Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

FACTORES FUNDAMENTALES Y PRINCIPALES VÍAS PARA EVITAR COMETER ERRORES AL NAVEGAR POR INTERNET

Francisco Alejandro Coloj Marroquín
Asesorado por el Ing. Luis Fernando Quiñónez López

Guatemala, septiembre de 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

FACTORES FUNDAMENTALES Y PRINCIPALES VÍAS PARA EVITAR COMETER ERRORES AL NAVEGAR POR INTERNET

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

FRANCISCO ALEJANDRO COLOJ MARROQUÍN
ASESORADO POR EL ING. LUIS FERNANDO QUIÑÓNEZ LÓPEZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, SEPTIEMBRE DE 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Luis Diego Aguilar Ralón
VOCAL V	Br. Christian Daniel Estrada Santizo
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. Pedro Pablo Hernández Ramírez
EXAMINADOR	Ing. Herman Igor Véliz Linares
EXAMINADOR	Ing. César Augusto Fernández Cáceres
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

FACTORES FUNDAMENTALES Y PRINCIPALES VÍAS PARA EVITAR COMETER ERRORES AL NAVEGAR POR INTERNET

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha 6 de julio de 2018.

Francisco Alejandro Coloj Marroquín

Universidad de San Carlos de Guatemala

Facultad de Ingeniería

Guatemala 22 de abril de 2019

A QUIEN INTERESE:

Por medio de la presente hago constar que **Francisco Alejandro Coloj Marroquín,** identificado con el carné **201122766** y dpi **2236666880401**, estudiante de la carrera de Ingeniería en Ciencias y Sistemas, me ha presentado la totalidad de su trabajo de graduación, ante el cual doy el visto bueno al trabajo de investigación titulado **"Factores Fundamentales y Principales Vías Para Evitar Cometer Errores al Navegar por Internet"**.

Sin otro particular me despido de la manera más cordial.

LUIS QUIÑÓNEZ
INGENIERO EN C.C. Y SISTEMAS
COLEGIADO No. 7514

Luis Fernando Quiñónez
Ingeniero en ciencias y sistemas
Colegiado No. 7514

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 2 de mayo de 2019

Ingeniero
Marlon Antonio Pérez Türk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **FRANCISCO ALEJANDRO COLOJ MARROQUÍN** con carné **201122766 y CUI 2236 66688 0401** titulado **FACTORES FUNDAMENTALES Y PRINCIPALES VÍAS PARA EVITAR COMETER ERRORES AL NAVEGAR POR INTERNET** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo aprobado.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE INGENIERÍA EN
CIENCIAS Y SISTEMAS
TEL: 24767644

*El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación "**FACTORES FUNDAMENTALES Y PRINCIPALES VÍAS PARA EVITAR COMETER ERRORES AL NAVEGAR POR INTERNET**", realizado por el estudiante, FRANCISCO ALEJANDRO COLOJ MARROQUÍN aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS

Ing. Carlos Gustavo Alonzo
Director
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 02 de septiembre de 2019

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 320.2019

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al Trabajo de Graduación titulado: **FACTORES FUNDAMENTALES Y PRINCIPALES VÍAS PARA EVITAR COMETER ERRORES AL NAVEGAR POR INTERNET,** presentado por el estudiante universitario: **Francisco Alejandro Coloj Marroquín,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Inga. Aurelia Anabela Cordova Estrada
Decana

Guatemala, septiembre de 2019

/gdech

ACTO QUE DEDICO A:

Dios	Por ser lo más importante en mi vida.
Mis padres	Francisco Coloj Mazate y María Elisa Marroquín Marroquín. Sus consejos, amor y enseñanzas han sido vitales para alcanzar mis metas.
Mis hermanas	Adriana y Nancy Coloj por apoyarme cuando lo necesite.
Mis sobrinos	Leonel y Monserrat Arriola, por alegrar mis días cuando más lo necesitaba.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser *la alma mater* que me acogió durante mi tiempo de estudio, día tras día.
Facultad de Ingeniería	Por abrirme las puertas y permitir realizar todo lo necesario para lograr alcanzar mis objetivos académicos.
Mis amigos de la Facultad	Por no desistir y estar siempre apoyándonos mutuamente a cumplir esta meta.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Amenaza	Posible causa de riesgo o perjuicio para alguien o algo.
ARPA	Advanced Research Projects Agency (Agencia de Proyectos de Investigación Avanzada).
Ataque	Tomar el control, desestabilizar o dañar cualquier sistema informático desde otro sistema.
Computadora	Maquina electrónica capaz de procesar y almacenar información a base de operaciones matemáticas y lógicas.
Disco duro	Unidad de almacenamiento no volátil.
Fraude	Acción contraria a la verdad y a la rectitud o ley.
Hacker	Persona que descubre las debilidades de un sistema o computador.
Hardware	Todas las partes físicas de un sistema informático.
Información	Conjunto organizado de datos que conforman un sistema.

Internet	Conjunto de redes de computadoras interconectadas entre sí.
Malware	Malicious software (programa malicioso) que tiene como finalidad infiltrarse o dañar un computador o sistema.
Procesador	Componente electrónico donde se realizan los procesos lógicos de un computador.
Protocolo	Conjunto de reglas definidas por las que hay comunicación dentro de una red.
Proveedor	Persona o entidad que provee o abastece un producto o servicio.
RAM	Random Access Memory (memoria de acceso aleatorio), dispositivo de almacenamiento volátil que procesa las instrucciones dentro de un ordenador.
Red de computadoras	Conjunto de equipos informáticos y software conectados entre sí.
Redes sociales	Estructura capaz de comunicar entre sí a personas o instituciones a través del internet.
Script	Archivo de instrucciones que se ejecuta en un sistema.

Sistema informático	Sistema que permite almacenar y procesar información.
Software	Conjunto de componentes lógicos necesarios que hacen posible la realización de tareas específicas.
Usuario	Persona que habitualmente hace uso de un servicio o sistema.
Virus	Software que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático o sistema.
Vulnerabilidad	Debilidad o fallo en un sistema de información que pone en riesgo la seguridad y/o integridad del mismo.

RESUMEN

El presente informe de graduación se realizó con la finalidad de concientizar a las personas sobre los más comunes ataques y posibles vulnerabilidades a las que están expuestos todos los días al navegar por internet.

Tomando como base que muchas personas simplemente con el papel de usuario final y siendo el que accede a internet, no toma las medidas necesarias para protegerse, siendo este el mayor problema, el error humano.

Las personas no acatan recomendaciones y no previenen todo este tipo de fraudes que puedan existir debido a que quizá ni logren darse cuenta de dichos problemas, para ellos simplemente será pasar un rato de ocio, compartir información mediante correos o visitar páginas probablemente porque el trabajo requiera de ello, pero pasa desapercibido todo aquello que pueda dañar el computador o dispositivo con el que se accede a internet, vulnerando la información, considerada lo más valioso del ser humano digitalmente hablando, o incluso robo de la misma.

OBJETIVOS

General

Brindar una herramienta escrita para todos los usuarios que accedan a internet, haciendo conciencia de los posibles ataques que pueden suscitarse, los principales fraudes que existieron en la historia y los que actualmente afectan a los usuarios.

Específicos

1. Recabar la información necesaria para hacer llegar a las personas y que sepan las vulnerabilidades existentes, para tomar las medidas preventivas necesarias.

2. Convergir en que se está expuesto a todo tipo de fraudes o de herramientas mal intencionadas con la finalidad de robar información, suplantar identidad de otras personas, y todo ello evita una navegación segura y de confianza.

3. Proporcionar un soporte escrito que permita a las personas saber que deben hacer y que deberían evitar al momento de navegar por internet, para no verse vulneradas y con problemas tanto del equipo con el que navegan, o la información que se pueda proporcionar al navegar.

INTRODUCCIÓN

En la actualidad se puede observar que la mayoría de personas tiene acceso a internet, siendo esta una herramienta fundamental para lograr objetivos como investigar, informarse y divertirse. Siempre se observa que el comportamiento de las personas es la utilización de cualquier sistema, red social y todo tipo de herramientas que estén al alcance en internet, sin tomar en cuenta que existen muchos riesgos al no tomar las medidas mínimas de seguridad; esto Implica que las personas puedan ser víctimas de fraude, falsificación de información y por si fuese poco, robo de cuentas bancarias, tarjetas de crédito y todo tipo de cosas que puedan involucrar una comunicación entre el usuario final y el internet.

Las personas no están conscientes que la mayoría de ocasiones que hacen uso de internet están potencialmente en riesgo ante los posibles ataques, estos en su gran mayoría en vez de desaparecer, se vuelven cada día más fuertes hablando de la dificultad de combatirlos, e incluyendo que muchas personas consideran un antivirus el escudo que los protege en su totalidad de todo este tipo de problemas.

Es por ello que hablar de ese tipo de amenazas, la prevención y posibles soluciones ante los problemas existentes, ayudarán de gran manera a todas las personas que empiezan o actualmente ya están dentro del mundo del internet. Este será el punto clave que se deberá entender para lograr obtener lo necesario para saber que se puede y lo que se debe evitar al navegar por internet.

1. PROBLEMAS RECURRENTES AL NAVEGAR EN INTERNET

1.1. Datos históricos de internet y sus principales problemas

La mayoría de personas que hacen uso de internet no saben el origen y evolución de todo lo que tuvo que pasar el ahora llamado internet, para ser lo que actualmente es, y ser esta herramienta fundamental que se utiliza todos los días por millones de personas alrededor del mundo.

1.1.1. Inicio ARPA

Todo inicio bajo la necesidad de los militares estadounidenses durante la guerra fría en el año de 1947 de comunicarse entre sí para evitar ser detectados de las tropas enemigas.

Siendo hasta el año de 1957 donde se organiza Advanced Research Projects Agency (Agencia de proyectos para la investigación avanzada de Estados Unidos), conocido como ARPA y se vincula con el departamento de defensa. Todo eso se dio debido a los avances tecnológicos obtenidos por la Unión Soviética.

Siendo ARPA considerada en los años posteriores como la organización que fundamento todo lo necesario para dar el paso a el internet.

Siendo en el año 1962 donde Paul Baran que era investigador del Gobierno de los Estados Unidos, presentó un sistema, este interconectaba

computadoras mediante una red descentralizada, para evitar cualquier tipo de ataques externos y así garantizar el envío de la información, garantizando que si algún punto de los muchos interconectados quedaba inutilizable, los otros podían seguir funcionando sin problema alguno.

Basándose en la teoría de conmutación de paquetes que pretendía explicar que toda la información que proviene de un punto mediante un dispositivo, es segmentada para su posterior transmisión y así llegar a su destino, y dichos segmentos se les denominaba paquetes, creada por Leonard Kleinrock, fue donde partió todo lo relacionado a esa comunicación entre dispositivos.

Los trabajos eran arduos, pero se luchaba constantemente para poder crear una red a la que se pudiera acceder desde cualquier parte del mundo a la que denominarían red galáctica. En el año 1965 se estableció conexión entre un ordenador TX2 que se encontraba en Massachusetts y un Q-32 que estaba en California, los cuales fueron conectados a través de una línea telefónica que era de baja velocidad y con limitaciones. Con todos los intentos se logró trabajar como se requería, sin embargo, había problemas que no iban a poder solucionarse con este tipo de comunicación, y muchos debido a las limitaciones que presentaba la línea telefónica.

1.1.2. Evolución a ARPANET y WWW

Durante los años posteriores a la creación de ARPA para la comunicación, los trabajos de investigación fueron arduos hasta que en el año 1969, Michel Elie que en su momento fue considerado uno de los pioneros del internet, ingresa a la Universidad de California, y retoma el proyecto ARPA mediante una beca de investigación. Para el final de este año mediante los trabajos realizados

se logra conectar una computadora de la Universidad de California con una del Instituto de Investigación de Stanford. Siendo en este momento ya cuatro entre universidades e institutos interconectados, siendo denominado este proyecto de red como ARPANET.

En el año 1970 ARPANET logró establecerse de manera permanente, siendo Ray Tomlinson el que con sus trabajos lograría establecer las bases para la realización posterior de lo que conocemos como correo electrónico, partiendo de la necesidad que los que trabajaban en el proyecto necesitaban una manera de comunicarse para coordinar todo lo relacionado al proyecto.

Siendo las agencias militares las encargadas de todo este proceso iniciando como la necesidad de comunicación durante la guerra fría, pero dando paso a brindar dicha tecnología a las universidades para sus investigaciones y avances tecnológicos. Siendo en el año 1972 donde alrededor de 50 universidades ya formaban parte de este gran proyecto denominado ARPANET, un año después de todo ese avance con las universidades lograse establecer comunicación con otros países como Inglaterra y Noruega.

Transcurriendo los años 80, tomo mayor auge todo esto de las redes, debido a que ya existía mucha demanda de computadoras, las cuales fueron conectándose a redes diversas, dichas volvieron un caos todo lo previamente iniciado, todos querían hacer uso de la nueva tecnología existente, pero después de la tormentosa lucha, vino la consolidación y unificación de todo, es ahí donde se denomina el nacimiento del internet.

Siendo el año de 1983 el departamento de defensa de Estados Unidos decidió utilizar el protocolo TCP/IP en su red, era conocida como ARPANET, y

la denominaron Arpa Internet. Transcurriendo los años el nombre fue consolidado únicamente a Internet.

En el año de 1991 Tim Berners Lee fue quien dio origen a la World Wide Web o como comúnmente se le conoce WWW, y hacía uso de 3 recursos completamente nuevos, estos fueron HTML, TTP y un programa denominado Web Browser.

El año 1993 dio vida alrededor de 100 sitios conocidos como World Wide Web Sites, pero con un crecimiento alto y rápido llegó a ser más de 200,00 World Wide Web Sites en el año de 1997.

1.1.3. Internet y la era de las redes sociales

A mediados de los años 90 da inicio la era de las redes sociales directamente con la creación del sitio GeoCities, esta red consistía en la creación de sitios web que se alojaban en GeoCities, y la principal función era la comunicación e interacción de los usuarios que estaban dentro del segmento al que había registrado sus sitios.

Posterior al manejo de sitios mediante GeoCities, fueron apareciendo las redes sociales como tal, y fue donde apareció la red social sixdegrees, esta tenía como finalidad conectarse entre usuarios mediante una invitación (un usuario enviaba invitación a otro, para posteriormente poder enviarse mensajes y ver cuando estaban conectados, y dicha red social (que en su momento no fue conocido por ese nombre), llegó a tener muchos usuarios aproximadamente una cifra mayor a un millón de usuarios, pero tuvo su fin este sitio en el año 2001.

En el siguiente año (2002), fueron apareciendo más redes sociales y en ese año se crea Friendster, dicha red social era para las personas que tenían como afición todo lo relacionado a los videojuegos. En el año 2003 aparece en internet una red social que llegó a contar con aproximadamente 70 millones de usuarios, denominada Hi5, en ese mismo año fue creado MySpace y Linkedin; Linkedin es una red social que tiene actualmente la finalidad de empleo, es decir una red social para contactar personas las cuales podrían desempeñar un empleo. Pero en el año 2004 todo hubo un giro trascendental debido a que el joven universitario de Harvard Mark Zuckerberg dio vida a lo que hoy se conoce como Facebook. Se podría denominar a Facebook, como la red social más utilizada por las personas (actualmente aún lo es) a nivel mundial.

A mediados de 2005 existió un precedente que marcaría una nueva era en redes sociales, las cuales tenían como finalidad la transmisión de vídeos, y es como surgiría en ese año la idea de YouTube. Pero fue en el año 2006 donde Google adquiere YouTube por una cantidad de 1650 millones de dólares, una cantidad demasiado grande, pero casi insignificante al valor actual de la misma.

