host, un archivo, etc.) para difundirse. Por lo tanto, un gusano es un virus de red. (CCM)

Rootkids: es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el

acceso al sistema, a menudo con fines maliciosos. (Infospyware)

Crackers/Hackers: Los hackers y crackers son individuos de la sociedad moderna que poseen conocimientos avanzados en el área tecnológica e informática, pero la diferencia básica entre ellos es que los hackers solamente construyen cosas para el bien y los crackers destruyen y cuando crean algo es únicamente para fines personales. (Informatica hoy)

Antivirus: Es un programa de seguridad que se instala en la computadora o dispositivo móvil para protegerlo de infecciones tipo malware, virus, troyanos, o spyware. (SANS Security The Human)

Cortafuegos/Firewall: Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. (Etapa)

Control Parental: Es una característica especialmente útil para padres y responsables educativos que desean impedir que niños o adolescentes puedan acceder a páginas Web inapropiadas. (Panda Security)

Analizador URL: Son herramientas que permiten comprobar la seguridad de las páginas web individuales que está a punto de visitar o enlaces sospechosos que se reciben en un correo electrónico. (Karmany)

Protocolos de seguridad: Puede ser un documento o una normativa que establece cómo se debe actuar en ciertos procedimientos. De este modo, recopila conductas, acciones y técnicas que se consideran adecuadas ante ciertas situaciones. (Definicion).

Comercio Electrónico: Es el proceso de compra, venta o intercambio de bienes, servicios e información a través de las redes de comunicación. Representa una gran variedad de posibilidades para adquirir bienes o servicios ofrecidos por proveedores en diversas partes del mundo. (Profeco).

Administración Electrónica: La Administración electrónica o e-Administración es el conjunto de soluciones que permite a la ciudadanía y a las empresas poder relacionarse con las administraciones públicas a través de medios electrónicos. Podría asimilarse a la creación de una "ventana virtual" única que permite la prestación de los servicios públicos por parte de las administraciones a la ciudadanía y a las empresas. (https://www.xunta.gal/administracion-electronica-definicion-antecedentes-vantaxes?langId=es_ES, s.f.)

Banca Online: La **banca** electrónica, o también llamada **banca** virtual o **online**, es un servicio prestado por las entidades financieras que tiene como misión permitir a sus clientes realizar operaciones y transacciones con sus productos de forma autónoma, independiente, segura y rápida a través de Internet. (simple, s.f.)

Scam: Manera de identificar fraudes, estafas, timos a través de internet fundamentados en la práctica de un engaño cuyo objetivo final es obtener un beneficio económico a costa de una

víctima catalogado penalmente como un delito.

2.2 MARCO TEÓRICO

El desarrollo de esta investigación aborda las estrategias y protocolos para implementar en los hogares colombianos en estrato 3 y 4 de la ciudad de Bogotá para mitigar los ciberataques en el hogar, para ello se abordó la información de los controles desarrollados para contener este tipo de incidencias.

Los ciberataques han sido una gran problemática a lo largo de los años y se han venido incrementando conforme al crecimiento en el uso de la tecnología con múltiples plataformas tecnológicas que soportan multiplicidad de servicios entre los más importantes nombramos organizaciones tales como: **Shapchat** red social que sufrió un impacto alrededor de 4.5 millones de nombres y números móviles comprometido; **EBay** sector de compras reconocida donde su base de datos fue comprometida con 145 millones de sus compradores; **Icloud** sector de entretenimiento donde se vieron comprometidas cuentas de celebridades; **Inception Framework** sector público que sufrió una operación de ciberespionaje; **Presidencia de la republica Senado de la republica Gobierno en línea y los Ministerios del interior de Justicia de Cultura y de Defensa** sector publico dejando por fuera por varias horas sus páginas web, este último generó la necesidad de abordar las incertidumbres, los riesgos, las amenazas y vulnerabilidades de manera más proactiva; debido a ello el gobierno expidió en el año 2011 el documento CONPES 3701 (Consejo Nacional de Política Económica y Social, República de Colombia,Departamento Nacional de Planeación, 2011) lineamientos de política de ciberseguridad y ciberdefensa para contrarrestar el incremento de las amenazas informáticas y desarrollar un marco normativo que

permitiera proceder ante este tipo de eventualidades con cooperación internacional. (CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, 2016)

Gracias a esta iniciativa se conformó el grupo de respuesta a emergencias cibernéticas de Colombia (coICERT) del Ministerio de defensa Nacional, el comando conjunto cibernético (CCOC) del comando general de las fuerzas militares de Colombia, el centro cibernético policial (CCP) de la policía nacional de Colombia, el equipo de respuesta a incidentes de seguridad informática de la policía nacional (CSIRT PONAL), la Delegatura de protección de datos en la Superintendencia de Industria y Comercio, la Subdirección técnica de seguridad y privacidad de tecnologías de información del Ministerio de Tecnologías de la Información y las Comunicaciones, el Comité de Ciberdefensa de las Fuerzas Militares, y las Unidades cibernéticas del Ejercito Nacional y la Fuerza Aérea Colombiana para contrarrestar el incremento de las amenazas informáticas que afectan significativamente al país. (CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, 2016)

En la actualidad los hábitos del consumidor en américa latina se encuentran principalmente en las tendencias de los ecommerce con porcentajes del 20 % de compras online, pero con cifras en alza para el 2018 con ventas por unos 8500 millones de dólares a una taza del 30% anual de acuerdo con el instituto latinoamericano del comercio electrónico posicionándose como uno de los rubros más importantes para la economía de la región. Debido a la importancia que los gobiernos impulsan para la inclusión tecnológica se provee que en 2025 alcanzara en un 85 % de la población de los cuales 459 millones serían usados para internet móvil, es decir, 2.5 millones de dispositivos contactados con un promedio de 3.5 dispositivo por persona aumentando el número

de usuarios y compradores en el mercado por la facilidad y los precios ofrecidos pero con ello la aumento en fraudes o recepción de ataques para vulnerar la información privada de una persona, las plataformas de este tipo cuentan con contramedidas especializadas que se auto protegen pero se deben cambiar conductas de quienes van a darle uso para no verse comprometidos y entender a utilizar la tecnología con responsabilidad con controles fácil de implementar que se brindaran en el desarrollo de la presente investigación. (acis.org.co, 2017).

Por otra parte el uso de la tecnología que sin duda alguna es un diario vivir para gran parte, se encuentran como tendencia y en gran preocupación para muchos padres de hoy en día, está en sus hijos y el uso al que le pueden dar al internet, fenómeno que con los años va en aumento y que se encuentra expuesto por cibercriminales que se encuentran a diario al acecho, imprescindiblemente son usuarios que en promedio pasan alrededor de 6.5 horas al día utilizando computadores, teléfono, Tablet u otro dispositivo digital, en este punto se ha preguntado ¿Qué tan seguros se encuentran sus hijos al utilizar los dispositivos? o las consecuencias que se adquieren al no saber si no se está consciente de ello.

Se conocen por temas de psicología que una persona en desarrollo físico y emocional como son los niños y adolescentes son blancos predilectos y se han presentado casos que impactan en gran medida por su caracterización tales como suicidios o abrumadas por fenómenos como el ciber bulling y por ello es importante tener conocimientos en la materia para lograr no por medio de la represión sino la buenas prácticas que debieran tenerse en un entorno familiar para el uso adecuado de las tecnologías y en gran medida dar a conocer a que se encuentran expuestos ya que la divulgación de políticas son el pilar para desarrollar las actividades cotidianas de manera más

segura. (ACIS, 2017).

De igual manera es importante además de tener conocimientos sobre la manera en que se debe utilizar de forma responsable la tecnología también es de gran importancia las leyes, como por ejemplo la ley de protección de datos personales (habeas data) 1581 de 2012 que nos asegura que nuestra información dispersa en sin números registros de base de datos archivos públicos o privados solo pueda ser utilizada por la entidad para desarrollo de su objeto de razón social únicamente con la autorización del propietario de dicha información. En este punto es considerable que se conozca que con esta ley también cuentan con derechos de conocer, actualizar y rectificar dicha información personal y que existen lineamientos establecidos para que pueda imponer una queja ante la Superintendencia Financiera de Colombia colocando un alto en el entorno financiero que es donde más se vulnera este derecho, que sus reportes en centrales de riesgo sean eliminados cuando el usuario se encuentre a paz y salvo o que dicha información no puede ser utilizada divulgada a entidades del mismo entorno o como de utilizar información para ofrecer créditos de consumo o cursos de idiomas; debe tenerse claro que son dueños de su información personal y tener cuidado con los datos que se brindan como por ejemplo en una encuesta sin identificar con qué fin va a ser utilizada. (Senado, 2012)

De acuerdo a los objetivos planteados en la investigación se utiliza la especificación de los estándares ISO 27001 y la ISO 27002 para el desarrollo de análisis de riesgos requeridos que se alinean a las necesidades del mismo.

ISO 27001

La NTC ISO 27001 es una norma colombiana que permite a las organizaciones asegurar al mismo tiempo la confidencialidad y la integridad de la información que ellos poseen.

La versión vigente es la ISO 27001:2013 es el referente mundial a la hora de implementar sistemas de gestión de seguridad de la información. El objetivo de implantar la NTC ISO 27001 es el de evaluar los riesgos y ejecutar los controles existentes para lograr la mitigación de ellos. (Autores que

Con la ISO 27001, se puede lograr un aumento competitivo, el cual mejora la imagen de la marca o del sector al que se le está aplicando.

A continuación, se nombra brevemente la estructura que la ISO 27001:

- **Objeto y campo de aplicación**: Permite establecer las orientaciones necesarias para el uso, finalidad y aplicación de la normativa.
- **Referencias normativas**: Se indica que es importante relacionar los documentos con la seguridad de la información.
- **Términos y Definiciones**: En este punto se indica la terminología que se planteara a utilizar a lo largo de la norma.
- **Contexto de la Organización**: Permite que una organización conozca el contexto en el que se desarrollan las actividades internas como externas, de esta forma es

posible conocer las necesidades de los clientes y adoptar medidas para cubrir esas necesidades.

- **Liderazgo**: Este punto permite tener un grado de obligación de hacer que todo el personal relacionado con la información participe activamente en la implementación de la norma ISO 27001.
- **Planificación:** En este punto se debe tener claridad de los objetivos y la manera de cómo llegar a materializarlos.
- **Soporte:** Se destaca que el SGSI funcione con éxito, se deben tener los recuro, además de contar con la información y comunicación adecuada.
- **Operación:** El cumplimiento de todos los requisitos de un SGSI a lo largo de la planificación, implementación y control de los procesos, llevando a cabo la validación de los riesgos y su posterior tratamiento.
- **Evaluación del desempeño:** Este punto hace mención a la importancia en realizar los seguimientos, mediciones, análisis, evaluación, auditoria para asegurar que funciona según lo planificado.
- **Mejora:** El último punto establece la estructura para la mejora continua, es decir, que sean capaces de detectar no conformidades y saber qué medidas aplicar para ponerle solución, esto conlleva l mejoramiento continuo del SGSI (Colombia, s.f.)

Si se habla de la ISO 27001 de la mano va la ISO 27002 la cual es el complemento para esta norma.

ISO 27002

ISO 27002 establece un parámetro para las buenas prácticas, que determinan una serie de objetivos y controles que se integran con la ISO 27001 con relación en el tratamiento de los riesgos.

La ISO 27002 se encuentra estructurada en 14 capítulos, en la cual encontramos las áreas en las que se deben considerar para garantizar la seguridad de la información, continuación se nombran esos 14 capítulos a tener en cuenta.

1. Políticas de la seguridad de la información.
2. Organización de la seguridad de la información.
3. Seguridad relativa a los recursos humanos.
4. Gestión de activos.
5. Control de acceso.
6. Criptografía
7. Seguridad física y del entorno
8. Seguridad de las operaciones
9. Seguridad de las operaciones
10. Seguridad de las comunicaciones
11. Adquisición, desarrollo y mantenimiento de los sistemas de información.
12. Relación de proveedores.
13. Aspectos de seguridad de la información para la gestión de la continuidad de negocio.
14. Cumplimiento.

(Gestión, s.f.)

ISO 27005

La ISO 27005 se encuentra estructurada con 14 numerales de control de seguridad de la información que en su conjunto contiene más de 35 de categorías de seguridad principal y 114 controles para realizar el análisis evaluación tratamiento y reducción de los riesgos proporcionado directrices para gestionar los riesgos en una organización apoyándose con las pautas de la ISO 27001 y 27002 facilitando la implementación satisfactoria de la seguridad de la información con base en el enfoque de gestión del riesgo.

Todas las actividades para la gestión del riesgo en la seguridad en la información se describen posteriormente en los siguientes numerales:

- establecimiento del contexto
- valoración del riesgo
- tratamiento del riesgo
- aceptación del riesgo
- comunicación del riesgo
- monitoreo y revisión del riesgo ((ICONTEC), 2009-08-19)

2.3 MARCO JURÍDICO

La legislación pertinente a la temática se basa en el Documento CONPES 3701, se creó la Comisión Nacional Digital y de Información Estatal, mediante el Decreto 32 de 201311 del Ministerio de Tecnologías de la Información y las Comunicaciones. Instancia que tiene el objeto

de ejercer la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para interacción con los ciudadanos, y el uso efectivo de la información en el Estado colombiano. (Consejo Nacional de Política Económica y Social, República de Colombia,Departamento Nacional de Planeación, 2011).

2.4 ESTADO DEL ARTE

En los últimos tres años podemos definir que la seguridad de los hogares ha ido en mejora debido a diferentes casos que se han presentados en todo el mundo y que ha replicado en cada parte de él, en este tiempo el aumento de los sistemas informáticos y electrónicos da cabida a nuevos ataques cibernéticos y a fraudes en la red. El cibercrimen, el ciberterrorismo y la ciberguerra han pasado a ser tres de las más importantes amenazas que parecen acechar a las sociedades. Por tal motivo, en este artículo hemos analizado el uso que están haciendo de la red, los terroristas, los delincuentes y los servicios de seguridad de los Estados, y las medidas que se están adoptando para evitar en la medida de lo posible estos ataques y actividades delictivas. (Facultad de Ciencias Políticas y Sociología / Universidad Complutense de Madrid, 22 de junio de 2012).

Se enuncia el caso encontrado, un récord de "denegación de servicio" fue efectuado contra el sitio de noticias de seguridad KrebsOnSecurity. Durante 24 horas, los usuarios registrados no pudieron tener acceso. Una semana después, un ataque similar contra otro Sitio destrozó el registro en 1.1 terabytes por segundo. Estos Ataques cada vez más grandes fueron posibles gracias a la llamada Internet de cosas, Debido a un diseño de seguridad deficiente, una

red de dispositivos Que pueden ser controlados y coordinados por hackers. Los hackers utilizan estos dispositivos para dirigirse a un sitio web específico o Servicio de internet con inundaciones de tráfico falso. (www.americamagazine.org, 2016).

