ESTUDIO DE RIESGOS EN USUARIOS DE LAS REDES SOCIALES Y LA INTERNET APLICADO A JOVENES UNIVERSITARIOS DE LA CIUDAD DE SAN JOSÉ DE CÚCUTA

JOSE ANDRES RANGEL QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CÚCUTA
I-2017

ESTUDIO DE RIESGOS EN USUARIOS DE LAS REDES SOCIALES Y LA INTERNET APLICADO A JOVENES UNIVERSITARIOS DE LA CIUDAD DE SAN JOSÉ DE CÚCUTA

JOSE ANDRES RANGEL QUINTERO

Proyecto de grado presentado como requisito para optar al titulo de Especialista en Seguridad Informática

Director de Curso
ING. EDGAR ALONSO BOJACA GARAVITO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CÚCUTA
I-2017

NOTA DE ACEPTACIÓN

_____
_____
_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

_____
Ciudad y Fecha de entrega

CONTENIDO

pág.

LISTA DE GRÁFICAS

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

Hoy en día las redes sociales son medios que proveen de toda clase de posibilidades a las personas para relacionarse con otros individuos de otros países y culturas lejanas, con el fin de intercambiar conocimiento y experiencias, realizar manifestaciones sociales y políticas a través del intercambio de ideas.

Por todas estas razones es que dichos espacios en la web proveen de riesgos a las personas que hacen uso de las mismas, no obstante no quiere decir que en otros espacios de la red no genere inquietudes de seguridad pero son estos espacios abiertos de opinión e intercambio de contenido que son tan atrayentes para delincuentes ávidos de personas ingenuas que timar.

Los jóvenes están sujetos a dos riesgos tanto los que puedan ellos ser víctimas por amenazas o también los que pueden ocasionar cuando desconocen las políticas y leyes de seguridad de la información obteniendo información o datos personales de otras personas sin autorización.

Pero estos riesgos infortunadamente son más propensos de ser víctimas los jóvenes debido a sus capacidades de relacionarse con más facilidad y su poco conocimiento y/o experiencia en el medio, para identificar las amenazas que sobre ellos se ciernen.

El presente documento tiene como finalidad el análisis de los riesgos y amenazas sobre los cuales los jóvenes universitarios cucuteños están inmersos en las redes sociales y proveerles de herramientas ya sean de tipo psicológicas como tecnológicas para que puedan estar atentos para reducir o mitigar los peligros que corren en el Internet.

1. TITULO DEL PROYECTO

ESTUDIO DE RIESGOS EN USUARIOS DE LAS REDES SOCIALES Y LA INTERNET APLICADO A JOVENES UNIVERSITARIOS DE LA CIUDAD DE SAN JOSÉ DE CÚCUTA.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DESCRIPCIÓN DEL PROBLEMA

El entorno actual que apunta a un mundo más globalizado y pequeño a través de la conectividad de las redes y el internet permite poner en clara evidencia la importancia de que todos los usuarios sean conocedores de los riesgos a los cuales se enfrenta una persona en Internet.

Diversas amenazas en las que se ven inmersos los usuarios en la red como son el grooming, sexting, reputación virtual, ciberbullying, usurpación de las cuentas, estafas a través de las redes sociales, son potenciales riesgos que las personas pueden ser víctimas, si existe un desconocimiento de los riesgos y de métodos para evitarlos.

Con el auge del internet en Colombia dichos delitos que parecían ser más un problema de naciones desarrolladas, se han convertido en un problema de tipo local con agravantes como son las pocas restricciones que hay sobre los contenidos en la red y una laxa penalización a los infractores de este tipo de delitos informáticos.

Tal análisis de los riesgos en la internet se hace necesaria para tener un contexto claro de cuáles son las vulnerabilidades que los usuarios en la red los convierten en un blanco para los delincuentes cibernéticos.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cómo el estudio de riesgos en usuarios de las redes sociales ayudará disminuir el nivel de impacto al que se ven expuestos los jóvenes universitarios de la ciudad de San José de Cúcuta?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Disminuir los riesgos a que se ven expuestos los usuarios de las redes sociales y la Internet mediante la difusión de resultados del estudio de riesgos aplicado a los jóvenes universitarios de la ciudad de san José de Cúcuta.

3.2 OBJETIVO ESPECIFICO

Analizar los riesgos en las redes sociales y en el internet que afectan a los usuarios.

Identificar las amenazas en las redes sociales y el internet más recurrente en Jóvenes Universitarios de la Ciudad de San José de Cúcuta.

Diseñar un manual que contenga Tips, configuraciones y herramientas de software libre que puedan seguir los usuarios de las redes sociales y de internet para permitir una navegación segura.

4. JUSTIFICACIÓN

Internet abre un nuevo mundo de posibilidades en cualquier circunstancia de las personas, desde la forma en que se comercian con artículos hasta las relaciones con otros individuos. No obstante, la protección de nuestros datos, nuestros bienes y buen nombre debe ser siempre una prioridad. Analizar y tener una descripción clara de cuáles son los riesgos que son víctimas los usuarios en la red es imperativo en la actualidad, donde los usuarios al mundo de la información globalizada son cada vez más jóvenes y sin un criterio claro de la percepción del riesgo.

Para las personas las redes sociales son llamativas, debido a que en estos espacios las personas se sienten más apreciadas, permitiendo relacionarse con los demás, usando un lenguaje propio y donde se ven inmersos gustos e intereses reales. Por tanto la propuesta brindar herramientas para el uso de la internet y las redes sociales, combinando con unas pautas de prevención, con un proceso pedagógico donde estén involucrados todos los entes relacionados con el usuario y que este asuma un rol de mayor importancia.

El objetivo es concientizar a los Usuarios de Internet y redes sociales sobre el responsable uso de las tecnologías de la información. Permitiendo así que no sean herramientas vacías, que permitan un cambio y prevención de riesgos tecnológicos que coloquen en riesgo el buen nombre y la identidad de cada persona como principales actores de su personalidad, teniendo en cuenta que los habitantes del país son libres de tendencias y que a su vez se les garantiza todos sus derechos.

Teniendo en cuenta lo anteriormente fundamentado podemos deducir que el manejo de la seguridad informática en las redes sociales y el internet es la base

principal de los jóvenes de la época ya que se presentan alteraciones en las contraseñas y usuarios, para acceder a toda la información de carácter privado de los jóvenes y así utilizar la violación de la intimidad en factores vulnerables y en un riesgo individual y familiar de los usuarios.

5. ALCANCE Y DELIMITACIÓN

En este proyecto buscamos Precisar riesgos y vulneraciones de usuarios en Jóvenes de La Ciudad De San José de Cúcuta; en Establecimientos Educativos Universitarios como principal población de manejo y acceso a las Redes sociales y el Internet; teniendo en cuenta Tips de Conocimiento y herramientas de prevención desde el análisis de los riesgos identificados en la población; teniendo en cuenta que en la actualidad no estamos vinculando a las redes abiertas de navegación de internet que permiten que todos los usuarios tengan nuestro número de usuario u otro que nos identifique como tal en cualquier red.

6. MARCO REFERENCIAL

6.1 ANTECEDENTES

El origen de las redes sociales data desde el año 1971, el cual se debe al envío del primer correo electrónico entre dos pc; posterior a esto más exactamente 7 años tras este descubrimiento Ward Christensen y Randy Suess desarrollan el BBS (Bulletin Board Systems) con el propósito de dar a conocer temas como reuniones, noticias e información a sus amigos. En el año 1994 es desarrollado y puesto en marcha GeoCities, herramienta que permite a los usuarios la creación propia de páginas web y que estos sean catalogados según el tema de creación, siendo tan popular que alcanza al millón de páginas en un año de su lanzamiento, posterior a esto en este mismo año es desarrollado Classmates por Randy Conrads, la cual es una red social cuyo objetivo principal es encontrar antiguos compañeros de estudios, siendo considerada la primera red social, puesto que esta sería la precursora de entornos similares como es Facebook y demás redes sociales que sus principales características consistían en la búsqueda de amigos, conocidos y ex compañeros de estudio en diferentes sectores de la sociedad.

En el año 2005 es lanzado al público YouTube el cual permite compartir y visualizar videos siendo muy popular en su creación por las características de ser libre y abierto, durante ese mismo año MySpace es considerada la red social más utilizada en los Estados Unidos; al transcurrir un año es inaugurado Twitter el cual permitía dar a conocer opiniones de las personas en 140 caracteres, siendo viral su concepto novedoso de dar a conocer los pensamientos de la gente en determinados temas de forma rápida, los buscadores se convierten en herramientas muy útiles para encontrar información siendo Google el líder con 400 millones de búsquedas al día. En este mismo periodo de tiempo en España se

lanza Tuenti una red social orientada a los jóvenes y Badoo se posiciona como una herramienta social para la búsqueda de parejas.

En el año 2008 Facebook alcanza su mayor potencial al poseer 400 millones de usuarios, siendo relegada MySpace con 57 millones de usuarios y es lanzado a producción Tumblr el cual se convierte en el principal competidor de Twitter en su esquema de transmisión de comentarios sociales.

Durante el año 2010 Google lanza al público Google Buzz el cual es una red social que está ligada al sistema de envío de correo electrónico Gmail, siendo novedosa como se esperaba y registrando 9 millones de entradas por sus usuarios en tan solo una semana, durante este mismo año los usuarios de la internet alcanzan la cifra de 1,97 billones de personas siendo para ese momento el 30% de la población mundial, los usuarios de Tumblr realizan 2 millones de post al día, y Facebook llega a una astronómica cifra de 550 millones de usuarios, y a su vez Twitter promedia 65 millones de post al día y LinkedIn registra 90 millones de profesionales de diversas áreas en busca de oportunidades laborales, y YouTube alcanza la increíble cifra de 2 billones de visitas diarias.

En el año 2011 redes sociales que quedaron relegadas por Facebook y Twitter se ven obligadas a rediseñarse para estar al día con las exigencias de los usuarios que en dichos aspectos se convirtieron en ávidos consumidores en línea como son el caso de MySpace y Bebo. En este mismo año Google lanza al público Google+ popularizando dicha red social entre los usuarios de Gmail.

Durante el año 2012 Facebook llega a un tope de 800 millones de usuarios, por su parte Twitter pasa a tener 200 millones de usuarios y a su vez Google+ ya ha llegado a una cifra de 62 millones, siendo una proyección que va en aumento

permitiendo pensar que la mayoría de la población mundial pertenecería a alguna red social.

El crecimiento de las redes sociales se basa en el hecho de las distancias entre las personas por tal motivo que estos entornos virtuales permiten acercar a las personas, permitiendo a las personas compartir toda clase de información Multimedia, juegos multiplataforma en línea, bases de datos, comercio en línea entre otros, permitiendo masificar los contenidos y abriendo espacios para el pensamiento libre. El mundo globalizado y actual se caracteriza por el cambio rápido en el pensamiento y actitudes de las personas, esto ha provocado que entre los usuarios de las redes sociales riesgos que son necesarios solucionar a través de la generación de conciencia en el uso correcto de las redes sociales como también de técnicas aplicadas con tecnología de la información para mitigar la exposición a riesgos en la internet, puesto que se ven afectada la intimidad y la capacidad de las personas de expresarse libremente de algún tema, puesto que son los mismos usuarios son los que actúan sin pensar en la información que divulgan poniendo hasta en riesgo su integridad física.

No obstante no solo es la exposición de información personal de forma inadecuada, sino las acciones poco éticas que asumen los usuarios de las redes sociales tal es el caso de la suplantación de la identidad, las cadenas de correos electrónicos de forma indiscriminada más conocidos como spam, obtener información de un usuario sin su permiso el cual es denominado Phishing, el ingreso no autorizado a correos electrónicos, entre otras acciones que pueden ser consideradas como bromas o que puedan ser actividades que tengan la intención de dañar a otro usuario.

En ese orden de ideas este proyecto permitirá brindar un análisis de las vulnerabilidades en la intimidad de los usuarios de las redes sociales, para tal fin

se analizara la seguridad de la información, desde varios contextos desde el punto de vista de los riesgos que asumen los usuarios hasta los que en si se ven sometidos los usuarios por el uso indiscriminado de las redes sociales, y esto se debe a que todos los riesgos en los que se ven inmersos los usuarios radican en la falta de conocimiento sobre el uso correcto de las mismas, generado por descuidos e ingenuidad en el momento de compartir información, relacionado con la falta de medios de orientación pedagógica que preserve su identidad y privacidad en la internet.

6.2 MARCO TEÓRICO

Los jóvenes en la actualidad crean o hacen uno de grupos de redes sociales, dependiendo de sus gustos particulares, debido a que la internet ofrece diversidad de tendencias sobre las cuales los jóvenes pueden compartir u opinar, siendo esta situación lo que ha hecho que las redes sociales se convirtieran en un éxito y que a su vez tengan tal acogida entre la juventud.

Existen riesgos y beneficios en las redes sociales teniendo en cuenta el impacto de las mismas en el entorno de los jóvenes y su cotidianidad; basado en un fenómeno actual que trae consigo riesgos y beneficios; los aspectos que se desprenden son de tipo físico puesto que estos pueden afectar la parte física de la persona que hace uso de estos medios, a su vez son de tipo psicológicos, ya que afectan el actuar del individuo, de tipo económico en vista de estos pueden ser aspectos que mejoren o empeoren la adquisición de dinero del usuario y por ultimo de tipo social puesto que aliena al individuo de un entorno de interacción con las personas. El concepto de red social y de igual manera tener en cuenta su historia.

El concepto de red social puede considerare como el compuesto de varias personas, las cuales se relacionan a través de diversas razones de diferentes tipos como gustos, parentescos, etc.

Según el Autor Zamora (2006) el cual tras asistir a una disertación sobre Gestión en Organizaciones del Tercer Sector, que se realizó en la Universidad Di Tella de Buenos aires (2001), lo siguiente: “Las redes sociales pueden considerarse como como medios en los cuales las personas mantienen una interacción, a través de la corresponsabilidad de información de cualquier índole entre las personas, agrupaciones o instituciones. Se entrevé que las redes sociales son medios en desarrollo constante que incluyen personas que poseen las mismos problemas y pensamientos sobre un tema en particular, y los cuales se unen en pos de solución de dicha problemática. Los grupos que conforman las redes sociales están compuestos por personas solitarias y discriminadas, que son segregadas por la sociedad convencional, puesto que en la sociedad de la cual han sido marginados no tienen relevancia, puesto que en su pensamiento no poseen habilidades que los diferencien de los demás.”

Las redes sociales se pueden considerar como entornos virtuales que las personas utilizan para relacionarse con todo tipo de individuos ya sean conocidas o no a su cotidianidad las cuales generan el primer choque cuando se acepta o invita a quien es desconocido; Permite Intercambiar información, y a su vez ser partícipe de disertaciones y comentarios sobre temas específicos que interesen a la comunidad. Las redes sociales según lo dice el autor Zamora lleguen a tener un sistema abierto, significaría que los usuarios son los protagonistas de cada blog social; que hace que la red sea más conocida según los usuarios que tenga; puede considerarse una red social es la unión de varias personas. Angelina Biesot (2011), periodista española, a través de su artículo ilustra los riesgos que existen puesto que siendo en su mayoría menores de edad los que acceden a las redes sociales y que estos se relacionen con desconocidos, los expone puede que

suene muy alarmante que las redes sociales están incluidas todo el tipo de personalidades lo que genera la vulnerabilidad y pueda ocurrir algo. El hecho es alarmante pero según las personas que lo utilizan también hay individuos que acceden a estos medios para realizar acciones condenadas por la ley.

Las redes sociales generan un interés particular en los jóvenes y se ha incrementado con el tiempo y la vulnerabilidad que existen en la accesibilidad a las mismas; en la actualidad se evidencia la relevancia sobre lo que expone la internet a lo que se plantea la pregunta ¿el Internet como ha fluido tanto? los jóvenes utilizan la internet y las redes sociales como un soporte a la que no pueden encontrar en la vida real en sus familias o en su entorno, Las redes sociales en ocasiones se convierten en vicio o adicción, lo que genera en el ser humano la mismas situaciones específicas de una persona con adicción al consumo de sustancias psicoactivas o alcohol, ya que por estar en el blog social y no omitir detalle de lo que sucede en el mundo, se deteriora su persona y si integridad física; la dependencia generada es amplia y destructiva cuando no se infiere lo positivo que muestra el internet y la red social.

Según Costa en el artículo publicado en el año 2010 Las redes sociales aportan a las personas muchos beneficios, pero asociado a estos beneficios existen muchos riesgos, puesto que poner a disposición de las demás personas información personal y demás contenidos permite dar a la sociedad virtual medios para de manera deshonesta atacar a los usuarios. Las redes sociales se convierten en medios que distraen a los jóvenes en sus labores cotidianas como lo son estudiar y demás responsabilidades, las aplicaciones que se han adicionado a las redes sociales tales como juegos en línea, han adoptado código puede ser virus o troyanos, siendo objeto de robos de información o que los archivos sean dañados o sus pc a través de estos juegos que en imagen lucen inofensivos.

Las redes sociales y las pruebas que verifican en Las redes sociales desde su inicio tienen como parte de sus principios de funcionamiento, la teoría de los 6 grados de separación, que consiste en que si dos personas cuya distancias entre si se les puede encontrar relación a través de varias personas que sean conocidos simultáneamente y el otro principio consiste en la teoría de los 10 saltos, la cual consiste en que las personas pueden tener cosas en común a través de máximo 10 eslabones, esto se puede explicar de esta forma:

Si una persona está relacionada con 100 individuos, y a su vez estos están relacionados con otros 100, de esta manera si la primera persona solicita que sus conocidos envíen un documento a cada uno de las personas con la que está relacionada, la relación para a ser de 10000 conocidos.

En la evidencia de la vulnerabilidad de los datos en cada red social, las personas aun teniendo en cuenta los estudios realizados y los respectivos resultados no encuentran claridad a su adicción lo que hace que sigan conectados compartiendo fotos, lugares de ubicación, que permite a los incluidos en la red acceder y conocer cada situación realizada por los usuarios, sin importar la población que comparta el entorno con el usuario teniendo en cuenta los dos principios de prueba mencionados anteriormente.

6.3 MARCO CONCEPTUAL

6.3.1 Avatar. Corresponde a una imagen o una fotografía con la cual los usuarios se identifican en el internet[1].

[1] COLOMBIA DIGITAL. Conceptos TIC [en línea]. [Citado 25 mayo 2017]. Disponible en Internet en: https://colombiadigital.net/actualidad/articulos-informativos/conceptos-tic.html

6.3.2 Chain e-mail. Corresponde a un correo electrónico enviado de manera masiva a varios destinatarios, el cual está sujeto a un premio en caso de envío y una penalidad por no enviarlo; los Jóvenes no tienen prudencia y cautela sobre a quién le reenvían los mensajes con su usuario personal; tener evidencia de la fase de navegación[2].

6.3.3 Chat. Es una aplicación que permite enviar y recibir mensajes de forma instantánea en la Internet[3].

6.3.4 La Ciberintimidación. Corresponde a la intimidación repetitiva a través de las tecnologías informáticas, que ocasiona en la victima problemas de seguridad y este corresponde a un delito que puede ser denunciado, lo anteriormente expuesto se presenta porque los Jóvenes no tienen prudencia en la conectividad de las redes sociales. Otro de los más grandes factores es el Ciberacoso (cyberbullying) es ataque psicológico a través de las redes sociales y aplicaciones de comunicaciones, el cual busca lastimar o presionar a la persona, en dicho abuso la persona afectada no conoce la identidad de su agresor. Con esto propende una figura importante el Cyberstalker es una persona que de manera constante revisa o está pendiente de lo que hace otra persona, es un acosador cibernético. Este en su obsesión puede recurrir a la suplantación de la identidad de un individuo, a través del borrado o la adulteración de la información, para cometer grooming que consiste en el abuso de menores de 18 años. Posterior a esta conducta antisocial corresponde el Hacker, el cual es un individuo con habilidades informáticas para ingresar en sistemas de información sin autorización a través de unos códigos éticos en contraposición de los Crackers los cuales corresponden a individuos que realizan dichas incursiones en sitios no autorizados con propósitos delictivos. Inician o parecen diferentes factores como Nomofobia la

[2] GLOSARIO DE INFORMÁTICA E INTERNET. Chain e-mail [en línea]. [Citado 25 mayo 2017]. Disponible en Internet en: http://www.internetglosario.com/849/Chainemail.html
[3] COLOMBIA DIGITAL. Op. cit., p. 1.

cual consiste en un temor asociado al no disponer de un equipo móvil. Pharming es un fraude que se da a través de la suplantación de páginas web, las cuales conducen a los usuarios a sitios falsos para realizar estafas. Phishing es una estafa que consiste en que a través de correos electrónicos se inviten a los usuarios a visitar páginas falsas donde a través de engaños se les captura información tales como claves bancarias y demás. Sexting consiste en compartir imágenes propias con contenido sexualmente explícito a través del celular o el internet. Síndrome del mensaje múltiple consiste en uso simultáneo de varias conversaciones en chats, redes sociales, etc. Con el propósito de sentirse como una persona incluida en diversos temas o grupos[4].