Tabla I. **Cronología de evolución de internet**

Elemento	Año creación	Descripción
ARPA	1957	Aparece bajo la necesidad del ejercito de los Estados Unidos de comunicarse sin ser interceptados por las tropas enemigas.
ARPANET	1969 - 1970	Evolución de lo que se conocía como ARPA, y ya involucraba conexión entre dos y más puntos de diferentes lugares.

Continuación de la tabla I.

Elemento	Año creación	Descripción
WWW	1991 y 1993	Da origen WWW siendo este la evolución de ARPANET y contaba con tres protocolos los cuales eran HTTP, TTP y un programa que recibía el nombre de Web Browser.
Redes sociales	1990-Actualidad	Da origen con la creación de GeoCities, que era considerado el sitio para comunicarse entre personas y posterior a ello nacieron las redes sociales formales, las que se conocen actualmente, y evolutivamente vinieron desde MySpace, Hi5, Twitter, Facebook y muchas más.

Fuente: elaboración propia.

1.2. Vulnerabilidades y principales fraudes en internet

Las amenazas están siempre presentes al navegar por internet, las cuales existen de muchos tipos y formas, las cuales siempre van a tener como finalidad primordial aprovecharse de la información del usuario; Sabiendo que las amenazas son diferentes a las vulnerabilidades, una amenaza viene dada como cualquier intento de hacer caer o robar a la víctima todo tipo de información que sea posteriormente utilizada para generar ingresos por parte del atacante, pudiendo ser, información personal, cuentas bancarias y cualquier información sensible del usuario, pero una vulnerabilidad es todo aquello que

carezca de las medidas de seguridad básicas o complejas, que permitan que los atacantes puedan ingresar de una forma más fácil para tener acceso a la información del usuario.

Partiendo de lo anterior, se sabe que mediante las vulnerabilidades con que cuenta un sistema, o que se tienen presentes en el equipo que se utiliza, se sabe que todas las amenazas tomarán como puerta de entrada las misma, siendo eso una manera muy eficiente por parte del atacante para poder violar la privacidad del usuario, máxime en circunstancias donde el usuario mismo es quien proporciona la información ya sea por error o por no tomar las precauciones necesarias. Siendo estos puntos los que permitirán al atacante realizar el fraude y así lograr el propósito principal: dejar al usuario con pérdidas de información, o monetarias, las cuales son las más comunes en este tipo de situaciones.

1.2.1. Vulnerabilidades

Haciendo referencia a que todos los usuarios están expuestos a los ataques de cualquier tipo siempre que se navega por internet, se debe evitar a toda costa que estos ataques y los atacantes logren su cometido, y para ello es necesario evitar dejar cabos sueltos al navegar; implicando muchas veces el evitar realizar cosas que comúnmente se realizan y que ponen en riesgo la integridad (hablando de integridad virtual), el atacante siempre va a buscar los puntos débiles de los sitios a los cuales el usuario accede, o las vulnerabilidades presentes en el ordenador o dispositivo en el que se conecta a internet.

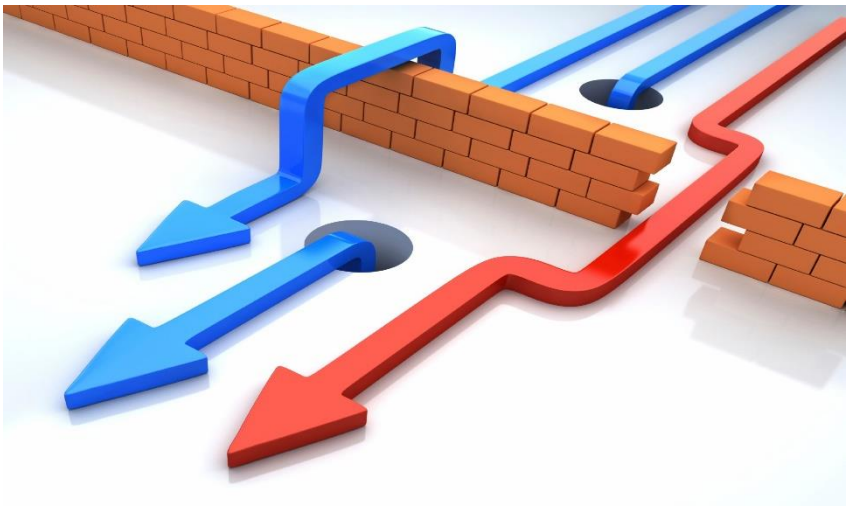
Los principales problemas del ordenador son aquellos que permiten al usuario navegar sin mayor protección siendo estos no visibles muchas veces, y

para las personas o usuarios finales basta con que el computador pueda encenderse y abrir cualquier tipo de navegador para poder navegar, siendo estos problemas muy recurrentes en todo el mundo. La principal fuente de problemas generados en el ordenador que se trabaja, van a ser los errores que el usuario cometa, muchas veces se realizan acciones que evaden por completo todas las recomendaciones de seguridad que se tengan presentes para una navegación segura porque comúnmente será el usuario que por desconocimiento e ignorancia permita todo este tipo de acciones maliciosas.

Muchas veces las personas consideran que al contar con un software (programa) que sea de protección, generalmente denominados antivirus, ya están completamente a salvo de este tipo de problemas o amenazas, y es todo lo contrario, los atacantes siempre buscan evadir este tipo de barreras que ayudan de gran manera, pero al final de todo solo serán una herramienta útil, que se vuelve inútil al verse evadida por el mismo usuario.

Los usuarios han caso omiso a todas las advertencias debido a que generalmente al navegar desean descargar algún tipo de archivo y/o programa que pareciera inofensivo y muchas veces si lo es, pero otras veces es un programa alterado que le será la puerta de entrada al atacante para sustraer lo que necesite.

Figura 1. **Vulnerabilidad**



Fuente: *¿Por qué es importante detectar las vulnerabilidades?* https://blog.cerounosoftware.com.mx/por-qu%C3%A9-es-importante-detectar-las-vulnerabilidades. Consulta: marzo de 2019.

Vulnerabilidad siempre van a ser las puertas de acceso que tendrán los atacantes para lograr su objetivos, es decir, el diagrama muestra que el muro se puede violar mediante varias formas, esto implica que la vulnerabilidad es múltiple, es por ello que se debe evitar a toda costa cualquier tipo de amenazas.

1.2.2. Amenazas

Habiendo dejado claro que todas las amenazas siempre buscarán la puerta de entrada mediante las vulnerabilidades de un sistema u ordenador, existen muchos tipos de amenazas las cuales siempre van evolucionando, implicando que con el pasar del tiempo muchas desaparecen, siendo combatidas por los navegadores o programas antivirus, pero el desaparecer muchas veces no es porque se hayan esfumado, simplemente han cambiado la

manera de atacar o simplemente ya lograron el objetivo que tenían planificado con los ataques realizados con anterioridad.

Entonces una amenaza siempre será el aprovechamiento de una vulnerabilidad, o simplemente la mala utilización de un sistema. La mayor vulnerabilidad será siempre el error humano, debido a que es más probable que un sistema se proteja solo con las medidas básicas de seguridad, a que el usuario haga alguna acción que comprometa directamente la integridad de su privacidad o del sistema en el que está navegando.

Entonces con los conceptos ya proporcionados individualmente de amenaza y vulnerabilidad, se puede hacer la relación que está directamente ligada a ambos casos mediante el concepto que una vulnerabilidad es cualquier situación que implique esta propenso a cualquier tipo de ataque, y la amenaza es cualquier ataque que vaya directamente a aprovecharse de cualquier vulnerabilidad.

Figura 2. **Amenaza**

Fuente*: Alerta sobre contenidos en Internet que ponen en riesgo a niñas, niños y adolescentes.* https://policia-mas.blog/2018/01/23/alerta-sobre-contenidos-en-internet-que-motivan-a-ninas-ninos-y-adolescentes-a-ponerse-en-riesgo/. Consulta: marzo de 2019.

Muchas veces puede parecer algo inofensivo pero los atacantes siempre buscarán la manera más sutil de lograr sus objetivos, es decir, seducirán al usuario mediante detalles atractivos los cuales serán simplemente una trampa.

Figura 3. **Vulnerabilidades y amenazas**

Fuente: INCIBE (Instituto de Ciberseguridad de España S.A). https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian. Consulta: marzo de 2019.

Teniendo en cuenta que una vulnerabilidad y una amenaza podrían depender entre ellas, debido a que una amenaza tratará de aprovechar cualquier tipo de vulnerabilidad en un sistema de información, sabiendo eso, se define que el riesgo es esa probabilidad de que dicho ataque o amenaza sea haga real y cause daños y pérdidas, las cuales implican que el atacante o la amenaza cumplió su objetivo.

1.2.3. Amenazas web y fraudes en internet

Generalmente son programas de tipo malicioso que pueden atacar a las personas cuando se hace uso de internet. Estas amenazas tienen como puerta de entrada un navegador, es decir cualquier tipo de programa que permita navegar por internet, las cuales tienen como finalidad infectar el ordenador o dispositivo del usuario que pasará a ser víctima.

Para detallar todo lo necesario que una persona necesita o en su defecto debería tener para estar lo más seguro posible, viene dado a programas que jueguen el papel de guardias mientras se navega por internet.

Muchas veces los ataques y fraudes ocurren principalmente porque no se cuenta con un producto de seguridad instalado en el equipo (antivirus, antimalware, antispyware, etc), el sistema operativo se encuentra obsoleto, el sistema es de dudosa procedencia (pirata), o simplemente poseer el mejor sistema pero sin tener las actualizaciones al día; Implicando que estas actualizaciones generalmente las libera el proveedor del sistema, pero será el usuario quien decide si instalarlas o simplemente ignorarlas.

Es por ello que todas estas situaciones que muchas veces son costosas económicamente hablando, o por carecer de los conocimientos necesarios para llevarlas a cabo por parte del usuario, es que se tiene a estar vulnerables. Las personas prefieren muchas veces ahorrarse dinero en la compra de programas, pero muchas veces han sido alterados para su teórico óptimo funcionamiento, aunque se conoce que muchas veces no es así, como se mencionó, los programas pudieron ser alterados para poder ser detectados como válidos y originales por el sistema. Esto lleva a una de las más grandes situaciones en

las cuales el usuario será el principal responsable del daño que pueda ocasionar a su equipo mediante el atacante a través de un software.

1.2.3.1. Aplicaciones y sistemas más vulnerables

La lista de los programas o aplicaciones y sistemas, como también sistemas operativos se podría definir a todos, debido a que todo lo mencionado tendrá alguna vulnerabilidad, sin embargo, los proveedores son mucho más cuidadoso con el pasar de los días para evitar todo ese tipo de situaciones, mejorando la seguridad en todo sentido para poder evadir este tipo de amenazas.

Lo más común por parte de los atacantes será siempre generar amenazas para los sistemas o programas más utilizados para poder alterar el orden de las cosas mediante pequeños cambios que quizá sean invisibles para los usuarios, pero serán los necesarios por el atacantes para llevar a cabo su objetivo, concretar el ataque.

Java es uno de los programas más atacados debido a que muchas aplicaciones necesitan de este tipo de programas para funcionar y otras veces complementes de ellos mismos, siendo este uno de los programas más utilizados, los atacantes se han fijado en ello y han desviado la atención muy directa, sin embargo existen otros programas como Adobe Reader que ha venido siendo víctima constante con el transcurrir del tiempo debido a que de la misma forma que posee herramientas gratuitas tiene herramientas de pago, las cuales han sido atacadas, claro está que ellos como proveedores trabajan arduamente para corregir algún problema que pueda suscitarse o simplemente para corregir problemas, pero los ataques tampoco se detienen y es por ello que van luchando cuerpo a cuerpo constantemente para mejorar en ambas

vías, las cuales son una perjudicial para el usuario siendo esta beneficiosa para el atacante y la otra vía beneficiosa para el usuario siendo esta no conveniente para el atacante.

Windows incluye Internet Explorer, y ambos, uno como sistema operativo y otro como programa del sistema operativo en mención, y ambos han sido víctimas constantes de los ataques, y esto ha sucedido porque han tenido demasiados vulnerabilidades, que han ido corrigiendo con el pasar de los años, sin embargo han generado pérdidas millonarias para la prevención y corrección de todo este tipo de situaciones que dañen el sistema, o simplemente hagan perder información de suma importancia para el usuario.

A raíz de tantos problemas y ver una pequeña línea que siguen los atacantes, se dio a conocer más adelante que los problemas ya no iban directamente a programas de computador o sistemas operativos, también se veían reflejados en los dispositivos móviles con sistema Android, que venía a perjudicar de gran manera a los usuarios, el atacante podía hacer uso pleno del dispositivo violando todas las medidas de seguridad de dicho sistema, los cuales han venido fortaleciéndose y volviéndose cada vez más eficientes sin embargo, los ataques no se detienen, y máxime si son esos que logran acceder mediante el usuario, así como anteriormente se mencionó, muchas veces el usuarios es quien permite dichos ataques quizá sin darse cuenta de ellos, pero basta con cosas sencillas para hacer caer al usuario.

Según estadísticas recopiladas por el software antivirus Karpesrky mediante sus laboratorios de investigación se estimó que para el año 2012, el número de ataques basados en el uso del navegador había ascendido a la cifra de 1 595 587,670, esto pareciera un simple número o un número simplemente grande, pero si se llega al trasfondo de todo eso, esa cantidad de veces han

sido atacados los usuarios por programas maliciosos que han hecho caer los sistemas o siendo evitados por algún programa de protección, pero esa cantidad refleja lo que en verdad se define, todos al navegar por internet están expuestos a este tipo de ataques, y quizá cualquiera sin darse cuenta fue víctima, y pues forma parte de ese gran número de veces que fueron los ataques realizados.

1.2.3.2. Amenazas en internet

Todas las amenazas por internet vienen tomando diversidad de formas y buscando muchos tipos de objetivos, pero todos tienen el papel de amenaza debido a que siempre van a buscar a toda costa apoderase tanto de información, destrucción de sistemas, control parcial o total de los dispositivos o computadores en los que se tenga acceso a internet, sin embargo muchas veces no es necesario estar conectado a internet para lograr completar el ataque, algunos atacantes se alojan directamente en la raíz de equipo o dispositivo generando problemas evolutivos que podrían destruir por completo el sistema, o recabar la información del usuario que pueden utilizar posteriormente.

- Sitios web maliciosos: este tipo de ataques hace referencia a todos esos ataques que pueden ocurrir o son llevados a cabo mediante páginas que tienen algún código malicioso que será perjudicial para el equipo o para la información del usuario. Generalmente las personas ignoran los certificados de seguridad y los anuncios que puedan aparecer en la página, y los cuales son de vital importancia, muchas veces los anuncios que aparecen pueden ser scripts o código ejecutable que llevará a cabo alguna acción sin que el usuario se dé cuenta, o simplemente al hablar de códigos de seguridad o certificados de seguridad, es otra rama pero

igual o más importante debido a que toda la comunicación, es decir envío y recepción de información que pueda suscitarse entre el usuario y la página web va a ir encriptado o en términos menos complejos va a ser la misma información pero en forma distorsionada e inentendible para el humano, solamente por los sistemas o programas que tengan que recibir dicha información, es decir que para dichos sistemas será legible.