Sin duda alguna la tecnología es de gran importancia y ha traído consigo grandes beneficios, pero también se han adquirido unos riesgos inherentes que traen consigo impacto de gran magnitud, como en el año 2008 a través de Facebook se identificó un caso de infiltración en el que a través de amenazas intimidatorias trataron de extorsionar con publicaciones en el muro utilizando palabras de fuerte calibre. Sin duda este tipo de situaciones en un principio podría no causar ninguna exaltación pero de acuerdo al grupo investigativo de delitos informáticos gran parte de las actividades que se veían cometiendo en el mundo físico han evolucionado al entorno virtual, detrás de cada uno de estos mensajes que podrían verse sin mucha atención se encuentran bandas organizadas enfocadas a realizar ventas ficticias, estafas nigerianas, falsas loterías, suplantación de páginas bancarias o portales de información, correos con cadena de ofertas de trabajo que resultan ser secuestro y en este caso en particular generando pánico con imágenes falsas redistribuyendo en muchos de sus contactos esta información para forzar al pago para finalizar con el delito. Es importante saber que existe un canal de atención a este tipo de delitos y lo importante que es tomar evidencia o identificar el sitio web donde se haya realizado la suplantación para que los investigadores logren identificar de manera más efectiva el autor material. (EL ESPECTADOR, 2008)

Con base en varios escenarios, pretendemos presentar algunos de las amenazas más representativas para el entorno de la casa Inteligente/Red inteligente. Se calificaron amenazas detectadas según los objetos de seguridad establecidos y se evalúa su impacto en la seguridad del sistema. (Nikos Komninos, 2014)

3 METODOLOGÍA

La metodología que se utiliza en el suscrito trabajo de investigación está basada en enfoque cuantitativo que nos permite realizar la recolección y análisis de información para el iniciar el desarrollo de los objetivos planteados a través de una encuesta identificando los riesgos y vulnerabilidades como las conductas desarrolladas en el hogar aplicando fórmula matemática que permite completar la media poblacional requerida y apoyar el uso estadística para tabular la información.

La finalidad de la investigación es utilizar el tipo de investigación Descriptiva que permite presentar el estado de seguridad de un nicho poblacional relacionando las conductas desarrolladas para así identificar los riesgos y vulnerabilidades que se encuentran expuestos para brindar a través de unos protocolos las contramedidas que mitiguen la exposición; esto beneficia a personas de los hogares brindando una clara imagen de los riesgos y controles que ayudaran a asegurar la información sensible utilizada en las actividades diarias, los protocolos aumentaran la confianza y culturización de las personas en casos de robos, perdidas, fraudes y usos indebidos de la información en la red.

3.1 FASES DEL TRABAJO DE GRADO

Las faces realizadas partiendo de los objetivos a realizar

- FASE 1 PLANEACION
- FASE 2 EJECUCION
- FASE 3 VERIFICAICON

- FASE 4 CONTROL

3.2 INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

- Formula estadística para seleccionar una tasa de población desconociendo el tamaño para realizar encuesta.
- Formularios de google para generar y tabular la información estadística de la encuesta.
- Metodología gestión de riesgos ISO 270005
- Pentesting utilizando Kali utilizando Crunch para generar diccionario y el Aircrag para penetrar las redes inalámbricas

3.3 POBLACIÓN Y MUESTRA

Cálculo del tamaño de la muestra desconociendo el tamaño de la población.

Muestra de población se encuentra centralizada en estratos 3 y 4 de la ciudad de Bogotá a través de la siguiente formula:

$$n = \frac{Z_a^{\,2} \times p \times q}{d^2}$$

En donde:

Z = nivel de confianza,

P = probabilidad de éxito, o proporción esperada

Q = probabilidad de fracaso

D = precisión (error máximo admisible en términos de proporción)

3.4 ALCANCES Y LIMITACIONES

- El tiempo para el desarrollo de las actividades de cada fase en el cronograma sea insuficiente para la elaboración de la guía.
- La elaboración del documento con protocolos para mitigación de los ciberataques en el hogar focalizada a los estratos 3 y 4 de la ciudad de Bogotá.
- Las herramientas para mitigar las vulnerabilidades deben ser de licenciamiento libre para aumentar el interés por parte de los usuarios

4 LEVANTAMIENTO DE VULNERABILIDADES

Informe de vulnerabilidades, se determina el estado actual de seguridad a través de una primera encuesta utilizando la herramienta de Google Forms y que a continuación se relaciona con su tabulación respectiva de la apoyada con un laboratorio de penteting para estratos 3 y 4 de la ciudad de Bogotá.

De acuerdo con la encuesta realizada a continuación presentamos los resultados tabulados.

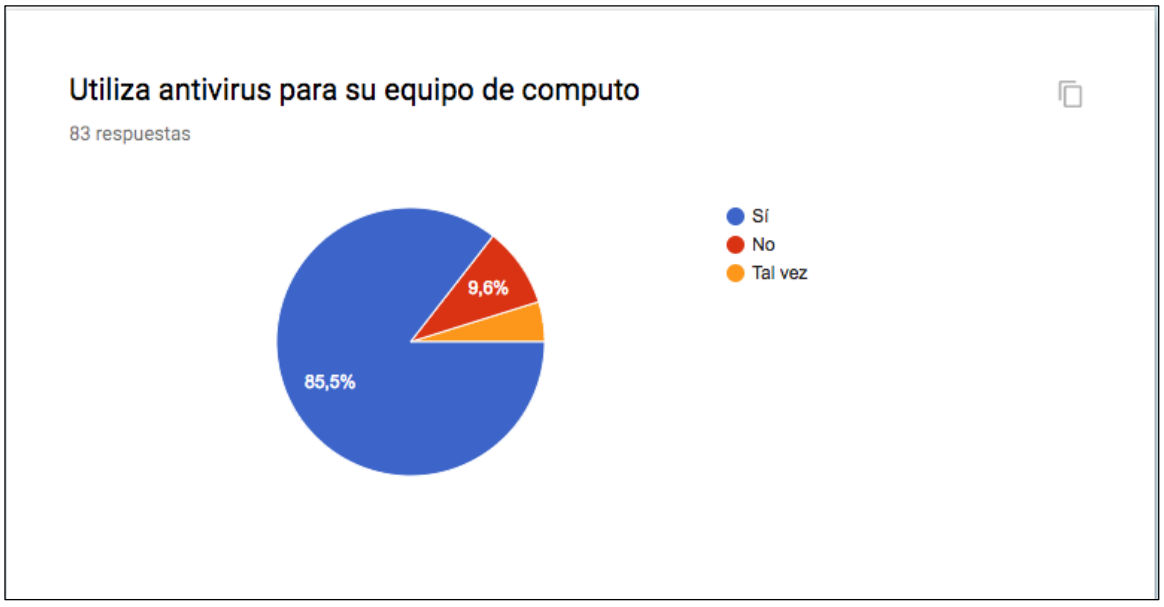

Figura 3.Uso de antivirus en equipos de cómputo. Fuente: Elaboración propia

Según los resultados el 85,5% de las personas en los estratos 3 y 4 de la ciudad de Bogotá D.C. utilizan antivirus en sus equipos de cómputo conectados a internet contra un solo un 9,6% de la población no que no lo utiliza.

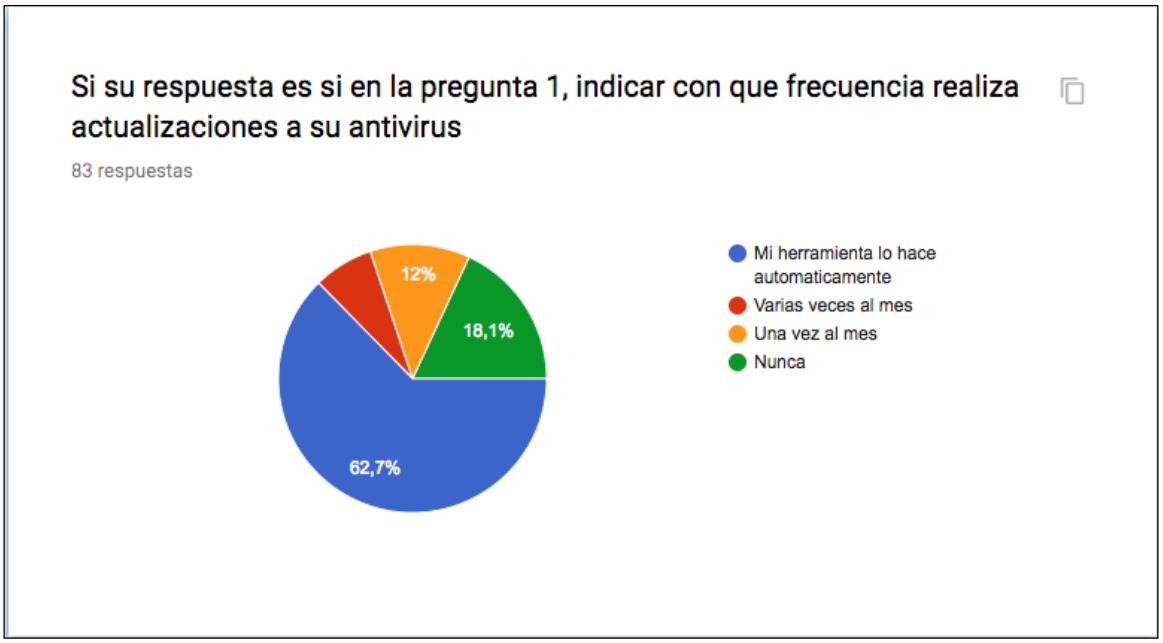

Figura 4.Resultados frecuencia actualización de antivirus. Fuente: Elaboración propia

De acuerdo a la primera pregunta se ha determinado que solo el 62,7% de las personas espera a que su Antivirus se actualice de forma automática, y que existe un 18,1% nunca efectúan la actualización ni automática ni manualmente a su antivirus.

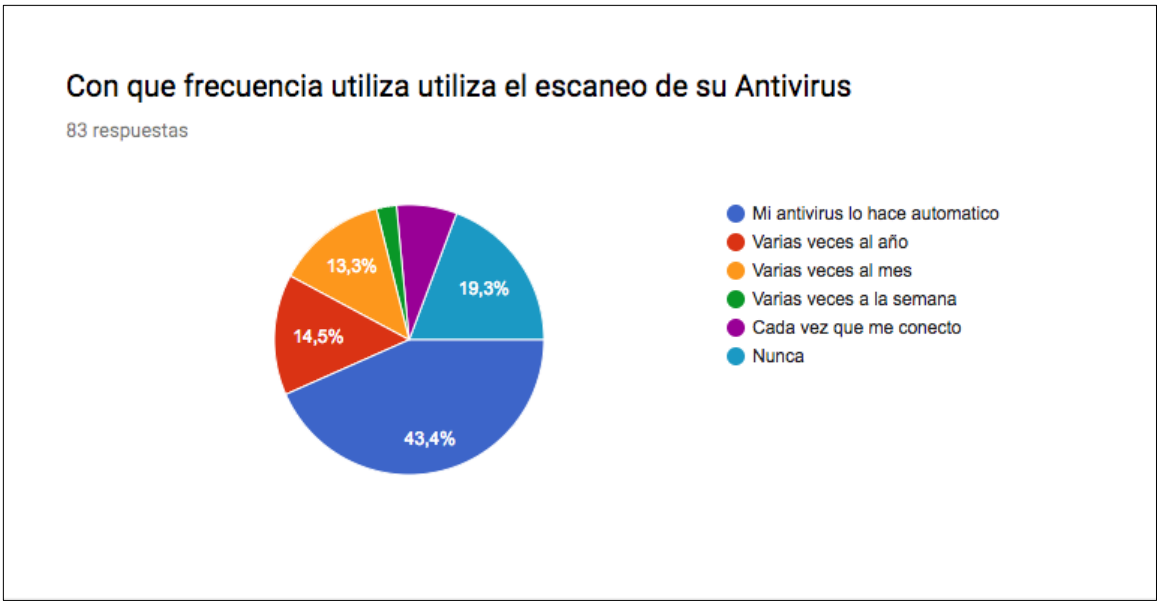

Figura 5.Resultados frecuencia escaneo de antivirus. Fuente: Elaboración propia

En la frecuencia que utiliza el Antivirus el 19,3% indica que nunca utiliza el escaneó de su Antivirus para la revisión de archivos, un grupo se divide en porcentajes iguales el cual utiliza el escaneo del Antivirus varias veces al mes con un 13.3% y un 43,4% espera que al descargar o abrir un archivo su escaneó del Antivirus lo haga automáticamente.

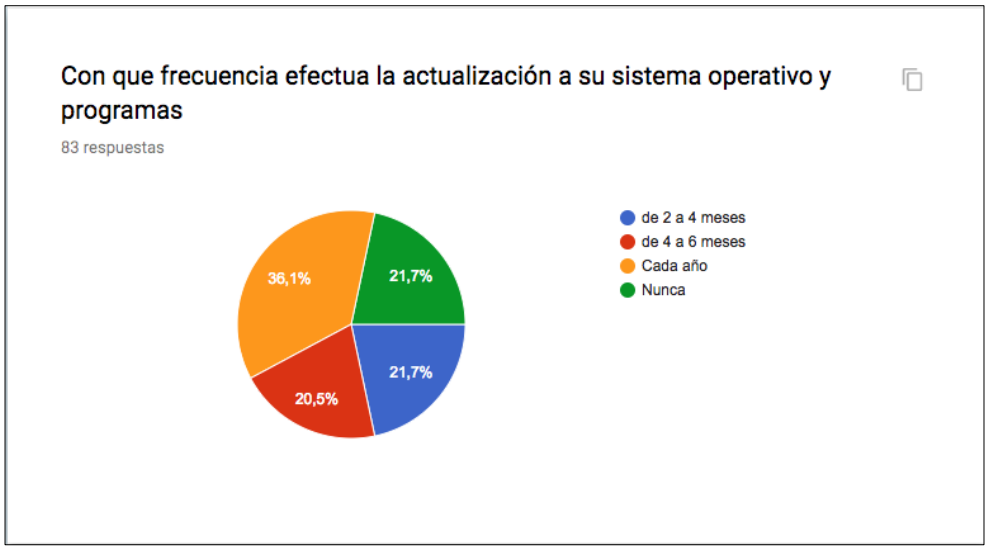

Figura 6.Resultados actualización sistema operativo y programas. Fuente: Elaboración propia

Al indagar con las actualizaciones que realiza las personas de estratos 3 y 4 sobre su sistema operativo se identifica que el 21,7% nunca efectúa una actualización, el 36.1% efectúa anualmente la actualización del sistema operativo de sus equipos, el 20.5% lo realiza de 4 a 6 meses, teniendo en cuenta que los sistemas operativos son encontrados una gran cantidad de vulnerabilidades por sus aplicaciones y versiones es de suma importancia la actualización continua del sistema operativo.