6.3.5 Smishing. Es una variación del phishing el cual consiste en el envío de correos electrónicos o enlaces que redirigen a los usuarios a sitios web falsos, que a través de software malicioso descargan la información de manera automática sin conocimiento del usuario. Las víctimas de Smishing reciben mensajes de texto por celular similares a estos:

“El crédito bancario está listo, por favor ponerse en contacto para completar el proceso a través del siguiente enlace”, cuando se accede al sitio web, los usuarios son forzados a realizar la descarga de una aplicación el cual consiste en un software malicioso[5].

6.3.6 Spoofing. Consiste en la suplantación de la identidad para usos delictivos, y tiene varias facetas entre las cuales está la suplantación de la IP, la suplantación

[4] UNICEF. ¿Qué es la ciberintimidación? [en línea]. [Citado 25 mayo 2017]. Disponible en Internet en: http://www.alguien.do/quiero-estar-bien/en-mi-comunidad/que-es-la-ciberintimidacion
[5] MOLINA. Leonela. Delitos informáticos [en línea]. [Citado 26 mayo 2016]. Disponible en Internet en: http://es.calameo.com/books/005155407963f214f1a28

de un ARP, la suplantación de un DNS, la suplantación de una página web o un correo electrónico[6].

- IP Spoofing: Suplantación de IP. Dicho proceso se basa en el reemplazo de la dirección IP por otra, a través de software especializado y puede ser aplicado a cualquier protocolo contemplado dentro de TCP/IP, las respuestas realizadas por parte del host serían los paquetes alterados estarían conducidas al a la IP falsa[7].

- ARP Spoofing: Consiste en suplantar la identidad a través de la adulteración de la tabla ARP. Este tipo de suplantación se desarrolla cuando las tramas de solicitud y respuesta de ARP se modifican para engañar la tabla ARP del equipo víctima y este se forzado a que se dé respuesta a un host que no corresponde con el legítimo[8].

Ethernet es un protocolo que se ejecuta a través de las direcciones MAC. El protocolo ARP tiene como función la traducción de las direcciones IP a MAC permitiendo la comunicación; cuando un equipo que hace las veces de host envía una trama ARP-Request solicitando la MAC del equipo que tiene dicha IP con la que se desea comunicar, el equipo con la IP que está siendo solicitado realiza la respuesta con ARP-Reply diciendo cuál es su MAC[9].

- DNS Spoofing: Consiste en la suplantación de un nombre de dominio a través del cambio de la IP, a través de engañar los ingresos del nombre de dominio-IP

[6] MENDEZ, L. Que es el Mail Spoofing y como evitarlo usando SPF [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: https://www.webempresa.com/blog/que-es-el-mail-spoofing-y-como-evitarlo-usando-spf.html
[7] Ibid., p. 1.
[8] GARCIA, Carlos. Hablemos de Spoofing [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/
[9] Ibid., p. 1.

de un servidor de nombres, esto se debe a las vulnerabilidades que este puede presentar[10].

- Web Spoofing: Consiste en suplantar una página web que existe en realidad, con el propósito de adquirir información de un usuario ya sea cookies, contraseñas y datos personales.[11].

- E-Mail Spoofing: Consiste en suplantar los correos electrónicos, a través de la configuración de un servidor SMTP[12].

- GPS Spoofing: Consiste en engañar a un equipo receptor de GPS al transmitir una señal más fuerte de que se recibe por parte de los satélites GPS, esta se organiza de tal manera que es similar a las señales GPS comunes, no obstante esta variación hace que el equipo receptor concluya una posición diferente a la real[13].

6.4 MARCO LEGAL

La Norma Premium del País Como es la Carta magna la **CONSTITUCIÓN POLÍTICA DE COLOMBIA** a través de sus artículos se han gestionado determinaciones jurídicas que han regulado el uso de la internet y las redes sociales sobre las cuales se cometen delitos. Desde el año 2018 se han

[10] PAEZ, Andrea. Tipos de spoofing [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: http://andrea0712.blogspot.com.co/2011/05/ejercicios_11.html
[11] Ibid., p. 1.
[12] LEON ROJAS, Juan. Ataque de suplantación de identidad (mail-spoofing) [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: http://cala.unex.es/cala/cala/mod/forum/discuss.php?d=7875
[13] EDUCATIVO SEGURIDAD INFORMÁTICA. Spoofing [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: http://segurdadenredes.blogspot.com.co/2014/11/pagina-en-construcion.html

promulgado varias regulaciones que conllevan a salvaguardar los derechos de las víctimas a causa de estos medios virtuales.

Es de suma importancia comenzar desde el aprendizaje de todos los derechos que han sido estipulados en la constitución política de Colombia que tienen relación con el tratamiento de la información de las personas y como estas pueden ser expresadas, según esta consignado en el **ARTÍCULO 15**, el cual explica que todas personas tienen derecho a la intimidad y que el estado debe proveer para que este derecho prevalezca y de igual manera tienen por ley el derecho a tener conocimiento de toda clase de información consignadas en diversas bases de datos, ya sean públicas o privadas.

Este articulo corresponde a un criterio sobre el cual se basa la ley colombiana para salvaguardar la intimidad y el buen nombre de los ciudadanos, este derecho se garantiza a través de la tutela, cual viene soportada en el ARTICULO 86, a través de este mecanismo los ciudadanos pueden solicitar ante los jueces restitución de los derechos vulnerados.

Continuando sobre la regulación jurídica el ARTÍCULO 20, permite regular y garantizar como las personas pueden expresar sus pensamientos, informando y recibiendo información de carácter real sin parcialidad, de ser críticos y crear medios que difundan la información; toda vez manteniendo la honra y el buen nombre de las personas, manteniendo la libertad de expresión y manteniendo la posibilidad de la rectificación.

Llevando al contexto de las redes sociales los artículos anteriormente en mención, se debe tener en cuenta que el derecho a la libre expresión tiene limitaciones, puesto que estos van hasta el punto de la vulneración de los derechos de los demás individuos.

Tras realizar el análisis de la constitución política sobre la cual se cimienta la sociedad en materia de derechos y deberes, es pertinente abordar las leyes que brindan las garantías legales los personas que han sido víctimas del uso indiscriminado y poco ético de las tecnologías de información y comunicación. En primer medida se encuentra la Ley 679 de 2001, la cual penaliza la creación y distribución de pornografía con menores de edad en la internet, brindando protección a las víctimas de toda clase de formas de abuso sexual en la cual estén relacionados menores de edad, según lo estipula el artículo 44° de la constitución política de Colombia.

El CAPITULO II de la ley 679 de 2001, permite generar factores de autocontrol y comportamientos éticos en el uso de la internet y los sistemas de información, siendo acreedores de penas administrativas y de tipo penal a las personas que incurran en estos hechos, con el propósito de prevenir la creación y comercialización de pornografía infantil a través de la internet.

Tiempo después se promulgo una norma la cual regularía el Habeas data a través de los proyectos de Ley 05 del 2006 y Proyecto de Ley 27 de 2006, ambos textos aprobados por el senado en Octubre del 2006, en base a los anteriores mencionados se produjo la Ley 1266 del 31 de diciembre del 2008, la cual es conocida en la actualidad como la Ley del Habeas Data, en base a esta ley se regula toda clase de información de los ciudadanos contenida en las diversas bases de datos de las entidades públicas y privadas, con el propósito de brindar las garantías de actualización y uso responsable de los datos y de esta manera no sean afectados los derechos y honra de los ciudadanos.

Con la masificación de la internet y las redes sociales se consideró pertinente por parte del congreso promulgar la Ley 1273 del 5 de enero del 2009, con el propósito de proteger la información y los datos, para proteger los sistemas de

información en contra de intrusión no autorizada, robo y adulteración de los datos, incorporando penas pecuniarias y privativas de la libertad dependiendo de la relevancia del hecho.

Se puede destacar que en Colombia a través de los años se ha construido un marco legal que brinde garantías y protección a los ciudadanos en delitos relacionados con la internet y las redes sociales, pero en ese mismo accionar y masificación de estos escenarios de participación virtual es necesario que se siga accionando desde el congreso leyes que cobijen a las víctimas de toda clase de hechos delictivos.

7. MARCO METODOLÓGICO

7.1 METODOLOGÍA DE INVESTIGACIÓN

El proceso investigativo está desarrollado en un enfoque mixto, el tema de investigación es sobre el Estudio de Riesgos de las Redes Sociales en la población Universitaria, haciendo referencia en cuál es su pensamiento y accionar, es aquí donde se implementa un método Cuantitativo en donde se hace una medición de la cantidad de personas que se ven influenciadas por las redes sociales, y para obtener dicho análisis se hace uso de instrumento tipo encuesta con una serie de preguntas cerradas en base a este se observa la utilización y el propósito de las redes sociales sobre las cuales se está relacionando.

A través de un método cualitativo donde se observe y no se interactúe en el establecimiento educativo universitario, en el cual se analice las reacciones físicas que pueden acarrear el uso indiscriminado de las redes sociales de esta manera determinar su desenvolvimiento con otras personas, como es su estilo al vestir y si esta vestimenta se ve relacionada con las personas vinculadas a sus redes sociales, siendo esta una característica de la aplicación de un enfoque mixto.

El análisis y gestión de los riesgos que afectan a los jóvenes en el uso de las redes sociales esta soportado a través de la metodología MAGERIT, el cual permite realizar una identificación y caracterización de los riesgos que conllevan el uso de los sistemas de información y todos sus contextos asociados, que para efectos de este proyecto son las redes sociales, y esto permite la creación de políticas que deben aplicarse para mitigar los riesgos que han sido identificados en esta investigación.

MAGERIT ha determinado el concepto de seguridad como el proceso de soportar a través de un mínimo de estándares de confiabilidad, las actividades ilegales que afectan el funcionamiento y la calidad de la información albergada en los sistemas de información.

MAGERIT hace uso de conceptos para su análisis los cuales son: activo, amenazas, vulnerabilidad, nivel de impacto, riesgos y controles.

7.2 FUENTES DE RECOLECCIÓN

Las fuentes de recolección a utilizar serán la Encuesta Cerrada, con rango de Datos como Sexo, Edad y Preguntas de respuesta Si o No, para evidenciar así la fase cuantitativa de acuerdo a las respuestas de la Población, Así mismo desde el Enfoque cualitativo, se llevara a cabo la Observación no Participante, que permita analizar el uso del tiempo en las Redes sociales de los Jóvenes Universitarios de la Ciudad de Cúcuta.

Se aplicará las fuentes de recolección en los planteles Universitarios de la Ciudad de Cúcuta, con el fin de tener clara la población identificada en el título del proyecto y así mismo la viabilidad de la información se de jóvenes que estén en la población Universitaria y que manejen las Redes Sociales, teniendo el objetivo principal y lo que se busca general con el resultado final de la Investigación.

7.3 MUESTRA

La Muestra a utilizar es Población universitaria de rango de 17 a 20 años, que se encuentren en las Universidades Públicas de la Ciudad de Cúcuta, con el fin de dar confiabilidad a los Datos y a la Población a entrevistar, se realizara la aplicación de los instrumentos de recolección en las Universidades Directamente.

8. PRODUCTO RESULTADO A ENTREGAR

El resultado será un documento escrito final del desarrollo del proyecto de investigación cuyo enfoque es el Estudio De Riesgos En Usuarios De Las Redes Sociales Y La Internet Aplicado A Jóvenes Universitarios, será una guía de socialización en el Medio educativo de las Universidades Donde se aplicaran los Instrumentos, de la misma Forma se Realizara una Presentación en Línea, para que las personas interesadas en el tema u otros estudiantes cuyo enfoque sea la misma temática, tengan un soporte claro y conciso de los factores incidentes en la sociedad.

Analizar cuáles son los riesgos en las redes sociales y en el internet que afectan a los usuarios.

Cuando se habla de riesgos en las redes sociales se puede evidenciar con claridad la afectación que tienen los usuarios. Cada vez son más los delitos a los que se ven expuestos los menores de edad al utilizar el computador el Smartphone, lo cual hace parte del método que utilizan los padres para subsanar el poco tiempo o espacio para compartir con ellos, solo recibiendo recomendaciones básicas tales como:

Las recomendaciones de años atrás a los niños previo a la incursión de la internet y las redes sociales a la sociedad consistían en “no aceptar cosas de extraños” o “mira si no vienen vehículos al pasar de un lado de la calle al otro”, estas han sido reemplazadas por no “chatear con extraños” o “cuidado con lo que pones en las redes sociales”.

Las redes sociales han modificado nuestra manera de comunicarnos en el mundo, la necesidad de estar en línea en todo momento ha brindado múltiples beneficios,

pero a su vez acarrea consecuencias tales como toda clase de delitos informáticos en lo que los menores se ven inmersos en el momento de utilizar el computador, los celulares de última generación y abrir una página de Internet sin previo acompañamiento de un adulto o responsable del contenido evidenciado en estas páginas ya que no tienen bloqueo sino que son abiertas a toda la población y de acceso fácil para la información.

Analizar e identificar cuáles son las amenazas en las redes sociales y el internet que son más recurrentes en los Jóvenes Universitarios de la ciudad de San José de Cúcuta. Desde la perspectiva de la ciudad de Cúcuta como una zona fronteriza que involucra dos naciones junto con sus actores democráticos y políticos, se identifica que la línea virtual es cada vez más delgada de la del mundo real, lo cual despierta muchas necesidades en las condiciones y vulneraciones que pueden tener los niños, niñas, adolescentes y jóvenes con respecto a cada situación específica cuando ingresan a las Redes Sociales, por lo cual las familias no han despertado a la realidad que el mundo está mostrando, si existiera percepción sobre el riesgo que se corre cuando un niño, niña, adolescente o joven que aun desconozca la realidad de lo virtual, ingresa sin acompañamiento o con la precaución de lo que los blogs sociales puedan mostrarle y adicional a ello como los problemas de robo de identidad o información se muestran a diestra por la mal intención de las personas que hacen daño, teniendo en cuenta la situación específica y los antecedentes de desapariciones de jóvenes en la zona de frontera cuando contactan amigos por internet y se proponen citas, se evidencia en el año que han existido múltiples desapariciones de cada uno de los países, por ello se deroga una gran responsabilidad sobre los padres teniendo en cuenta que sus hijos son abordados por personas mal intencionadas que buscan sacar provecho de la desinformación en la que se encuentran, es allí donde inician los Ciber delitos, los cuales dañan y vulneran la imagen de los Jóvenes de la Ciudad de Cúcuta.

Análisis de resultados de encuestas aplicadas en las universidades públicas, teniendo en cuenta el siguiente esquema de recolección. La muestra de los jóvenes universitarios se tomó de la Universidad Francisco de Paula Santander, cuyo tamaño de medición corresponde al 10% de la población universitaria matriculada, la UFPS es una universidad pública de San José de Cúcuta, con una proyección de generar profesionales de alta calidad para el departamento y el país, siendo la selección aplicada en la biblioteca del campus universitario en una hora de alta concurrencia por parte de los estudiantes un periodo regular de parciales, seleccionados de manera aleatoria con el fin de abarcar la mayor cantidad de disciplinas académicas y de todo ámbito universitario.

8.1 INSTRUMENTO DE RECOLECION DE INFORMACION

"Riesgos y amenazas en las Redes sociales e internet"

1. Riesgos más evidentes en los Blogs Sociales

Robo de Contraseña____ Suplantación de identidad_____ Perfiles Falsos____ Otros ____

2. Conoces los siguientes delitos informáticos (Marca con una X)

	SI	NO
Ciberintimidación	____	_____
Ciberbullying	____	_____
Cyber stalker	____	_____
Smishing	____	_____
Spoofing	____	_____

3. De los siguientes aportes cuales consideras VERADEROS o FALSOS

- La responsabilidad de la edad de ingreso en Niños, Niñas, Adolescentes y jóvenes a los blogs sociales es de los Padres V (___) F(___)
- Todas las personas conocen cuales son las combinaciones para una contraseña segura Alfa numérica V (___) F(___)
- Debemos aceptar todas las invitaciones que ingresan a nuestras páginas o redes sociales aun desconociendo la procedencia de la persona o grupo V (___) F(___)

4. Usa la Internet Para

Paginas sociales_____ Buscar amigos _____ Consulta trabajo _____ Otros_____

5. Comparte sus Contraseñas con

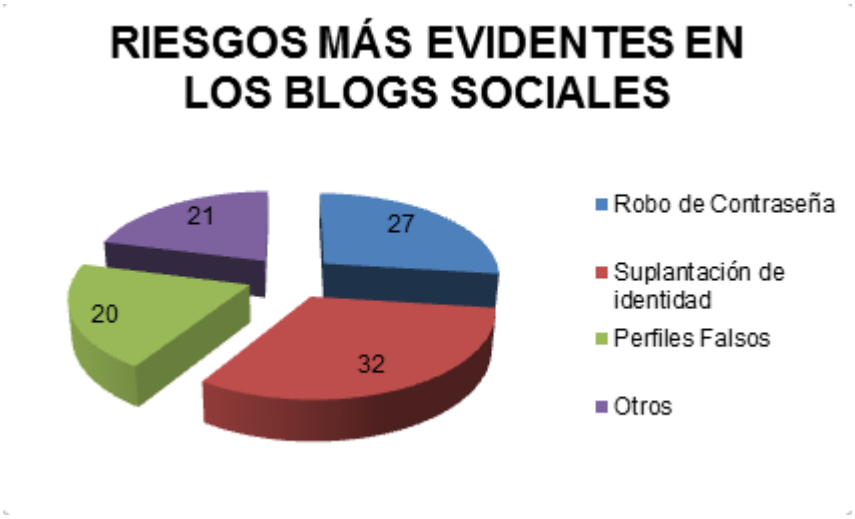
Nadie ____ Amigos____ Pareja___ Familia ____ Otro____

De lo anterior y tras aplicar la encuesta a 100 jóvenes universitarios, se obtuvieron los siguientes resultados.

1. Riesgos más evidentes en los Blogs Sociales:

Robo de Contraseña: 27 estudiantes con un porcentaje de 27%
Suplantación de identidad: 32 estudiantes con un porcentaje de 32%
Perfiles Falsos: 20 estudiantes con un porcentaje de 20%
Otros: 21 estudiantes con un porcentaje de 21%

Gráfica 1. Riesgos más evidentes en los Blogs Sociales

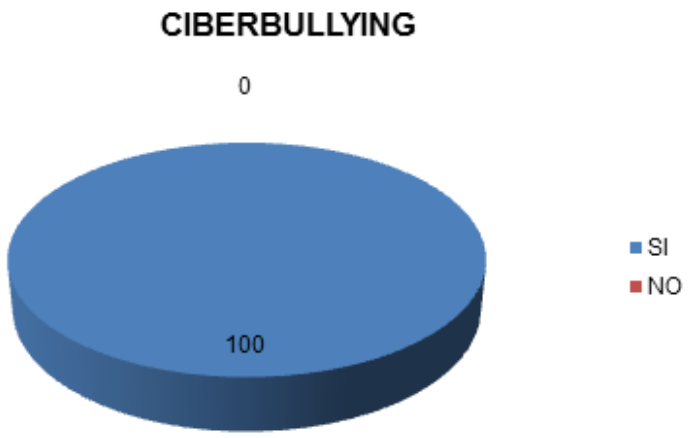


Fuente: El Autor.