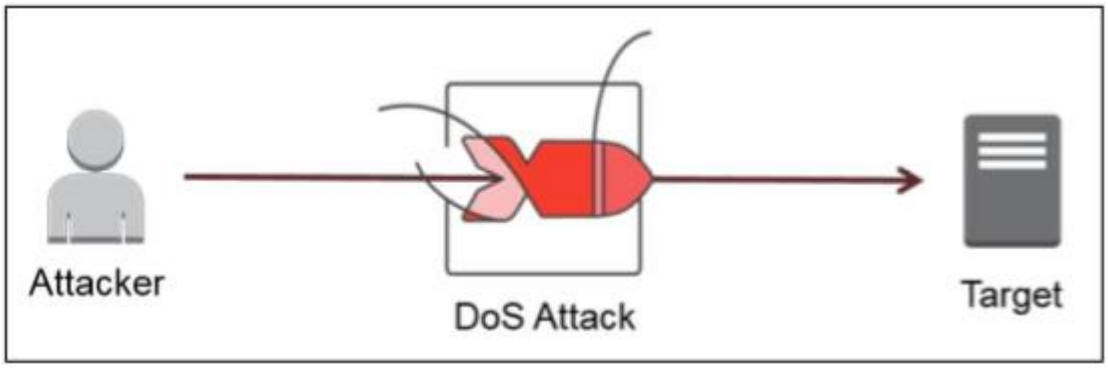
- Scripts o códigos maliciosos: cuando se navega en cualquier sitio por internet, muchas veces los atacantes han logrado clonar de manera casi idéntica o simplemente en la página original pero alterada por ellos, introducir todo tipo de código que se ejecutará cuando el usuario realice alguna acción específica, será generalmente la más común para que siempre la pueda ejecutar el usuario, sin embargo todo este tipo de amenazas actualmente son prevenidas por el navegador y esto es porque existe casi siempre bloqueos por parte del sistema, sin embargo este te da la libertad de ejecución es decir, a pesar de haberlo bloqueado, de alguna forma puedes quitar ese bloqueo y continuar con la ejecución y muchas veces sin notar que está pasando, ya se habrá ejecutado el código malicioso y pues afectará directamente el equipo o simplemente ya habrá recopilado la información que necesitaba.

- Cross-site scripting: este ataque se ejecuta mediante una secuencia detallada por el atacante que atacará mediante el navegador web de la víctima. Este es de los ataques más frecuentes porque este tipo se ejecuta cuando el usuario visita un sitio web malicioso o simplemente cuando el usuario realiza algún clic en un enlace y dicho enlace está considerado como malicioso. Este ataque es muy peligroso debido a que las consecuencias que pueden surgir mediante el mismo es permitir el acceso a las cookies o archivos temporales que el usuario ha

intercambiado con los sitios que ha visitado, realizar capturas de pantalla y también puede tener control de la víctima o acceder a la red en la que se encuentra el ordenador, y siendo esto muy perjudicial porque al tener acceso al computador, puede ejecutar las acciones que desee y en cualquier momento.

- Denegación de servicio (Denial-of-service): este ataque es conocido generalmente como ataque DoS, este realiza acciones generalmente sobre los servidores y consiste en alterar el funcionamiento de los mismos, mediante el gasto innecesario de los recursos, y dicho gasto incensario es el responsable que dichos servidores queden inaccesibles por los usuarios. Este tipo de ataques es utilizado muchas veces cuando los atacantes quieren bloquear algún servicio en línea o páginas a las cuales se tenga mucha concurrencia de usuarios, y de esta forma evitar que dicha concurrencia pueda tener acceso al mismo, teniendo como problemas las famosas caídas de los servidores o caídas del sistema como se conoce generalmente en la actualidad.

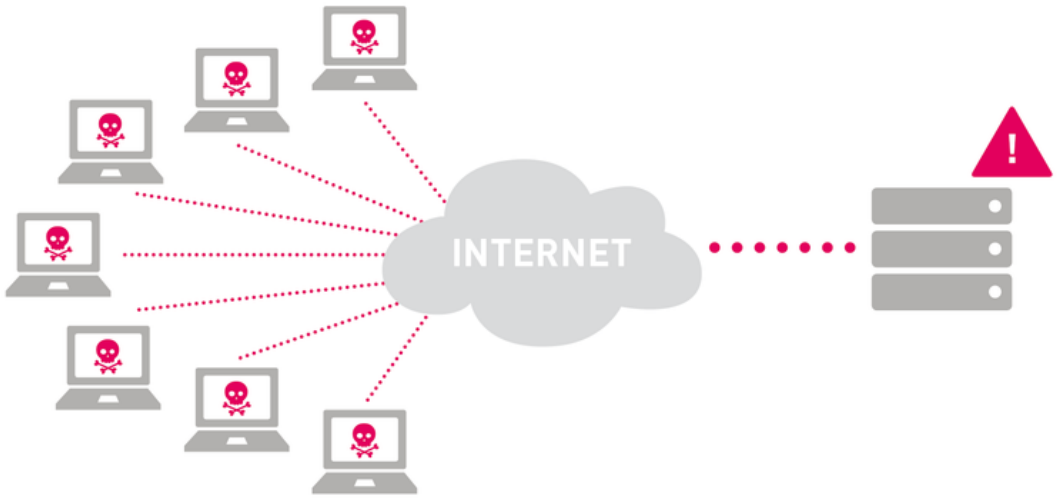
Figura 4. **Diagrama DoS (denegación de servicio)**



Fuente: *File: DoS-atack.png*. https://commons.wikimedia.org/wiki/File:DoS-attack.png. Consulta: marzo de 2019.

- Denegación de servicio distribuido (Distributed denial-of-service): a diferencia del ataque de denegación de servicio, este posee una red de computadoras zombi las cuales se denominan bots, los cuales son computadoras controladas por ellos mismos, siendo estas computadoras esclavos de ellos que han tomado con anterioridad y la finalidad será la misma, la realización del uso innecesario de los recursos de los servidores para que la caída del sistema sea inminente, pero se realiza el ataque desde muchas computadoras en simultaneo, sumando un ataque mucho más eficiente y rápido que el DoS.

Figura 5. **Diagrama DDoS (denegación de servicio distribuido)**



Fuente: Know Your Enemy: *What Happens Behind the Scenes in a DDos Attack*. https://blog.paessler.com/types-of-ddos-attacks. Consulta: marzo de 2019.

- Bomba lógica: este ataque viene dado al momento de que el atacante coloca código malicioso en el código original existente del sistema o programa, y se dispara al momento de realizar la combinación de

acciones correspondientes o al realizar la acción que lo accionara de tal forma que perjudicará al usuario de muchas y diversas formas, las cuales pueden pasar por alto por el usuario, debido a que puede que sean solamente escuchas de la información que maneja el usuario, o simplemente puede robar información al momento de su ejecución.

- Phishing: este ataque ocurre cuando el atacante tiene como objetivo la recopilación de información valiosa para el usuario, siendo estas cuentas bancarias, tarjetas de crédito y todo ese tipo de información. En este caso el phisher o atacante puede violar la confidencialidad del usuario suplantando sitios frecuentados por el usuario haciéndose pasar por el original sistema, mediante correos electrónicos, cualquier tipo de mensajería instantánea, llegando hasta llamadas telefónicas, las cuales siempre tendrán como finalidad suplantar identidad de cualquier empresa o sistema de confianza.

Figura 6. **Objetivos de phishing**

Fuente: *Comalis, GROUP MAGIC ONLINE*. https://www.comalis.com/blog/5-tipos-de-phising-que-puedes-evitar/phishing-illustration-vector/. Consulta: marzo de 2019.

El phishing se muestra como ese ataque que inicia mediante enlaces distribuidos por correo electrónico, redes sociales, interacción con el teléfono móvil y puede también ser mediante una infección de algún software malintencionado o malware, y que tiene como objetivo el robo de datos personales tales como correo electrónico, número de documentos de identificación, y datos de localización; también busca el robo de información financiera del usuario como los números de tarjetas de crédito y/o débito, también las cuentas bancarias del usuario; y en cuanto a lo social, pretende el robo de las credenciales de acceso de las redes sociales del o los usuarios que utilicen dicho ordenador.

- Interception (Passive wiretapping): en este tipo de ataque existirá una persona que sea ajena a la red en la que se esté trabajando, este intercepta el tráfico plano o cifrado, y en cuanto a tráfico se refiere a toda la información que se envía y recibe mediante la red, siendo esta mediante cables o redes alámbricas, o inalámbricas, siendo el objetivo capturar usuarios, contraseñas o cualquier tipo de información para su posterior uso por el mismo atacante.

- SQL Injection: esta modalidad de ataque es muy perjudicial para los sistemas si no se toma en cuenta las medidas de seguridad necesarias por parte de los desarrolladores de software, esto permite recabar información probablemente almacenada dentro de un sistema, pertenece a una base de datos, y dicha información puede ser obtenida mediante el SQL injection, este tiene la capacidad de evadir las barreras mínimas de protección del sistema si este no cuenta con las validaciones necesarias al momento del envío y recepción de la información.

- Caballo de Troya (Trojan Horse): este ataque se produce al momento de tener un programa potencialmente confiable, se ejecuta exclusivamente por el usuario, evadiendo cualquier tipo de barrera de seguridad y el usuario será quien le dé permiso de ejecución y este aparte de cumplir con lo deseado, es decir ejecutar lo que sea requerido por el usuario, podrá llevar alguna tarea oculta con la que puede dañar el equipo.

- Virus: se le conoce o denomina de esta forma al ataque que tiene lugar por alguna intervención del usuario, sin darse cuenta quizá por algún correo electrónico recibido, con algún enlace o programa de dudosa procedencia que se ejecuta mediante el usuario, es decir este lo acciona, quizá sin darse cuenta, pero este es muy grave pudiendo causar pérdida de información directa del disco duro causando graves consecuencias para el usuario.

- Worm (gusano): este ataque es igual al virus que se ha mencionado y cumple las mismas modalidades de ataque, sin embargo este no necesita ser activado por el usuario para poder ejecutarse y propagarse, este tiene la habilidad de propagarse mediante la red, es decir basta con que algún equipo conectado a la red tenga el problema, para que el resto de computadores estén propensos a adquirir este virus y sin darse cuenta.

Figura 7. **Principales objetivos de los ataques**

Fuente: *CYBERTRAINING 365 BLOG.* http://blog.cybertraining365.com/2017/03/24/big-cyber-threats-breakdown-types-cyber-attacks/. Consulta: marzo de 2019.

Los objetivos de los ataques están gráficamente representados por dinero, rompimiento de la seguridad, robo de información, violación de los sistemas de seguridad, debido a que el objetivo de la mayoría viene dado que todo atacante busca mediante su amenaza el robo de información como cuentas bancarias, tarjetas de crédito y/o débito, secuestro de información para después solicitar dinero a cambio de la misma, o robo de información que genera grandes pérdidas de dinero.

2. DAÑOS Y CONSECUENCIAS POSTERIORES A UN ATAQUE

2.1. Daños y consecuencias sobre los sistemas

Posterior a que el atacante logre su objetivo, y este haya sido de sustracción de información, borrado de la misma, y en muchos casos el secuestro de información, se tiene muchos problemas. Si una persona o usuario final fue víctima de un ataque los daños vienen directamente al equipo en el que trabaja, es decir para esa persona será lo más lamentable, sin embargo esto incurre a una perdida mínima si se compara con el ataque exitoso llevado a cabo a una empresa o sistema grande, para ellos puede incurrir en un costo elevado tanto para corrección de dichos problemas, tanto como la magnitud de daños que haya causado siendo estos de perdida de información o robo de la misma.

Los daños que incurren sobre los sistemas son diversos en los cuales siempre la magnitud puede ser muy grande, debido a que no se sabe el valor potencial que pueda tener lo que haya sido sustraído, borrado o secuestrado.

2.1.1. Robo de información

Cuando una empresa logra contabilizar que todo el daño realizado a ellos mediante un ataque es relacionado a información, repercute en el flujo primordial de la misma, debido a que la información que ellos poseen se vio alterada, y esto puede implicar un daño que sea irreparable, es decir que quizá se tenga que volver a realizar todo lo necesario para poder establecer la misma

a un punto seguro, se podría decir que este daño puede ya no solamente contabilizarse en el robo de dicha información porque esto recae a lo monetario, debido a que para ellos implicaría un gasto potencialmente elevado para reestablecerse o simplemente para reponerse de dicho ataque.

Sin embargo posterior a ese robo de la información se esperaría que dicho robo haya sido únicamente con información poco sensible, si posee cuentas de usuario, credenciales de cualquier índole, cuentas bancarias, pues ya se tiene un problema mayor, debido a que las personas que utilizan dicho sistema, estarían poniendo en duda la confiabilidad de uso de dicho sistema, por ese tipo de ataque puede tener un problema aún mayor que la pérdida de la información y puede recaer directamente al cierre de la misma, no logrando reestablecerse como tal, simplemente habrá perdido el sentido planteado inicialmente.

Sin embargo si dicha información no fue sensible, es decir que la información sustraída por el atacante no genera mayor problema, pues recae a una prevención para protegerse de una mejor manera, debido a que en posteriores ocasiones deberá tener las medidas de seguridad que permitan que no vuelva a ocurrir un suceso como el que ha ocurrido, y así seguir con el flujo normal, pero a todo esto implica quizá una inversión monetaria para lograr la seguridad en sus sistemas.

2.1.2. Secuestro de información

Cuando ha ocurrido un secuestro de información, el problema es que simplemente las personas deberán realizar una acción que implica en su gran mayoría un pago para la liberación de la misma, asumiendo que el atacante podrá devolver la información. Este tipo de secuestros se ven muchas veces cuando los ataques han logrado situarse en el sistema operativo en el que se

encuentra alojado el sistema, o simplemente en el computador de uso personal del usuario, este sistema no tendrá información legible nuevamente a menos que se pague dicho rescate de la misma, tomando en cuenta como se mencionó anteriormente que no garantiza en lo absoluto que dicho atacante permita la recuperación de la misma.

Muchos optan por el reinicio completo de los sistemas, trabajando duro para ver que pueden rescatar y que pueden descartar, y así volver a utilizar con confianza dicho equipo, tendrían que tomar las medidas necesarias, y muchas veces para la mayoría implicaría dicho reinicio del sistema, dejando el sistema a un estado de fábrica y a su vez implicaría nuevamente un factor económico molesto para el usuario o empresa, será un gasto que no se tenía contemplado.

2.1.3. Pérdida de información

Generalmente habrá ataques que logren un objetivo mayor, y sería tener control pleno de los dispositivos o equipos que tengan el sistema, esto implicaría que muchas veces los sistemas quedan completamente inutilizables, y esto es aún más grave, debido a que dicha información quizá nunca se pueda volver a recuperar y el sistema es el encargado de tener todo almacenado en el mismo, sin embargo puede quedar este con problemas serios.

Los problemas posteriores a la pérdida de la información, recaen a que se requerirá una acción inmediata debido a que prácticamente el sistema habrá quedado sin mayor funcionalidad, y esto muchas veces ocurre cuando los atacantes han tomado como computadoras zombis o bots, los cuales al ya no ser utilizados por ellos, puede proceden a la destrucción del sistema.

Los atacantes siempre que hayan violado las vulnerabilidades y hayan logrado su objetivo, el ataque, pues si consideran que ya no es necesario dicho computador, o sistema, simplemente pueden optar por retirarse sin dejar secuelas en cuanto al manejo del sistema, pero en otras ocasiones las secuelas, pueden grandes.