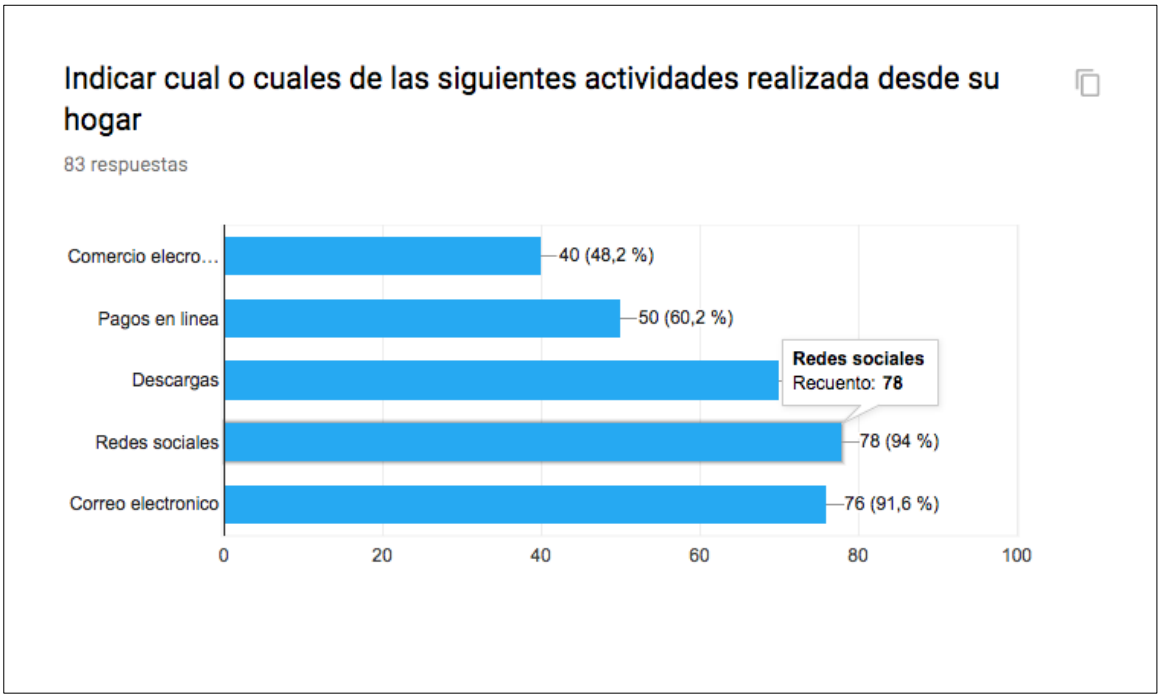

Figura 7.Resultados actividades realizadas desde el hogar. Fuente: Elaboración propia

De las actividades más realizadas por parte de las personas del común hogar, la más realizada es redes sociales con el 94%, seguida de la revisión de los correos electrónicos con un 91,6%, con el 84,3% efectúan descargas y el 60,2% esta los pagos en línea, se ve que el hogar se siente con la tranquilidad de efectuar estas actividades, por la comodidad y facilidad que le brinda la internet, evidenciando el crecimiento de estas actividades en los hogares de la

ciudad de Bogotá D.C.

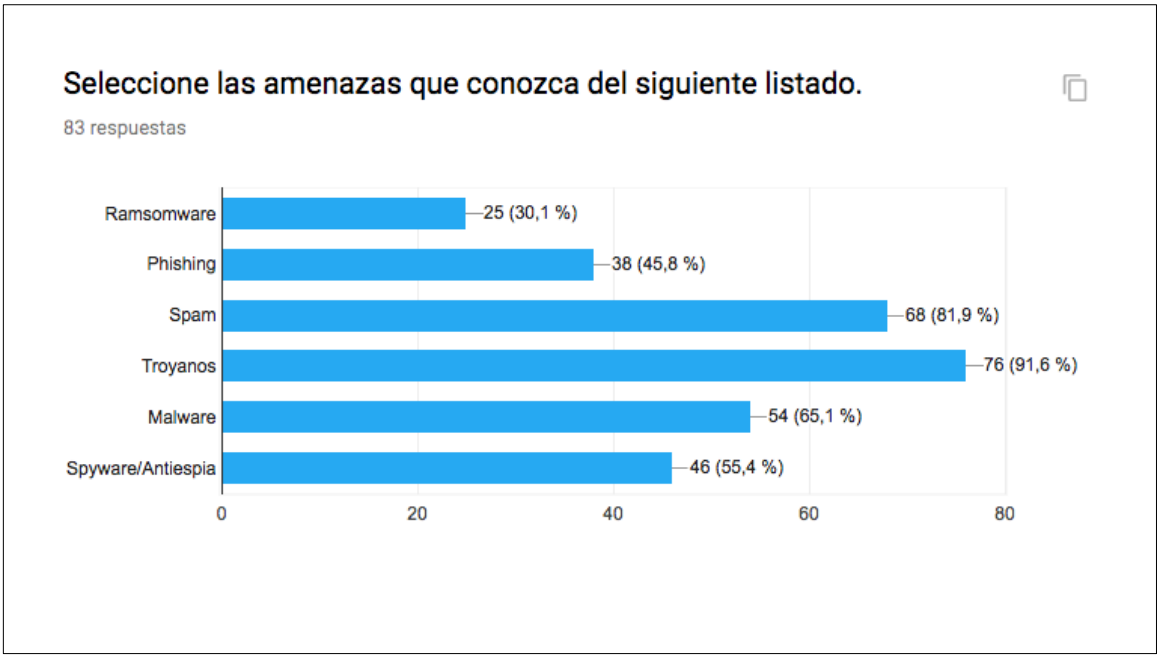

Figura 8.Resultados conocimiento de amenazas. Fuente: Elaboración propia

Indagando en el conocimiento de las personas sobre las diversas amenazas que puede está expuesto, con el 91,6% se conoce que es un troyano, con el 81,9% se conoce que es un spam y entre los menores porcentajes, pero más peligrosos están el Ramsomware con 30,1% y Phishing con el 45,8%, evidenciando que el Phishing y el Ramsomware son de menor conocimiento, pero son de gran impacto y de gran afluencia como son en el robo de perfiles y en el secuestro de información sensible de los clientes respectivamente.

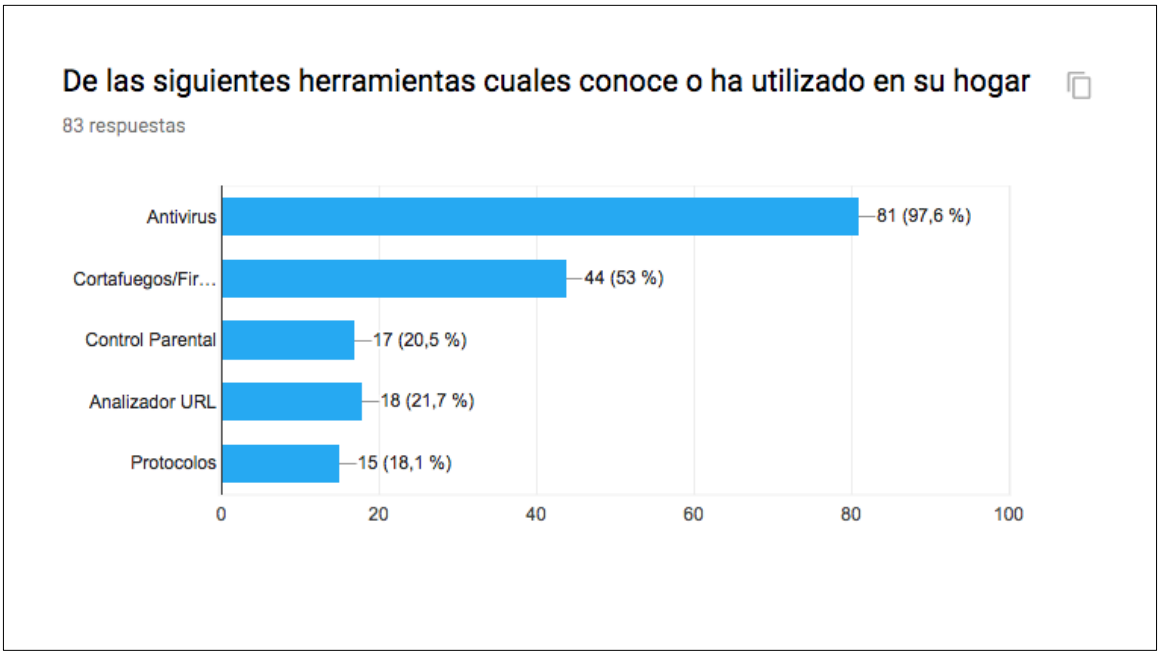

Figura 9.Resultados herramientas conocidas o utilizadas en el hogar. Fuente: Elaboración propia

En el conocimiento de herramientas para la prevención y protección de infección, la más utilizada es el Antivirus con un 97,6% aunque el Antivirus es una de las herramientas más potentes para la prevención, existen muchas más y que son importantes, con un 53% esta los cortafuegos o firewall, con el 21,7% esta los analizadores de URL, y uno de los más importantes, pero menos conocido por las personas en sus hogares son los protocolos ya que solo un 18,1% tiene el conocimiento.

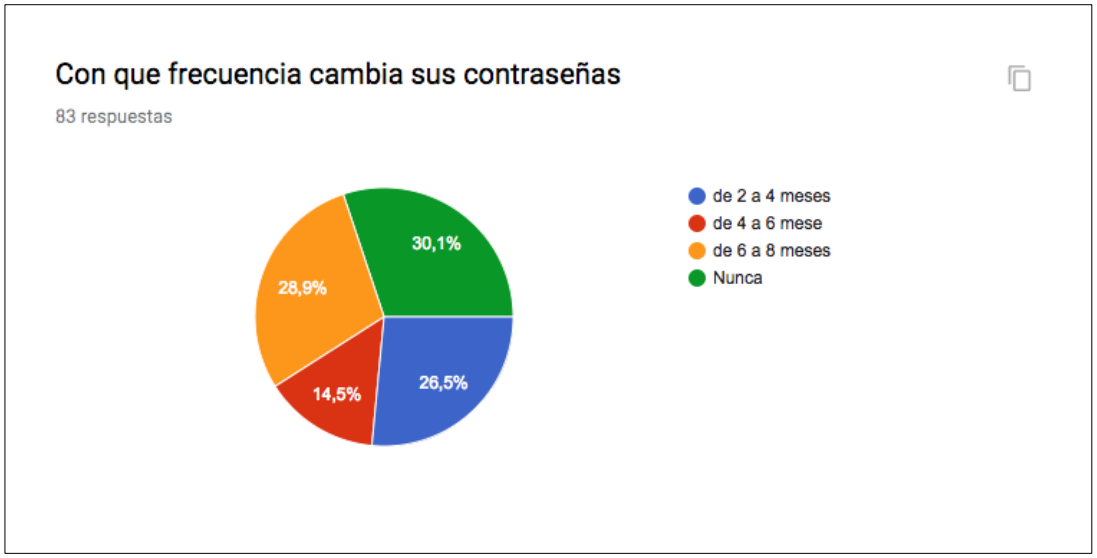

Figura 10.Resultados frecuencia del cambio de contraseñas. Fuente: Elaboración propia

Gran curiosidad causa el saber que la gran mayoría de la población encuestada no cambia su contraseña periódicamente, ya que el 30,1% nunca lo hace, y solo el 26,5% lo hace en un periodo corto de 2 a 4 meses.

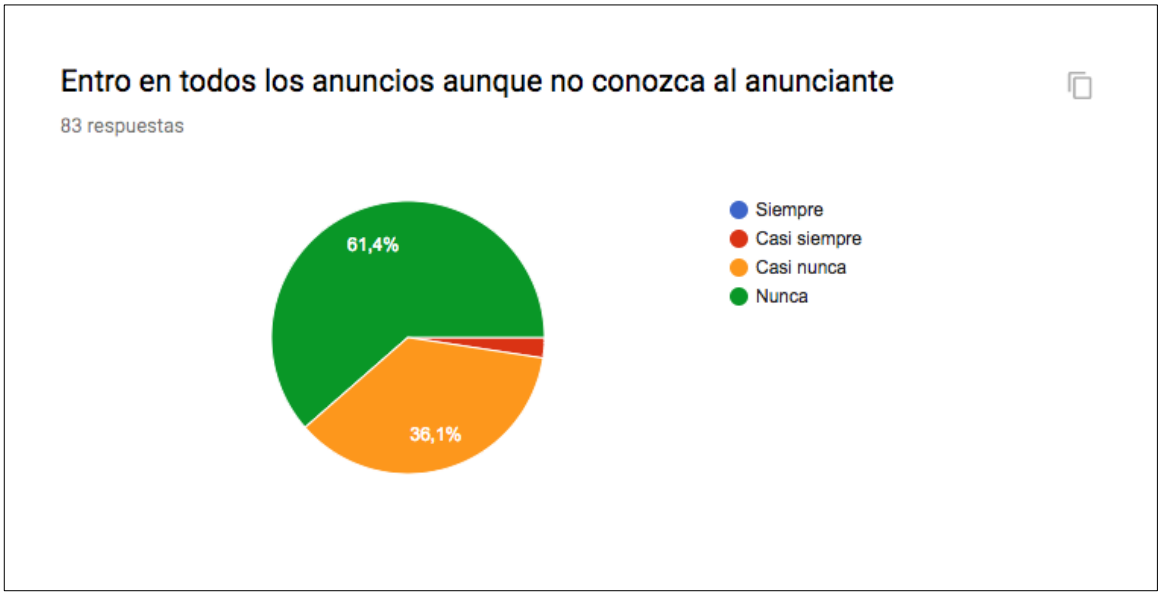

Figura 11.Resultados sobre anuncios que no conozca al anunciante. Fuente: Elaboración propia

Las personas encuestadas indican que son cuidadosas al recibir anuncios ya que el 61,4% nunca acepta anuncios que no conoce y que el 36,1% casi nunca lo realiza.