2. Conoces los siguientes delitos informáticos:

	SI	NO
Ciberbullying	100 (100%)	0 (0%)

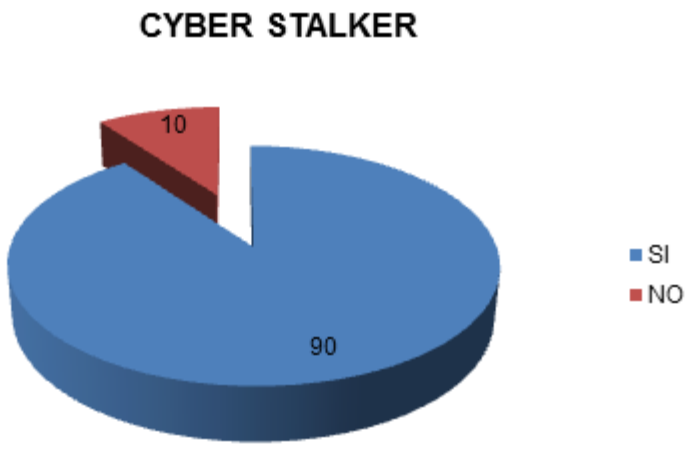
Gráfica 2. Ciberbullying



Fuente: El Autor.

Cyber stalker	90 (90%)	10 (10%)

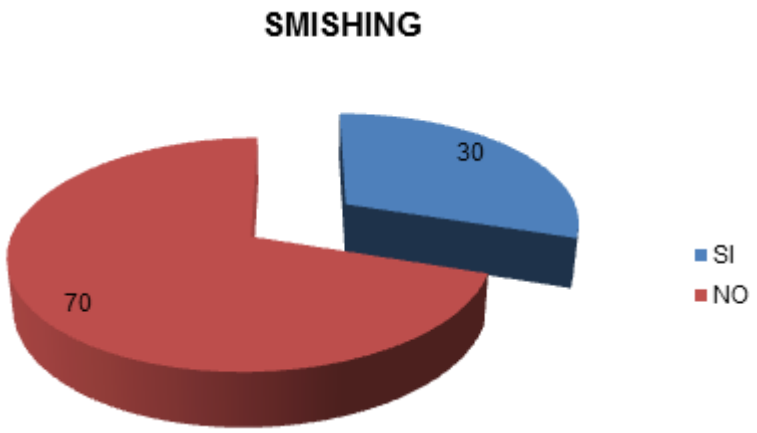
Gráfica 3. Cyber Stalker



Fuente: El Autor.

Smishing	30 (30%)	70 (70%)

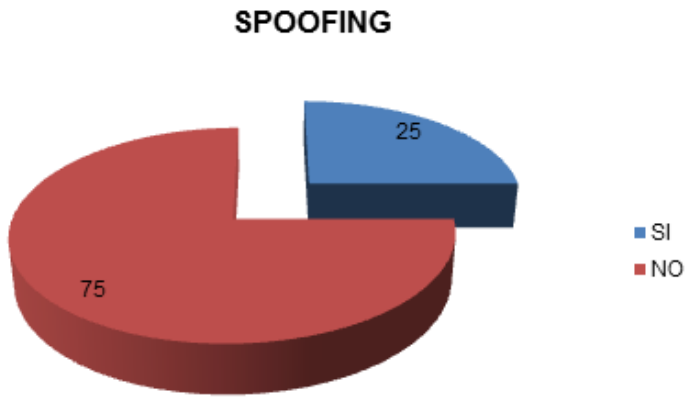
Gráfica 4. Smishing



Fuente: El Autor.

Spoofing	25 (25%)	75 (75%)

Gráfica 5. Spoofing



Fuente: El Autor.

3. De los siguientes aportes cuales consideras VERADEROS o FALSOS

- La responsabilidad de la edad de ingreso en Niños, Niñas, Adolescentes y jóvenes a los blogs sociales es de los Padres V (85%) F (15%)

Gráfica 6. Responsabilidad del uso de internet en los jóvenes

Fuente: El Autor.

- Todas las personas conocen cuales son las combinaciones para una contraseña segura Alfa numérica V (45%) F (55%)

Gráfica 7. Generación de claves alfanuméricas

Fuente: El Autor.

- Debemos aceptar todas las invitaciones que ingresan a nuestras páginas o redes sociales aun desconociendo la procedencia de la persona o grupo V (65%) F (35%).

Gráfica 8. Aceptación de Solicitudes de amistad

Fuente: El Autor.

4. Usa la Internet Para

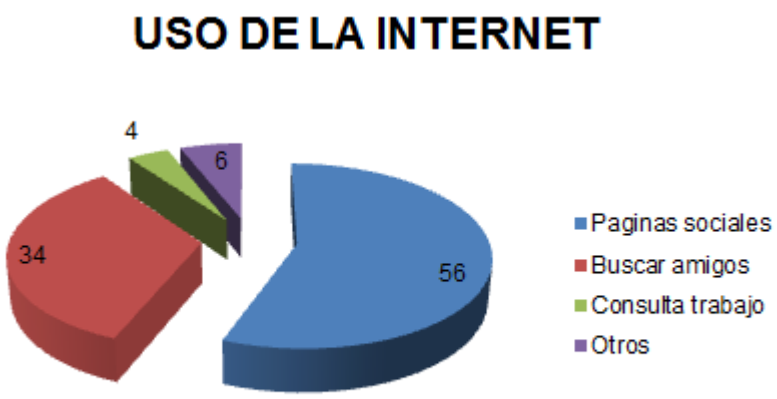
Paginas sociales 56%

Buscar amigos 34%

Consulta trabajo 4%

Otros 6%

Gráfica 9. Uso de la Internet



Fuente: El Autor.

5. Comparte sus contraseñas con

Nadie 60%

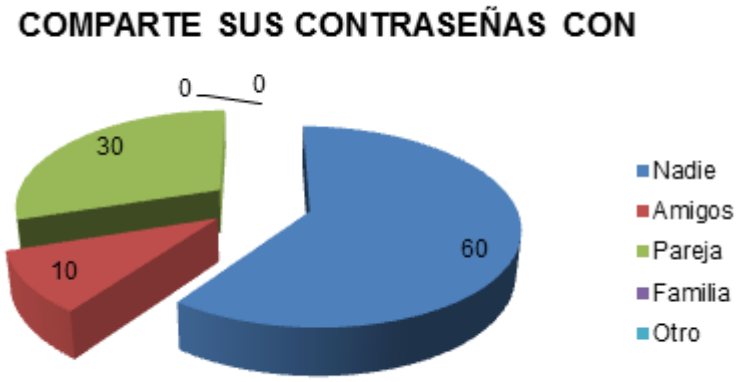
Amigos 10%

Pareja 30%

Familia 0%

Otro 0%

Gráfica 10. Comparte contraseñas



Fuente: El Autor.

De lo anterior se infiere que las amenazas que los jóvenes universitarios de San José de Cúcuta de las cuales se han visto más afectados radican en un 32% de la suplantación de la identidad, siendo esto un temor más arraigado puesto que se enfoca en la imagen que se proyecta hacia los demás puesto que a través de esto se pueden fomentar comentarios o burlas que puedan ser riesgosas para los jóvenes en su integridad física.

A través de este análisis se ha podido indagar acerca del conocimiento que tienen los jóvenes sobre los riesgos en las redes sociales, lo cual dentro del saber popular cabe destacar que todos los jóvenes conocen los términos del bullying en su versión cibernética, la intimidación en línea y el ciber stalker o acosador en línea, puesto que son características negativas que se han incrementado en los últimos años con el auge de la internet en Colombia, siendo todo lo contrario en términos como Smishing y Spoofing con un conocimiento entre los jóvenes entre un 30 % y un 25 %, y por lo cual su desconocimiento entre los jóvenes hace que sean más propensos a ser víctimas de ello.

Dentro del análisis de la corresponsabilidad de los padres en el uso o abuso de las redes sociales entre los niños y jóvenes, los jóvenes universitarios cucuteños consideran que los padres son los responsables de su ingreso en un 85% en contra de un 15% que piensan que los niños y jóvenes pueden ingresar sin ningún tipo de control, esto permite inferir que los jóvenes si tienen noción de los riesgos que existen entre las redes sociales y que entre menos edad tiene el menor más propenso es a sufrir de algún percance en la red, esto es un punto de partida para generar mecanismos de auto protección de los jóvenes en la red.

Un tema preocupante dentro del mundo digital y más aún cuando se manejan tantas cuentas de diversa índole llámese correos electrónico, Facebook, twitter, Instagram, etc. y siendo estas accesadas desde cualquier pc ya sea público o privado, es el manejo de contraseñas seguras y entender cómo se pueden crear, siendo un 55% de los jóvenes encuestados manifestaron tener desconocimiento de que es una contraseña alfanumérica ni cómo implementarla, preocupante situación cuando existen técnicas entre los delincuentes digitales para romper contraseñas.

Un tema delicado en cuanto al manejo de las redes sociales consiste en si las personas deben aceptar las invitaciones de amistad de cualquier persona, puesto que es un riesgo que el usuario de la red social posee al dar aceptar, permite que el individuo tenga acceso a información más privada de la cual puede disponer para tomar ventaja de cualquier índole, es inquietante ver que un 65 % de los jóvenes cucuteños encuestados aceptaría o acepta la solicitud de amistad por parte de desconocidos, peligrosa practica partiendo que puede ser un perfil falso creado para acechar a la persona que ingenuamente acepta.

El uso recreativo de la internet es un análisis que se ha querido realizar en este estudio de los jóvenes universitarios cucuteños, para permitir identificar cuáles son

sus intereses y gustos, siendo un 56 % de los encuestados argumenta que ingresan a paginas sociales, 34 % para buscar amigos, 4 % para buscar empleo y un restante del 6% para otras actividades, permitiendo inferir con mucha claridad que las redes sociales monopolizan el tiempo en la internet en los jóvenes.

El compartir las contraseñas es otro tema que forma parte de las acciones poco seguras de los jóvenes, que desde un tiempo atrás ha sido criterio de análisis, puesto que se manejan interés sentimentales basados en la confianza, tras realizar el análisis permitió identificar que un 60% de los jóvenes encuestados jamás revelaría su contraseña, en contra posición de un 30% la cual se la facilitaría a su pareja y un 10% a su familia, aunque la cifra de jóvenes que jamás revelaría su contraseña es grande existen riesgos en ese 40 % que si la revelaría, son acciones de tipo penal las que se vería la persona involucrada en un acceso no autorizado a sistema de información.

Por lo anterior se aplica el instrumento de recolección que tiene como fin identificar las amenazas más recurrentes en los jóvenes universitarios.

8.2 GESTION DE RIESGO DE LOS JOVENES EN LAS REDES SOCIALES

Identificación de los activos. Dentro del proceso del análisis del riesgo se han determinado los activos sobre los cuales se pueden evidenciar amenazadas, los cuales son:

Aplicaciones o Software. Dentro de las aplicaciones se pueden identificar:

- SISTEMA OPERATIVO

- ANTIVIRUS

- SOFTWARE DE OFIMATICA

Equipos. Dentro de los equipos se pueden identificar:

- COMPUTADOR

- TELEFONO INTELIGENTE

Comunicaciones. Dentro de los medios de comunicación se pueden identificar:

- CONEXION WIFI

Información. Dentro de la información se puede identificar lo siguiente:

- Información de carácter personal (Fotos, Videos, Archivos, etc.)

Valoración de los activos. La valoración de los activos se realiza a través de los siguientes parámetros:

- Relevancia del activo por cada parámetro.

- Determinación del valor en cada parámetro.

Cuadro 1. Criterios de valoración

NIVEL	CRITERIO
10	Nivel 10
9	Nivel 9
8	Nivel 8(+)
7	Alto
6	Alto(-)
5	Medio(+)
4	Medio
3	Medio(-)
2	Bajo(+)
1	Bajo
0	Despreciable

Fuente: MAGERIT v.3.

[D] disponibilidad

[I] integridad de la información

[C] confidencialidad de la información

[A] autenticidad de la información

[T] trazabilidad de la información

Cuadro 2. Activos

	PARAMETRO				
ACTIVOS	**D**	**I**	**C**	**A**	**T**
APLICACIONES O SOFTWARE					
SISTEMA OPERATIVO					[8]
ANTIVIRUS					[8]
SOFTWARE DE OFIMATICA					[8]
EQUIPOS					
COMPUTADOR					[9]
TELEFONO INTELIGENTE		[9]			
COMUNICACIONES					
CONEXIÓN WIFI		[8]			[8]
INFORMACION					
INFORMACIÓN DE CARÁCTER PERSONAL		[9]	[9]		

Fuente: El Autor.

Estandarización de las amenazas. Las amenazas se pueden estandarizar en las siguientes áreas:

[N] Desastres Naturales

[I] De origen industrial

[E] Errores y fallos no intencionados

[A] Ataque intencionados

Cuadro 3. Proceso para Identificar las Amenazas

ACTIVOS	AMENAZAS
SISTEMA OPERATIVO	[E.1] Errores por causa de los usuarios [E.8] Descargas de software malicioso [E.10] Debilidades de los programas
ANTIVIRUS	[E.8] Descargas de software malicioso [E.10] Debilidades de los programas [E.11] Errores al realizar el mantenimiento y actualización de los programas
SOFTWARE DE OFIMATICA	[E.8] Descargas de software malicioso [E.10] Debilidades de los programas [E.11] Errores al realizar el mantenimiento y actualización de los programas
COMPUTADOR	[A.11] Acceso no autorizado [A.11] Manipulación del hardware [I.5] Daño lógico [E.11] Errores al realizar el mantenimiento y actualización de los programas [I.5] Avería de origen físico o lógico [A.6] Abuso de privilegios de acceso [A.7] Utilización no prevista
TELEFONO INTELIGENTE	[A.11] Acceso no autorizado [A.11] Manipulación del hardware [I.5] Daño lógico [E.11] Errores al realizar el mantenimiento y actualización de los programas [I.5] Avería de origen físico o lógico [A.6] Abuso de privilegios de acceso [A.7] Utilización no prevista
CONEXIÓN WIFI	[I.8] Fallo de servicios de comunicaciones
INFORMACIÓN DE CARÁCTER PERSONAL	[E.12] Alteración de la información [E.13] Fugas de información [A.16] Modificación de la información [A.15] Revelación de información

Fuente: El Autor.

Valoración de las amenazas. Para dicha caracterización se tiene en cuenta la posibilidad de que ocurra y el valor que se le puede atribuir.

Cuadro 4. Degradación del valor

MA	MUY ALTA
A	ALTA
M	MEDIA
B	BAJA
MB	MUY BAJA

Fuente: MAGERIT v.3.

Cuadro 5. Posibilidad de que ocurra el incidente

CS	CASI SEGURO
MA	MUY ALTO
P	PROBABLE
PP	POCO PROBABLE
MB	MUY BAJA
MR	MUY RARA

Fuente: MAGERIT v.3.

Valoración de amenazas a cada uno de los activos. Para valorar las amenazas de cada activo se han tomado en cuenta la degradación de valor y la probabilidad de ocurrencia.

Para realizar la valoración de las amenazas se tiene en cuenta lo siguiente:

- Estimar el grado de posibilidad de que ocurran las amenazas descritas por activo.

- Determinar el daño que originaría la posible amenaza en cada parámetro de los activos si existe la posibilidad de que ocurra.

De tal manera que para darle un valor a las posibles amenazas se tiene determinado la posibilidad de que ocurra y el daño que causaría.

Cuadro 6. Valoración de amenazas a cada uno de los activos

ACTIVOS	AMENAZAS	P	[D]	[I]	[C]	[A]	[T]
SISTEMA OPERATIVO	[E.1] Errores por causa de los usuarios	P	M	M	M	-	-
	[E.8] Descargas de software malicioso	P	M	M	M	-	-
	[E.10] Debilidades de los programas	P	M	M	M	-	-
ANTIVIRUS	[E.8] Descargas de software malicioso	P	M	M	M	-	-
	[E.10] Debilidades de los programas	P	M	M	M	-	-
	[E.11] Errores al realizar el mantenimiento y actualización de los programas	P	M	M	M	-	-
SOFTWARE DE OFIMATICA	[E.8] Descargas de software malicioso	P	M	M	M	-	-
	[E.10] Debilidades de los programas	P	M	M	M	-	-
	[E.11] Errores al realizar el mantenimiento y actualización de los programas	P	M	M	M	-	-
COMPUTADOR	[A.11] Acceso no autorizado	PP	-	M	M	-	-
	[A.11] Manipulación del hardware	MA	-	A	A	-	-
	[I.5] Daño lógico	P	M	-	-	-	-
	[E.11] Errores al realizar el mantenimiento y actualización de los programas	P	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[A.6] Abuso de privilegios de acceso	PP	M	M	M	-	-
	[A.7] Utilización no prevista	P	M	B	M	-	-
TELEFONO INTELIGENTE	[A.11] Acceso no autorizado	PP	-	M	M	-	-
	[A.11] Manipulación del hardware	MA	-	A	A	-	-
	[I.5] Daño lógico	P	M	-	-	-	-
	[E.11] Errores al realizar el mantenimiento y actualización de los programas	P	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[A.6] Abuso de privilegios de acceso	PP	M	M	M	-	-
	[A.7] Utilización no prevista	P	M	B	M	-	-
CONEXIÓN WIFI	[I.8] Fallo de servicios de comunicaciones	PP	M	-	-	-	-
INFORMACIÓN DE CARÁCTER PERSONAL	[E.12] Alteración de la información	PP	-	B	-	-	-
	[E.13] Fugas de información	PP	-	-	B	-	-
	[A.16] Modificación de la información	PP	-	B	-	-	-
	[A.15] Revelación de información	PP	-	-	B	-	-

Fuente: El Autor.

Impacto potencial. El impacto se puede definir como la medición del deterioro de los activos cuando ocurren las amenazas. A través de la estimación de los activos, los cuales fueron determinados a través de parámetros para su medición y el deterioro que pueden acarrear las amenazas, es posible determinar el impacto potencial.

Cuadro 7. Impacto potencial

ACTIVOS	[D]	[I]	[C]	[A]	[T]
APLICACIONES O SOFTWARE					
SISTEMA OPERATIVO		[7]	[7]		
ANTIVIRUS		[6]	[6]		
SOFTWARE DE OFIMATICA		[6]	[6]		
EQUIPOS					
COMPUTADOR		[6]	[6]		
TELEFONO INTELIGENTE		[6]	[6]		
COMUNICACIONES					
CONEXIÓN WIFI			[6]		
INFORMACION					
INFORMACIÓN DE CARÁCTER PERSONAL		[8]	[8]		

Fuente: El Autor.

Impacto residual acumulado. Este corresponde al impacto residual generado después de analizar la estimación de los activos y amenazas, con el fin de aplicar controles que puedan mitigar su ocurrencia, de acuerdo a la siguiente formula:

Impacto residual= impacto potencial X (1 – ei)

Cuadro 8. Impacto residual acumulado

ACTIVOS	[D]	[I]	[C]	[A]	[T]
APLICACIONES O SOFTWARE					
SISTEMA OPERATIVO		[4]	[4]		
ANTIVIRUS		[3]	[3]		
SOFTWARE DE OFIMATICA		[0]	[0]		
EQUIPOS					
COMPUTADOR		[3]	[5]		
TELEFONO INTELIGENTE		[3]	[5]		
COMUNICACIONES					
CONEXIÓN WIFI			[2]		
INFORMACION					
INFORMACIÓN DE CARÁCTER PERSONAL		[3]	[4]		

Fuente: El Autor.

Estimación del riesgo. Riesgo potencial:

Este se determina a través del conocimiento previo del impacto que pueden tener las amenazas sobre los activos analizados, puesto que el riesgo de que ocurran se puede estimar a través de la posibilidad de que ocurra.

Cuadro 9. Riesgo potencial

ACTIVOS	PARAMETROS				
	[D]	[I]	[C]	[A]	[T]
APLICACIONES O SOFTWARE					
SISTEMA OPERATIVO	-	{5,4}	{5,4}	-	-
ANTIVIRUS	-	{5,4}	{5,4}	-	-
SOFTWARE DE OFIMATICA	-	{5,4}	{5,4}	-	-
EQUIPOS					
COMPUTADOR	-	{4,5}	{4,5}	-	-
TELEFONO INTELIGENTE	-	{4,5}	{4,5}	-	-
COMUNICACIONES					
CONEXIÓN WIFI	-	-	{4,5}	-	-
INFORMACION					
INFORMACIÓN DE CARÁCTER PERSONAL	-	{6,6}	{6,6}	-	-

Fuente: El Autor.