Cuando una pérdida de información se ha concretado con éxito, puede ser parte de dicho robo, y si esa información que perdió es parte del sistema para su óptimo funcionamiento, podrá quedar inutilizable el mismo, sin embargo si la información almacenada fue la única pérdida, podrá asegurarse que se tendrá problemas, pero el sistema pude funcionar aún, debido a que los archivos perdidos no son vitales para el funcionamiento óptimo del sistema.

2.2. Daños y consecuencias sobre los equipos o dispositivos

Posterior a un ataque muchas veces cuando se encontrarán problemas en los equipos, cabe mencionar que no siempre serán un daño de hardware, muchas veces recae todo sobre el software o la información, sin embargo las secuelas pueden alterar el funcionamiento y comportamiento del hardware, que en términos comunes es todo lo que se puede tocar físicamente.

Los daños principalmente vienen afectando los módulos de memoria o memoria RAM (los cuales no directamente van a dañar este dispositivo), daños sobre los discos duros, daño sobre los procesadores.

2.2.1. Problemas sobre la memoria RAM

Cuando los ataques se vieron directamente a la sobrecarga de los sistemas, acelerando los procesos logrando las caídas de los servidores, o

servicios, habrá en su momento logrado la acortar la vida útil de la memoria, y esto se refiere a que la memoria no se va a arruinar directamente con un ataque, sin embargo puede que el daño del ataque vaya contribuyendo a los futuros desperfectos de la memoria.

Todo eso es relativo al uso, debido a que un dispositivo como la memoria RAM, es poco probable que se arruine con los ataques sin embargo puede que pase, no está completamente libre de estos ataques, pero como se mencionó anteriormente, lo que se podrá lograr muchas veces es simplemente acortar la vida útil del mismo, pero los fabricantes actuales de estos módulos de memoria siempre andan innovando para evitar este tipo de problemas y muchas veces tiene mecanismos de defensa para evitar ese tipo de situaciones.

2.2.2. Problemas sobre los discos duros

Este dispositivo es el encargado de almacenar toda la información dentro de un computador o servidor, y posterior a un ataque la fragmentación del mismo puede ser el principal problema.

Cuando se menciona el termino fragmentación, cuando una unidad de almacenamiento o disco duro tiende a segmentar lo que se almacene en el de una forma no lineal, es decir un archivo puede no guardarse en un solo lado, y eso implica que porciones estén almacenadas junto a otras del mismo archivo, pero puede que otras partes no estén ni cerca (se habla de cerca, debido a que el disco duro se divide por segmentos los cuales están divididos físicamente para almacenar la información en partes diferentes), entonces el problema viene a que cuando un disco se está fragmentando la información será más y más partida de tal forma que siempre tendrá que tardarse más y más (conforme la fragmentación tenga lugar) para leer porque deberá ir a varios segmentos del

disco para leer un archivo, mientras que si la fragmentación fuese mínima, el problema no sería tan grave como parece.

El problema a simple vista se desconoce para las personas, debido a que a la mente siempre vendrá que la computadora se está volviendo lenta y pues esto muchas veces es debido a la fragmentación del mismo. Es por ello que van quedando sectores sin utilizar dentro del disco y esos sectores pasarán a ser inutilizables, pero al momento de lectura el disco duro pasará por ellos para encontrar lo que se necesite, entonces la lentitud se nota por estos factores.

2.2.3. Problemas sobre los procesadores

Anteriormente los procesadores podrían sobrecargarse al momento de ejecutar las acciones, y ocurría porque el procesador es el cerebro del computador, y es mediante el procesador que pasan todas las tareas, realiza operaciones aritméticas y lógicas y junto a los módulos de memoria RAM, logran ejecutar los procesos solicitados por el usuario.

Cuando un ataque acelera drásticamente los procesos dentro de un sistema, es decir que el atacante va a sobrecargar el sistema, todo ese recargo adicional al convencional viene afectando el procesador, y pues este en su momento poco probable, pero cabe la posibilidad, que pueda presentar fallas debido a que siempre ha estado sobre cargado, y esto es raro o poco común debido a que los procesadores están actualmente con las características de protegerse ante este tipo de eventualidades, debido a que ellos mismos tienen sus mecanismos de defensa, que van desde el rebotar todo tipo de procesos apagando el equipo para evitar los datos anteriormente mencionados, sin embargo estos cambios bruscos pueden dañar el procesador o ir dañándolo sin

que el usuario se dé cuenta del problema que se está suscitando internamente en el computador o servidor.

Es por eso que un ataque puede afectar este dispositivo, como se menciona no dañándolo directamente pero pudiendo al igual que los módulos de memoria RAM reduciendo su vida útil.

3. HECHOS HISTÓRICOS DE ATAQUES

3.1. Ataques concretados, consecuencias y pérdidas

Históricamente ha existido infinidad de ataques mediante sistemas, virus u ordenadores, los cuales han sido principalmente con la finalidad de obtener recursos monetarios o aprovecharse de cualquier tipo de información que puedan obtener con dicho ataque.

Las personas o empresas, siempre están tratando de lidiar con este tipo de situaciones, sin embargo los atacantes nunca están descansando debido a que siempre buscan la forma a toda costa de vulnerar los sistemas para poder obtener el beneficio anteriormente mencionado. Muchas veces las personas o empresas ignoran que están siendo víctimas hasta que sufren daños severos o simplemente se dan cuenta que en algo anda mal en algún momento debido a que el comportamiento o flujo principal a los que están regidos se ve alterado, o está funcionando de forma poco habitual o con ligeros cambios, sin haberse realizado dichos cambios por ellos.

En la actualidad las personas o empresas logran tener un mayor índice de seguridad, debido a que las mismas, toman las medidas necesarias para satisfacer todo tipo de demandas tomando en cuenta que las realizarán con las mejores prácticas y mejor manejo de la información; por ende se ha logrado establecer que a lo largo de todo este tiempo desde que ha existido el internet y los ataques, hasta la actualidad, han surgido muchos ataques, pero son pocos los que han logrado sonar a nivel mundial, los cuales provocaron en su

momento perdidas millonarias, sin embargo, algunas empresas lograron detener los ataques a tiempo, el resto no.

3.1.1. Morris

Uno de los ataques que se registró históricamente fue en el año 1988 logró infectar a una gran cantidad de computadoras, existían un aproximado de 60 000 ordenadores en todo el mundo, los cuales tenían conexión a internet, sin embargo dicho virus conocido como gusano, logró infectar a un aproximado del 10% de esa cantidad anteriormente citada. Para esta cantidad de ordenadores infectados y para la fecha en la que se registró, logró contabilizar en pérdidas una cantidad de 96 millones de dólares, que era una cantidad demasiado grande para la época en la que se presentaba.

Cabe mencionar que el gusano o virus Morris, marcaría el inicio de una serie de posteriores ataques los cuales serían igual o peor de devastadores, de tal forma que esos ataques siempre tienen un fin en común, devastar los ordenadores para provocar daños irreversibles y económicos.

3.1.2. ILOVEYOU

Este ataque fue uno de los peores ataques que se registró, debido a que este virus era el responsable de replicarse y lograr sobrescribir los ficheros que tenían las extensiones de .VBS, y .VBE, podía eliminar los ficheros con extensiones .JS, .JSE, .CSS, .WSG, .SCT y HTA, creando otro archivo idéntico con el mismo nombre pero con extensión .VBS, también lograba eliminar los archivos con extensión .JPG, .JPEG, .MP3 y MP2.

Dicho virus logró propagarse demasiado rápido mediante el correo electrónico, este se distribuía por los correos electrónicos y dichos correos eran enviados a sus víctimas y ellos lo replicaban a su lista de contactos. Así era como lograba colarse por millones de personas, y este virus logró infectar un aproximado de 50 millones de ordenadores los cuales ascenderían a una cantidad aproximada de 5 500 millones de dólares en pérdidas.

3.1.3. Code Red

Code Red es otro de los ataques más devastadores, dicho virus, era catalogado en la categoría de gusano, fue descubierto en el año 2001, lograba acceder mediante la vulnerabilidad conocida como desbordamiento de buffer, o sobrecarga, dicho proceso consiste en enviar muchas solicitudes al servidor hasta lograr el desborde del mismo y provocar que el mismo colapse, sufriendo así una conocida como caída del sistema, las cuales a gran escala, pueden incurrir en pérdidas millonarias, y este caso no fue la excepción, dicho virus consiguió infectar un aproximado de 225 000 sistemas alrededor del mundo, incluyendo los servidores web de la Casa Blanca de los Estados Unidos, mediante un ataque DDoS, y logrando alcanzar la cifra catalogada como pérdida en unos 1 200 millones de dólares.

3.1.4. Conficker

En el año 2008 logró escabullirse en la historia de los ataques cibernéticos conocido como conficker, era catalogado como un gusano. Dicho malware lograba explotar la vulnerabilidad que yacía en el servicio Windows Server en los sistemas operativos Windows 2000, Windows XP, Windows Vista, Windows Server 2003 y Windows Server 2008.

El gusano se propagaba a sí mismo mediante el desbordamiento de buffer del servicio de Windows Server, logrando colarse en el ordenador víctima, posteriormente a ser infectado el ordenador desactivaba varios servicios tales como, Windows Automatic Update, Windows Security Center, Windows Defender y Windows Error Reporting, los cuales se puede notar, que son los servicios de seguridad suministrados por Windows.

Mediante los ataques según reportes citados en ese tiempo que duró ese virus antes de volverse perceptible por antivirus y prevenido por los sistemas, logró infectar aproximadamente a unos 15 millones de ordenadores ascendiendo a una perdida aproximada en 9,100 millones de dólares.

3.1.5. Zeus

En el año 2011 aproximadamente en septiembre dio inicio su desarrollo, catalogado también como otro de los ataques más peligrosos de la historia. Esta ocasión el protagonista fue llamado Zeus, era un malware que lograba propagarse mediante las campañas de pishing. Posteriormente a infectar un ordenador el malware era capaz de interceptar todo tipo de transacciones bancarias de la víctima y poder copias todo tipo de credenciales para poder iniciar sesión suplantándose como el usuario original.

Teniendo como base ZeuS nació una botnet llamada GameOver Zeous, dicha botnet tenía como característica distinta, porque utilizaba el tipo de comunicación P2P para controlar de forma remota los ordenadores zombi, los cuales principalmente eran con sistema operativo Windows, desde Windows XP, Windows Vista, Windows 7 y Windows 8.

Los expertos estiman que la botnet GameOver Zeus estaba compuesta por un aproximado de 500 000 y 1 millón de equipos zombi las cuales lograron generar una pérdida de aproximadamente 100 millones de dólares en pérdidas.

3.1.6. Carbanak

Esta amenaza es una campaña de tipo APT (Advanced Persistent threat o en español amenaza persistente avanzada), estaba dirigida a instituciones financieras.

El origen o inicio del ataque sucedía cuando los encargados o criminales cibernéticos lograban infiltrarse a la red interna del banco, algo que conseguían mediante campañas de correo electrónico los cuales eran fraudulentos y de esa forma lograban tomar el control del equipo y poder tener una puerta de acceso a dicha entidad financiera.

Generalmente estando dentro de dicha institución financiera utilizaban todo tipo de estrategias las cuales eran utilizadas para lograr crear todo tipo cuentas las cuales simplemente eran destinadas para los atacantes y lograr sustraer grandes cantidades de dinero.

Este malware era capaz de que los criminales sustrajeran todo el dinero que pudieran, y se estima que lograron extraer una cantidad aproximada de 1,000 millones de dólares a más de 100 instituciones financieras en unos 40 países distintos.

La policía logró establecer de donde provenían los ataques y así pudieron detener al líder de este grupo que había logrado sustraer bastante dinero, sin embargo el ataque ya se había consumado y las pérdidas eran muy altas.

3.1.7. WannaCry

Este ransonware es uno de los peores ataques de los que se tiene precedentes a lo largo de la historia, debido a que las pérdidas fueron demasiadas y este mismo logró marcar un antes y después de la ciberseguridad que actualmente se conoce.

Logró detener a muchas empresas a nivel mundial para dar a conocer que las vulnerabilidades eran demasiadas y se podían aprovechar de las mismas.

Lo que lograba el atacante era secuestrar un ordenador y el atacante encriptaba todos los archivos y bloqueaba el acceso del administrador y de los otros usuarios, siendo esto algo grave, debido a que sin acceso al computador o sistema, era simplemente imposible trabajar en él, la única forma de lograr obtener acceso nuevamente al mismo era pagando un rescate; dicho rescate era un aproximado de 276 euro, y tomando en cuenta que logró infectar a más de 360 000 equipos en alrededor de 180 países, se estimó 200 millones de euros en pérdidas, solamente por WannaCry, y esto que son únicamente los pagos de rescate, sin tomar en cuenta las pérdidas que pudieron ser indirectas y los problemas posteriores para evitar posteriores ataques.

3.1.8. PlayStation Network

Fue en el año 2011 donde Sony dio a conocer que sus sistemas habían sido vulnerados, de tal forma que varios servicios y funciones habían sido derribados. Dicho sistema se vio afectado por un transcurso aproximado de un mes, afecto a un aproximado de 77 millones de personas quienes no podían acceder a sus cuentas por este mismo ataque.

Sony se vio obligado a asumir las consecuencias que dicho ataque implicaba, de tal forma que aproximadamente tuvieron una pérdida de 137 millones de dólares debido a que sus sistemas fueron dados de baja durante ese ataque, por eso es que se considera uno de los mayores ataques en la historia.

3.2. Ataques corregidos a tiempo y sus consecuencias

A pesar de que la gran mayoría de ataques lograron su objetivo, robar información o dinero, en varias ocasiones, algunas empresas lograron a tiempo verificar dichos ataques y no los pudieron prevenir definitivamente, pero lograron detener dicho ataque sin mayor problema, evitando una catástrofe o todo tipo de situaciones que pudiese perjudicar a la misma.

3.2.1. Google China

Durante el año 2009 la plataforma de Google China, que había sido lanzada pocos años atrás, fue atacada mediante criminales informáticos, los cuales aparentemente habían obtenido diversidad de información de muchas empresas, pero posterior a todo esto el mismo Google China, dio un comunicado informando que todo eso era falso, debido a que lograron constatar que lo único que lograron obtener los atacantes fue simplemente una parcialidad de dos cuentas de correo electrónico de Gmail.

Los ataques provenían del explorador Internet Explorer, y muchos gobiernos recomendaron omitir ese tipo de navegadores, debido a su poca seguridad, y así garantizar una mayor protección al navegar por internet, sin embargo por todo lo acontecido, se considera como ataque, pero también como algo que fue fallido, y no logró su objetivo final que era genera grandes pérdidas

hablando de dinero, y robo de información, les daba mucha ventaja sobre la empresa y permitiendo así a los atacantes obtener aún más ganancias de eso mismo.

3.2.2. Evernote

Se estima que tuvo un alcance de unos 50 millos de usuarios, los cuales hubiesen sido vulnerados mediante el robo de su información, sin embargo esa cifra es la que se estimó, pero debido a que muchas veces las empresas intentan ocultar dicha información para no parecer vulnerables o poco confiables por las personas que intentan adquirir sus productos o servicios, y fue por ende que dicha empresa al detectar algún tipo de anomalías decidieron enviar un correo electrónico a sus usuarios haciéndoles ver que hubo un posible fallo de seguridad que dejaba expuesta su información ante personas que no harían buen uso de la misma, he ahí donde en base a eso se estimó el número de usuarios afectados, sin embargo, con esa medida del restablecimiento de las contraseñas, se pudo evitar una pérdida millonaria por ese ataque, y solo quedo catalogado como un intento de ataque masivo a Evernote.