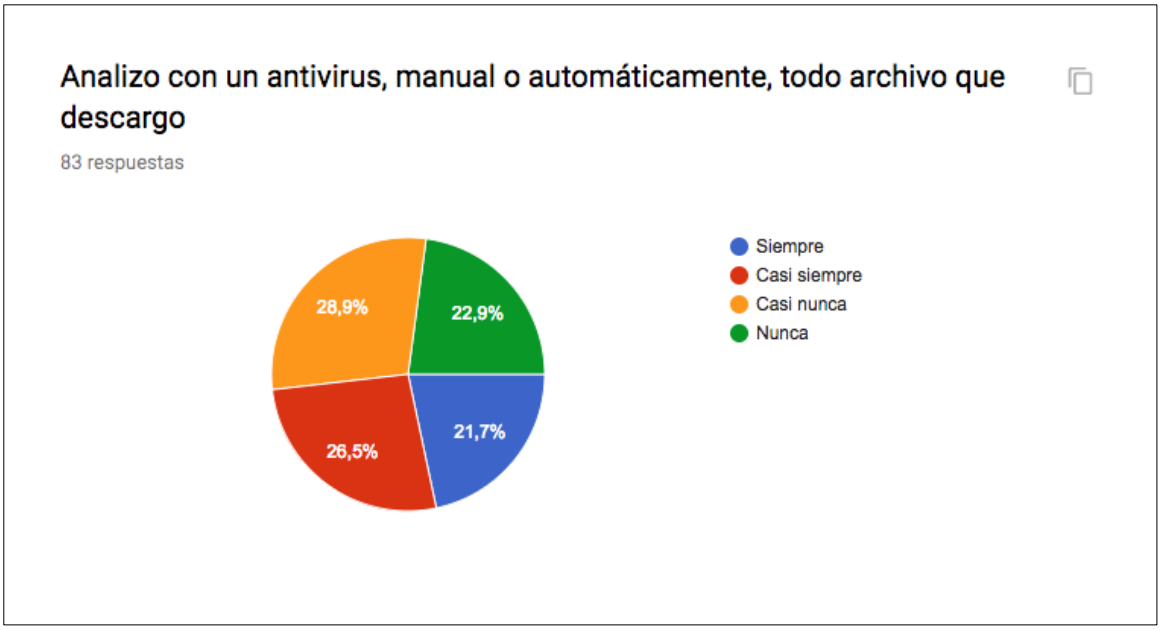

Figura 12.Resultados de análisis con antivirus, manual o automáticos de archivos descargados.

Fuente: Elaboración propia

Algo que se evidencio en esta pregunta realizada es que existe poco cultura para el uso de un Antivirus ya que las respuestas estuvieron muy de la mano, encontrando que 21,7% efectúa el análisis automático o manual al descargar un archivo, con el 26,5% casi siempre efectúa este proceso, el 28,9% casi nunca lo realiza y con el 22,9% nunca lo realiza siendo un porcentaje muy alto ya que todo archivo descargado, copiado a su equipo de cómputo debe ser escaneado automáticamente o manualmente antes de ser utilizado.

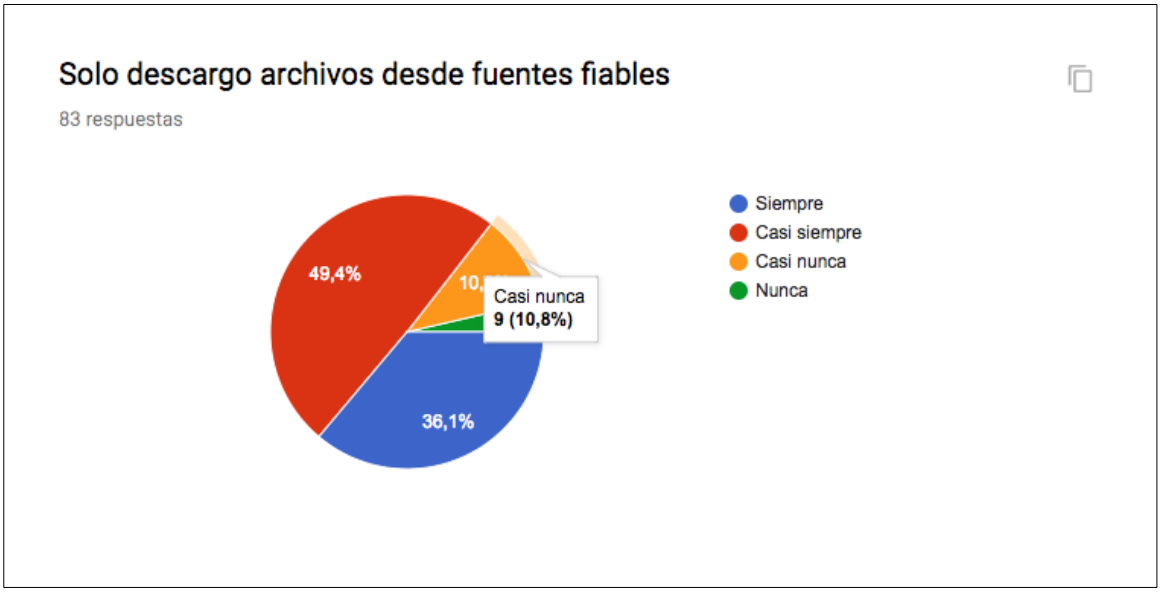

Figura 13.Resultados sobre descarga de archivos de fuentes fiables. Fuente: Elaboración propia

De acuerdo con la encuesta indica que con un 49,4% casi siempre descarga desde fuentes fiables los archivos, dando cabida a infecciones y vulnerabilidades en sus equipos, y tan solo un 36,1% siempre descarga archivos de fuentes confiables.

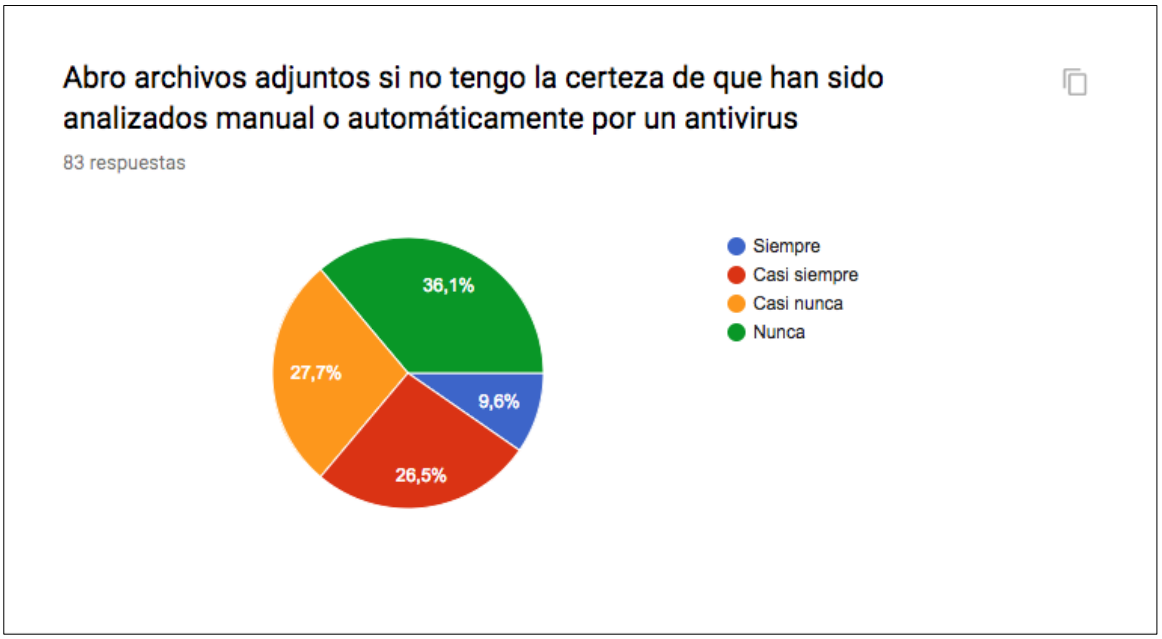

Figura 14.Resultados sobre archivos analizados manual o automáticamente por antivirus.

Fuente: Elaboración propia

El 36,1% no se asegura de que los archivos descargados fueron previamente escaneados por el Antivirus antes de ser utilizados, y tan solo un 9,6% se asegura de que los archivos descargados fueron escaneados por su Antivirus.

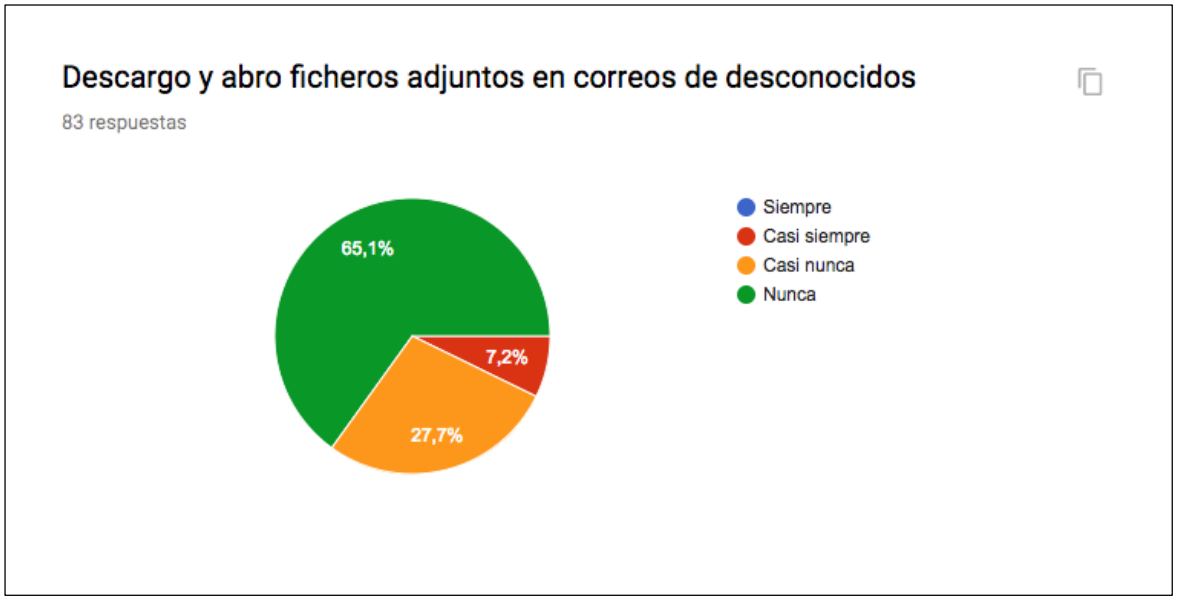

Figura 15.Resultados sobre descarga y apertura de ficheros adjuntos en correos desconocidos. Fuente: Elaboración propia.

Según la encuesta el 65,1% de las personas no descarga o abre adjuntos de correo desconocidos y un 27,7% casi nunca lo efectúa.

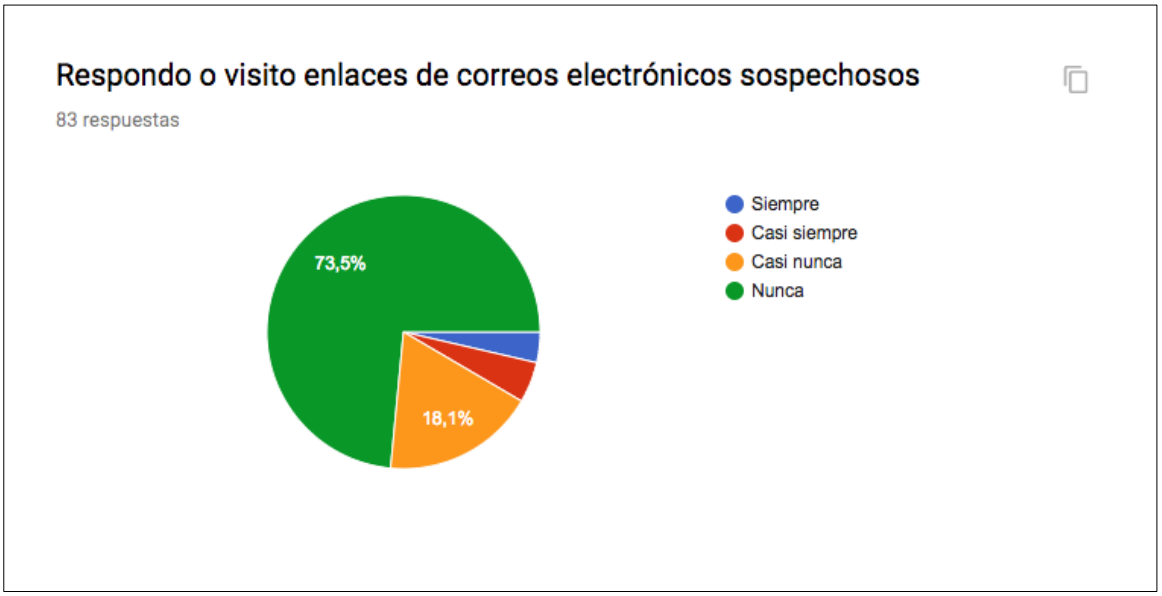

Figura 16.Resultados sobre análisis de respuesta o visita enlaces de correos electrónicos sospechosos.Fuente:Elaboración propia

con un 73,5% las personas no ingresan a enlaces suministrados por correos electrónicos sospechosos, teniendo en cuenta que es una de las actividades más realizadas por la persona del común desde sus hogares.

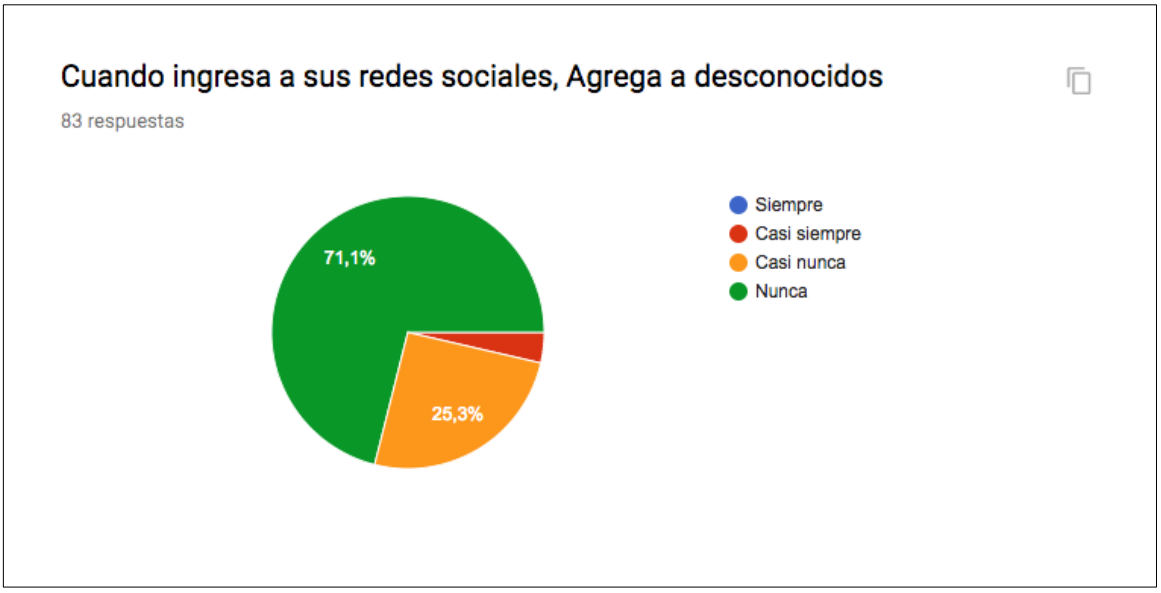

Figura 17.Resultados sobre el ingreso a redes sociales. Fuente: Elaboración propia

Teniendo en cuenta la parte más joven de los hogares y la que más utiliza redes sociales se determinó que el 71,1% no agrega desconocidos en sus redes sociales, dando cabida a una ingeniería social para determinar información sensible y personal de cada persona.