Riesgo residual. Riesgo residual acumulado:

La determinación del riesgo residual acumulado, da a conocer el valor de cuanto es la afectación de los activos más importantes, los cuales son acumulados que dependen de valores previos y pueden considerarse como riesgos altos los que poseen un valor superior a 3.

Cuadro 10. Riesgo residual acumulado

ACTIVOS	PARAMETROS				
	[D]	[I]	[C]	[A]	[T]
APLICACIONES O SOFTWARE					
SISTEMA OPERATIVO	-	{3,1}	{3,1}	-	-
ANTIVIRUS	-	{3,2}	{3,2}	-	-
SOFTWARE DE OFIMATICA	-	{0,83}	{0,83}	-	-
EQUIPOS					
COMPUTADOR	-	{1,7}	{3,3}	-	-
TELEFONO INTELIGENTE	-	{1,7}	{3,3}	-	-
COMUNICACIONES					
CONEXIÓN WIFI	-	-	{1,1}	-	-
INFORMACION					
INFORMACIÓN DE CARÁCTER PERSONAL	-	{2,1}	{3,8}	-	-

Fuente: El Autor

Matriz de valoración del riesgo. Consiste en la determinación del riesgo a través de la siguiente formula:

Riesgo= Probabilidad de amenaza x Magnitud del daño

Cuadro 11. Resultado de evaluación de riesgo

REFERENCIA	RIESGO IDENTIFICADO	PROBALIDAD DE AMENAZA	MAGNITUD DEL DAÑO	RIESGO
R1	[E.1] Errores por causa de los usuarios	5	1	5
R2	[E.8] Descargas de software malicioso	5	3	15
R3	[E.10] Debilidades de los programas	3	2	6
R4	[E.8] Descargas de software malicioso	4	3	12
R5	[E.10] Debilidades de los programas	2	2	4
R6	[E.11] Errores al realizar el mantenimiento y actualización de los programas	2	2	4
R7	[E.8] Descargas de software malicioso	5	3	15
R8	[E.10] Debilidades de los programas	2	2	4
R9	[E.11] Errores al realizar el mantenimiento y actualización de los programas	2	2	4
R10	[A.11] Acceso no autorizado	3	4	12
R11	[A.11] Manipulación del hardware	3	3	9
R12	[I.5] Daño lógico	2	2	4
R13	[E.11] Errores al realizar el mantenimiento y actualización de los programas	2	2	4

Cuadro 11. (Continuación)

REFERENCIA	RIESGO IDENTIFICADO	PROBALIDAD DE AMENAZA	MAGNITUD DEL DAÑO	RIESGO
R14	[I.5] Avería de origen físico o lógico	3	2	6
R15	[A.6] Abuso de privilegios de acceso	3	4	12
R16	[A.7] Utilización no prevista	3	4	12
R17	[A.11] Acceso no autorizado	3	4	12
R18	[A.11] Manipulación del hardware	2	4	8
R19	[I.5] Daño lógico	2	3	6
R20	[E.11] Errores al realizar el mantenimiento y actualización de los programas	2	2	4
R21	[I.5] Avería de origen físico o lógico	3	2	6
R22	[A.6] Abuso de privilegios de acceso	3	4	12
R23	[A.7] Utilización no prevista	3	4	12
R24	[I.8] Fallo de servicios de comunicaciones	2	3	6
R25	[E.12] Alteración de la información	4	4	16
R26	[E.13] Fugas de información	4	3	12
R27	[A.16] Modificación de la información	4	4	16
R28	[A.15] Revelación de información	4	4	16

Fuente: El Autor.

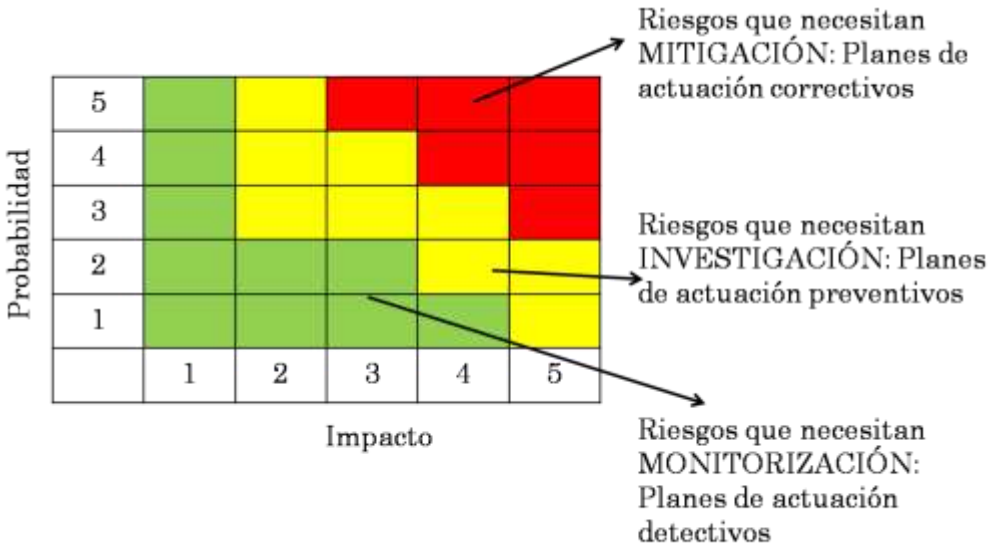
Alto riesgo (12 - 16): Color Rojo

Medio Riesgo (8 - 9): Color Amarillo

Bajo Riesgo (1 - 6): Color Verde

Matriz de tratamiento de los riesgos:

Figura 1. Matriz de tratamiento de los riesgos



Fuente: BELTRAN, Martha. Matriz de riesgos [en línea]. [Citado 20 octubre 2016]. Disponible en Internet en: http://redindustria.blogspot.com.co/2010/05/matriz-de-riesgos.html

Cuadro 12. Matriz de tratamiento de los riesgos

	PROBABILIDAD DE AMENAZA				
MAGNITUD DEL DAÑO	R1		R2, R7		
	R5, R6, R8, R9, R12, R13, R20	R18	R4, R10, R15, R16, R17, R22, R23, R26	R25, R27, R28	
		R3, R14, R19, R21, R24	R11		

Fuente: El Autor.

9. DIVULGACIÓN DEL MANUAL

9.1 REALIZAR Y DIVULGAR UN MANUAL QUE CONTENGA TIPS, CONFIGURACIONES Y HERRAMIENTAS DE SOFTWARE LIBRE QUE PUEDAN SEGUIR LOS USUARIOS DE LAS REDES SOCIALES Y DE INTERNET PARA PERMITIR UNA NAVEGACIÓN SEGURA

El manual es una herramienta anexa a este proyecto sobre el cual se le instruirá a los jóvenes técnicas en la configuración y manejo de las herramientas básicas de seguridad en su computador personal como se puede apreciar en el anexo A.

Se ha divulgado el manual en las redes sociales Facebook y twitter, en grupos conformados por estudiantes y egresados de la Universidad Francisco de Paula Santander de Cúcuta - Norte de Santander, manifestando el objetivo del manual, que le brinda los jóvenes consejos en el uso adecuado de las redes sociales y configuraciones para el computador que le permiten al usuario una navegación segura por la internet.

La primera publicación del manual se ha realizado en el grupo amigos UFPS de la red social Facebook, el cual está conformado por estudiantes activos y egresados de la universidad Francisco de Paula Santander y es utilizado para publicar noticias sobre el campus universitario, actividades estudiantiles y logros de la universidad.

Figura 2. Divulgación del manual en Facebook

Fuente: El Autor.

La segunda publicación del manual se ha realizado en twitter compartiendo el enlace del documento, el cual ha sido subido a un link de google drive y el mensaje reenviado a las personas que siguen la cuenta de la universidad Francisco de Paula Santander.

Figura 3. Divulgación del manual en Twitter

Fuente: El Autor.

10. RECOMENDACIONES

Debido a que la Universidad Francisco de Paula Santander no poseía ningún manual o herramienta que brindara a sus estudiantes las pautas para una navegación segura en las redes sociales, es pertinente que se socialice de manera apropiada dicho documento, que tenga como objetivo mitigar los riesgos inherentes en el uso de los medios de comunicación a través de la internet.

Por tal motivo es de suma importancia sensibilizar a la población estudiantil sobre los riesgos y amenazas sobre los cuales están inmersos en las redes sociales, de una manera pedagógica y constructiva que genere cambios en las conductas que propician consecuencias tanto de tipo físico como psicológico, teniendo en cuenta ciertas consideraciones:

- Evitar la publicación de contenido multimedia sin el consentimiento de las personas.

- Abstenerse de publicar información muy personal o de un familiar que pueda representar riesgos tales como la dirección de la vivienda, placas de vehículos, etc. los cuales pueden permitir fácilmente la ubicación de las personas.

- Cuando se realicen envíos de correos electrónicos a muchos destinatarios utilizar la copia oculta para no revelar información adicional.

- Antes de brindar información personal o bancaria verificar el URL para determinar que esta sea una conexión segura.

11. CONCLUSIONES

Las redes sociales son medios de comunicación que han tenido un auge de manera exponencial, siendo parte importante de nuestra vida diaria, a su vez son un medio valioso con un gran potencial para exponer las ideas y pensamientos de las personas sin restricción, debido a esto los jóvenes ven en las redes sociales un medio para liberarse de las presiones de la sociedad, convirtiéndolos en un blanco fácil ante los riesgos inherentes de estas aplicaciones sociales.

La identificación de los riesgos y amenazas que enfrentan los jóvenes en las redes sociales es un tema de suma importancia, en vista de la alta proliferación de casos de acosos no solo de tipo personal sino sexual que ha ocasionado que los jóvenes se aíslen o busquen salidas como el suicidio, por tal motivo este proyecto busco brindar herramientas a los jóvenes tanto desde el punto de vista social, psicológico y técnico para que estos cuenten con los criterios suficientes para hacer su navegación en la red y su uso de las redes sociales algo más seguro.

Desde el respectivo análisis evidenciado según los aportes de los jóvenes de San José de Cúcuta, se clarifica que la suplantación de la identidad es el riesgo más evidente, del cual se desprenden otras formas de acoso en las redes sociales entre ellas el ciberbullying.

Adicional a esto se determinó que el riesgo más conocido entre los jóvenes universitarios corresponde al ciberbullying, el cual corresponde a la intimidación en línea, y que el conocimiento de términos como el Smishing y Spoofing entre los jóvenes es menor o casi nulo lo cual los hace vulnerables a ser víctimas tanto de captura de datos personales como la de la suplantación de la identidad.

Para los jóvenes universitarios de San José de Cúcuta la generación de mecanismos de seguridad en el internet es competencia exclusiva de los padres de familia, lo que sugiere que los padres de familia deben tener un rol más importante en la aplicación de controles de contenido de información, sin desconocer que entre los jóvenes deben existir pautas de autocuidado que les permitan madurar y ser más críticos en las redes sociales.

El determinar a quién o a quien no aceptar como amigo en una red social es un punto que se ha analizado con este instrumento, lo cual entre los jóvenes cucuteños se ha determinado que están abiertos en su gran mayoría de aceptar a cualquier persona aun desconociendo su identidad, ya que al aceptar dicha solicitud se le permite al usuario tener acceso a toda la información personal que haya publicado la persona, permitiendo que esta pueda ser propensa a cualquier actividad delictiva con el mal uso de la información que se haya compartido en el perfil.

Desde la perspectiva del análisis evidenciado en cada una de las preguntas aplicadas a la población objetivo de este estudio la cual correspondía a jóvenes universitarios de la ciudad de Cúcuta, se puede determinar la existencia del desconocimiento de los riesgos en los cuales se pueden ver afectados, determinados por la ingenuidad en el uso de las redes sociales, como en la capacidad de no prever los riesgos inherentes asociados en la divulgación indiscriminada de información personal o en la baja dificultad de las contraseñas, y en el uso recreativo de la internet como medio para conocer gente y relacionarse con el entorno.

12. IMPACTO DEL PROYECTO

Con este proyecto se busca crear un impacto positivo entre los jóvenes universitarios de Cúcuta, en el cual les permita identificar con claridad los riesgos en los que se ven inmersos cada día en las redes sociales y la internet, dándoles las herramientas que les permitan identificar las amenazas y cuáles son los patrones o índices más altos de vulnerabilidad para que vean en las redes sociales no un medio de escape para sus dificultades si no a su vez espacios de compartir sanamente y con responsabilidad.

Se le brindo a los jóvenes las herramientas tecnológicas básicas para que su navegación en la Web sea lo más segura posible, indicándoles procesos, aplicaciones gratuitas y su configuración para que esta sea intuitiva y amigable puesto que las configuraciones están diseñadas para usuarios finales sin conocimientos adicionales en sistemas.

13. MEDIOS DE DIVULGACIÓN

Se parte del hecho que la información que se maneja en la totalidad del documento pertenece a la Universidad Nacional Abierta y a Distancia UNAD. De esta forma, la estrategia de divulgación del proyecto se hará teniendo en cuenta los resultados del proyecto, su potencial impacto para la sociedad y los beneficios que este proyecto, de manera proyectada, le trae a los jóvenes y demás partes interesadas en la preservación de los jóvenes en el manejo y uso de la internet.

Redes sociales. Aunque es el medio sobre el cual analiza sus riesgos este proyecto no se pude desconocer su alcance, en vista que la difusión del mismo a través de Facebook que permitirá que los jóvenes se aprendan a reconocer los riesgos y amenazas que traen consigo las redes sociales y aplicar medios para su protección.

BIBLIOGRAFÍA

AVILA GUERRERO, Edward. Influencia de las redes sociales en los jóvenes [en línea]. [Citado 20 octubre 2016]. Disponible en Internet en: http://influredes sociales.blogspot.com.co/p/fichas-bibliograficas.html

COLOMBIA DIGITAL. Conceptos TIC [en línea]. [Citado 25 mayo 2017]. Disponible en Internet en: https://colombiadigital.net/actualidad/articulos-informativos/conceptos-tic.html

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones [en línea]. [Citado 20 octubre 2016]. Disponible en Internet en: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

EDUCATIVO SEGURIDAD INFORMÁTICA. Spoofing [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: http://segurdadenredes.blogspot.com .co/2014/11/pagina-en-construcion. html

ESPINOZA TRUJILLO, Sarita. Influencia de las redes sociales en los jóvenes [en línea]. [Citado 29 octubre 2016]. Disponible en Internet en: http://es.slideshare.net/ SAwuita15/redes-socialesppt-34459822

GARCIA, Carlos. Hablemos de Spoofing [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/

GLOSARIO DE INFORMÁTICA E INTERNET. Chain e-mail [en línea]. [Citado 25 mayo 2017]. Disponible en Internet en: http://www.internetglosario.com/849/Chainemail.html

LEON ROJAS, Juan. Ataque de suplantación de identidad (mail-spoofing) [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: http://cala.unex.es/cala/cala/mod/forum/discuss.php?d= 7875

MENDEZ, L. Que es el Mail Spoofing y como evitarlo usando SPF [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: https://www.webempresa.com/blog/que-es-el-mail-spoofing-y-como-evitarlo-usando-spf.html

MOLINA. Leonela. Delitos informáticos [en línea]. [Citado 26 mayo 2016]. Disponible en Internet en: http://es.calameo.com/books/005155407963f214f1a28

PAEZ, Andrea. Tipos de spoofing [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: http://andrea0712.blogspot.com.co/2011/05/ejercicios_11.html

ROSERO, Manuel Antonio. Los riesgos en las redes [en línea]. [Citado 23 octubre 2016]. Disponible en Internet en: http://cucuta.extra.com.co/noticias/columnistas/los-riesgos-en-las-redes-231027

SALUD INVESTIGA. Población, unidad de análisis, criterios de inclusión y exclusión. Muestra: identificación y reclutamiento [en línea]. [Citado 29 octubre 2016]. Disponible en Internet en: http://www.saludinvestiga.org.ar/pdf/tutorias/poblacion ymuestra.pdf

SITES GOOGLE. Principales riesgos en redes sociales [en línea]. [Citado 20 octubre 2016]. Disponible en Internet en: https://sites.google.com/site/riesgosredes sociales2011/home

UNICEF. ¿Qué es la ciberintimidación? [en línea]. [Citado 25 mayo 2017]. Disponible en Internet en: http://www.alguien.do/quiero-estar-bien/en-mi-comunidad/que-es-la-ciberintimidacion

VELÁSQUEZ DÍAZ, Noé. Redes sociales, gran influencia en los jóvenes [en línea]. [Citado 1 noviembre 2016]. Disponible en Internet en: http://es.slideshare.net/ Velnoesitho/redes-sociales-gran-influencia-en-los-jvenes

ANEXOS

Anexo A. Manual para jóvenes sobre el uso seguro del Internet y las Redes Sociales

CONTENIDO

pág.

.

LISTA DE FIGURAS

pág.

1. IMPORTANCIA DE LA PREVENCIÓN

1.1 TIPOS DE MÉTODOS DE PREVENCIÓN: PRIMARIA, SECUNDARIA Y TERCIARIA

El motivo de la prevención radica en la implementación de metodologías que conducen a mitigar los riesgos para integridad física del joven, el entorno familiar y la comunidad en general, implementando normas y acciones ligadas a la disminuir las causas que lo originan.

Existen distintos niveles de prevención:

- Prevención primaria: Identifica y acciona mecanismos para evitar que ocurra el factor amenazante, orientándose no solo a jóvenes sino a la comunidad en general que pueden estar en riesgos inherentes en la red y medios tecnológicos.

- Prevención secundaria: Dicha prevención se ejecuta en situaciones donde se presentan ya las dificultades por los riesgos, a través de acciones que tratan de que estos desaparezcan de manera parcial o completa, evitando que las consecuencias del riesgo aumenten.

- Prevención terciaria: Esta acción se presenta cuando ya el conflicto está avanzado, su ideal primario es frenar el avance y desenlaces fatales.

La aplicación de la prevención de manera eficaz es algo más complejo de informar al joven de los riesgos a los que se ve expuesto, puesto que solo brindándole la mismas no hace que los comportamientos y el accionar del joven se modifique, por tal motivo es necesario buscas alternativas para que dicho cambio resulte a través del desarrollo de habilidades, fortalecer la autoestima del joven, fomentar el desarrollo de espacios de compartir con los demás.

1.2 PREVENCIÓN A TRAVÉS DEL CÍRCULO FAMILIAR

La familia es considerada la base de la sociedad, partiendo que de ella se imparten los primeros años de conocimiento del individuo, brindándole las pautas para la interacción social, y a su vez los conceptos éticos y morales del bien y el mal, a través de la aplicación de normas.

A través del entorno familiar es donde los jóvenes construyen su autoestima y generan confianza en sí mismos, ponen en práctica formas de ser y pensar para luego ser accionadas en la sociedad, por tal razón los padres deben inculcar valores como son la superación personal, disciplina, libre albedrio, ética y que a través de la sociedad puedan obtener sentido de justicia, solidaridad por el otro, lealtad ante el prójimo y generosidad ante el que lo requiera.

Es por tal motivo que la familia se transforma en la base del desarrollo de las actitudes positivas del adolescente, para que este pueda decidir sabiamente ante cualquier situación que se le presente en la sociedad.

2. DIFERENCIAS ENTRE MANIPULACIÓN, USO EXCESIVO Y ADICCIÓN A LAS TECNOLOGÍAS

A lo largo de los años se entendió por adicción al consumo de drogas que generaban en la persona la necesidad de seguir consumiendo dicha sustancia, pero con la llegada de las nuevas generaciones ha hecho que el termino de adicción se extendiera a toda clase de conductas o acciones que generan en el ser humano la necesidad de seguirla realizando, siendo esto un factor que altera el desarrollo normal de sus actividades diarias.