3.3. Ataques cibernéticos en Guatemala y Latinoamérica

Estudios realizados por Karpersky Lab, que es una empresa dedicada a la seguridad informática, posee un software antivirus denominado de la misma forma, se logró constatar que Guatemala, posee un lugar poco privilegiado en cuanto a seguridad informática, debido a que está en el cuarto lugar de los países más propensos a ser atacados mediante ciberataques.

Eso quiere decir que Guatemala no cuenta con la suficiente fuente de información o simplemente no se da cuenta de las amenazas que existen actualmente en el mundo del internet.

Brasil encabeza el lista de países más propensos a ataques cibernéticos con un 30% de usuarios que han sido víctimas de ataques, seguido de Honduras con un 23,5% de usuarios, después de este país está Panamá con un 22,6% y Guatemala con un 21,6%.

Los principales ataques cibernéticos que han sido detectados en Guatemala no han sido nada nuevos, esto se debe que generalmente todos los ataques que han ocurrido a nivel mundial, también en Guatemala han logrado su objetivo.

Los ataques a usuarios en internet, que tienen como objetivo Latinoamérica tienen su origen de diferentes lugares y formas las cuales no implica la utilización de internet, generalmente logran propagarse por dispositivos volátiles o USB, en las que si implica relación con internet se contabilizó que un 85% de los ataques se logra mediante sitios web y el otro 15% restante logra el ataque mediante correos electrónicos.

Las modalidades favoritas de los atacantes es generar publicidad o alterar con contenido no relacionado con la página con la finalidad de enviar a otro sitio al usuario, y dicho sitio web poseerá contenido malicioso.

Los usuarios generalmente dudan en pagar las licencias necesarias para el funcionamiento correcto de los programas que necesita, y por ende descarga programas alterados o descarga los genuinos pero los altera mediante la utilización de los denominados parches de terceros, los cuales alteran el

funcionamiento correcto del software para que engañe al sistema y parezca genuino, sin embargo no lo es, y puede generar daño en un futuro y quizá no se tenga conocimiento de que paso.

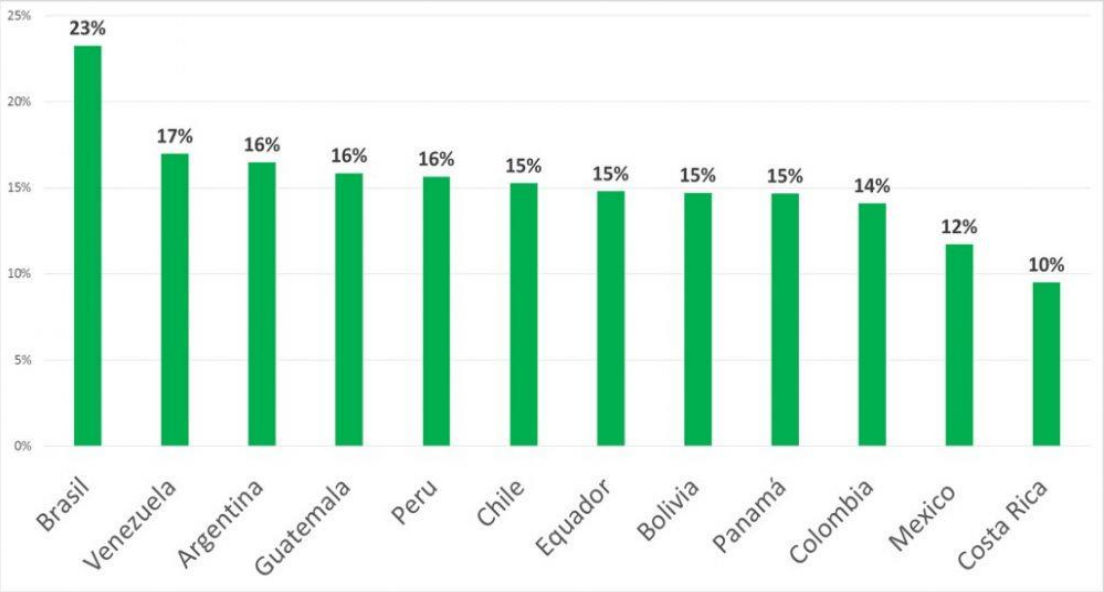
En la actualidad el ataque que ha cobrado un mayor número de víctimas ha sido el phishing debido a que la generación de los teléfonos móviles es la actual, se ha propagado mediante el uso de los mismos, esto es porque en los teléfonos móviles se cuenta con redes sociales o sistemas de mensajería instantánea, que llega de manera muy rápida a los usuarios que se desee, y se ha aprovechado esa rapidez para propagarse por toda la red.

Dichos ataques generalmente se ven más propagados en días específicos, esto quiere decir que en un día común siempre existirán pero en días especiales se aumenta el número debido a que dichos días tienen algo en particular y es que las personas puedan hacer uso de su información generalmente bancaria para adquirir algún producto o servicio. Esto se vio reflejado cuando llega el llamado Viernes Negro, o Black Friday en inglés, las personas se ven atraídas por los precios más bajos del año en la mayoría de comercios y en los cuales se podrá adquirir dichos productos o servicios solamente durante ese día, entonces es un día propicio para los atacantes lograr el objetivo y sería el robo de la información necesaria para poder obtener información o dinero de las personas que ingenuamente no tomaron las precauciones necesarias.

Estadísticamente las empresas encargadas de la creación de software para la protección informática, han constatado que existe un ataque aproximadamente cada 33 segundos, esto quiere decir que en un minuto al menos una persona ha sido atacada y otra está siendo víctima del ataque.

- Phishing: el ataque cibernético denominado phishing tiene sus objetivos principales y es el robo de información mediante la propagación de algún enlace por el que acceden las personas y de esa forma logran su acometido.

Figura 8. **Phishing en Latinoamérica 2018**



Fuente: *Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina.* https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-ataques-ciberneticos-en-america-latina/13266/. Consulta: marzo de 2019.

La gráfica muestra de mayor a menor los países que fueron más afectados por phishing, mostrando el porcentaje de usuarios afectados por país. Siendo el phishing el ataque más utilizado, debido a que este se propaga como si fuese algo que normal o no implica algún tipo de riesgo, sin embargo termina con el robo de todo tipo de información, y este robo no solo implica datos personales del usuario, también su información bancaria. Se puede observar que Guatemala ha sido uno de los países más afectados por phishing.

- Ransomware: este ataque una vez concretado no podrá existir marcha atrás a menos que se pague el llamado rescate; dicho pago debe realizarse en criptomonedas o su equivalente a dinero real, para que el atacante aplique la liberación del computador y se pueda recuperar toda la información y el sistema.

Figura 9. **Ransomware en Latinoamérica 2018**

Fuente: *welivesecutiry*. https://www.welivesecurity.com/la-es/2019/01/04/paises-mas-afectados-ransomware-latinoamerica-durante-2018/. Consulta: marzo de 2019.

La anterior gráfica muestra el porcentaje en cada país de ataques mediante ransomware los cuales afectaron con el secuestro del computador, a los que las personas debieron pagar un rescate o simplemente repararla, mediante un reinicio a estado de fábrica del computador, perdiendo toda la

información que se tenía. Gráficamente se logra apreciar que Guatemala no ha sido víctima muy constante de ransomware, sin embargo otros ataques han afectado directamente al país.

3.3.1. América Latina y los ataques cibernéticos

Muchas amenazas afectan todo el mundo desde que son creadas, sin embargo en Latino América, todo se ve más propenso debido a que hay varias situaciones que afectan directamente a todo el continente, las cuales vienen desde la poca inversión en la seguridad por parte de las empresas para la protección de sus datos, también el uso de sistemas sin estar actualizados o que han sido alterados mediante activadores, los cuales dejan expuesto el sistema, y por ende, la seguridad del sistema.

Las empresas muchas veces ignoran todo tipo de amenazas que puedan estar presentes en el mundo virtual, sin embargo son conscientes del daño que conlleva la pérdida de su información, sin embargo muchos parece que deciden tomar el riesgo por ahorrarse una cantidad de dinero que pueden utilizar para invertir en su empresa pero ignorando invertir en la seguridad de la misma, y lamentablemente cuando llega el momento de un ataque en el que se logra tener con exactitud las cifras económicas que han logrado catalogarse como perdidas por dicho ataque, se podrán dar cuenta que siempre será más barata la prevención que la corrección, sin embargo en América Latina, no se piensa de esa forma, porque aunque se sepa que la prevención es mejor, la mayoría termina siendo afectada por esos problemas.

Una de las empresas dedicadas a la seguridad informática es denominada Kaspersky Lab, tiene la ardua tarea de estar constantemente monitoreando todo tipo de amenazas a nivel mundial, mediante su catálogo de software, que

van desde antivirus, antimalware y otro tipo de sistemas de seguridad que ayudan a proteger los equipos informáticos, que son diversos, siendo desde dispositivos móviles, computadores y todo tipo de dispositivos con acceso a internet e incluso sin acceso a internet. Kaspersky se encarga de que su software siempre este capturando toda actividad maliciosa ya sea por error humano o por el flujo habitual de internet, para poder ayudar a los usuarios ante todo ese tipo de amenazas.

Kaspersky se ha dedicado a realizar diversidad de estudios, los cuales han descubierto cosas totalmente abrumadoras de las que quizá nadie se da cuenta, para el año 2018 ha existido un aumento del 60% de los ataques a equipos ubicados en América Latina, siendo esto una cantidad escandalosa en cuanto a seguridad informática se refiere, y contabilizar esa cantidad en número de ataques, lograron magnificar que la cantidad de ataques cibernéticos era aproximadamente de 9 ataques por segundo.

La mayoría de los ciberataques ocurren cuando los usuarios están utilizando internet, debido a que todo el tráfico de datos (intercambio de información), que ocurre, puede implicar contener información que sea maliciosa para el sistema donde se esté trabajando, sin embargo no implica que aún sin tener internet no se esté expuesto, debido a que mediante el uso de dispositivos volátiles o cualquier otro dispositivo que pueda estar infectado, podrá afectar directamente el equipo y aunque este nunca se haya conectado a internet.

Lo habitual es escuchar que las empresas son víctimas de ataques cibernéticos, pero se escucha pocas veces que las personas particulares o usuarios son víctimas de dichos ataques, debido a que generalmente las personas no estiman las pérdidas que les puede conllevar el haber sido

víctimas de los ataques, es por ello que se cuándo se habla de ataques cibernéticos siempre tendrá relación a una gran empresa de tecnología. Los estudios han revelado que las personas son las más afectadas por ataques que las propias empresas, debido a que las empresas siempre tratarán de protegerse aunque para ellos sea una simple restricción de sitios, es decir que los usuarios tendrán prohibido ingresar a ciertos sitios, será una pequeña medida de seguridad aunque puede ayudar un poco más a fortalecer la seguridad, sin embargo los usuarios normales por curiosidad o simplemente por ignorancia, fácilmente son víctimas de estos ataques debido a la falta de conocimientos mínimos de cómo protegerse para poder evitar este tipo de ataques en internet.

3.3.2. Medidas adoptadas por Latinoamérica para la seguridad informática

En países desarrollados a nivel mundial han optado por prácticas de seguridad en todo sentido, desde la prevención hasta la corrección, debido a que en esos países si se tiene conocimiento amplio de que la información de las personas es valiosa y por ende han empleado esfuerzos para mejorar la seguridad, tal es el caso de los países de Rusia y China, quienes han creado programas para mejorar la seguridad informática y también han creado leyes que permiten catalogar como delitos los ciberataques.

Sin embargo basándose en la mayoría de las estadísticas de los ataques detectados en América Latina, muchos países de este continente también han optado por medidas preventivas de seguridad y también correctivas, sin embargo siempre será mejor prevenir que corregir. Así es como México, Chile y Brasil sufrieron ataques a entidades bancarias, que les generaría pérdidas millonarias a esos países, debido al dinero que sustrajeron los atacantes y el

daño ocasionado en cuanto a la violación de la privacidad. Partiendo de que esos países fueron atacados, iniciaron a tomar medidas de seguridad las cuales ayudarían a evitar estos ataques cibernéticos, los cuales ya le habían hecho daño a la economía de dichos países.

Así fue como México opto por tomar medidas que fuesen directamente enfocadas a la economía del país e innovación para poder estar seguros de una mejor manera, Chile lo hizo de una forma diferente, ese país opto por ir directamente a mejorar la infraestructura y crear una cultura de ciberseguridad, también promover la industria de ciberseguridad para de esta forma tener una mejor barrera ante cualquier tipo de ataques que pudiesen afectar la economía del país. Argentina opto también por crear una forma de protegerse y fue de una forma similar a Chile y México, debido a que crearon un programa denominado Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad.

Cada país del mundo debe tomar medidas para ayudar a la seguridad cibernética, sin embargo, en América Latina hay muchos países que dejan en segundo plano este tipo de prioridades debido a que la cultura no ha sido modificada de tal forma que se entienda que esto perjudica a la economía total de cada país al ser víctimas de los ataques cibernéticos, por ello es que velar por la seguridad de la información es una cultura que debe ser parte vital en todos los países y no dejarla pasar por alto, para que América Latina no sea un blanco fácil para los atacantes en cuanto a ciberataques.

3.4. Implicaciones legales relacionadas a ataques cibernéticos

Internet se ha vuelto parte fundamental en la vida de las personas actualmente, sin embargo este crecimiento exponencial ha traído a su vez, una

serie de acciones mal intencionadas, y dichas acciones tendrán diversas finalidades pero todo ocurre mediante el uso de sistemas informáticos.

Las personas que se ven afectadas por ataques cibernéticos, pudieron ser atacados sin darse cuenta, o están siendo víctimas de dichos ataques y podrán tener pérdidas, sin embargo puede considerarse casi imperceptible, actualmente muchas personas utilizan sistemas sin licencia, esto quiere decir que no son originales y debido a este tipo de acciones, tienen claro que en cualquier momento podrán deshacerse del sistema e instalar uno nuevo y limpio, pero para una empresa no es tan fácil, debido a que las perdidas pueden catalogarse como catastróficas debido que pueden lograr una caída completa de la misma, o pérdidas millonarias que no se pueden recuperar en la mayoría de casos; y si la pérdida es la información que generalmente es lo que buscan los atacantes, la empresa habrá quedado expuesta.

Los crímenes informáticos actualmente en muchos países ya cuentan con penas de cárcel, sin embargo en muchos más países no tienen penas de cárcel, debido a que no se ha considerado algo de urgencia para los países, pero si lo es, debido a que el daño no es físicamente hacia una persona, pero puede dañar su imagen como persona, o si es una empresa, puede lograr que la empresa pueda perder sus bienes y lograr el cierre definitivo de la misma.

En Guatemala se pueden realizar las denuncias ante el Ministerio Público, si ha sido víctima de un ataque cibernético, pero generalmente los ataques logran realizarse desde fuera del país y los delitos informáticos internos en el país juzgaran a personas que hayan realizado dicho ataque y se encuentren dentro del territorio nacional de Guatemala, pero los ataques acá son de una escala aún física o palpable, debido a que pueda ser destrucción de algún

equipo informático, robo de equipos, pero los ataques como phishing o ransomware generalmente no son denunciados.

El Ministerio Público ha logrado condenar a personas por delitos informáticos, y cuenta con muchas denuncias de dichos delitos, pero en el país los delitos que se han registrado son generalmente derechos de autor, destrucción de registros informáticos, lo cual deja una gran brecha por cubrir y va con pasos demasiado lentos, los cuales no logran abarcar los casos más comunes como ransomware o phishing.