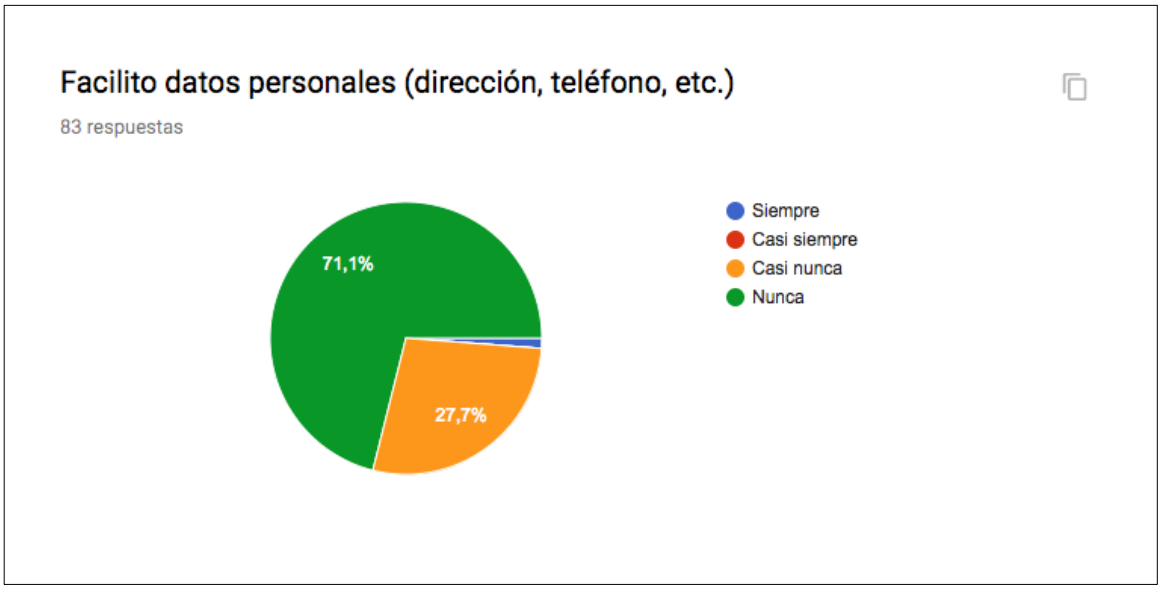

Figura 18.Resultados sobre entrega de datos personales. Fuente: Elaboración propia

Podemos evidenciar que el 71,1% no facilita o publica información sensible como son su dirección, teléfono, etc. pero el 27,7% casi nunca publica su información privada.

Figura 19.Resultados sobre rechazo de invitaciones a usuarios desconocidos. Fuente: Elaboración propia

Se encontró que el 60,2% rechaza solicitudes de desconocidos en sus redes sociales y tan solo un 3,6% acepta este tipo de solicitudes de desconocidos.

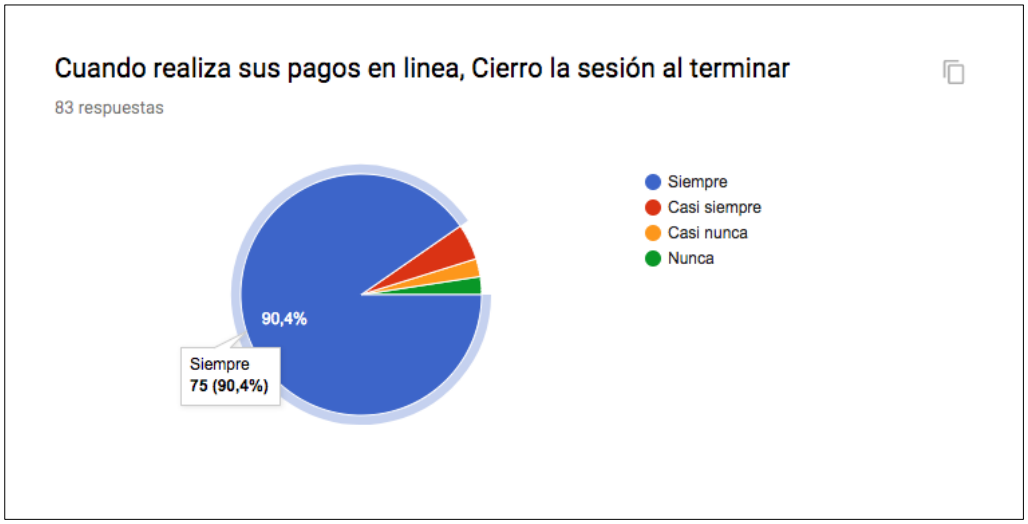

Figura 20.Resultados sobre el cierre de sesión al realizar pagos en línea. Fuente: Elaboración propia.

Se ha encontrado un buen proceder que parte de las personas ya que con un 90,4% las personas cierran sus sesiones al terminar sus transacciones electrónicas.

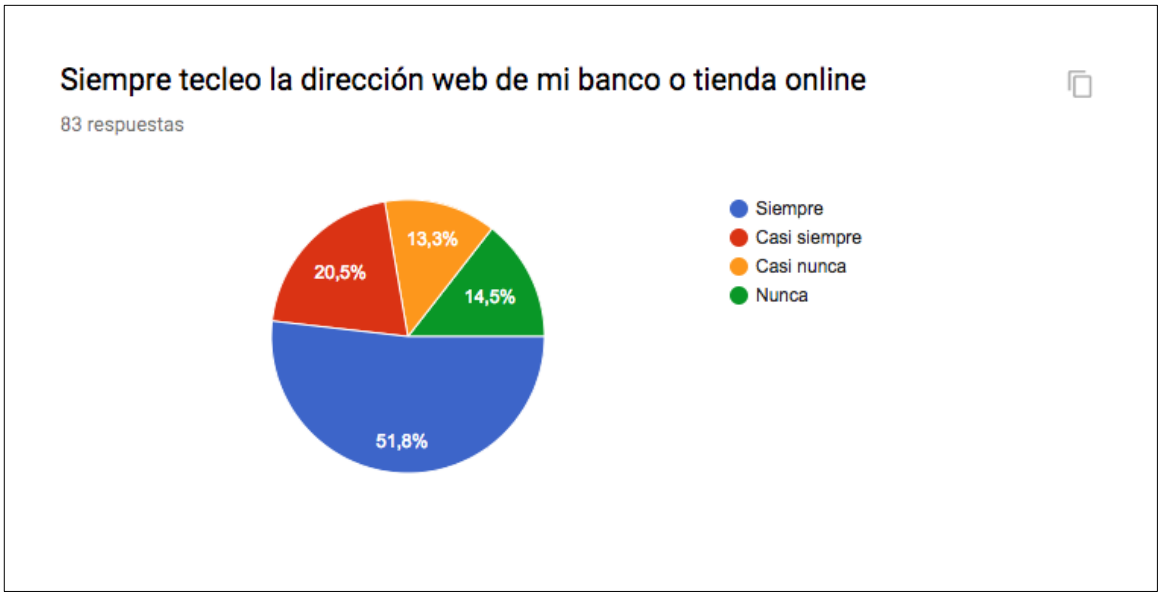

Figura 21.Resultados tecleo de la dirección web del banco o tienda online. Fuente: Elaboración propia

El 51,8% de las personas desde su hogar cargan el sitio web del banco o de la tiendo en línea a comprar, sin utilizar un navegador de búsqueda, esto afianza la seguridad, pero se determina que el 14,5% no lo realiza.

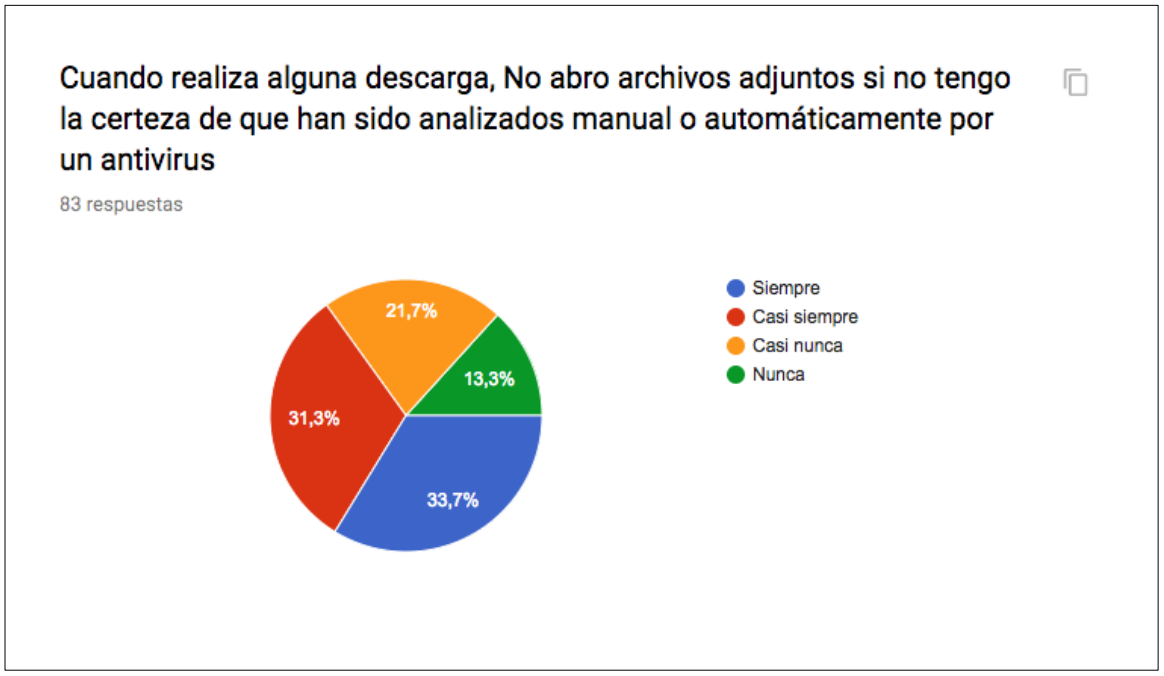

Figura 22.Resultados sobre la certeza que existe sobre descargas de archivos analizados manual o automáticamente. Fuente: Elaboración propia

El 33,7% toma los correctivos de ejecutar el escaneo previo descargue de algún archivo y tan solo un 13,3% no realiza el procedimiento adecuado para los archivos descargados.

Como primera medida para implementación de los protocolos se contemplan las directrices de acuerdo a la Organización Internacional de Normalización ISO 27001 y ISO27002 que contienen los lineamentos para diseñar los controles requeridos en un ambiente de estratos 3 y 4 de la ciudad Bogotá.

Como buena práctica la estrategia contemplada deberá ser aplicada por cada uno de los integrantes del grupo familiar esto, para generar un ambiente de seguridad que sea conocido y aplicado generando un ambiente de control de la seguridad.

Casos de prueba efectuado para apoyar los datos de la encuesta, en este laboratorio efectuado se vulnero la red Wifi de un hogar, en donde se puede dar cuenta que las personas no manejan un protocolo de estándar para la generación de contraseñas, para estas pruebas utilizamos una antena USB T-Link para Linux y el Kali Linux ver figura 23, el cual posee una herramienta llamada Aircrack-ng, acompañada de ingeniería social, realizando preguntas a las personas que dieron el permiso para hacer el laboratorio y la utilización del cruch para la generación de diccionarios, llegamos a obtener la clave de la red.

Datos recopilados una vez se hizo el laboratorio, al iniciar y solicitar el permiso para este procedimiento se empleó la ingeniería social la cual, se hicieron preguntas al azar como, “cada cuanto cambia su contraseña de internet”, “utiliza en sus claves letras, números, caracteres especiales”, “cuantos caracteres utiliza para su contraseña”, con esta información se utilizó para acotar la creación de los diccionarios, así aumentar la efectividad para romper las contraseñas, a continuación mostraremos los pasos utilizados para llegar a materializar el rompimiento.