2.1 EVIDENCIA DE MANIPULACIÓN EXCESIVA

El uso de las redes sociales y la internet por parte de los jóvenes no sugiere en si una conducta adictiva, si este viene presentando una regularidad en su uso sin caer en los excesos que puedan alterar su normal desarrollo de actividades diarias como son estudiar, compartir con amigos y familiares, puesto que se pretende es identificar conductas que sean dañinas del uso de la tecnología.

Se empiezan a presentar síntomas de adicción a las tecnologías cuando el joven presenta cambios en su vida cotidiana, se puede apreciar que su rendimiento académico se ve mermado, pierde el interés en actividades cotidianas que regularmente venía desarrollando como hacer deportes, planes con sus amigos y familiares, desencadenando actitudes y cambios de temperamento con sus familiares y surgen mentiras que permitan justificar el porqué del uso excesivo del computador o de los celulares.

2.2 CONDUCTAS QUE PUEDEN SER SÍNTOMAS DE ADICCIÓN A LAS TECNOLOGÍAS

En la actualidad ningún ente de la comunidad científica se ha pronunciado o ha enunciado características de la “Adicción a las Redes sociales y la internet”,

aunque cabe destacar que se usa el término adicción en vista de que se presentan síntomas similares como el de la drogadicción o la adicción al juego.

Los síntomas principales del uso excesivo de las Redes sociales y el internet se condensan en las siguientes características:

Tolerancia: Hace referencia al aumento excesivo en horas de uso sin encontrar saciedad aparente de las redes sociales y el internet, para obtener el efecto deseado.

Pérdida de control: Es la acción reiterada de la conducta adictiva para aliviar su malestar de no realizarlo.

Ocultación: Es la negación del problema a pesar de que las consecuencias son evidentes como bajas calificaciones, deterioro social y mentiras reiteradas.

Abandono de Otras Actividades: Como la conducta adictiva aumenta esto hace que el tiempo se agote para realizar otro tipo de actividades como estudiar y compartir con la familia.

Cambios de comportamiento: Es la alteración de la conducta, actitudes e incluso cambios físicos asociados a la acción adictiva.

2.3 REACCIONES RELACIONADAS CON LA ABSTINENCIA DE LA TECNOLOGÍA

El síndrome de abstinencia como cualquier ausencia de la adicción conlleva a notorios efectos tanto en la conducta y estado físico del individuo, como es el malestar emocional, lo que sugiere irritabilidad, insomnio, cambios de humor, etc.

Al hacerse más evidente la dependencia, ya no se encuentra placer en la adicción, sino que se va presentando sensaciones tales como miedo, preocupación ante la acción desbordada, de esta manera y a través de esta sensación de rechazo se

pueden aplicar métodos para que la persona dependiente deje progresivamente su adicción.

3. FACTORES DE RIESGO

No todos los jóvenes en general son propensos a las adicciones de las redes sociales y el internet, para que estas se den intervienen muchos factores, entre los cuales se presentan:

3.1 INDIVIDUALES

Los problemas personales juegan un papel importante en el momento de ocasionar una adicción, determinando cuales son los potenciales personas de acuerdo a sus características emocionales pueden ser más propensos a una adicción, tal es el caso de las personas impulsivas, con euforia excesiva, sensibilidad a reacciones no tan placenteras en lo físico o psíquico, constante necesidad experimentar cosas nuevas y que estas personas no tienen la capacidad de sobrellevar los problemas.

3.2 ENTORNO FAMILIAR

Desde el entorno familiar se pueden presentar situaciones que pueden ocasionar dentro el joven conductas que lo hagan ser una persona propensa a las adicciones de todo tipo, es necesario que dentro del entorno se dialogue y se tenga claro cual deben ser las acciones a seguir para dichas situaciones no afecten al adolescente.

3.3 SOCIALES

Las tecnologías de la información y comunicación en la actualidad forman parte de nuestro entorno social, siendo este un medio sobre el cual se transmiten tendencias y cultura popular que son del agrado de los jóvenes.

3.4 CARACTERÍSTICAS DEL JOVEN ENTRE LOS 12 A 16 AÑOS

Al llegar a esta fase en su desarrollo el joven experimenta sensaciones que pueden chocar entre sí, puesto que por un lado prima su necesidad de

independencia a través de la toma de decisiones sin supervisión de su familia y por otro lado el hecho de que aún se siente protegido por sus padres, el cual le permite al adolescente sentirse protegido en caso de cometer errores.

El adolescente para sentirse adulto toma decisiones sin medir consecuencias aun arriesgando su integridad física, para sentirse plenamente realizado ante sí mismo y así de esta manera pensar que es una persona adulta que ya puede tener el control de su vida, no obstante de manera contradictoria aun busca sentirse protegido por sus padres en caso de que sus acciones se salgan de control.

Cuando se llega a la adolescencia el joven adquiere una serie de riesgos en el uso de las tecnologías de la información, las cuales son:

Búsqueda de Independencia: Los jóvenes sienten la necesidad de vivir sus vidas sin tener que rendir cuentas a sus padres, lo cual puede generar en toda clase de riesgos para los cuales no están lo suficiente preparados.

Búsqueda de una imagen propia: Los jóvenes debido a su inmadurez no tienen en sus mentes que hacer con sus vidas en todos los ámbitos ya sea personal o en un perfil universitario que les permita crear un futuro, por tal motivo es importante que los padres sirvan de guía a los jóvenes para que estos puedan tomar las decisiones más apropiadas.

Pensar únicamente en sí mismo: Lo que más identifica el periodo de la adolescencia es la capacidad del sentirse invencibles, el joven asume que nunca le pasara nada que eso le ocurre a alguien más y no a él o ella, y es a través de esta inmadurez lo que lleva a que se cometan errores en todos los ámbitos en especial en lo que se refiere a las redes sociales y la internet.

Influencia negativa de compañeros y amigos: Durante la adolescencia los amigos y compañeros de los jóvenes son una potencial fuente de riesgos puesto que la presión del que dirán y la sensación de miedo que puede ocasionar la burla,

propician que los que los jóvenes asuman riesgos que puedan no solo afectar su imagen ante la sociedad si no peor a un sus vidas.

No asumir consecuencias del riesgo: El adolescente tiende a no ver más allá de lo que puedan producir sus acciones, sin tomar precisión de los riesgos que puedan ocasionar las acciones irresponsables desde el punto de vista físico o psicológico.

4. FACTORES QUE MITIGAN LOS RIESGOS

4.1 DESARROLLO INTERPERSONAL

La Autoestima

Hace referencia al concepto que tiene la persona de sí misma, en la cual persona identifica cualidades y rasgos que la hacen única, esto hace que la autoestima sea la base de la personalidad de una persona, y esto se va creando y fortaleciendo desde la infancia determinando el grado de estabilidad emocional y mental de la persona al llegar a la adultez.

La baja autoestima en una persona permite que se desencadene en la persona sensaciones de creerse menos, dolor físico, sensación de angustia, ansiedad, sensación de culpa e impotencia, lo cual pueden ocasionar en el joven acciones tales como asilarse de la sociedad, dificultad para concentrarse en sus estudios, agresividad, depresión, anorexia y bulimia, drogadicción, entre otras.

Si la autoestima es la adecuada el joven tiene mejores actitudes que le permiten tener ser una persona abierta al cambio, poco influenciable, con criterios propios, comunicación positiva con el entorno, asumirá sus acciones con madurez y seguridad de sí mismo.

Las Habilidades Sociales

Las personas requieren tener habilidades para poder comunicarse con los demás, por tanto es necesario que el individuo a través de su entorno familiar y escolar desarrolle mecanismos tales como los turnos conversacionales, poner atención al que habla, corroborar con ideas la conversación, que le permitirán a la persona tener aspectos positivos que lo ayuden a desarrollarse como un individuo activo en la sociedad.

Durante el periodo de la infancia y la adolescencia es importante que los jóvenes aprendan a relacionarse adecuadamente con las personas con el fin de crear unas bases sólidas para su desarrollo ante la sociedad.

La solución de problemas

Un problema hace referencia a casos o situaciones que ocurren para los cuales no se está preparado, por lo cual para su solución es necesario analizar la opción más apropiada. Las personas a lo largo de su desarrollo desde niños aprenden a solucionar problemas o dificultades a través del apoyo del entorno familiar, a través del ambiente escolar o por experiencia propia, permitiendo ser autónomos y personas más equilibradas en su entorno.

4.2 APOYO POR PARTE DE LA FAMILIA

A través de la familia se pueden ejercer mecanismos de prevención para apoyar a los jóvenes. Los padres, docentes y en general los establecimientos educativos deben trabajar de la mano para contrarrestar los riesgos, y de esta manera proteger a los jóvenes en lo que refiere a adicciones no solo de las redes sociales si no en general.

Habilidades de comunicación familiar

La comunicación familiar permite que exista buena convivencia. Dialogar consiste solo en hablar, sino en interpretar al interlocutor. Uno de los errores característicos de los padres es saber que saben todo de sus hijos solo por hablar frecuentemente con ellos. Es necesario que los padres puedan estar al mismo nivel que los menores, con el fin de entender sus problemas e inquietudes y exista un dialogo constructivo.

Aprender a escuchar es la acción principal para que las personas se entiendan en el momento de expresar sus ideas, y esto se basa no solo en captar sonidos del emisor sino en comprender y darle un sentido claro a lo que está escuchando,

para comprender a la otra persona es necesario tener la capacidad de entender lo sentimientos del que está emitiendo el mensaje.

5. INTERNET Y LAS REDES SOCIALES

5.1 CARACTERÍSTICAS

Los medios de comunicación virtuales y las tecnologías de la información se han transformado en un eje principal en las vidas de los seres humanos, siendo cada vez más dependientes de la misma para el quehacer diario de las personas en cada tarea de la vida diaria.

El internet seguido por la televisión es el medio de comunicación más utilizada, en vista que se ha convertido en un medio que permite de una manera más sencilla, ágil y de bajo costo comunicarse con la personas, entretener a través de sus contenidos, adquirir productos, etc. La Internet está presente en todos los ámbitos que a tal punto de transformarse en un medio de mucha importante no solo en la parte profesional, sino en el desarrollo normal de los individuos.

La internet es la bandera de la globalización, a través de un clic del ratón podemos saber lo que ocurre en cualquier parte del mundo instantáneamente, puesto que permite a las personas comunicarse online en cualquier parte del mundo, facilita el acceso a cualquier tipo de información, brinda la posibilidad de obtener y realizar ventas de productos, realizar juegos online, interactuar con otras personas, acceder a toda clase de contenido multimedia, etc. desde la comodidad de nuestro hogar, oficina o donde sea.

5.2 REDES SOCIALES

Entre lo más utilizado en Internet hoy en día son las Redes Sociales, su objetivo principal es la de crear lazos entre los individuos en la internet, creando espacios donde las personas puedan comunicarse entre sí, brindando comentarios sobre un tema en particular. Las redes sociales permiten formar grupos de personas que compartan gustos en común.

En la actualidad las redes sociales han alcanzado unas cifras de usuarios que se cuentan por millones debido a que los jóvenes han hecho de estos medios herramientas para comunicarse y conocer gente nueva, las más utilizadas son Facebook , Twitter e Instagram en la cual se pueden compartir fotos.

Por medio de las redes sociales se comparte todo tipo de opiniones sobre diversos temas y contenido multimedia. Su principal propósito es conocer la opinión de los usuarios y la exhibición de nuestros gustos, pasatiempos y actividades.

Las personas adultas cuentan con espacios para buscar empleo y relacionarse con otras personas de su perfil profesional, la más popular es Linkedin.

Herramientas en línea que permiten realizar búsquedas, contar con e-mail, jugar en línea, comunicación instantánea, ver videos en línea, etc.

El internet abre espacios muy variados, puesto que a través de la navegación de las páginas web se puede acceder a toda clase de contenidos, y complementado con los buscadores, que a través de la combinación de una o más palabras, es posible encontrar lo que sea en cuestión de segundos.

La internet revoluciono la forma en la que las personas se comunican, una de ellas fue el correo electrónico, que permite enviar y recibir comunicaciones con la característica de poder adjuntar archivos a las conversaciones. Los chats o mensajerías de texto instantáneas son aplicaciones que permiten a los usuarios comunicarse entre sí, enviando y recibiendo mensajes de manera automática y de manera complementaria a esto incorporar voz y video a las conversaciones.

El internet ha alcanzado todos los campos de la cotidianidad entre esos el de entretenimiento, el cual se ve apoyado por aplicaciones que permiten realizar descargas de manera fácil y gratuito todo tipo de contenido como música, películas, juegos, etc.

Además de lo descrito existen en la internet los Juegos Masivos para Multijugador Online, el cual consiste en que cada usuario diseña un personaje el cual es conocido como avatar el cual interactúa por todos los ambientes del juego, y permite dialogar con otros usuarios que estén en línea jugando en ese momento, el objetivo de dichos juegos en línea es obtener experiencia a través de la solución de objetivos que le permitan subir de nivel, una de las características del juego es que este avanza sin que el algún usuario no esté conectado, y esta es una de las razones que obliga al usuario a estar siempre en línea jugando en vista de que puede cambiar muchas situaciones en un tiempo corto.

5.3 VENTAJAS EN COMPARACION A LOS RIESGOS

Es difícil negar las amplias ventajas de la internet y que a través de ella el mundo se ha reducido y como esta ha permitido darle un giro radical en cómo se maneja la información, en cómo se disfrutan los contenidos para el entretenimiento, la comunicación de las personas y demás, no obstante todas estas ventajas están sujetas a riesgos inherentes asociados a como las personas hacen uso de todas estas herramientas en detrimento de sí mismos y de los demás, entre las que cabe mencionar las siguientes:

El ciberbullying se origina principalmente en las redes sociales, debido a que estas permiten que los usuarios emitan opiniones sobre comentarios y publicaciones de la gente, que en algunos casos puede ser mal intencionada.

El ciberbullying se manifiesta generalmente a través de comentarios ofensivos en las redes sociales y correos electrónicos, desencadenando otras acciones tales como son el robo de contraseñas con el propósito de obtener información de la víctima con la que pueda ser chantajeada.

Los jóvenes no dimensionan el dolor que pueden generar en un amigo o compañero de clase. Se sienten protegidos por el supuesto secreto que permite el internet al momento de emitir un comentario y que este como tal no tiene

restricciones. Debido a esto, este documento tiene como finalidad que exista un respeto en la internet entre los usuarios como existe en la vida real.

Cuando es evidente el acoso por las redes sociales se debe ejercer un correctivo inmediato con el fin de que la victima de dicha agresión sienta un apoyo por su entorno familiar y no se convierta en una situación que sea lamentable en casos donde las personas atentan contra sus vidas en momentos de depresión o desesperación.

Compartir cualquier tipo de información de carácter personal, le brinda herramientas a las personas mal intencionadas en la red, que pueden hacer un uso indebido de dicha información, que pone en riesgo al joven que la ha compartido.

Se debe tener en cuenta cómo y en calidad de que se comparten datos personales, diversas paginas solicitan información para concursos, actualizar datos crear cuentas, etc, debido a esto es necesario tener claro las políticas de privacidad y manejo de información parte de la página web.

Cuando se publique una imagen en una red social se debe tener claro que la posesión de la misma pasa ser de dominio público y sobre la cual se emiten datos personales, por tal motivo se les deben de aplicar filtros de privacidad para que el usuario sea conocedor de hasta qué punto será visible o a quienes se les va a permitir el acceso a dicha imagen, haciendo claridad de que se deben de contar con los permisos para divulgarla cuando en ella aparezcan más personas. Puesto que publicar fotos en las redes sociales sin el permiso de las personas que aparecen en las mismas es considerado un delito.

La suplantación de la identidad en las redes sociales es algo muy común debido a la facilidad en la creación de perfiles que cuentan con imágenes similares e información pública que hacen pensar a los demás que dicho perfil es el real, esto

con el fin de cometer actos sexuales maliciosos contra menores de edad, generalmente son capturados adultos por llevar cabo dichas prácticas.

El acoso sexual en el internet se conoce como grooming, frecuentemente este delito es ocasionado cuando un adulto ingresa a redes sociales o chats suplantando a un adolescente, y a través de charlas se hace amigo de los jóvenes para luego intentar perpetrar abusos sexuales.

La internet se caracteriza por tener información de todo tipo la cual es de fácil accesibilidad para cualquier persona, lo cual representa una amenaza para los jóvenes debido a la naturaleza de dicho contenido, que pueden ser de violencia explícita, pornografía o apuestas en línea, las cuales tienen restricciones de acceso para menores de edad, es necesario aplicar acciones tales como filtrar el contenido de lo que ven los jóvenes, a través de la aplicación de controles parentales que pueden ser de acceso gratuito, puesto que las empresas proveedoras de internet cuentan con dichas medidas de seguridad.

Para ejercer un mayor seguimiento a las acciones que realizan los jóvenes en el internet es relevante instalar dichos controles a los computadores, de igual forma para obtener información sobre dichas restricciones de seguridad es necesario realizar la consulta a las empresas que distribuyen el servicio de internet, los cuales disponen de esta tecnología al servicio de los usuarios.

El internet está conformado por un universo de información de todo tipo, dicha información compartida por toda clase de personas en algunos casos sin fuentes citadas para corroborar la veracidad de lo publicado, debido a esto es necesario ingresar a páginas que sean confiables, de esta manera podamos comparar la información y tener la capacidad de ser críticos respecto a lo que es verdad o mentira en la red.

Adicionalmente el internet acarrea un problema sobre la formación académica de los jóvenes, el cual corresponde al copiar y pegar información de la red sin

entender lo que se extrae y a su vez sin realizar redacción con sus propias palabras, esto trae como consecuencia una baja calidad de las actividades académicas y disminución de la producción intelectual.

5.4 PAUTAS DE USO ADECUADO

La internet es un medio de comunicación que al ser global y sin restricciones posee muchos riesgos en especial para los jóvenes cuya población hace uso de la internet de una manera más prolongada y sin medir riesgos, debido a esto es necesario socializarles a los jóvenes sobre los impactos negativos de la internet y se les debe orientar en las pautas del buen uso de este medio de comunicación, para que estos dispongan de espacios seguros aprovechando todas las cosas positivas de la internet y las redes sociales.

Las tecnologías de la información y la comunicación poseen medios y mecanismos para fortalecer la seguridad de los usuarios y la información como tal, pero ni todos las aplicaciones de seguridad pueden reemplazar el sentido común ante los peligros y riesgos, es necesario a través de los diversos entornos que comparten los jóvenes ya sea dentro de la familia y la universidad o colegio, se les oriente de cómo aprovechar la internet de forma segura, educativa y divertida, entendiendo en primer lugar que esperan los jóvenes de la internet, como la usan y que opinan del uso que se les está dando.

Consejos para los Jóvenes:

1. Ser más crítico con la información que veas en el internet, puesto que existe mucha información falsa que se ha posteado en la red, debido a que la creación de páginas web ya no requiere de vastos conocimientos en informática, debido a esto es necesario identificar fuentes oficiales que permitan garantizar que la información obtenida es confiable.

2. Navegar en la web ofrece muchas distracciones debido a la cantidad de contenido tan variado que ofrece, es por tal razón que se deben crear patrones claros en las búsquedas manteniendo el objetivo y la intención de lo que se está consultando, y corroborando fuentes con el fin de obtener la información que sea acorde con la investigación.

3. Al momento de crear un correo electrónico, es más seguro utilizar cuentas de correo que sean gratuitas debido a que estas solicitan menos información personal para ser creadas, y como recomendación adicional es conveniente no utilizar datos personales tales como el nombre, apellido y la fecha de nacimiento en la dirección de correo electrónico, como se puede apreciar en el siguiente ejemplo: pedro.perez@.....com, maria.perez170886@.....es.

4. Hacer caso omiso de promociones o premios, puesto que estos son timos para obtener algo a cambio, esta clase de mensajes tiene un propósito siempre de tipo fraudulento con el objetivo de robar información o dinero de los usuarios.

5. Cuando recibas correos electrónicos con contenido amenazante o con información sensible no responderlos, puesto que al realizar esto se entra en un juego en el cual el agresor obliga al agredido a revelar datos personales, por tal razón si este no es contestado el agresor no obtendrá su cometido y desistirá de enviar dichos correos.