Esto quiere decir que simplemente en otros países como Estados Unidos, España, Rusia, entre otros, si cuentan con un sistema de investigación especializado para dar con el paradero de los criminales, pero en el resto de países donde hay otros problemas más importantes, como la delincuencia, la desnutrición, educación, etc., estos crímenes se podrían catalogar como inexistentes, y es por ello que aún falta mucho para que las personas puedan tener la confianza necesaria para denunciar con mayor confianza haber sido víctimas de los ataques informáticos.

4. METODOS DE PREVENCIÓN Y CORRECCIÓN ANTE LOS ATAQUES

Históricamente las personas siempre reaccionan ante un problema posterior a encontrarse con él, pero son pocas las que previenen dicho problema, y en el caso de la navegación por internet y las medidas de seguridad que se deben tomar para navegar de una forma más segura no son la excepción.

Las personas piensan muchas veces que el contar con software original, o un antivirus será todo lo necesario para poder estar seguros ante las eventualidades que puedan suscitarse al navegar, sin embargo descartan todos los problemas que puedan ser provocados por el mismo usuario, siendo este el problema mayor al momento de navegar.

Los usuarios saben de los riesgos, pero no de la magnitud de los mismos, ellos han escuchado de los fraudes, de los virus, sin embargo hasta que no se encuentren en el punto donde comprueben que todo esto es cierto, muchas veces van a ignorar la forma de prevenir todo eso.

4.1. Software o programas para la seguridad en los equipos

Los programas son herramientas indispensables en los sistemas operativos, los cuales serán los encargados mediante la interacción del usuario con ellos, de la realización de todas las tareas que se lleven a cabo dentro del sistema.

Las computadoras o dispositivos siempre van a depender de los programa, así como los programas dependen del dispositivo, uno sin el otro puede existir sin embargo, no puede funcionar independientemente. Es por ello que la dependencia es vital para la seguridad del mismos, existen demasiadas formas de instalar aplicaciones o programas en un computador, sin embargo existirán aplicaciones que no son completamente compatible con los dispositivos siendo esto una desventaja para garantizar una mayor seguridad del sistema y/o equipo, y esto es porque al no ser completamente compatibles pueden generar las vulnerabilidades y estas mismas pasarán a ser las puertas por las que un atacantes podrá entrar.

Los programas para poder garantizar en gran parte la seguridad del usuario vienen siendo aquellos que permiten al computador o dispositivo tener la menor probabilidad de ser atacado o de tener vulnerabilidades por las cuales el atacante pueda entrar al sistema y concretar dicho ataque.

4.1.1. Antivirus

Los software antivirus o programas antivirus son aquellos que tienen funcionalidades limitadas para proteger el sistema, de esta forma el sistema puede prevenir ciertos ataques o ciertos problemas que puedan surgir, sin embargo, no garantiza la seguridad plena del usuario, debido a que dicho software siempre será un muro que deberán romper los atacantes, pero como se sabe, cualquier barrera puede ser derribada y posterior a ser derribada pues automáticamente pasa a estar nuevamente expuesto, pero el antivirus será un arma fundamental, porque siempre tendrá un paso extra que deberán vencer los atacantes para causar daños al equipo.

Los antivirus han venido trabajando por años sin ningún problema, sin embargo, los atacantes también han venido realizando tareas contrarias, es decir, buscando la manera de violar los códigos de seguridad y atacando los sistemas, esto implica que los antivirus siempre van a estar propensos ante los atacantes debido que ellos mejoran y los atacantes también, los atacantes incluso crean nuevas estrategias las cuales deberán ser descubiertas por los desarrolladores o creadores de los antivirus para poder solucionarlas y para todo ello, el atacante ya habrá logrado muchas veces su objetivo.

Existen diversidad de antivirus tanto para plataformas móviles como para ordenadores y su diversidad de sistemas operativos, sin embargo hay muchos sistemas operativos los cuales son mucho más seguros que otros, y esto debido a que las empresas creadoras de todo este tipo de sistemas, se han dedicado de gran manera a la seguridad el usuario y por ende el costo es mucho más elevado y siendo esto una mayor garantía para el usuario, sin embargo no dejan de tener vulnerabilidades, porque las mismas siempre estarán presentes.

Mientras una investigación exhaustiva se realiza para encontrar las mejores formas de proteger y se llega a encontrar el primer punto y es elegir un antivirus, se tendrá muchas interrogantes las cuales convergen a lo mismo, ¿Qué antivirus se debe elegir? Teniendo esas interrogantes las personas deberán elegir cual antivirus elegir, pues ellos son los que van a adquirir los servicios de alguna empresa que brinde la seguridad mediante el antivirus.

Las principales formas de saber cómo elegir, vienen siempre dadas al precio, las funcionalidades, la capacidad del equipo donde será instalado y el soporte que pueda brindar dicho antivirus.

- El precio: será una de las características más importantes para el usuario al momento de elegir un antivirus, porque si generalmente lo considera relativamente caro, desistirá de su uso o adquisición, aunque muchas veces se aplicará el dicho de *"lo barato sale caro"*, esta situación es la que significa que muchas veces no es necesario irse por lo más barato, o lo más caro, siempre se deberá evaluar cuáles son las funcionalidades que ofrece el antivirus y decidir si son las que se necesita, porque puede ser que otro antivirus se adapte de una mejor forma a lo que necesite el usuario, y el costo sea mucho menor al que quiera adquirir.

- Funcionalidades: las funcionalidades que ofrece un software antivirus, vienen detalladas por cada proveedor, sin embargo es el usuario quien decide cuales le serán de utilidad, como podría decirse que un software antivirus contenga un firewall, siendo este quien controla el tráfico (es decir toda la información que se manda y se recibe mediante la red, incluyendo internet), y verificando al momento posibles amenazas, ficheros (archivos), o situaciones que puedan vulnerar el sistema, o generar un ataque del cual será derivado muchos problemas posteriores, entonces si el usuario considera que no le es necesario, aunque es importante contar con uno, puede optar por adquirir uno o el mismo con un plan diferente, de tal forma que el costo pueda variar, pero como se explicó, las funcionalidades serán diferentes, y todo depende del factor primero, el precio.

- Recursos del sistema: esto involucra todo lo que necesita el software en cuanto a recursos o mejor conocido como memoria RAM, espacio de disco duro, o cualquier otra situación que pueda influir directamente en el funcionamiento del software, estos deberán ser estrictamente cumplidos por lo que recomienda el proveedor del software, debido a que ellos

habrán hecho las pruebas necesarias para determinar las capacidades mínimas, para un óptimo funcionamiento de dicho software.

4.1.2. Antispyware

Este tipo de software está diseñado para detectar y eliminar todo tipo de programas maliciosos que puedan afectar al ordenador. Actualmente la mayoría de los antivirus ya incluye este tipo de software, antes era independiente y debía adquirirse por separado cada uno de ellos, sin embargo ahora generalmente vienen incluidos en el mismo antivirus. La idea de todo esto o de las grandes compañías distribuidoras de software antivirus es reducir a toda costa el número de amenazas y ataques mediante la actualización constante de sus sistemas así como la investigación exhaustiva para determinar las posibles futuras amenazas y así estar un paso adelante, aunque generalmente se previene posterior a que dichas amenazas hayan salido a la luz, es decir es difícil detectarlas antes de que ataquen, después de que ellas ya han concretado ataques, será mucho más fácil prevenir a futuro estas situaciones, sin embargo, en algún momento ya habrá obtenido todo aquello por lo que fueron creadas dichas amenazas.

4.1.3. Error humano

Cuando se habla de mecanismos de prevención de errores o ataques dentro de un ordenador, sistema o red de equipos, cabe mencionar que la mayor fuente de ataques viene dada por fallas en el uso de los mismos de los usuarios finales.

Las personas no consideran las medidas necesarias para trabajar de una manera más segura, simplemente se consideran autosuficientes o expertos en el tema y terminan adquiriendo problemas innecesarios.

La mayoría de los problemas surgen por la mala utilización de un sistema, un computador o navegación en internet. Cuando se habla de mala utilización no simplemente implica realizar algo que aparentemente este malo, debido que en este mundo aunque se realicen cosas que habitualmente se realizan, se puede estar cometiendo algún error que repercuta en el funcionamiento del sistema; tal es el caso de que las personas introducen memorias volátiles o USB, sin analizar y con auto reproducción, de tal forma que sin darse cuenta que realizan una actividad rutinaria y normal, pueden haber desde ese instante haber dañado permanentemente el ordenador o sistema, debido a que generalmente se piensa que todo está bien, sin embargo esas acciones no fueron tomadas en cuenta. Otro claro ejemplo es al momento de navegar por internet, las personas piensan que es simplemente abrir páginas y utilizarlas, sin tomar las precauciones necesarias, tal es el caso de que ignoran los protocolos de seguridad, los certificados de las páginas, entre otros, los cuales son muy importantes, porque un sitio al tener certificados de seguridad, garantiza de gran manera que la información que se intercambie entre dicho sitio y el ordenador, será cifrada, esto quiere decir que no será legible ante cualquier persona; estas garantías siempre deben ser tomadas en cuenta, y de esta forma se sabrá que la navegación será un poco más segura, sin embargo el factor de fallo siempre estará presente.

Otro factor fundamental es no abrir enlaces desde el correo electrónico, debido a que esta modalidad generalmente es utilizada por los atacantes y las personas o usuarios finales siguen cayendo en estas prácticas fraudulentas las

que solo llevan al robo de información así como de cuentas bancarias, redes sociales, y toda información que se pueda tener en línea.

Es por eso que las personas deben tener en consideración que cada acción que realicen, la hagan con las medidas necesarias y no realizar clic en cualquier lado, este tipo de amenazas está en publicidad, enlaces y cualquier tipo de situación que generalmente sea independiente del sitio. Por ello se recomienda al usuario no abrir enlaces desde correos electrónicos, no ejecutar programas o cualquier tipo de complementos poco confiables, no hacer clic en cualquier lado, realizar lo necesario y no brindar información en cualquier lugar, a menos que fuese necesario, contar con un antivirus actualizado, navegar en sitios con certificados de seguridad, y no dejarse llevar por todo lo que se ve en internet, nadie va a regalar dinero, artículos o cualquier cosa, por simple gusto y gana, recuerda, internet mejora cada día más, tanto para facilidad del usuario y ayuda, así como métodos de ataques por parte de personas o empresas que buscan vulnerar internet.

Así que a partir de ahora, ya se puede deducir que muchas veces el usuario es quien permite que sucedan los ataques, simplemente por ignorancia o por descuido, por eso se realiza campañas de concientización para evitar todo este tipo de situaciones, debido a que robo de información no es tan grave, pero todo esto puede derivar a delitos reales y ni cibernéticos, es por eso que es necesario hacer consciencia a las personas para que puedan ser parte del cambio.

4.1.3.1. Errores comunes de los usuarios

Los usuarios a pesar de que actualmente existen demasiadas campañas de concientización para la protección cibernética, siguen cometiendo los

mismos errores, y se podría decir que con mayor frecuencia debido a que simplemente ignoran todo tipo de advertencias y no previenen dichos ataques, simplemente se sienten en la libertad de navegar por internet o utilizar sistemas sin tomar las medidas necesarias, sin embargo de todo esto, puede tener el mejor sistema de seguridad, en cuanto a sistemas antivirus u otro tipo de programas que protejan el sistema, pero es el usuario quien al final de todo, puede errar ante las barreras de seguridad, es decir, abrir las puertas que estaban cerradas por los programas de seguridad.

- No instalación de parches de seguridad: ante el lanzamiento de un nuevo programa o actualización de uno existente, pudieron haber quedado algunos cabos sueltos que pueden catalogarse como vulnerabilidades, las cuales con el pasar de los días las empresas que han creado dicho sistema, logran arreglar dichas vulnerabilidades, las cuales dejaban expuesto al usuario y su información, sin embargo el usuario decide ignorar dichas actualizaciones y por ende sigue dejando abierta las puertas a los ataques.

- Hacer clic en cualquier enlace: los usuarios se dejan llevar por la presión social, ataca mediante publicidad y sistemas conocidos, de tal forma que pudiendo ser un mensaje, o email de una persona de confianza, pero con un asunto poco común, debería generar sospechas, sin embargo al ser de una persona de confianza, eso mismo genera, una tranquilidad que simplemente se accede a lo que solicita, o se va a un sitio pudiendo ser víctima de un ataque, aunque parezca que todo pintaba a ser algo común, pero no lo fue así.

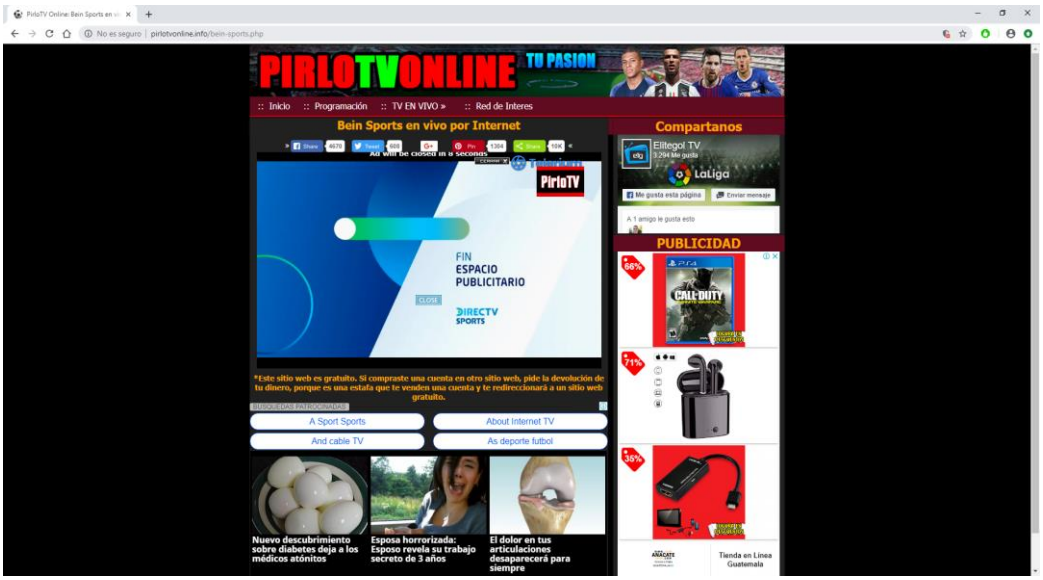
- Publicar información muy personal en las redes sociales: por más confiable y segura sea una red social, el compartir datos sensibles para

las personas resulta ser común en la actualidad, debido a que las mismas personas pareciera que no logran descifrar el enigma, que la información colgada en internet, pasa a ser pública para cualquier persona, claro, muchos lugares permiten restringir dicha información, sin embargo no deja de estar publica, pero las personas siguen haciendo caso omiso, a esto y por ende están expuestos a robo de información así como poder ser víctimas de crímenes reales y no cibernéticos.

- Navegar con conexiones desprotegidas: generalmente las personas al llegar a un lugar, lo primero que realizan es buscar una conexión a internet sin considera que segura puede ser, y en otros casos siendo esta aparentemente gratuita pero teniendo que registrarse, y de esta forma solicita información que simplemente les quedará a los que proporcionan el servicio que pareciera gratuito, pero no lo es, y esto es porque dicho pago habrá sido con la información de la persona.

- Navegar en sitios sin certificados de seguridad: los certificados de seguridad, implican que el sitio está siendo protegido mediante encriptación del envío y recepción de información, toda la información que se envíe y reciba de parte de dicho sitio, será encriptada y poco legible por los atacantes que pudiesen interceptar dicha comunicación, siendo para estos difícil o imposible descifrar la información, siendo esta navegación segura.