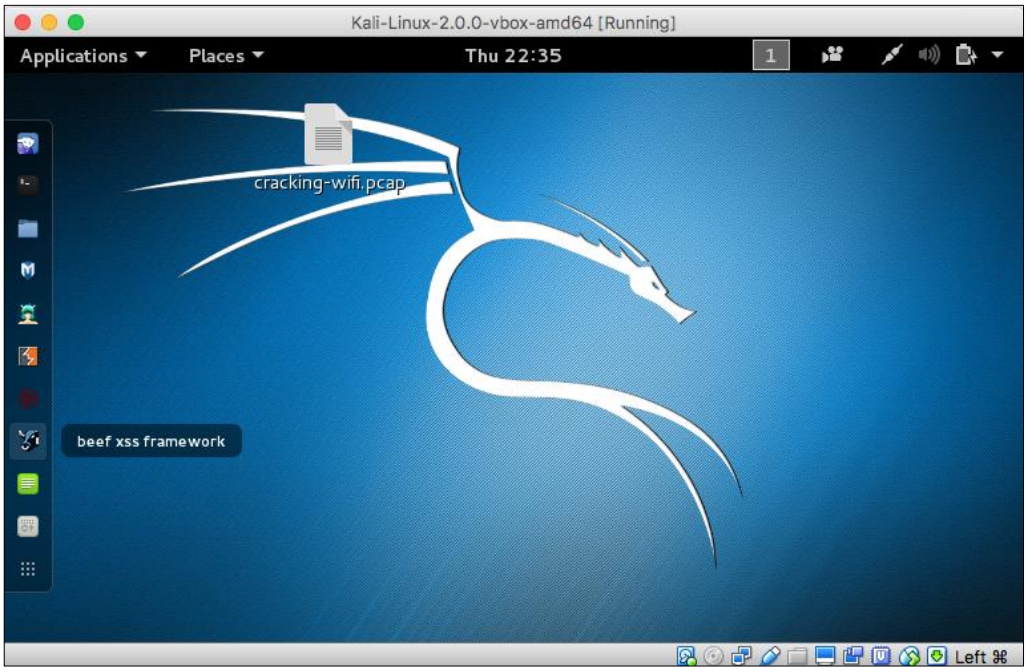

Figura 23.herramienta kali linux

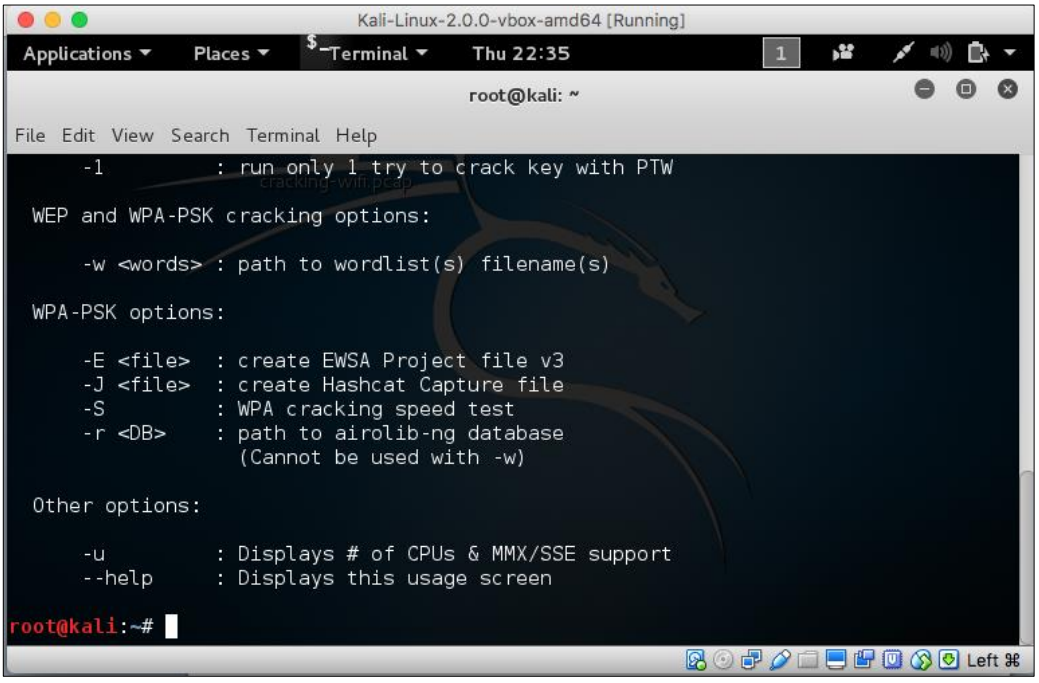

Figura 24.Herramienta para vulnerar redes inalámbricas WPA2

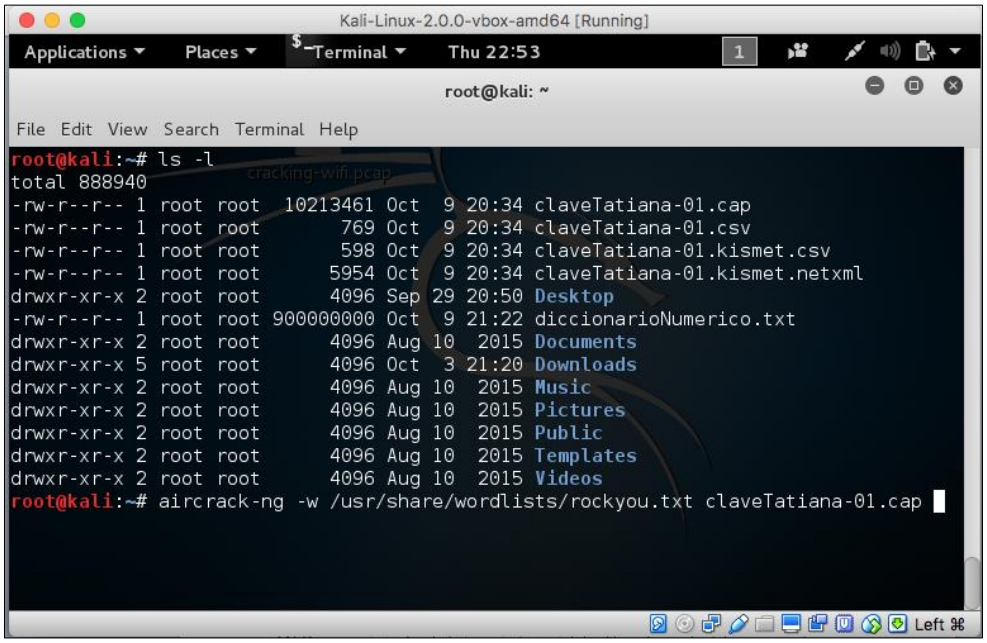

Figura 25.Captura de .cap para utilizar el diccionario y romper la clave de la red inalámbrica.

1) Instalación del Kali Linux, se utilizó una máquina virtual y se instaló la antena inalámbrica que servirá de monitor para detectar las redes cercanas a un rango de 150 mts. Tomamos la red en donde otorgaron el permiso.

2) Utilización de la herramienta aircrack la cual no permite dejar la antena en modo monitor, tomar los paquetes por medio de la MAC.

3) Una vez obtenida una cantidad significativa de paquetes se utilizó, Crunch el cual se hizo un diccionario con base en las preguntas efectuadas.

Así se determinó que las personas no cambian las contraseñas de la Wifi periódicamente, adicional no poseen un control de las personas que se conectan a ella, también observamos la baja complejidad en la construcción de la contraseña y la cantidad de caracteres utilizados en ella.

INFORME DE VULNERABILIDADES

A partir de la Listas de vulnerabilidades criticas encontradas en la encuesta y pruebas de campo.

1) Carencia en el manejo de los antivirus

2) Falta de conocimiento en el manejo de las herramientas de protección de los equipos.

3) Falta de conocimiento en el manejo de las herramientas de protección de los equipos.

4) Carencia en la actualización de los sistemas operativos.

5) Ausencia de protección para el ingreso de sitios web.

6) Desconocimiento de protección para redes sociales.

7) Desconocimiento en las mejores prácticas para la descarga de aplicaciones

8) Desconocimiento uso adecuado del manejo de correos personales.

9) Desconocimiento de certificados para realizar pagos en línea

10) Ausencia de buenas prácticas estableciendo la creación de contraseñas

11) Inadecuado el regular cambio de contraseñas

12) Ausencia en conocimiento de troyanos, malware, spam, Phishing, spyware y Ramsomware.

13) Insuficiencia de cambio de contraseña periódica

14) Falta de prevención para el acceso a correo electrónico, así como el scaneo de su contenido.

15) Conocimiento de los sitios en donde se descargan programas, app, documentos, etc.

16) Desconocimiento de la ingeniería social, facilita entrega de datos personales.

CONCLUSIONES PRIMERA ENCUESTA

Se logra determinar con la encuesta y el laboratorio, la falta de conocimiento y protocolos para asegurar la información sensible que se maneja en el hogar, se pudo determinar que en los hogares de estratos 3 y 4 de la ciudad de Bogotá la seguridad y el desconocimiento de los riesgos que se obtienen al ingresar a la internet y utilizar aplicaciones, realizar pagos en línea, chat, foros sin tener en cuenta los mínimos protocolos de protección a su información sensible.

5. EVALUACIÓN DE RIESGOS

Una introduccion en punto 5 evaluacion, explicar la tabla de riesgo y dejarla como anexo y colocar los mas criticos en referencia.

- Matriz de evaluación de riesgos identificados en las vulnerabilidades.
- Listado de herramientas para el protocolo de las vulnerabilidades.
- Protocolo de mitigación de las vulnerabilidades y riesgos
- Desarrollar protocolos que mitiguen los riesgos y vulnerabilidades más importantes. Aplicando los protocolos diseñados que demuestren que las contramedidas desarrolladas son útiles.

ANÁLISIS DE RIESGOS

De acuerdo a la normativa ISO 27005 que permite realizar el tratamiento de los riesgos iniciamos con el levantamiento de activos aplicado en el ambiente del hogar es estrato 3 y 4 de la ciudad de Bogotá.

- **Identificación de activos**

Activo: Es cualquier elemento al cual se le asigna un valor y por lo cual requiere protección. Loa activos pueden ser (infraestructura tecnológica, documentos electrónicos y físicos, personas).

TIPOS DE ACTIVOS		
TIPO		**DESCRIPCION**
GENTE	USUARIO	Personas que usan la información para desempeñar sus funciones diarias
INFRAESTRUCTURA	Infraestructura física	Hogares (Lugar de vivienda)
	Tecnología hardware	Equipos de cómputo, Routers, Televisores, IPad, Celulares, Tablets
	Tecnología software	Sistema operativo
INFORMACION	Electrónica	Información sensible de la persona que accede a los servicios de internet
SERVICIOS		Correo electrónico, descargar, comercio online, redes

	sociales

Tabla 17.Identificación de activos.Fuente:Elaboración propia

➢ Clasificación de activos de información

Se define la criticidad de un activo en función de cuan necesario resulta para las actividades de un área o la misma organización. Se establece un valor estandarizado que se prioriza sobre la CIA.

- Si todos son 0 ➔ Criticidad 0-Nula
- Si el máximo es 1 → Criticidad 1-Baja
- Si el máximo es 2 → Criticidad 2-Media
- Si el máximo es 3 → Criticidad 3-Alta

➢ Identificación de vulnerabilidades y amenazas

Una **vulnerabilidad** es toda debilidad de un activo de información, dada comúnmente por la inexistencia o ineficacia de un control

Una **amenaza** es todo elemento que haciendo uso o aprovechando una vulnerabilidad atenta o puede atentar contra la seguridad de un activo de información.

- **Determinación del riesgo**

Este punto es realizado para determinar el nivel del riesgo que cada amenaza conlleva en el ambiente del caso de estudio, la determinación del riesgo que cada par activo/amenaza resulta como función de:

- **La probabilidad** de que ocurra el evento, es decir, que la amenaza explote la vulnerabilidad
- **La magnitud** del impacto que el evento produce sobre el activo del caso de estudio

Para el desarrollo del control de riesgos se ha utilizado la norma ISO27005 el impacto y la frecuencia anual de acuerdo a las veces que se puede la amenaza aprovecharse de la vulnerabilidad en un periodo de tiempo de 1 año, y se determinan con el insumo de las vulnerabilidades y amenazas de la tabla 19 en donde podemos evidenciar que los riesgos que se ponderan en su calificación por encima de 10 se los determinados para desarrollar los controles. (ver matriz riesgos cibersecurity home anexo 1)

- **Recomendación de controles**

La recomendación de controles comprende la identificación de medidas adecuadas que mitiguen o eliminen los riesgos encontrados previamente. **Control o salvaguarda** contribuye reduciendo el impacto que produce una amenaza o la frecuencia con que esta sucede.

6. DESARROLLO DE PROTOCOLOS

Como se ha relatado a lo largo de este documento, el objetivo de esta investigacion se centró en establecer los riesgos de seguridad de la informacion a los cuales se encuentran expuestos los hogares de estrato 3 y 4 de la ciudad de Bogotá, identificados mediante la elaboracion de la encuesta No.1 y apoyados con el pentesting efectuado. Con base a estas detecciones se procedió a elaborar un protocolo que ayude a mitigar cada una de las vulnerabilidades con su respectivo control y herramientas para este fin (Ver anexo 2 Protocolo mitigacioìn ciberataques).

HERRAMIENTAS

Listas de herramientas encontradas para la prevención de las vulnerabilidades detectadas en los hogares colombianos de la ciudad de Bogotá en extractos 3 y 4.

1) Panda protection, Avast free antivirus, AVG antivirus free, estos antivirus son de fácil uso y dan a conocer una versión gratuita para proteger tus dispositivos conectados a la red.

2) Una de las mejores utilidades para el computador es utilizar una herramienta que mantenga limpio tu computador, tal como CCleaner, que es una herramienta gratuita que le permite mantener en control la basura que se puede estar acumulando en tu computador, permite que tus aplicaciones mantengan un mejor rendimiento.

3) Malewarebytes Anti-Malware Free posee una gran capacidad para la detección y eliminación de malware, brindando la ventaja de escanear archivos sospechosos con antivirus-

online.

4) Spybot, hace un buen trabajo identificando y eliminando ciertos tipos de software malicioso(malware).

5) Seguridad en el navegador, si se utiliza Firefox se puede instalar un complemento NoScript, HTTPS Everywhere, Privacy Badger, Click&Clean.

6) Cortafuegos limita y controla las conexiones predeterminados en los puertos, evitando que un dispositivo sea vulnerable a ataques externos, Comodo Firewall, PC tolos Firewall.

Según estudios encontrados la mejor configuración con herramientas gratuitas para garantizar una mitigación a estas vulnerabilidades descritas.

• Antivirus: Avast

• Cortafuegos: Comodo Firewall

• Anti-espías: SpyBot, Ad-Aware (o malwarebytes antimalware) y SpywareBlaster

CONCLUSIONES HERRAMIENTAS

Tener una buena configuración de seguridad no garantiza que estemos excentos de una

vulnerabilidad por virus, troyanos, spyware, malware, etc. La mejor manera de evitar la infección es tener precaución:

• Aunque una configuración de seguridad con estos programas gratuitos es fiable, se indica que periódicamente se efectúen semanalmente escaneos con antivirus en línea como el que ofrece Eset (nod32).

• Cuando se usan P2P, escaneado previamente con un antivirus actualizado, si no es lo que se deseaba descargar es mejor eliminarlo.

• No abrir correos electrónicos de personas que no conozcamos y tampoco correos sospechosos, lo mejor es eliminar estos correos. Desconfiar de los correos publicitarios, cadenas o reclamos (porno, mujeres desnudas, vídeos, fotos, etc.)

• Usar navegadores con bloqueo de ventanas emergentes activado, además de instalar complementos para evitar la publicidad. En IE (IE Ad-block, IE7Pro), Firefox (Ad-Block, No-Script). Nunca tener la configuración del navegador en seguridad baja.

• Desconfiar de sitios extraños e intentar no dar click sobre la publicidad, en caso de tener que cerrarla hacerlo siempre desde la ventana Windows, no hacerlo desde algunas x que aparecen en los pop-ups.

• Si notamos algo extraño como lentitud en la navegación, ralentización del sistema, aparición de ventanas publicitarias o tenemos la sospecha de estar infectados se recomienda

seguir este manual.

7. VALIDACIÓN DE PROTOCOLO

Posterior a la elaboración y difusión del protocolo “Protocolo mitigación ciberataques” (Anexo 2) se procedió a realizar la encuesta No. 2 a una muestra poblacional de aproximadamente el 20% de la muestra inicial, con el objetivo de validar la efectividad del protocolo difundido.

- Validar las vulnerabilidades y riesgos identificados.
- Aumentar la seguridad en los hogares de estrato 3 y 4 en la ciudad de Bogotá.
- Validar los comportamientos imprudentes por desconocimiento en los hogares 3 y 4 de la ciudad de Bogotá.
- Facilidad de implementación de la guía aumentando la satisfacción del cliente.

Valoración de protocolos, se envió nuevamente una encuesta con el protocolo, para las personas encuestadas en nuestro primer objetivo que definía el estado actual de la seguridad de la información en los hogares Bogotanos en estratos 3 y 4.