6. Cuando se reenvíen correos electrónicos, es conveniente diligenciar las direcciones de correo con copia oculta (CCO), con el fin de preservar la privacidad del destinatario puesto que dicha dirección no estaría a la vista de quien pueda recibir el correo electrónico.

7. Tener claro que información se publica en las redes sociales, puesto que al realizar esto brindas información que es publica y cualquiera podría verla, para mantener dicha información segura es conveniente configurar la cuenta de la red

social con esquemas privacidad más seguros, con el fin de determinar que personas pueden ver lo que compartes.

8. No brindar información de carácter personal a desconocidos y determinar los criterios de seguridad si vas a subirla en redes sociales, puesto que esta puede ser una herramienta para que los ciberdelincuentes se aprovechen de dicha información y realicen actos delictivos.

9. Abstenerse de chatear con desconocidos, puesto que no se saben las intenciones reales de dichas personas, es recomendable sostener dichas conversaciones con amigos o con quien reconozcas físicamente, puesto que el paso inicial del desconocido al hablarte es solicitar fotos o concretar encuentros y lo más probable es que dicha persona no sea quien dice ser.

10. Mantener una personalidad definida en el internet como la que se mantiene en la vida real, no permitiendo que desconocidos te agreden con la forma de expresarse.

6. TÉCNICAS PARA IMPLEMENTAR LA SEGURIDAD EN EL INTERNET

6.1 EL USO DE FIREWALLS Y DE PROGRAMAS ANTIVIRUS

Configuración del Firewall Propio del Sistema Operativo

Un firewall funciona como un filtro protector que coloca una barrera entre el computador y el internet cuando se accede a la misma, permitiendo que mientras se navegue por la web bloquee o impida accesos por determinados puertos del computador.

Para mantener un computador protegido durante la navegación es necesario activar el software de firewall que se encuentra en los diversos sistemas operativos ya se de Windows o Linux, siendo de caso particular Windows que viene predeterminado en su configuración, cabe destacar que existentes paquetes de protección adicionales pero son de tipo comercial y para este manual se manejara técnicas que puedan ser configuradas desde el equipo personal sin ningún costo, para realizar dicha configuración se debe realizar lo siguiente:

Se ingresa por la tecla Windows buscando la opción panel de control, de siguiente manera:

Figura 1. Botón inicio de Windows

Fuente: El Autor.

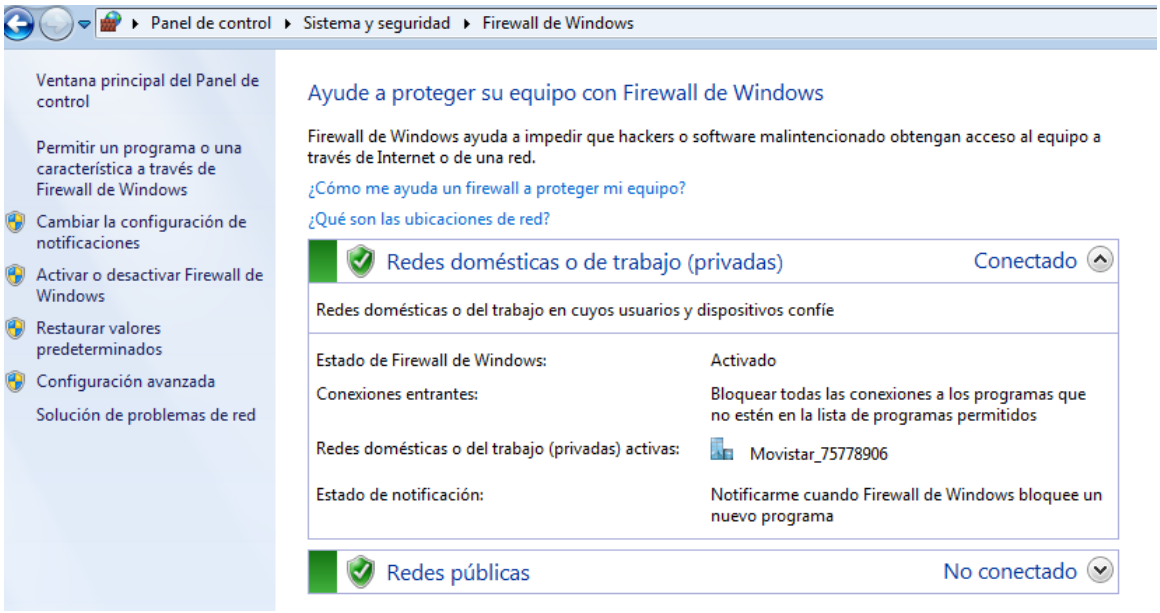
Se selecciona la opción Sistema y Seguridad, de la siguiente manera:

Figura 2. Panel de control de Windows

Fuente: El Autor.

Permitiendo identificar que la protección del firewall de Windows es automática siendo este un software bajo licencia.

Figura 3. Sistemas y Seguridad



Fuente: El Autor.

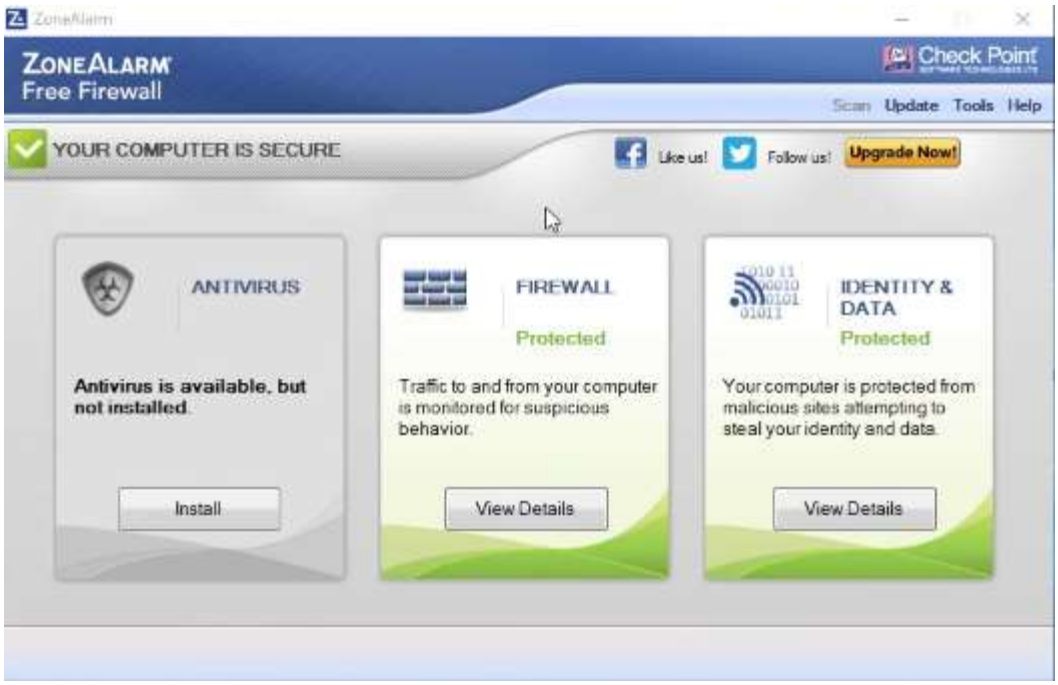
En casos donde el sistema operativo no tiene licencia el procedimiento de activar el firewall y las opciones de actualización automática hace que el sistema operativo Windows se bloquee a causa de la detección de software no adquirido de forma legal, para estos casos en particular existen opciones de software gratuito que realizan las funciones del firewall para suplir estas falencias de seguridad en el equipo con el que se accede a internet, siendo algunos ejemplos como:

- ZoneAlarm Free Firewall, el cual protege el pc contra intentos de hackeo, spyware, bots y demás ataques.

- Comodo Firewall, Protege el pc contra malware y ataques externos.

Para uso de este manual se toma en consideración el funcionamiento de ZoneAlarm Free Firewall, de la siguiente manera:

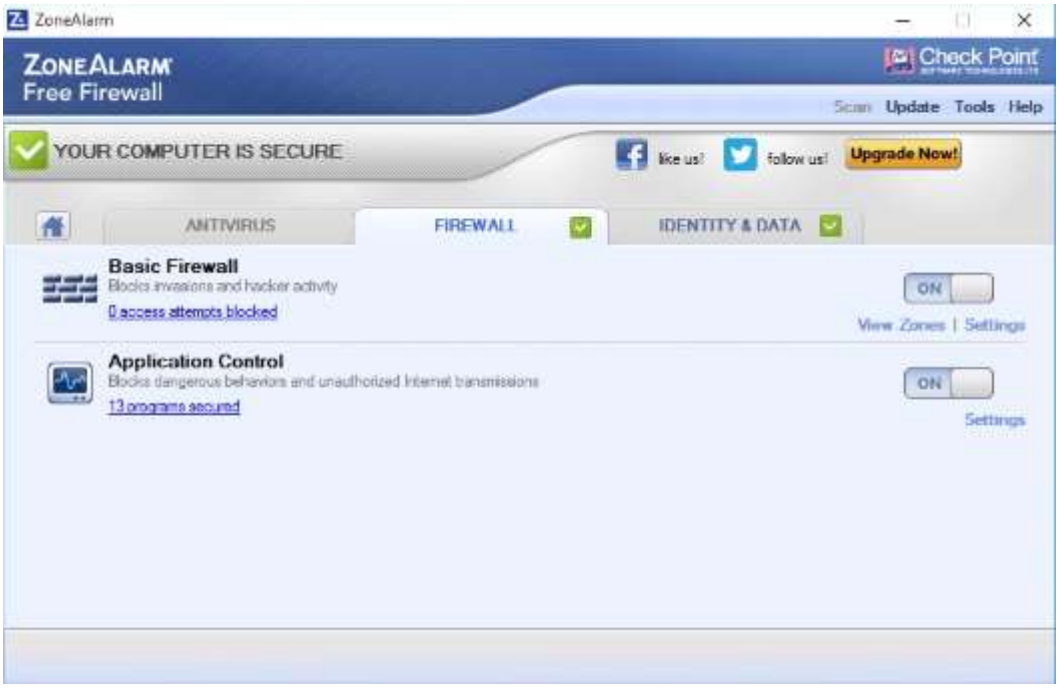
Figura 4. Software ZoneAlarm



Fuente: El Autor.

Ingresando a las opciones de firewall o view details se puede apreciar lo simple de su configuración:

Figura 5. Configuración del ZoneAlarm



Fuente: El Autor.

En la imagen anterior se aprecia que está encendida la protección al momento de inicializar la aplicación, manteniendo el pc protegido contra intrusiones.

Instalación y Configuración del Antivirus

Los programas de antivirus son software que protegen el computador ante el ataque de virus que pueden dañar los archivos del computador haciéndolo lento o realizar copias de archivos para sustraer información.

El software de antivirus realiza un escaneo completo o parcial del computador para identificar indicios que indiquen que el equipo está infectado, dichos indicios coinciden con virus conocidos, continuamente los hackers lanzan virus nuevos a la red, lo que hace necesario realizar las actualizaciones periódicas del antivirus.

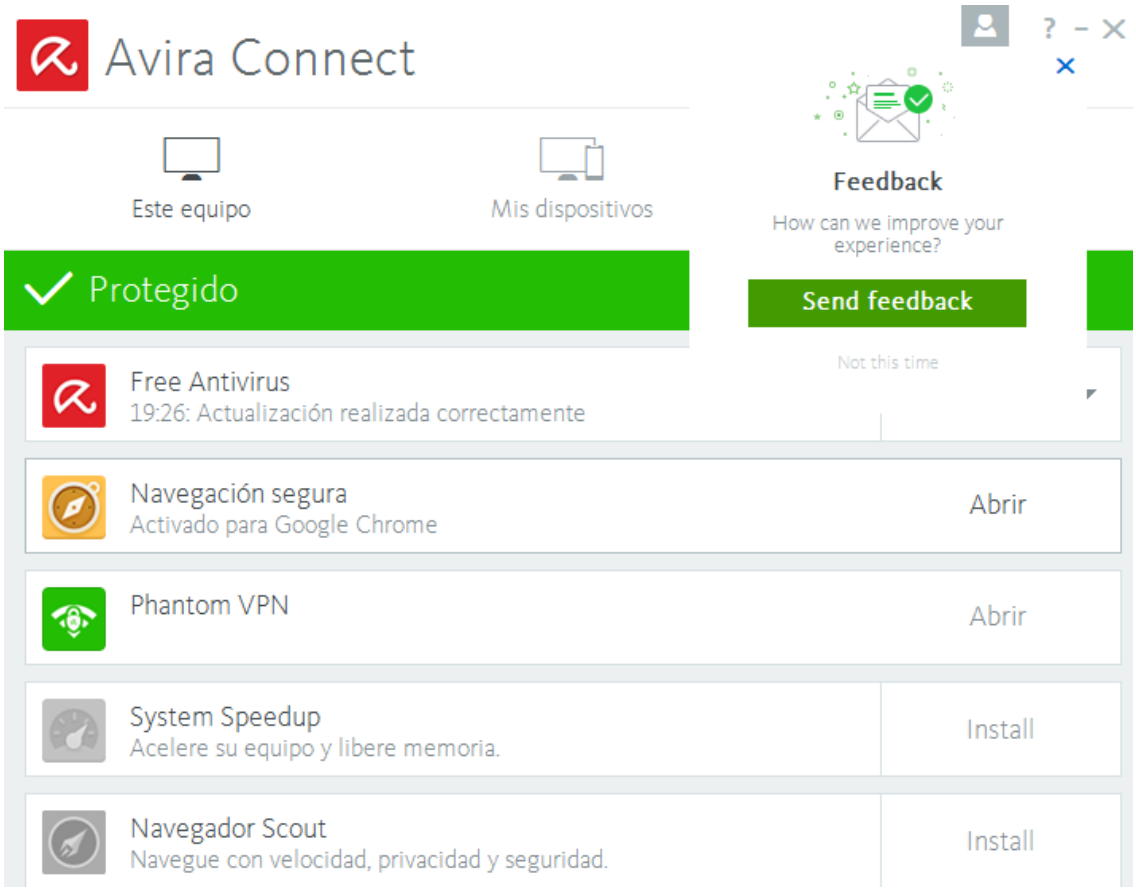
Cuando se adquiere un equipo de fábrica estos vienen con ciertos programas unos licenciados y otros en periodo de prueba con la opción de ser adquiridos de

forma completa a través del pago de la licencia, esto ocurre con el antivirus, el cual por descuido del usuario deja vencer y pasa por alto su desinstalación e instalación apropiada de una versión completa del antivirus para su protección efectiva en la red y medios locales.

Los sistemas operativos de Windows ofrecen a sus usuarios una alternativa gratuita de antivirus denominada Microsoft Security Essentials la cual es una gran opción de protección contra los virus, siendo la única dificultad que para que este sea instalado y utilizado la licencia del sistema operativo Windows debe ser autentica.

Para efectos de este manual y para el aprendizaje de la protección efectiva en la red se realiza la recomendación e instrucción de instalación de antivirus gratuitos que complementan la protección del sistema junto con el firewall previamente explicado, siendo claros en que hoy en día la mayoría de pc con los que usuarios cuentan son de adquisición sin licencia, este manual sugiere la instalación de avira free antivirus, el cual es un robusto software antivirus el cual es gratuito y ofrece características adicionales como la navegación segura en la internet funcionando como un enlace adicional para el navegador web, detectando características de riesgo de las páginas web y el Phantom VPN el cual es un mecanismo para proteger la conexión a internet, como se puede apreciar en la siguiente imagen:

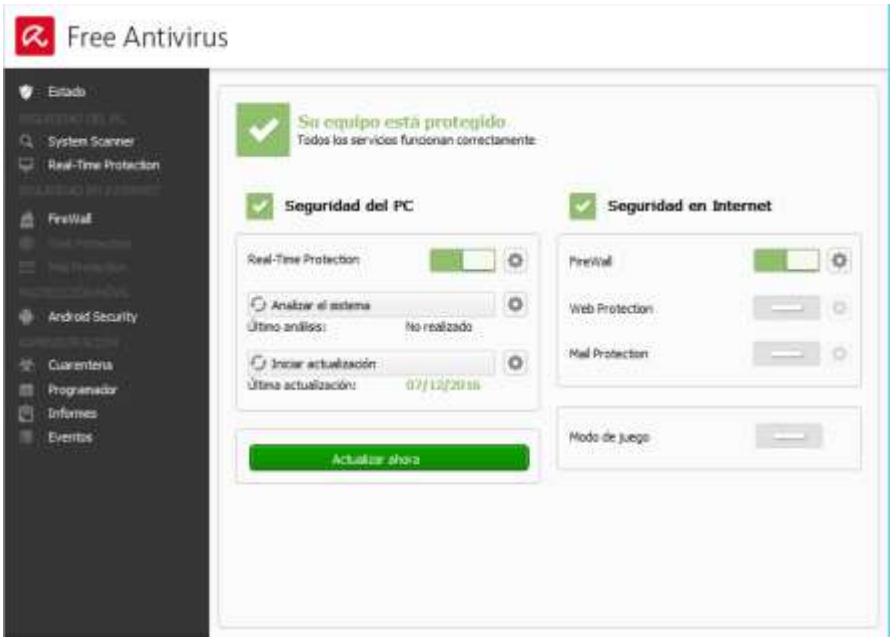
Figura 6. Avira Connect



Fuente: El Autor.

El Avira Free Antivirus proporciona características de protección en tiempo real, actualización automática cuando lo estipule el usuario y a su vez cuenta con su propio firewall que permite una protección efectiva del computador durante el proceso de navegación en el internet.

Figura 7. Configuración del Avira Free Antivirus



Fuente: El Autor.

Mantener un software de Antivirus debidamente actualizado es un medio muy eficaz para mantener alejado toda clase de software malicioso que se encuentra en la web e ingenuamente dando clic en cierta página o enlace se accede a algo que perjudique los archivos del computador o poner en riesgo archivos personales que luego sean objeto de chantajes por individuos mal intencionados.

6.2 CÓMO USAR EL COMPUTADOR DE FORMA SEGURA

Configuración de una Cuenta de Acceso Limitado o de tipo Estándar

Una cuenta de administrador es una cuenta de usuario que le permite al usuario que ha ingresado en la misma toda clase de permisos sobre el computador como instalación y desinstalación de software, capacidades de configuración en todo nivel y acceder a u cuentas de correo y contraseñas almacenadas previamente.

Por tal motivo es recomendable crear una cuenta de usuario estándar o con permiso reducido con el fin de minimizar los riesgos que estos puedan ocasionar

en caso de pérdida del equipo o a causa de un escritorio desatendido, para efectos de este manual se recomienda que se cree una cuenta estándar y siempre usarla a menos que se deba instalar algo, a continuación se describe los pasos para crear una cuenta estándar:

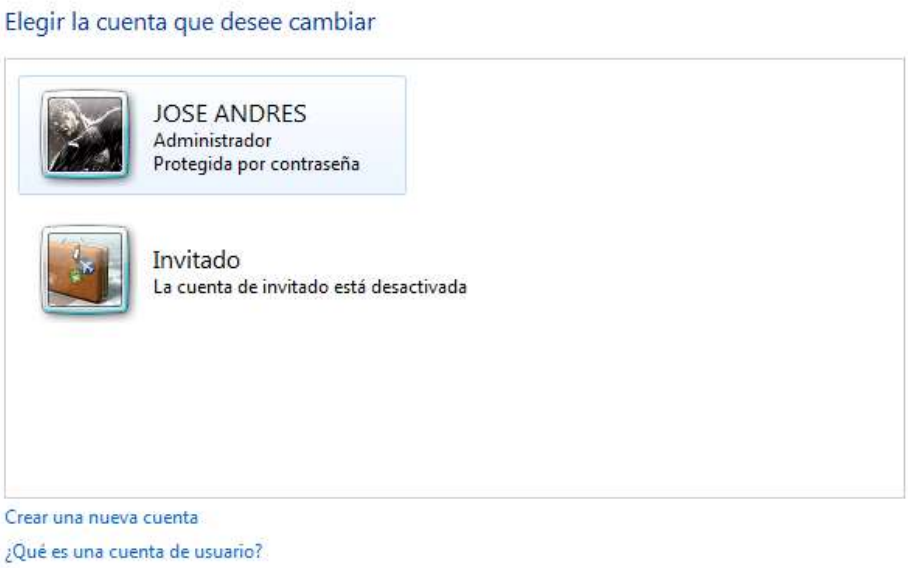
Se procede acceder al menú inicio y dar clic en panel de control, como se puede apreciar:

Figura 8. Panel de Control Cuentas de Usuario

Fuente: El Autor.