Figura 10. **Enlaces maliciosos y publicidad dentro de un sitio**



Fuente: *PIRLOTVONLINE*. http://pirlotvonline.info/bein-sports.php. Consulta: marzo de 2019.

En la anterior imagen se puede visualizar que este es un sitio frecuentado por muchas personas todos los días y en especial los días donde se juegan partidos internacionales, o de ligas atractivas, y es porque en este sitio permiten ver los partidos mediante la retransmisión original de los sitios de paga. Se puede observar la diversidad de anuncios que existen, los cuales en el mejor de los casos simplemente es publicidad que llevará al usuario a algún sitio, pero si es el caso que no lleva al usuario a otro sitio, sino al contrario pretende robar información, o infectar el sistema donde se encuentre trabajando.

4.1.4. Reinstalación del sistema

Cuando un ataque se ha concretado y simplemente ya cumplió su objetivo, muchas veces los atacantes deciden dejar el equipo como lo encontraron y otros alterar el funcionamiento por ello surgirán problemas que

muchas veces lamentablemente no podrán ser corregidos, y esto implicaría un reinicio del sistema.

Cuando se habla de reinicio de sistema, se refiere a una instalación completa o desde 0 del sistema, debido a que dicho sistema habrá quedado dañado por completo o partes fundamentales, siendo esta la última alternativa al no poderse haber corregido mediante otras alternativas, las cuales pueden ser desde la instalación de un software antivirus, análisis mediante dicho antivirus y corrección de los problemas, y algunos sistemas permiten regresar el equipo a un estado anterior donde el funcionamiento era optimo, es decir restaura el sistema a un punto anterior al del ataque, y de esta forma encontrar el sistema, funcionando en condiciones previas al ataque y ya si se logra, pues evitar cometer el mismo error.

4.2. Conocimientos básicos previos a navegar en internet

Los usuarios al tener acceso a internet tienden a conectarse a cualquier red e iniciar la navegación, abriendo sus cuentas de correo electrónico, sus redes sociales, noticias y muchos sitios más, pero la idea no es solo conectarse a internet e interactuar, porque siempre se deben saber cosas previas a navegar, y la idea es que dichos conocimientos sean los mínimos, pero indispensables, los cuales tenga el usuario siempre presente para que su experiencia no sea mala, al contrario siempre sea agradable y segura.

Entre los conocimientos básicos que todo usuario debería saber se puede clasificar:

- Principalmente los usuarios deben saber que siempre que se navega en internet se está expuesto a cualquier tipo de ataques, debido a que

siempre habrá personas malintencionadas que quieren aprovecharse de cualquier usuario mediante cualquier forma posible. Es por ello que los usuarios deben estar alerta y no acceder a cualquier sitio, de esa forma estarán en una zona más segura y no ponen en riesgo su información.

- El error humano es la mayor vulnerabilidad que existe, el dispositivo puede tener el mejor antivirus, y el mejor sistema estando actualizado, pero si el usuario hace caso omiso a todo tipo de advertencias por parte de su sistema, o antivirus, no habrá mayor barrera de seguridad, es por ello que el usuario debe estar consciente que el navegar tiene que tomar las precauciones necesarias y evitar todo tipo de aparentes ofertas mediante banners, enlaces y sitios que aparentemente sean confiables cuando en verdad no lo son.

- Es recomendable que los usuarios con acceso a internet tomen las precauciones necesarias y por ello si es necesario tener a la vista físicamente o en el computador las cosas que puede y no hacer al navegar, pudiendo hacerlas el mismo usuario, de esa forma podría colocar cosas como, no hacer clic en cualquier enlace, no creer en toda la publicidad que aparece en internet, así como actualizar el sistema siempre, y ese tipo de cosas que le recuerden toda situación que aumenten su seguridad al navegar por internet.

- No todo lo que está en internet es cierto, generalmente las personas se dejan llevar por lo llamativo de los sitios y la información dentro de ellos, sin embargo puede que sea falso, cabe mencionar que no todo es malo, pero hay cosas que resultan ser falsas y el usuario ignora ese tipo de cosas o no sabe diferenciar entre que es bueno y malo, por ello siempre

es importante verificar la fuente de la información y garantizar que en verdad sea útil o no.

- La información es lo más importante del usuario, es por ello que el usuario no debe compartir su información personal en cualquier lugar, incluyendo las redes sociales, debido a que las redes sociales muchas veces son de acceso público y la información esta visible para cualquier usuario, por ello es que se debe evitar compartir información privada, muchas veces es necesario ingresar información, para registrarse en algún sitio, para realizar una comprar o cosas similares, pero se debe constatar que donde se ingresa la información es un sitio de confianza, de lo contrario se estaría exponiendo la información y puede ser utilizada de mala forma por parte de quien la posea o para comercializar la misma.

- Nadie te va a regalar nada en internet, este es el típico caso de las personas al navegar, se ven invadidas por promociones atractivas, las cuales buscan seducir al usuario para poder cobrar algunos incentivos materiales o económicos mediante el ingreso de su información (personal, bancaria, etc.), pero nadie regala cosas sin motivo aparente, a menos que se haya participado en algún sorteo o algo similar, puede que la información sea verídica, de lo contrario, no se puede obtener algún premio simplemente por ser un afortunado usuario que se encontraba navegando y saliera favorecido.

4.3. Medidas de precaución necesarias para evitar cometer errores que vulneren la información mientras se navega en internet

Cuando los usuarios hacen uso de internet, siempre deberán tener en cuenta muchas cosas para una navegación más segura, debido a que siempre

se está expuesto, pero tomando las precauciones necesarias, debería reducirse el riesgo de ser víctima de cualquier tipo de fraude o ataque.

Los usuarios deberán estar conscientes que navegar en internet no significa simplemente hacer uso de un dispositivo sin tener las precauciones necesarias para evitar lamentarse posteriormente ante cualquier eventualidad siendo esta un ataque o volverse parte de una red zombi.

4.3.1. Principales medidas de precaución para navegar por internet

Para poder lograr una mejor experiencia del usuario en cuanto a navegar por internet se debe tomar en cuenta varios factores, entre los cuales se puede mencionar:

- Mantener el sistema donde se vaya a navegar actualizado, esto siempre será fundamental debido a que los sistemas han sido hechos para funcionar de manera óptima, pero puede ser que en algún momento presenten pequeños fallos o mejor conocidos como errores, los cuales son corregidos por las actualizaciones de los creadores de dichos sistemas, y por ende tener un sistema actualizado será vital para poder navegar de una forma más segura; en un caso puntual donde el sistema presenta muchas o algunas vulnerabilidades las cuales permiten que los atacantes puedan entrar y concretar una taque, y los creadores han logrado cerrar dichas vulnerabilidades pero todo esto llevándose a cabo mediante una serie de actualizaciones, las cuales tendrán como finalidad adherirse al sistema y cerrar dichas vulnerabilidades, pero si no se actualiza, se estará expuesto ante cualquier ataque y la idea es siempre minimizar el riesgo, pero todo depende de la responsabilidad del usuario,

porque él siempre será el quien deba actualizar el sistema, aunque actualmente muchos sistemas permiten actualizarse automáticamente sin interacción del usuario, pero el usuario es quien define todo esto, por eso se denomina al usuario como el responsable.

- Conectarse a internet mediante red wifi conocida y con contraseña será lo fundamental para estar con una seguridad mayor, debido a que las personas se ven tentadas a las facilidades actualmente existentes, y el caso más conocido es que los usuarios siempre que llegan a un lugar físico (centro comercial, restaurante, etc.) verifican si cuentan con acceso a internet gratuito, este permite la conexión a internet del dispositivo que se está utilizando, generalmente son redes sin contraseña, las cuales pueden ser utilizadas por cualquier usuarios, entonces acá viene el principal problema, que al ser redes poco seguras debido a que no cuentan con contraseña, y son de acceso público, cualquier atacante, también denominado como hacker, puede intentar capturar toda la información que se envía desde los dispositivos conectados hacia internet, es decir pudiendo obtener todo ese tipo de información, de esa forma es como los usuarios pueden conectarse sin mayor esfuerzo, los atacantes también lo pueden hacer, pero ellos no buscan navegar, ellos siempre buscarán interceptar la información de los usuarios, pudiendo ser credenciales de acceso, cuentas bancarias, tarjetas de crédito y muchas cosas más; es por ello que siempre se debe navegar mediante redes seguras, para que la experiencia de usuario sea agradable y este seguro en todo momento.

- Poseer software antivirus o cualquier variante pero que cumplan con las funciones de protección ante amenazas provenientes de internet, es decir al tener un antivirus instalado, se tiene una barrera que muchos

tipos de amenazas deberán vencer para poder concretar su ataque, sin embargo el antivirus jugará un papel muy importante, porque el mismo estará monitoreando lo que se realice en internet, es decir siempre estará de guardia para no dejar pasar a cualquier intruso o virus, de tal forma que es completamente necesario contar con un software antivirus para garantizar un nivel mayor de seguridad al navegar. Los software antivirus casi siempre bloquearan todo lo que ellos consideren que pueda poner en riesgo la navegación del usuario, sin embargo a pesar de todas las advertencias que pueda dar dicho antivirus, el usuario decide hacer caso omiso y continua su navegación, cayendo muchas veces en el mayor error (error humano), y dejando expuesto su dispositivo de navegación y su información por ignorar las advertencias, es por ello que dichos software han sido diseñados para proteger, y se debe tener siempre en cuenta que lo mejor siempre será confiar en que si da algún indicio de que el sitio al que se está accediendo no es seguro, detener la navegación en ese sitio, a menos que se esté completamente seguro que el sitio al que se está accediendo es de confianza, es por eso que los protocolos de seguridad para los sitios web tienen un costo, muchas empresas no lo ven como algo necesario, pero no le garantiza al usuario la seguridad optima, esto no quiere decir que el sitio contenga algún problema, aunque indique lo contrario, es por ello que siempre se tendrá la opción de acceder si el usuario autoriza hacerlo. Si el antivirus detecta que el sitio al que se está accediendo intenta ejecutar algo, generalmente el aviso será recurrente y sumamente importante debido a que hay una mayor certeza de que en ese sitio se quiere ejecutar un tipo de ataque que vulnere la información del usuario.

- Comprobar que el sitio web contenga el protocolo de seguridad HTTPS (Hypertext Transfer Protocol Secure) y no HTTP (Hypertext Transfer

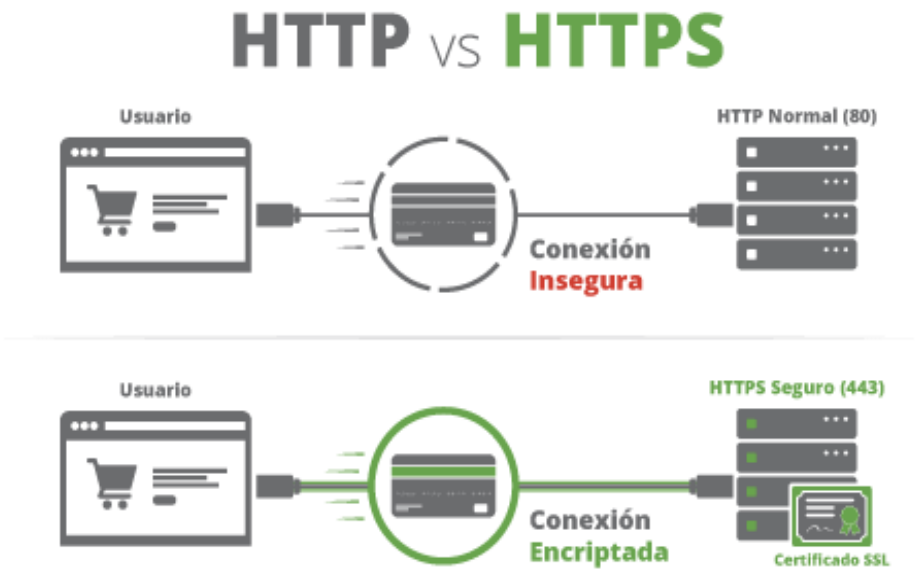
Protocol), debido a que utilizando HTTP la información que se envía desde el ordenador del usuario hacia cualquier sitio de internet, es enviada así como se escribe, es decir si se llena un formulario, la información irá en el internet así como se llenó el formulario, sin embargo al utilizar HTTPS la información será ilegible para el usuario, debido a que la misma va encriptada, y así se garantiza que no puedan interceptar y utilizar de mala forma la información del usuario. Cabe mencionar que esos protocolos son implementados por los sitios web, es decir que el usuario no tiene control sobre ello, entonces, es en este punto donde el usuario deberá comprobar si continúa en ese sitio o lo abandona. Un protocolo no garantiza que el usuario está libre de amenazas, pero asegura que la información que intercambie con el sitio es segura, es por ello que es la primera medida que debe tomar el usuario antes de navegar en un sitio web. La forma correcta de encontrar si el sitio está utilizando ese protocolo será verificar en la barra de direcciones, que se ubica en la parte superior del navegador, es donde se escribe la dirección del sitio web al que se está accediendo y generalmente tendrá un patrón similar a http://www.google.com o https://www.google.com, siendo estos los dos protocolos, y es acá donde se verifica que protocolo utiliza dicho sitio web.

Figura 11. **Forma de verificar el uso del protocolo HTTPS**

Fuente: *HTTP y HTTPS: ¿Qué son y en qué se diferencian estos protocolos?* https://www.softzone.es/2018/04/26/http-https-diferencia-protocolos/. Consulta: marzo de 2019.

En la anterior imagen, se puede verificar que muchos navegadores indican que el sitio al que se está accediendo es seguro mediante el uso del protocolo HTTPS, este protocolo se remarca en color verde, no siempre sucede esto en todos los navegadores, pero generalmente aparecerá un candado indicando dicha seguridad, es por ello que es necesario verificar el uso de este protocolo mediante la verificación de la barra de direcciones.

Figura 12. **HTTP vs HTTPS**



Fuente: *HTTP y HTTPS: ¿Qué son y en qué se diferencian estos protocolos?* https://www.softzone.es/2018/04/26/http-https-diferencia-protocolos/. Consulta: marzo de 2019.

4.3.2. Medidas de precaución para compartir información en internet

El típico error de los usuarios será compartir su información personal en las redes sociales o sitios web en los que navega; muchas veces se hace de

esa forma por ignorancia, pero sin importar cuál sea el motivo, siempre esa información será generalmente pública. Es por ello que las personas deben tomar todas las precauciones necesarias para evitar compartir información de más y así poder verse involucrados en problemas posteriores, como los casos donde hay clonación de identidad, siendo estas personas afectadas por terceros que solo buscan eso, ocultarse ante la web, pero poniendo en problemas a las otras personas.