Se obtuvieron los siguientes resultados:

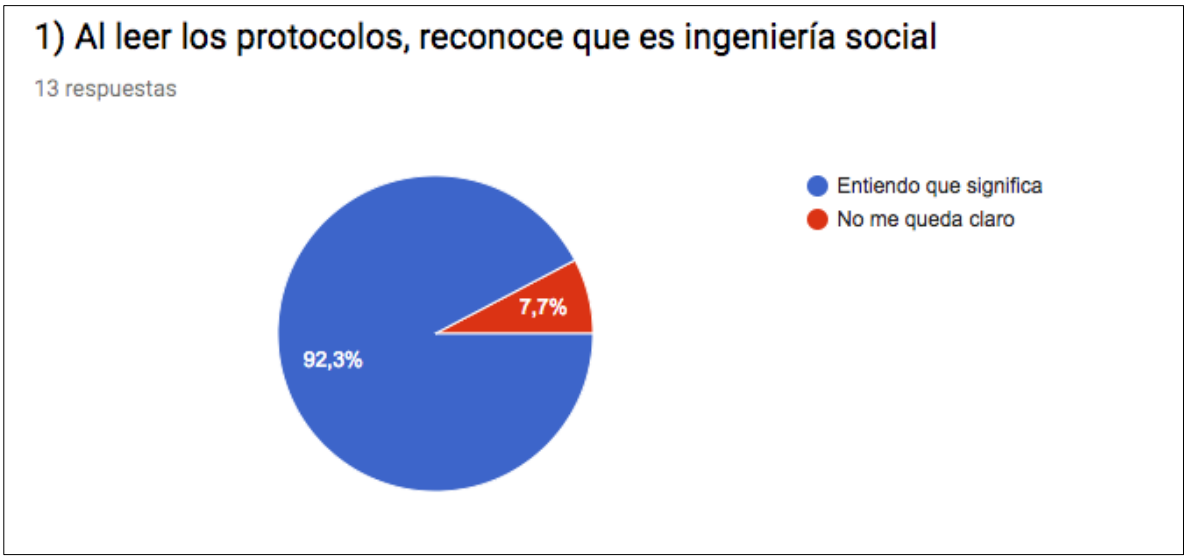

Figura 26.Resultado análisis reconocimiento ingeniería social. Fuente: Elaboración propia

Se encontró que al leer los protocolos entregados las personas del común en un 92,3% entiendeahora que es la Ingeniería Social, y que el 7,7% aun no les queda claro el término Ingeniería social.

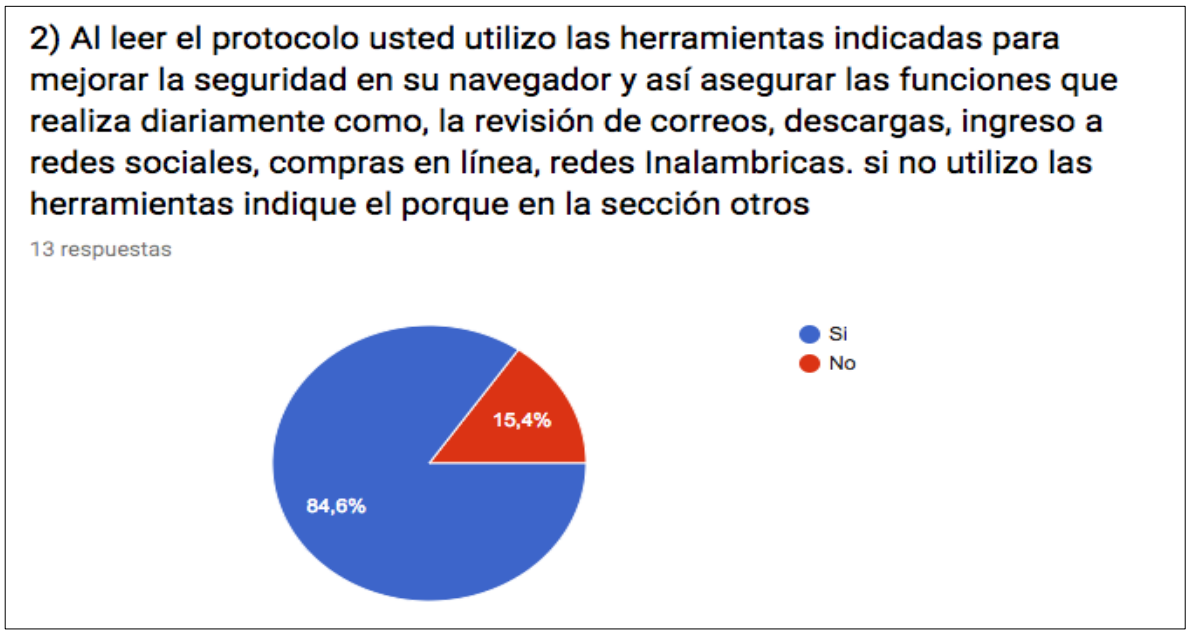

Figura 27.Resultados análisis de uso de herramientas de mejora de la seguridad. Fuente: Elaboración propia

Se logró determinar que al leer el protocolo el 84,6% de las personas utilizaron las herramientas complementarias para los navegadores y solo un 15,4% no las utilizo o no dio una respuesta del porque no utilizo alguna protección en los navegadores que utiliza actualmente.

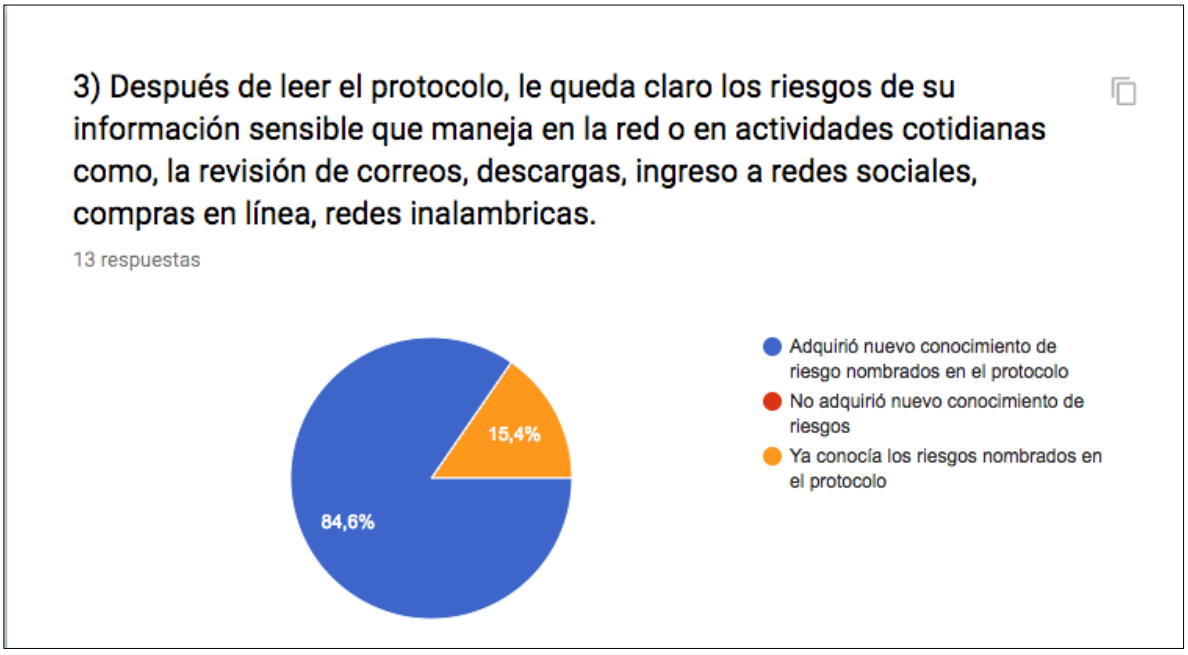

Figura 28.Resultado análisis de riesgos sobreinformación sensible. Fuente: Elaboración propia

Se logra determinar que el 84,6 por ciento no conocía la magnitud de los riesgos que podía adquirir en dentro de su hogar con la información sensible que maneja, y solo un 15,4% ya conocía estos riesgos.

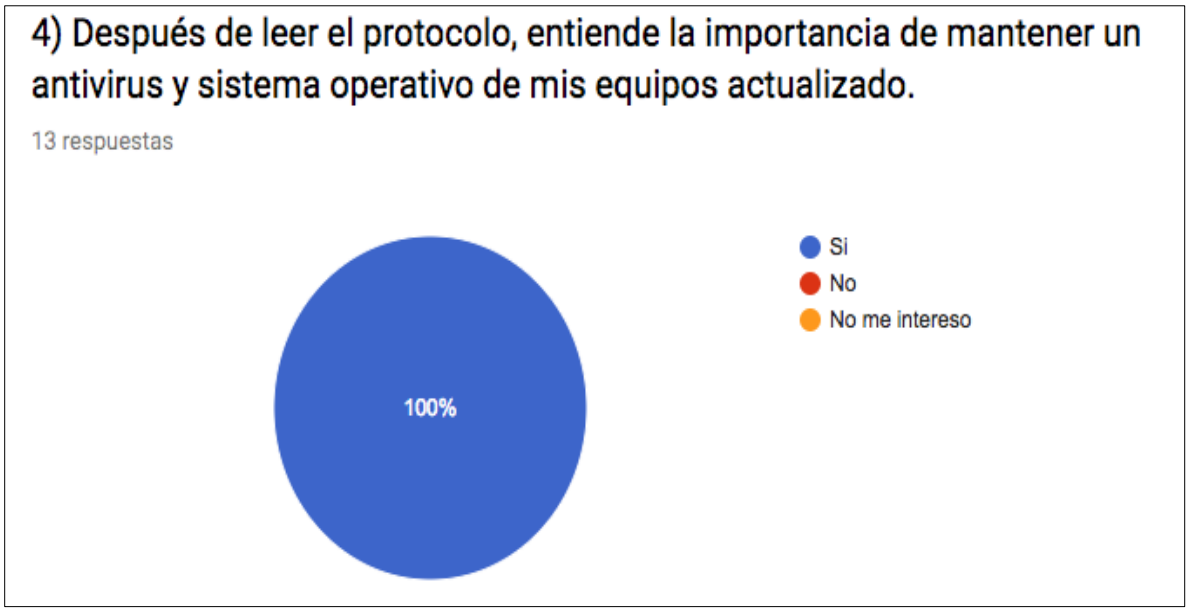

Figura 29.Resultado análisis de la importancia de mantener antivirus y sistema operativo actualizado. Fuente: Elaboración propia

Se logra alcanzar un 100% de concientización de la importancia de tener un sistema operativo y anti-virus actualizado, gracias al protocolo entregado.

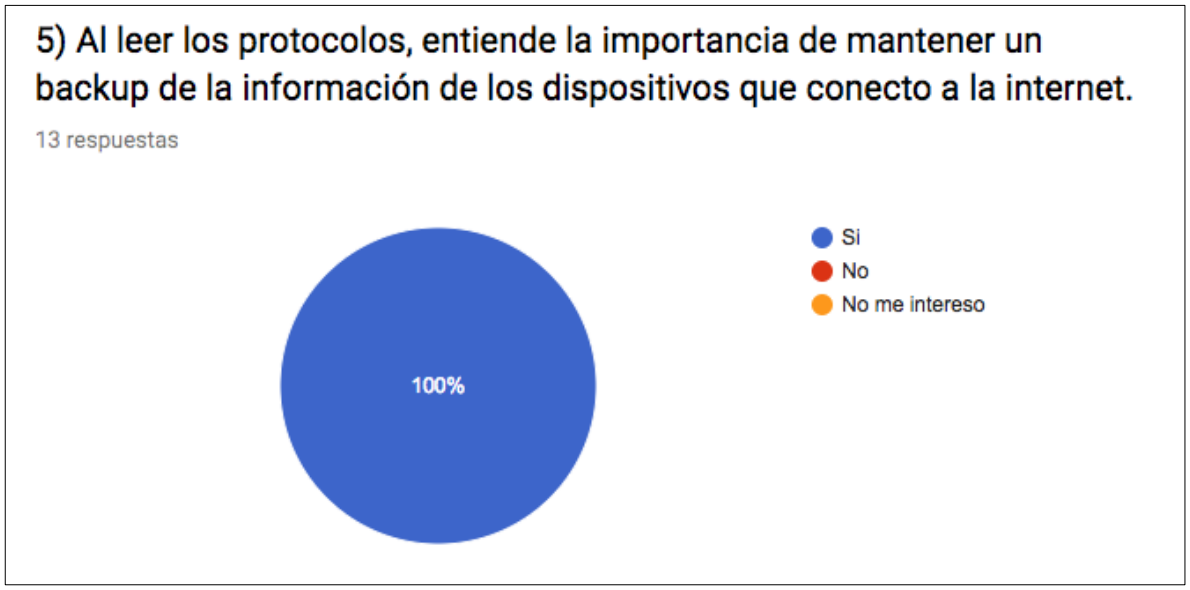

Figura 30.Resultado análisis de contar con backups. Fuente: Elaboración propia

Otra gran meta alcanzada por el protocolo en los hogares bogotanos de estrato 3 y 4 fue lograr que el 100% de las personas empezaran a realizar backup de todos los dispositivos que manejan dentro de su hogar y que tiene información sensible.