Se procede a dar clic dentro de las opciones de Cuenta de usuario y protección infantil la opción de agregar o quitar cuentas de usuario obteniendo lo siguiente:

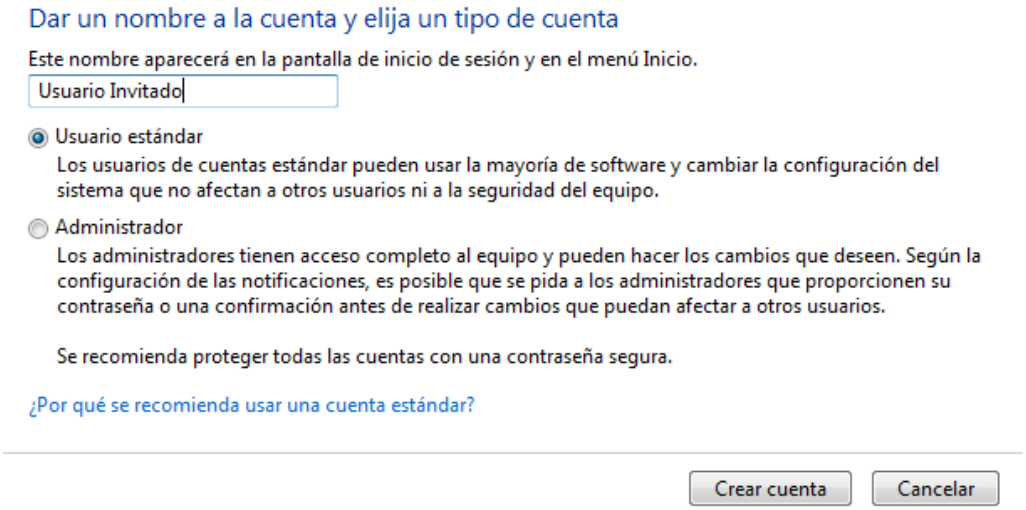
Figura 9. Cuentas de usuarios creadas



Fuente: El Autor.

Se procede a clic en crear una nueva cuenta, y se le ingresa un nombre al usuario estándar, y por defecto se le deja el tipo de usuario y por ultimo dar clic en crear cuenta.

Figura 10. Configuración de Usuario nuevo



Fuente: El Autor.

Configuración de las Actualizaciones Automáticas del Sistema Operativo

Las actualizaciones automáticas de los sistemas operativos son mecanismos de seguridad que se instalan para cerrar brechas que han sido halladas en el sistema operativo, por tal motivo es importante que esta configuración se encuentre activa en caso de que se requiera dicha instalación del parche en particular; debido que en muchos casos los equipos de cómputo son adquiridos con copias sin licencia estos son modificados para que su actualización automática no se activada, con el propósito de no alterar el funcionamiento del sistema operativo sin licencia, lo que acarrea riesgos para los usuarios en caso de daños por causa de incursión de un virus ingresado por alguna de estas brechas sin proteger.

Se recomienda la adquisición de un sistema operativo con licencia o en su defecto en algunos casos que este venga bajo Linux el cual es gratuito y viene soportado con interfaz gráfica en algunas de sus versiones finales. Para efectos de este manual se indicara el proceso de activación de las actualizaciones automáticas y su configuración.

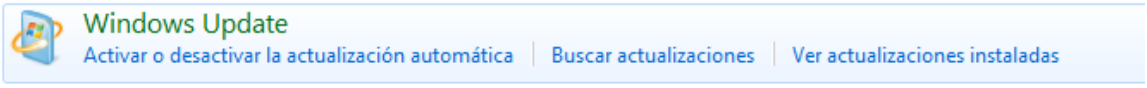
Se procede a clic en inicio y buscar la opción panel de control, de acuerdo a lo siguiente:

Figura 11. Selección de Windows Update

Fuente: El Autor.

Se selecciona la opción sistema y seguridad y luego dando clic en Windows Update, como se puede apreciar:

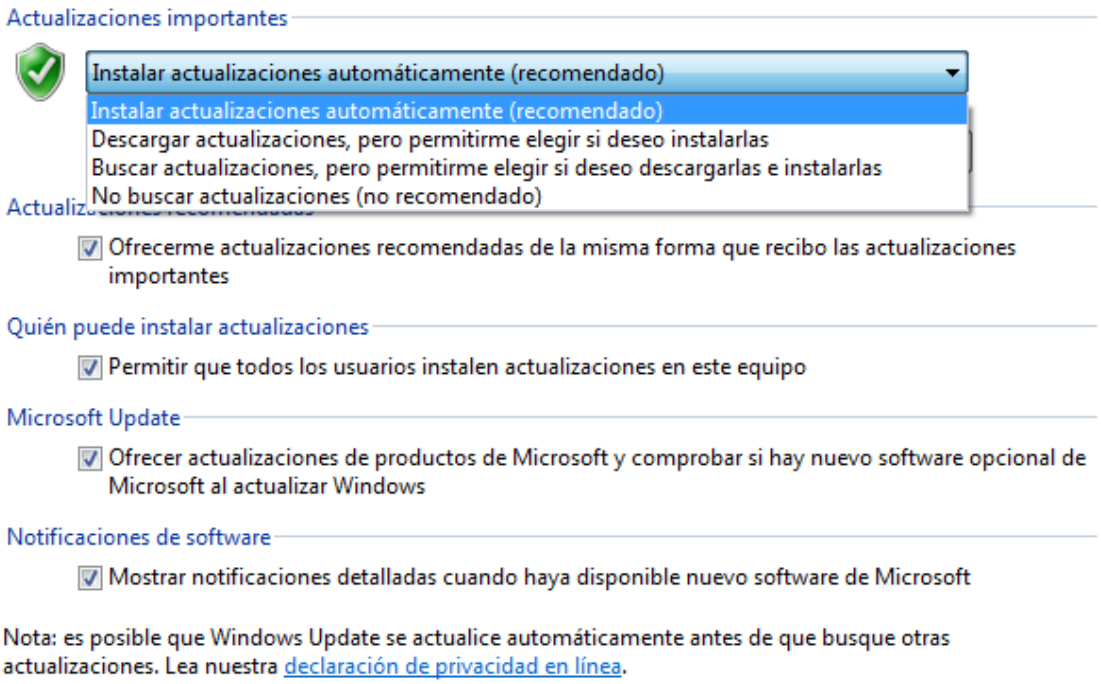
Figura 12. Activación de Windows Update



Fuente: El Autor.

Y posterior a esto se le da clic en activar o desactivar actualizaciones automáticas, seleccionado la configuración recomendada y el horario de instalación que mas le convenga al usuario, para que dichas actualizaciones de manera automática se realicen y pueda mantenerse el equipo protegido, como se puede apreciar:

Figura 13. Configuración de Windows Update



Fuente: El Autor.

Uso de Contraseñas Seguras

Puede ser uno de los riesgos más presentados hoy en día, debido a la poca complejidad en las contraseñas utilizadas por los usuarios que excusan la facilidad de la contraseña en que son medios para poder recordarla, casos como el nombre al revés, fechas de nacimiento, direcciones de residencia, son criterios muy fáciles de descifrar por cibercriminales que sin necesidad de complejas técnicas pueden acceder a ellas, si no únicamente usando la ingeniería social.

Pautas para crear una contraseña segura:

1. No utilice palabras completas, ejemplo: juanypedro

2. No utilice información personal, ejemplo: fechas de nacimiento, nombre de los padres, etc.

3. Utilice caracteres especiales, ejemplo: “#$%&/

4. Utilice contraseñas más largas, puesto que son más complicadas para los mecanismos de fuerza bruta, ejemplo: ERSjslg346”#$%

5. Nunca utilice la misma contraseña para todas sus cuentas.

6. Si tienes una contraseña muy fácil es recomendable cambiarla.

7. Utilizar asistentes para la creación de contraseñas, el navegador Firefox cuenta con un asistente para la creación de contraseñas llamado Sxipper el cual asiste en la creación.

8. Utilizar Mnemotecnia en la creación de claves con el fin de poderlas recordar haciéndolas lo más fuerte que se puedan, un ejemplo de contraseña segura: ERThgf345#$%, puesto que posee letras mayúsculas, minúsculas, números y caracteres especiales.

Codificar los Archivos del Computador y USB

A cada momento se presentan robos de computadores, a consecuencia de esto la información personal caería en manos de cualquier persona. Muchos computadores, discos duros extraíbles, y memorias USB, contienen archivos personales de las personas, al igual que información corporativa de las empresas en materia de transacciones financieras, relación de impuestos, historias médicas de clínicas, y demás que por su naturaleza sensible deben ser protegidos.

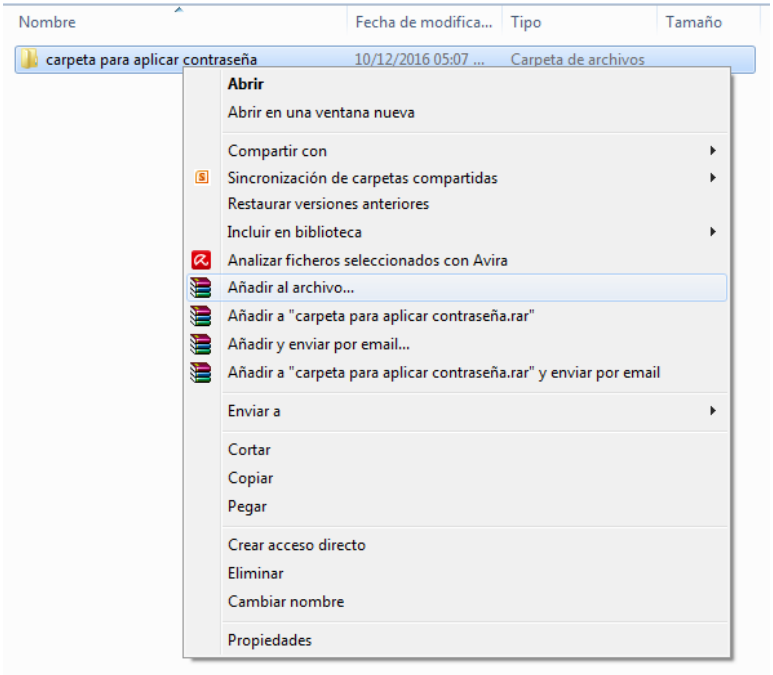
Los computadores portátiles así como los celulares debido a su reducido tamaño se pueden transportar con facilidad, lo cual los hace un elemento atractivo a los delincuentes.

Por tal motivo deben asegurarse de proteger los dispositivos móviles y la información almacenada. Es necesario aplicar códigos a la información importante en dichos dispositivos.

A través de este manual se le indicara al usuario como codificar archivos del portátil a través del Winrar y codificar las memorias USB a través de la herramienta de Windows BitLocker.

Se procede a ubicar la carpeta la cual se le aplicara la compresión y posterior protección con contraseña de la siguiente manera dándole clic derecho y seleccionando la opción añadir al archivo, como se puede apreciar:

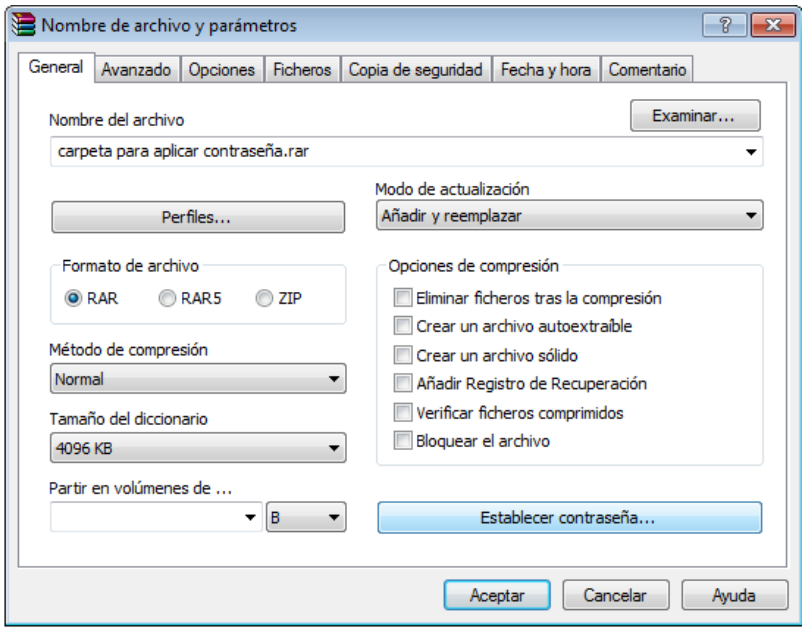
Figura 14. Selección de carpeta a codificar



Fuente: El Autor.

Se procede a seleccionar el formato del archivo que puede ser RAR, RAR5 o ZIP y se le da clic en establecer contraseña, como se puede apreciar:

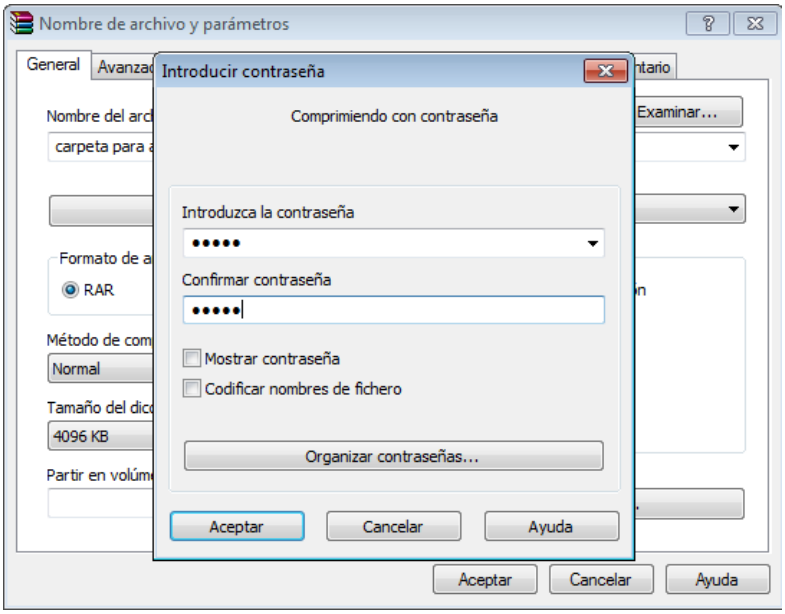
Figura 15. Selección de establecer contraseña



Fuente: El Autor.

Se ingresa la contraseña correspondiente y se repite, como se puede apreciar:

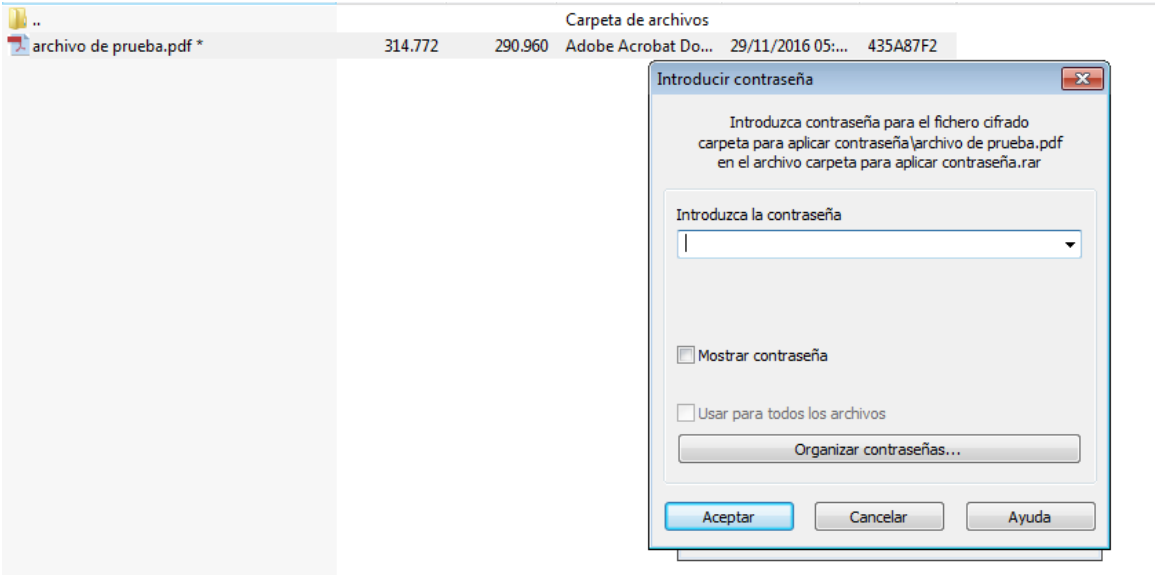
Figura 16. Establecimiento de la contraseña



Fuente: El Autor.

Unza vez dado clic en aceptar se comprueba que el archivo al ser abierto me solicita contraseña, como se puede apreciar en la siguiente imagen

Figura 17. Prueba de la contraseña



Fuente: El Autor.

Para la codificación de memorias USB y para propósitos de este manual se usara la herramienta que ofrece Windows la cual es BitLocker, que viene de forma gratuita con el sistema operativo y ofrece seguridad a las unidades extraíbles en caso de pérdida o robo para que nuestra información personal no caiga en manos inescrupulosas, la configuración se realiza de la siguiente manera:

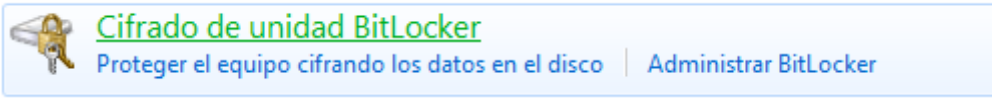
Dando clic en inicio se busca el panel de control y se accede a Sistema y Seguridad, como se puede apreciar:

Figura 18. Uso del BitLocker

Fuente: El Autor.

Y posterior a esto se accede a la opción cifrado de unidad BitLocker

Figura 19. Selección del BitLocker



Fuente: El Autor.

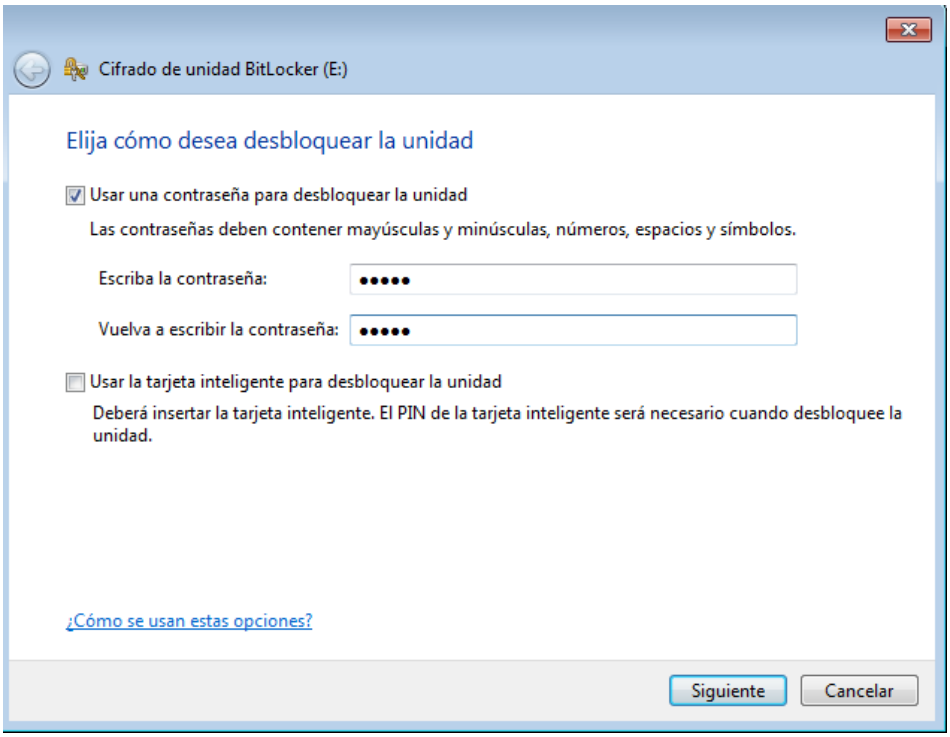
Se procede a seleccionar la unidad extraíble para realizar el proceso correspondiente de cifrado, dando clic en la opción activar BitLocker, como se aprecia

Figura 20. Selección de la unidad aplicar contraseña

Fuente: El Autor.

Se selección la opción de la contraseña, en la cual se le asigna una contraseña y se confirma, de la siguiente manera:

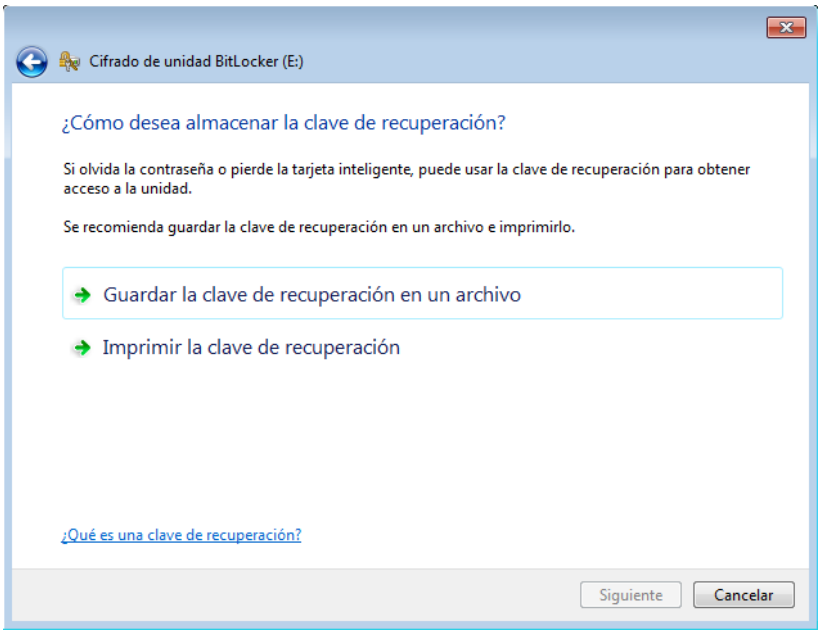
Figura 21. Asignación de la contraseña



Fuente: El Autor.

Por último se almacena o se imprime la clave, de acuerdo a lo siguiente:

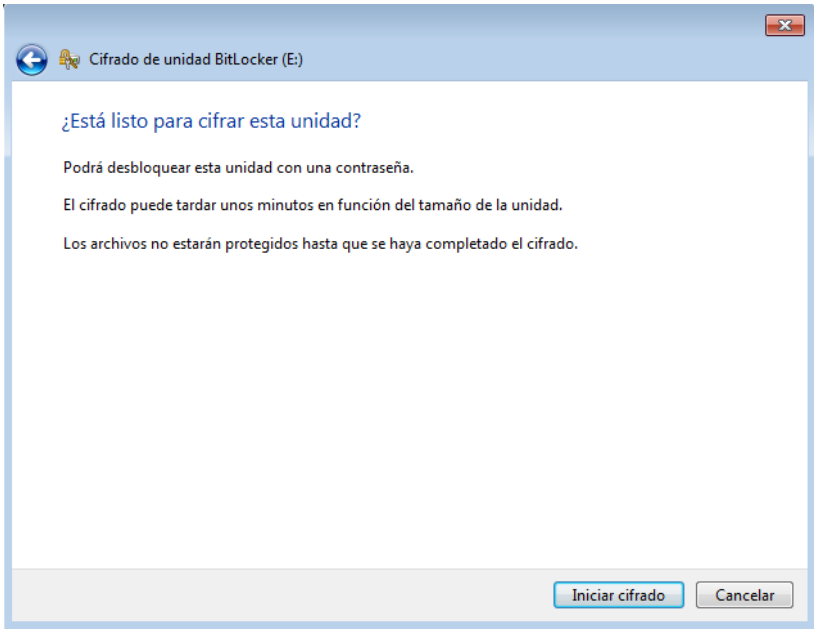
Figura 22. Guardado de la contraseña



Fuente: El Autor.

Se da inicio al proceso de cifrado de la unidad como se puede apreciar:

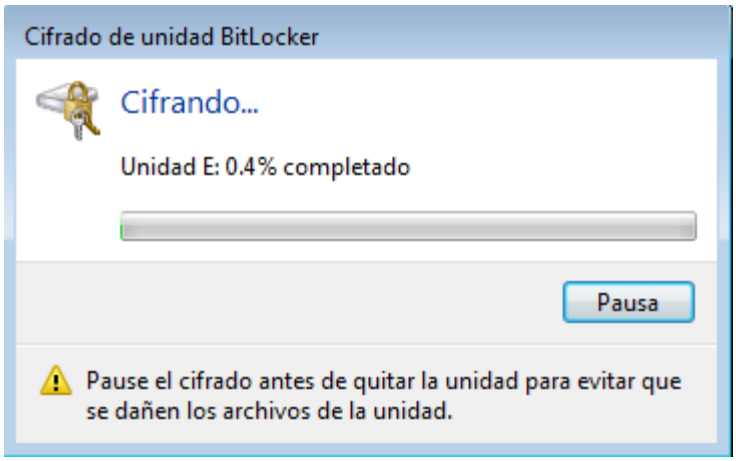
Figura 23. Inicio del cifrado



Fuente: El Autor.

El tiempo de cifrado dependerá de la capacidad de la unidad extraíble como se puede apreciar:

Figura 24. Procedimiento del cifrado



Fuente: El Autor.

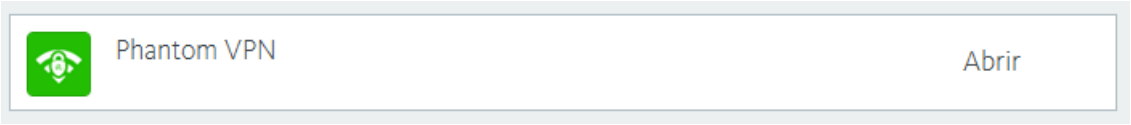
6.3 APLICABILIDAD DE LAS CONEXIONES INALAMBRICAS A LA INTERNET

INSTALACION DEL SOFTWARE VPN

El VPN en una herramienta de software que es considerado el primer filtro para proteger la red de los riesgos originados debido a una conexión Wi-Fi, puesto que esta realiza la transmisión de información de manera codificada sin que la conexión Wi-Fi la codifique, haciendo que cualquier información captada por los Hackers sea inútil por su alto grado de codificación.

Corresponde a la primera protección en contra de los ataques producidos en una conexión Wi-Fi, las VPN o Red Virtual Privada permite trasmitir información de manera codificada sin que la conexión Wi – Fi en si lo este, lo que permite que la información capturada por hackers no logre ser accesadas, en el mercado existen numerosos software VPN de tipo comercial y gratuitos para propósitos de este manual se utilizara el Phantom VPN el cual es gratuito y vienen con el paquete de antivirus de Avira Free, como se puede apreciar en la siguiente imagen:

Figura 25. Uso del Phantom VPN



Fuente: El Autor.

Al darle clic en abrir se puede apreciar una pantalla que nos alerta, que nuestra conexión no es segura, como se puede apreciar en la siguiente imagen:

Figura 26. Protección de la conexión con Phantom VPN

Fuente: El Autor.

Procedemos a darle clic en proteger mi conexión y el software comienza el proceso de conexión y de codificación de la conexión como se puede apreciar:

Figura 27. Estableciendo la conexión con Phantom VPN

Fuente: El Autor.

Una vez terminado el proceso puede apreciarse la conexión codificada para preservar la seguridad durante la navegación por internet.

Figura 28. Protección establecida

Fuente: El Autor.

Anexo B. Resumen Analítico de Educación RAE

Título de Documento.	ESTUDIO DE RIESGOS EN USUARIOS DE LAS REDES SOCIALES Y LA INTERNET APLICADO A JÓVENES UNIVERSITARIOS DE LA CIUDAD DE SAN JOSÉ DE CÚCUTA.
Autor	RANGEL QUINTERO José Andrés.
Palabras Claves	Redes Sociales, Internet, Riesgos, Amenazas, Metodología MAGERIT, UFPS.
Descripción El proyecto consiste en un estudio de riesgos en usuarios de las redes sociales específicamente aplicado a los jóvenes universitarios de San José de Cúcuta y la generación de un manual para mitigar dichas amenazas.	
Fuentes Bibliográficas	AVILA GUERRERO, Edward. Influencia de las redes sociales en los jóvenes [en línea]. [Citado 20 octubre 2016]. Disponible en Internet en: http://influredes sociales.blogspot.com.co/p/fichas-bibliograficas.html COLOMBIA DIGITAL. Conceptos TIC [en línea]. [Citado 25 mayo 2017]. Disponible en Internet en: https://colombiadigital.net/actualidad/articulos-informativos/conceptos-tic.html COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se

preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones [en línea]. [Citado 20 octubre 2016]. Disponible en Internet en: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

EDUCATIVO SEGURIDAD INFORMÁTICA. Spoofing [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: http://segurdadenredes.blogspot.com .co/2014/11/pagina-en-construcion. html

ESPINOZA TRUJILLO, Sarita. Influencia de las redes sociales en los jóvenes [en línea]. [Citado 29 octubre 2016]. Disponible en Internet en: http://es.slideshare.net/ SAwuita15/redes-socialesppt-34459822

GARCIA, Carlos. Hablemos de Spoofing [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/

GLOSARIO DE INFORMÁTICA E INTERNET. Chain e-mail [en línea]. [Citado 25 mayo 2017]. Disponible en Internet en: http://www.internetglosario.com/849/ Chainemail.html

LEON ROJAS, Juan. Ataque de suplantación de identidad (mail-spoofing) [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: http://cala.unex.es/ cala/cala/mod/forum/discuss.php?d= 7875

MENDEZ, L. Que es el Mail Spoofing y como evitarlo usando SPF [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: https://www.webempresa.com/ blog/que-es-el-

mail-spoofing-y-como-evitarlo-usando-spf.html

MOLINA. Leonela. Delitos informáticos [en línea]. [Citado 26 mayo 2016]. Disponible en Internet en: http://es.calameo.com/books/005155407963f214f1a28

PAEZ, Andrea. Tipos de spoofing [en línea]. [Citado 15 octubre 2016]. Disponible en Internet en: http://andrea0712.blogspot.com.co/2011/05/ejercicios_11.html

ROSERO, Manuel Antonio. Los riesgos en las redes [en línea]. [Citado 23 octubre 2016]. Disponible en Internet en: http://cucuta.extra.com.co/noticias/columnistas /los-riesgos-en-las-redes-231027

SALUD INVESTIGA. Población, unidad de análisis, criterios de inclusión y exclusión. Muestra: identificación y reclutamiento [en línea]. [Citado 29 octubre 2016]. Disponible en Internet en: http://www.saludinvestiga.org.ar/pdf/tutorias /poblacion ymuestra.pdf

SITES GOOGLE. Principales riesgos en redes sociales [en línea]. [Citado 20 octubre 2016]. Disponible en Internet en: https://sites.google.com/site/riesgosredes sociales2011/home

UNICEF. ¿Qué es la ciberintimidación? [en línea]. [Citado 25 mayo 2017]. Disponible en Internet en: http://www.alguien.do/quiero-estar-bien/en-mi-comunidad/que-es-la-ciberintimidacion

VELÁSQUEZ DÍAZ, Noé. Redes sociales, gran influencia en

	los jóvenes [en línea]. [Citado 1 noviembre 2016]. Disponible en Internet en: http://es.slideshare.net/ Velnoesitho/redes-sociales-gran-influencia-en-los-jvenes

CONTENIDO:

Estudio de riesgos en usuarios de las redes sociales y la internet aplicado a jóvenes universitarios de la ciudad de san José de Cúcuta.

DESCRIPCIÓN DEL PROBLEMA:

El entorno actual que apunta a un mundo más globalizado y pequeño a través de la conectividad de las redes y el internet permite poner en clara evidencia la importancia de que todos los usuarios sean conocedores de los riesgos a los cuales se enfrenta una persona en Internet.

Diversas amenazas en las que se ven inmersos los usuarios en la red como son el grooming, sexting, reputación virtual, ciberbullying, usurpación de las cuentas, estafas a través de las redes sociales, son potenciales riesgos que las personas pueden ser víctimas, si existe un desconocimiento de los riesgos y de métodos para evitarlos.

Con el auge del internet en Colombia dichos delitos que parecían ser más un problema de naciones desarrolladas, se han convertido en un problema de tipo local con agravantes como son las pocas restricciones que hay sobre los contenidos en la red y una laxa penalización a los infractores de este tipo de delitos informáticos.

Tal análisis de los riesgos en la internet se hace necesaria para tener un contexto claro de cuáles son las vulnerabilidades que los usuarios en la red los convierten en un blanco para los delincuentes cibernéticos.

OBJETIVO GENERAL.

Disminuir los riesgos a que se ven expuestos los usuarios de las redes sociales y la Internet mediante la difusión de resultados del estudio de riesgos aplicado a los jóvenes universitarios de la ciudad de san José de Cúcuta.

OBJETIVOS ESPECÍFICOS.

- Analizar los riesgos en las redes sociales y en el internet que afectan a los usuarios.
- Identificar las amenazas en las redes sociales y el internet más recurrente en Jóvenes Universitarios de la Ciudad de San José de Cúcuta.
- Diseñar un manual que contenga Tips, configuraciones y herramientas de software libre que puedan seguir los usuarios de las redes sociales y de internet para permitir una navegación segura.

RESUMEN DE LO DESARROLLADO EN EL PROYECTO.

El documento inicia con la Introducción, donde se analiza el crecimiento de las redes sociales y el internet en el mundo globalizado de hoy en día y la importancia de identificar los riesgos que estas pueden traer consigo.

El segundo capítulo corresponde a la Justificación del proyecto, se da una aclaración sobre como es el comportamiento de los jóvenes en las redes sociales y cuál podría ser sus amenazas enfocándose en el contexto de los jóvenes universitarios de San José de Cúcuta.

El tercer capítulo corresponde a los Objetivos del proyecto, siendo este en “disminuir en nivel de riesgos a que se ven expuestos los usuarios de las redes sociales y la internet mediante la difusión de resultados del estudio de riesgos aplicado a los jóvenes universitarios de la ciudad de san José de

Cúcuta". Se plantean tres objetivos específicos, que apuntan a logro del objetivo principal.

El cuarto capítulo es el marco referencial del proyecto, donde se muestran inicialmente estudios y ponencias similares sobre el comportamiento, riesgos y amenazas de los jóvenes en las redes sociales. En este mismo capítulo se encuentra el marco teórico y el marco teórico, marco legal y marco contextual del proyecto.

El capítulo 5 corresponde al análisis de los riesgos y determinación de las amenazadas sobre los cuales se ven involucrados los jóvenes universitarios de San José de Cúcuta, analizando los resultados de las encuestas aplicadas y generando un producto concerniente al manual con las recomendaciones para la protección de los jóvenes en las redes sociales y aplicaciones tecnológicas para mitigar los riesgos.

METODOLOGÍA DE DESARROLLO

El proceso investigativo está desarrollado en un enfoque mixto, el tema de investigación es sobre el Estudio de Riesgos de las Redes Sociales en la población Universitaria, haciendo referencia en cuál es su pensamiento y accionar, es aquí donde se implementa un método Cuantitativo en donde se hace una medición de la cantidad de personas que se ven influenciadas por las redes sociales, y para obtener dicho análisis se hace uso de instrumento tipo encuesta con una serie de preguntas cerradas en base a este se observa la utilización y el propósito de las redes sociales sobre las cuales se está relacionando.

A través de un método cualitativo donde se observe y no se interactúe en el establecimiento educativo universitario, en el cual se analice las reacciones físicas que pueden acarrear el uso indiscriminado de las redes sociales de esta manera determinar su desenvolvimiento con otras personas, como es su

estilo al vestir y si esta vestimenta se ve relacionada con las personas vinculadas a sus redes sociales, siendo esta una característica de la aplicación de un enfoque mixto.

El análisis y gestión de los riesgos que afectan a los jóvenes en el uso de las redes sociales esta soportado a través de la metodología MAGERIT, el cual permite realizar una identificación y caracterización de los riesgos que conllevan el uso de los sistemas de información y todos sus contextos asociados, que para efectos de este proyecto son las redes sociales, y esto permite la creación de políticas que deben aplicarse para mitigar los riesgos que han sido identificados en esta investigación.

MAGERIT ha determinado el concepto de seguridad como el proceso de soportar a través de un mínimo de estándares de confiabilidad, las actividades ilegales que afectan el funcionamiento y la calidad de la información albergada en los sistemas de información.

MAGERIT hace uso de conceptos para su análisis los cuales son: activo, amenazas, vulnerabilidad, nivel de impacto, riesgos y controles.

CONCLUSIONES

Las redes sociales son medios de comunicación que han tenido un auge de manera exponencial, siendo parte importante de nuestra vida diaria, a su vez son un medio valioso con un gran potencial para exponer las ideas y pensamientos de las personas sin restricción, debido a esto los jóvenes ven en las redes sociales un medio para liberarse de las presiones de la sociedad, convirtiéndolos en un blanco fácil ante los riesgos inherentes de estas aplicaciones sociales.

La identificación de los riesgos y amenazas que enfrentan los jóvenes en las redes sociales es un tema de suma importancia, en vista de la alta proliferación de casos de acosos no solo de tipo personal sino sexual que ha

ocasionado que los jóvenes se aíslen o busquen salidas como el suicidio, por tal motivo este proyecto busco brindar herramientas a los jóvenes tanto desde el punto de vista social, psicológico y técnico para que estos cuenten con los criterios suficientes para hacer su navegación en la red y su uso de las redes sociales algo más seguro.

Desde el respectivo análisis evidenciado según los aportes de los jóvenes de San José de Cúcuta, se clarifica que la suplantación de la identidad es el riesgo más evidente, del cual se desprenden otras formas de acoso en las redes sociales entre ellas el ciberbullying.

Adicional a esto se determinó que el riesgo más conocido entre los jóvenes universitarios corresponde al ciberbullying, el cual corresponde a la intimidación en línea, y que el conocimiento de términos como el Smishing y Spoofing entre los jóvenes es menor o casi nulo lo cual los hace vulnerables a ser víctimas tanto de captura de datos personales como la de la suplantación de la identidad.

Para los jóvenes universitarios de San José de Cúcuta la generación de mecanismos de seguridad en el internet es competencia exclusiva de los padres de familia, lo que sugiere que los padres de familia deben tener un rol más importante en la aplicación de controles de contenido de información, sin desconocer que entre los jóvenes deben existir pautas de autocuidado que les permitan madurar y ser más críticos en las redes sociales.

El determinar a quién o a quien no aceptar como amigo en una red social es un punto que se ha analizado con este instrumento, lo cual entre los jóvenes cucuteños se ha determinado que están abiertos en su gran mayoría de aceptar a cualquier persona aun desconociendo su identidad, ya que al aceptar dicha solicitud se le permite al usuario tener acceso a toda la información personal que haya publicado la persona, permitiendo que esta pueda ser propensa a cualquier actividad delictiva con el mal uso de la

información que se haya compartido en el perfil.

Desde la perspectiva del análisis evidenciado en cada una de las preguntas aplicadas a la población objetivo de este estudio la cual correspondía a jóvenes universitarios de la ciudad de Cúcuta, se puede determinar la existencia del desconocimiento de los riesgos en los cuales se pueden ver afectados, determinados por la ingenuidad en el uso de las redes sociales, como en la capacidad de no prever los riesgos inherentes asociados en la divulgación indiscriminada de información personal o en la baja dificultad de las contraseñas, y en el uso recreativo de la internet como medio para conocer gente y relacionarse con el entorno

RECOMENDACIONES

La determinación de los riesgos en el uso de la internet y las redes sociales debe ser considerado un tema prioritario para los padres de familia y la comunidad universitaria, por tal motivo se recomienda la aplicación de técnicas socializadas en el presente proyecto para mitigar los riesgos en los cuales se ven inmersos los jóvenes a través del uso de la internet