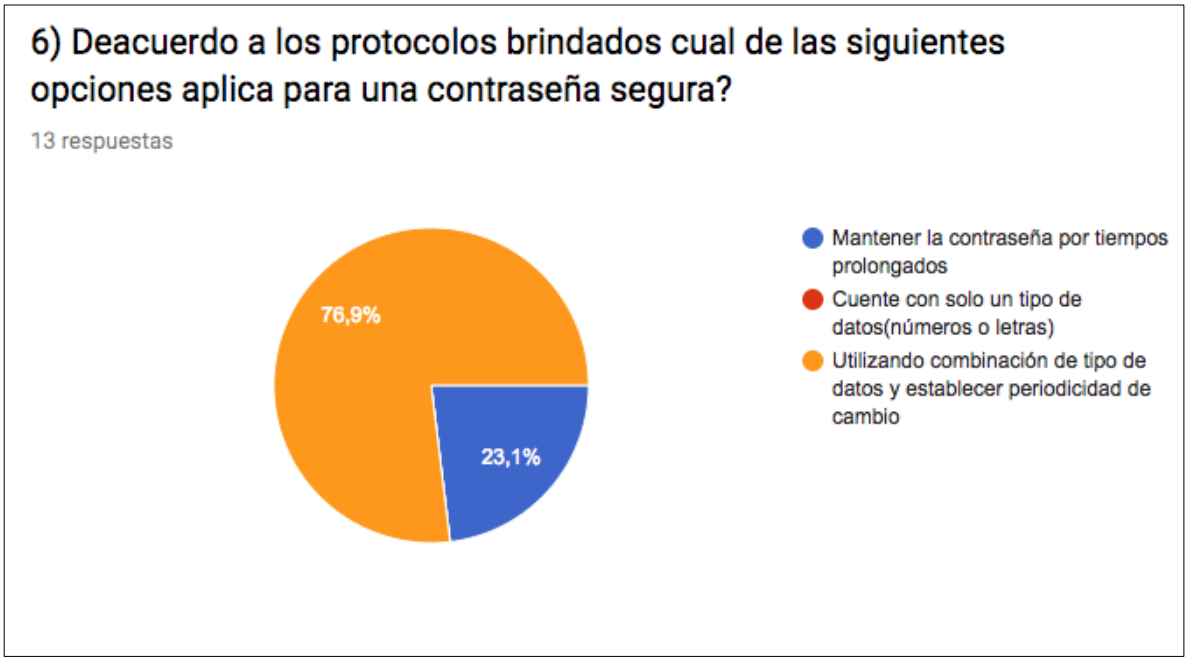

Figura 31.Resultado análisis de protocolos con contraseñas seguras. Fuente: Elaboración propia

Se logra determinar que solo el 23,1% de las personas siguen manteniendo sus contraseñas por un periodo prolongado y que el 78,9% ha tomado concientización de que una contraseña debe ser compleja, utilizando caracteres especiales, letras y números y estableciendo un ciclo de vida de contraseña más corto

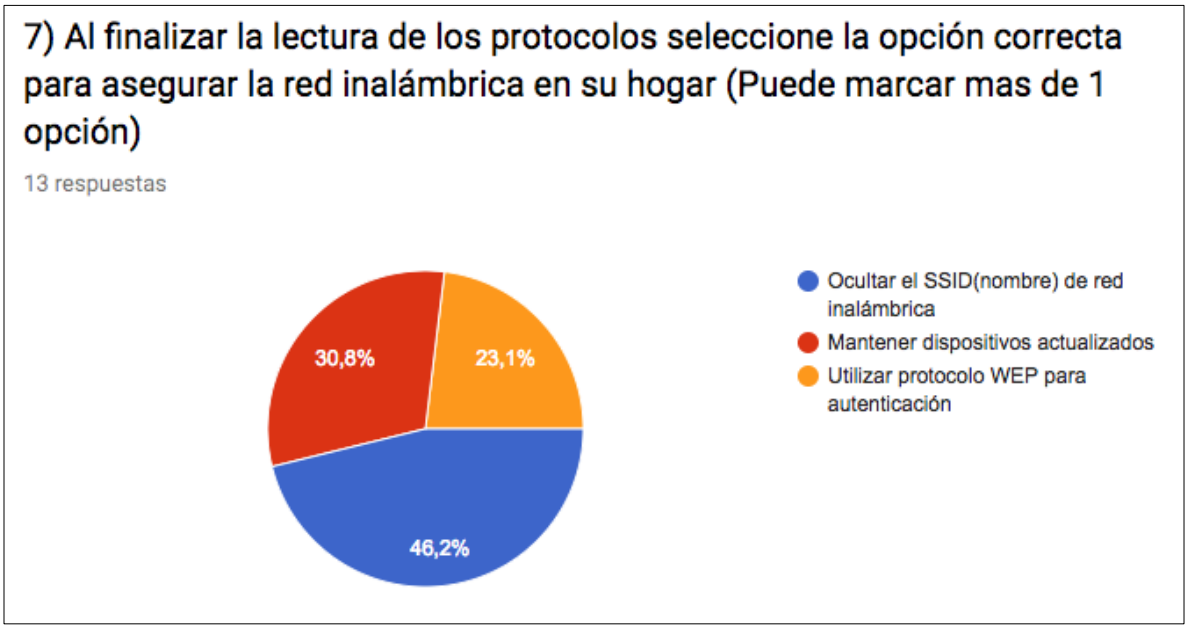

Figura 32. Resultado de los protocolos más sencillos de implementar. Fuente: Elaboración propia

Se logró otra gran meta la cual es hacer entender a las personas del común a utilizar buenas practicas tales como lo ha identificado la encuesta ya que el 46,2% efectúa el ocultamiento de su SSID, el 30,8% mantiene todos los dispositivos actualizados y el 23,1% utiliza protocolos WEP para la autentificación.

Figura 33. Resultado de los protocolos más sencillos de implementar. Fuente: Elaboración propia

Se logra determinar que después de leer el protocolo el 46,2% empezó a programas mantenimientos preventivos, y que el 46,2% empezó a utilizar backup en la nube para salvaguardar la información y tan solo un 7,7% lo hace en dispositivos extraíbles.

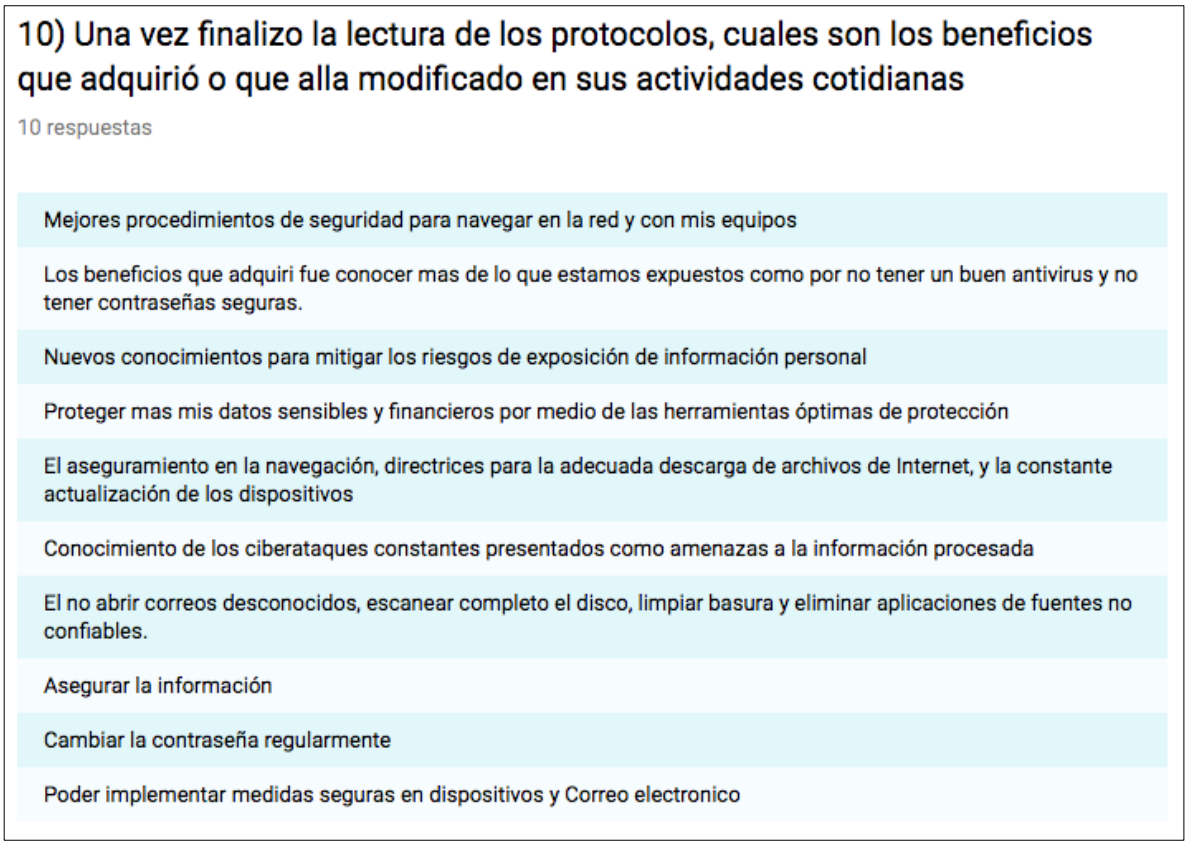

Figura 34.Resultados de beneficios adquiridos. Fuente: Elaboración propia

Se logra identificar que el 76,9% efectúa ahora una buena práctica para la verificación y revisión de sus correos electrónicos, gracias al protocolo entregado.

En la última pregunta se dejó abierta identificando el buen conocimiento adquirido por parte de los encuestado tales respuestas como: “Lods beneficios adquiridos fue conocer más de lo que estamos expuestos como por no tener un anti-virus y no tener contraseñas seguras”

“El aseguramiento en la navegación, directrices para la adecuada descarga de archivos de internet y la constante actualización de los dispositivos”

CONCLUSIONES

Desde que se elaboró esta propuesta de investigacion se establecieron unos objetivos específicos que involucraban el renocimiento de las vulnerabilidades asociadas a la seguridad de la informacion de los hogares, la elaboracion, difusion y validacion de un protocolo de mitigación de ciberataques, todos los cuales se alcanzaron con éxito.

En general los resultados obtenidos evidencian que el uso de la tecnología de manera inadecuada trae consigo consecuencias contraproducentes para la población que van desde el ambito económico e incluso hasta afectar socialmente a una persona. Adicional a lo anterior se puede deducir la baja seguridad que es implementada en los hogares con respecto a el tratamiento de la información sensible.

El protocolo de mitigación de ciberataques se consolida como una herramienta util, en primer lugar para dar a conocer los riesgos mas comunes y en segundo lugar para culturizar a la gente del común de como enfrentarse a ellos y lograr reducirlos o mitigarlos. Ademas, la divulgación de este tipo de herramientas cumplen con el objetivo de generar un cambio de cultura mediante la modificación conductas inseguras.

La seguridad de la información puede considerarse como una tematica compleja, especialmente por las malas conductas implementadas por la población, por lo cual es recomendable contar con

estudios que profundicen en este tema, puesto que en Colombia las investigaciones al respecto se consideran escasas, con base a ello, este proyecto puede catalogarse como un estudio pionero mediante el cual se logró aplicar un modelo de sistema de gestión de seguridad de la información utilizando estándares de calidad y difundiendose a la comunidad (Estratos 3 y 4 de la ciudad de Bogotá) facilitando sus actividades, mas no implementando controles que las restrinjan.

8. ESTRATEGIA DE COMUNICACIÓN

La evidencia que se mostró anteriormente demuestra que el uso de la tecnología inadecuada trae consigo consecuencias de gran calibre que van desde la parte económica hasta afectar socialmente a una persona, la seguridad de la información cuenta con múltiple información y requiere contar con estudios profundos para entender gran parte del mundo de la seguridad pero el enfoque que se dio en esta investigación para un especialista en este campo pasa además de velar por incidencias de seguridad es la de poder divulgar de manera sencilla las opciones disponibles para implementar en un campo de acción que en Colombia no se había llevado demostrando que es posible implementar un ambiente seguro y aplicar un modelo de sistema de gestión de seguridad de la información utilizando estándares de calidad y lograr entregarlo a la comunidad (Estratos 3 y 4 de la ciudad de Bogotá)facilitando sus actividades y no la de implementar controles que restrinjan su actividades.

Gran importancia en el estudio recae en la divulgación en el entorno para generar un ambiente más seguro, en la que cada integrante hace parte de un número de piezas que hacen cohesión para cumplir un mismo fin generando un cambio de cultura modificando conductas inseguras. Documento final

9. **BIBLIOGRAFÍA**

Para facilitar el proceso de elaboración de la bibliografía se recomienda que esta sea generada de manera automática como se muestra en el video: http://www.youtube.com/watch?v=uGgpzRxMvGA.

Periodico El Tiempo. (06 de 04 de 2017). From www.eltiempo.com: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/fallas-en-la-ciberseguridad-segun-microsoft-75456

Secretaria Distrital De Planeacion. (n.d.). *Proyecciones de poblacion.* From Proyecciones de poblacion: http://www.sdp.gov.co/portal/page/portal/PortalSDP/Encuesta_Multiproposito_2014/Resultados_2014/Boletin_Resultados_Encuesta_Multiproposito_2014.pdf

PANDA SECURITY. (12 de 2008). *PANDA SECURITY.* From PANDA SECURITY: http://www.pandasecurity.com/NR/rdonlyres/DF1A6ACC-FABD-4E32-87AD-D35CA7B6B49C/0/Seguridad_hogares.pdf

Noam Ben-Asher, C. G. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior , 48*, 51-61.

Arabo, A. (2015). Cyber Security Challenges within the Connected Home Ecosystem Futures. *Procedia Computer Science , 61*, 227-232.

ARBELAEZ, A. (6 de 06 de 2014). *LOS CINCO PROBLEMAS DE CIBERSEGURIDAD MÁS COMUNES EN AMÉRICA LATINA.* From ENTER.CO: http://www.enter.co/especiales/enterprise/comunicado-de-prensa-ciberseguridad/

Facultad de Ciencias Políticas y Sociología / Universidad Complutense de Madrid. (22 de junio de 2012). *Cyberspace and Organized Crime.* Madrid, España: Gema SÁNCHEZ MEDERO1.

www.americamagazine.org. (2016). Hacking at Home. *America Press Inc. 2016. All rights reserved. www.americamagazine.org* , 4.

Nikos Komninos, M. I. (2014). *Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures.* IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 16, NO. 4,.

Consejo Nacional de Política Económica y Social, República de Colombia,Departamento Nacional de Planeación. (14 de 07 de 2011). *https://colaboracion.dnp.gov.co.* From https://colaboracion.dnp.gov.co: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3701.pdf

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. (11 de 04 de 2016). *www.oei.es.* From www.oei.es: www.oei.es/historico/salactsi/Conpes.pdf

PANDA SECURITY. (n.d.). *http://www.pandasecurity.com.* From

http://www.pandasecurity.com: http://www.pandasecurity.com/mexico/homeusers/security-info/cybercrime/phishing/

Masadelante. (n.d.). *http://www.masadelante.com.* From http://www.masadelante.com: http://www.masadelante.com/faqs/que-es-spyware

Kaspersky. (n.d.). *https://blog.kaspersky.es.* From https://blog.kaspersky.es: https://blog.kaspersky.es/que-es-un-botnet/755/

CCM. (n.d.). *http://es.ccm.net.* From http://es.ccm.net: http://es.ccm.net/contents/755-gusanos-informaticos

Infospyware. (n.d.). *https://www.infospyware.com/.* From https://www.infospyware.com/: https://www.infospyware.com/articulos/que-son-los-rootkits/

Informatica hoy. (n.d.). *http://www.informatica-hoy.com.ar/.* From http://www.informatica-hoy.com.ar/: http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Cracker.php

SANS Security The Human. (n.d.). *https://securingthehuman.sans.org.* From https://securingthehuman.sans.org: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201412_sp.pdf

Etapa. (n.d.). *http://www.etapa.net.ec/.* From http://www.etapa.net.ec/:

http://www.etapa.net.ec/Portals/0/Productos%20y%20Servicios/Cortafuegos%20o%20Firewall.pdf

Panda Security. (n.d.). *http://www.pandasecurity.com/.* From http://www.pandasecurity.com/: http://www.pandasecurity.com/homeusers/downloads/docs/product/help/is/2013/sp/84.htm

Karmany. (n.d.). *http://www.karmany.net/.* From http://www.karmany.net/: http://www.karmany.net/seguridad/49-general/150-8-webs-para-analizar-si-una-url-es-maliciosa

Definicion. (n.d.). *http://definicion.de.* From http://definicion.de: http://definicion.de/protocolo/

Profeco. (n.d.). *https://www.profeco.gob.mx.* From https://www.profeco.gob.mx: https://www.profeco.gob.mx/internacionales/com_elec.asp