Por estas faltas de conciencia de parte de los usuarios, se han tomado en cuenta muchas fuentes y factores, y por ende las medidas de precaución necesarias que deben tomarse en cuenta son:

- Compartir información solamente si es necesario, debido a que la mayoría de sitios web te va a solicitar llenar un formulario para que tu información sea ingresada y almacenada por ellos, siendo esta accesible para ellos en cualquier momento, es por ello que si el sitio es de confianza y se sabe que llenar el formulario de registro es necesario para fines educativos, financieros o de cualquier índole pero que sean beneficiosos, estará bien poder compartir la información personal, pero hay un detalle que no se debe dejar pasar, y es que la información que se ingrese no sea sensible, y cuando se define sensible es de detalles como cuentas bancarias, números de tarjeta de crédito, direcciones físicas, números de teléfono, información familiar, y todo ese tipo de información demasiado personal. Es por ello que se debe tener el cuidado necesario de compartir la información, un claro ejemplo es el acceso a redes sociales, debido a que en ellas se solicita una cantidad mínima de información, siendo esta desde un correo electrónico, número de teléfono, direcciones, nombres y todo ese tipo de información, sin embargo los datos mínimos serán los personales y un correo electrónico,

para poder obtener una, y es por ello que hay que ser cuidadoso en no ingresar información de más, porque al estar dentro de una red social, la información muchas veces pasa a ser de tipo público. Es por estas razones que compartir información en redes sociales es actualmente una de las mayores formas de ser víctimas de ataques cibernéticos y porque no decirlo, de ser víctimas de ataques físicos, como secuestros, extorsiones y todo ese tipo de situaciones debido a que se podría acceder a las direcciones físicas, números de teléfono y nombres tanto del usuario como de las personas con las que interactúa. Siempre se trata de hacer conciencia en esta parte, porque es de las más importantes en cuanto a navegación, y especialmente en los niños, debido a que los niños ven esto como un juego o una forma de divertirse y pasar el tiempo, sin embargo se debe ser cuidadoso para evitar algún inconveniente.

- Los archivos cuentan como información, esto quiere decir que todo documento que se quiera pasar mediante internet, se deberá realizar por medios seguros, es decir, plataformas que garanticen la seguridad y confidencialidad de lo que se realiza, es decir muchas veces las personas quieren compartir información por correo electrónico, redes sociales, y otros medios que son seguros, pero cabe mencionar que todo sitio por el que se intente compartir información, deberá ser confiable, si no se tiene la plena confianza en el sitio, puede existir problemas posteriores, como que los archivos que se han compartido han pasado a ser propiedad de los sitios web, es por ello que se recomienda siempre tomar las precauciones necesarias, para compartir archivos, y si se puede realizar de forma segura, hacerlo, porque la otra forma conocida mundialmente, es el traslado de la información mediante dispositivos de almacenamiento volátiles, o mejor conocido como memorias USB, las

cuales almacenarán los archivos para poder ser replicados en cualquier dispositivo en el que sea reconocida.

- No todos los amigos virtuales no son amigos de verdad, muchas personas piensan que su popularidad va en aumento cuando se vuelven amigos de muchas personas en redes sociales o sitios de convivencia social; el número de amigos que pertenecen al núcleo de amistad de una red social puede que sea un número real, eso es porque las personas podrán tener agregados a sus amigos reales, es decir, con quienes convive fiscalmente, y pues es por ello que no siempre se trate de personas desconocidas, sin embargo, muchas veces así es, las personas creen que la popularidad social viene dada al número de amigos virtuales que se puedan tener. Mucho cuidado, muchas veces simplemente son personas catalogadas como delincuentes que buscan más que solo “ser amigos”, pueden buscar afectar al usuario de una forma física, tal es el caso de tantos problemas ocurridos por supuestas amistades virtuales que terminaron en algo completamente diferente, un secuestro, un asesinato o cosas trágicas de las que se puede lamentar, es por ello que muchas veces las redes sociales permiten el registro de personas usurpando identidades o simplemente inventando identidades para poder cometer algún tipo de delito.

4.3.3. Medidas de precaución para realizar compras en internet

Muchos usuarios prefieren adquirir sus productos o algún tipo de servicio mediante sitios web, o las denominadas compras por internet, las cuales consiste en realizar el mismo proceso donde se va a un supermercado, tienda de tecnología, entre otros, de tal forma que se busca el producto, se revisa, se

paga y listo, se puede retirar el producto, sin embargo en esta modalidad, todo es similar, pero tiene sus ventajas y desventajas, porque se puede buscar el producto, ver sus características, evaluar el precio y proceder a pagar; al verificar el proceso es el mismo, con las ventajas de no salir del hogar, comprar en tiendas de todo el mundo, entregas a la puerta de la casa del usuario.

El usuario tiene estas facilidades, pero siempre debe tomar medidas de precauciones necesarias las cuales son:

- El usuario debe contar con tarjeta de crédito o débito para realizar las compras, debido a que si el proceso es internacional (compras fuera del país de origen), deberá realizar los pagos correspondientes mediante el sitio del proveedor de los productos, esto implica un pago mediante tarjeta; hay empresas que poseen una modalidad denominada pago contra entrega, pero esto muchas veces aplica dentro del país donde se compra, o los pagos previos, y con estos hay que tener mayor cuidado, debido a que muchas veces puede ser estafas, en las cuales se hace el depósito y el producto no llegará jamás, por estos extremos es que se debe tomar las medidas de seguridad necesarias en las cuales se garantice que la compra será transparente y sin ningún problema posterior a realizar el pago.

- El usuario debe verificar que el sitio web donde está comprando sea seguro y esto lo puede lograr mediante muchas formas, pero las principales son que el sitio no te deberá pedir tu información de pago por algún medio externo, es decir por correo electrónico, algún enlace que consigas o te pasen por alguna red social, debido a que tienes que está completamente seguro y no brindar información alguna si la tienda virtual genera algún tipo de desconfianza.

- Verificar las descripciones de los productos antes de realizar una compra, esto es el típico problema de los usuarios que generalmente compran algo y les llega algo diferente, y esto sucede cuando las personas no se tomaron el tiempo de verificar detenidamente cada detalle del producto, muchas veces se utilizan imágenes con fines llamativos, sin embargo no es el verdadero producto, en la descripción detallan otra cosa, por eso es un detalle que no debe dejar pasar el usuario, para poder estar seguro de lo que está comprando.

- No compres por ningún motivo en un computador que no sea tuyo, este error común en los usuarios puede ser un problema posterior, nada garantiza que el computador que se esté utilizando cuente con programas especializados en leer todo lo que se está ingresando, y pudiendo ser utilizado posteriormente por terceros a los que únicamente les interesa aprovecharse de la situación para robar tu información, y peor aún lograr tener tus datos bancarios que podrán utilizar para ellos hacerse pasar por el usuario legítimo.

- Nunca compres en internet estando conectado a una red pública o gratuita, esto es muy importante, debido a que las personas cuando tienen la oportunidad de conectarse a una red gratuita o pública, pueden poner en riesgo toda su navegación mediante la interceptación de todo lo que envíen, es por ello que es siempre recomendable navegar para realizar compras en redes conocidas y seguras, pudiendo ser una red de hogar, o algún lugar donde se establezca que la conexión no puede ser intervenida para obtener tu información.

- Cotiza el precio final, este es el típico error por parte del usuario, en el que muchas veces no se toma en cuenta el valor final del producto, y

esto viene a repercutir muchas veces que el producto saldrá más caro que haberlo comprado en una tienda física; este problema viene derivado del principal factor que los usuarios desconocen y es que todo producto en el país de origen deben pagar un impuesto y un envío, en muchos sitios aparentemente es gratuito, sin embargo el precio que aparece en el sitio no incluye nada de esto, entonces siempre es necesario verificar que el producto puede tener cobros adicionales, e incluyendo que si el envío es gratuito y los impuestos son mínimos, puede adherirse que en el país receptor (de donde es el usuario), tendrá una taza de impuestos establecida que deberá cancelar el usuario para poder ingresar el producto, es decir que a pesar de que el precio final siga siendo favorable, es necesario averiguar el valor que las entidades encargadas de recolección de impuestos (Superintendencia de Administración Tributaria, SAT para Guatemala), tienen para los diferentes productos y así hacer un aproximado para poder tener el precio total de dichos productos, así que no hay que dejarse llevar por los aparentes bajos costos de los productos a simple vista mostrados en los sitios web.

4.3.4. Medidas de precaución para iniciar sesión en redes sociales, correos electrónicos y cualquier sitio web

Las situaciones en las que se permite el ingreso mediante un previo registro conlleva demasiadas cosas para tomar en cuenta, las cuales siempre van a tener motivos primordiales para los sitios en los que el usuario va a registrarse, y por ende siempre hay que tomar las medidas de precaución necesarias, entre las cuales se puede mencionar:

- El sitio web tiene que ser confiable, y este será el factor fundamental, debido a que si no se logra establecer que el sitio web es confiable no

será recomendable por ningún motivo seguir navegando en el mismo, y entonces es donde los usuarios deben siempre tomar en cuenta que este factor por ningún motivo se debe pasar por alto, porque toda la información que pueda ingresarse podría estar en riesgo.

- Un registro siempre será tomado como un nuevo elemento a la base de datos del sitio web, es decir ahora el usuario formará parte del banco de datos del sitio, por ello se debe ser cauteloso e ingresar de una forma prudente la información y evitar escribir información muy delicada.

- Siempre leer los términos y condiciones del sitio, mediante ello se podrá lograr establecer si aunque sea seguro podría ponerse en riesgo la información ingresada o no, entonces siempre es recomendable leer todo tipo de información que pueda ayudarnos a entender cuál será el fin de la información que se vaya a ingresar.

- Ningún sitio web te va a solicitar tus datos fuera de su sitio, esto implica que ningún sitio que visites y te vayas a registrar va a enviarte mediante correos electrónicos o cualquier otro lugar alguna petición para que puedas ingresar tu información, es por ello que los usuarios deben tomar todo tipo de precauciones necesarias y por ningún motivo ingresar información o todo tipo de credenciales mediante solicitudes fuera del mismo sitio.

- Ingresar información básica, cuando el usuario desea registrarse en algún sitio, los sitios permiten el ingreso de mucha información personal, pero en la mayoría restringen datos netamente básicos como obligatorios, es decir, que solo van a solicitar información básica y con eso sería suficiente, por esto es que solamente se necesita ingresar esa

información y nada más, de esta forma se garantiza que la información que se ingrese sea real pero no se expone más información como cuentas bancarias, direcciones, teléfonos y todo este tipo de información que pueda resultar perjudicial en manos poco adecuadas.

4.3.5. Medidas de seguridad para elección de contraseñas

Los usuarios tienden a utilizar contraseñas poco seguras, de tal forma que puedan ser predecibles con mucha facilidad siendo estas situaciones las primordiales para que los atacantes logren obtener dichas credenciales sin mayor esfuerzo, es por ello que los usuarios siempre tienen que tomar en cuenta los factores siguientes para tener un nivel de seguridad mayor:

- Contraseñas diferentes para cada sitio web donde se registre el usuario, esta medida es una de las primordiales en seguridad, debido a que los usuarios tienden por facilidad utilizar la misma contraseña en todos los sitios en los que se han registrado, sin embargo no se dan cuenta que si visitan un sitio inseguro y son víctimas de robo de su información, y tienen los mismos credenciales para diferentes sitios, es seguro que ya habrán utilizados dichos credenciales para acceder a cada uno de los sitios web, y máxime si también tienen acceso a los correos electrónicos, seguramente ya no se podrá recuperar la información.

- Cambiar los credenciales de manera recurrente, esto aplica a cada uno de los sitios a los que se tenga acceso, de esta forma se garantiza una constante medida de seguridad aún mayor ante los ataques, debido a que el nivel de seguridad del usuario habrá incrementado de manera considerable, es por ello que se debe y recomienda mantener en constante cambio las contraseñas, y lo recomendable es que no

sobrepase un máximo de 3 meses. Los usuarios consideran hacer esto algo tedioso y poco amigable, sin embargo es por la seguridad del usuario que se debe realizar.

- La utilización de autenticación de dos factores, este tipo de autenticación es poco común, pero una de las más seguras, debido a que las personas tendrán que autorizar mediante algún otro medio o dispositivo para poder acceder al sitio de lo contrario no se podrá de ninguna forma tener acceso, esto es utilizado por los sistemas y dispositivos Apple, porque ellos siempre que se quiere acceder a un sitio web de su propiedad, con los credenciales registrados en un dispositivo, se tiene que autorizar mediante ese dispositivo para garantizar que la persona es la dueña de quien se quiere autentica.

- La contraseña debe ser segura, este es un factor fundamental, debido a que las personas siempre buscarán algo fácil de recordar y generalmente es relacionado a su nombre, fechas importantes y cosas relacionadas al usuario, es por ello que se recomiendo a los usuarios hacer contraseñas seguras en las cuales se puede garantizar una mayor seguridad; Una contraseña para ser segura no simplemente debe ser larga, porque larga no es garantía de seguridad, sin embargo es mejor que cualquier contraseña corta, por esa situación los profesionales de la ciberseguridad recomiendan a los usuarios utilizar caracteres especiales o mejor conocidos como símbolos, así como números y letras, todas juntas, es decir que una contraseña deberá contener de todo lo anteriormente mencionado para poder considerase más segura.

Figura 13. **Cómo deben ser las contraseñas**

Fuente: *Aprende a gestionar tus contraseñas.* https://www.osi.es/es/contrasenas. Consulta: abril de 2019.

En este gráfico se detalla los factores fundamentales a considerar para que una contraseña cumpla como segura, de esta forma se garantiza en mayor parte la seguridad del usuario.

Figura 14. **Que contraseñas no se deben utilizar**

Fuente: *Aprende a gestionar tus contraseñas*. https://www.osi.es/es/contrasenas. Consulta: abril de 2019.

Toda contraseña no debe contener los factores mencionados en la imagen anterior, debido a que siempre esos serán los más propensos a ser encontrados por los atacantes, es por ello que siempre se debe elegir la contraseña evitando estos factores, así el usuario tendrá una navegación más segura.

Tabla II. **Contraseñas seguras vs contraseñas no seguras**

Contraseña no segura	Contraseña segura
Mi familia es genial	M¡ f@m¡1¡@ 3s g3n¡@1
Contraseña segura	C0ntr@s3n¡@ s3gur@
Password12345	P@ssw0rd!”#$%
Facebook	f@c3b00kk$
Instagram	¡nst@gr@mm$

Fuente: elaboración propia.

La idea de mostrar esas comparaciones de las contraseñas, es que el usuario note la diferencia de un texto convencional a algo más seguro, utilizando símbolos, y en el caso de la contraseña final se cambiaron los números por símbolos, los cuales convierten la contraseña más segura de lo que era al inicio, y las contraseñas finales aparentemente son para redes sociales, por ello se hizo referencia a Facebook e instagram, de tal forma que se deben utilizar diferentes para cada red social.

4.4. Como garantizar una conexión segura al navegar por internet

Una navegación segura se logra mediante todos los factores que debería saber el usuario previo a navegar por internet, sin embargo ya estando en internet siempre hay que seguir tomando las precauciones necesarias para lograr estar en una zona segura y no verse sorprendidos ante cualquier eventualidad, es por ello que los usuarios siempre serán los que tomarán las decisiones en su navegación, y es en este punto donde el usuario es el responsable de que y a donde ingresa estando conectado a internet.

4.4.1. Protocolo HTTPS y que implica al navegar por internet

Cuando los usuarios navegan por internet y acceden a los sitios, se tiene que en la mayoría de estos sitios, se accede mediante el protocolo HTTP o HTTPS, y cada uno funciona de manera similar, con variantes considerables, entonces muchos se preguntarán, ¿Cuál es la diferencia?, es por ello que en la siguiente tabla se detallan las diferencias:

Tabla III. **HTTP y HTTPS**

HTTP	HTTPS
URL comienza con “http://”	URL comienza con “https://”
Información legible ante una interceptación.	Información no legible por una interceptación.
No garantiza la seguridad de un sitio.	Hay mayor garantía de que el sitio es seguro.
La información no es cifrada	La información es cifrada

Fuente: elaboración propia.

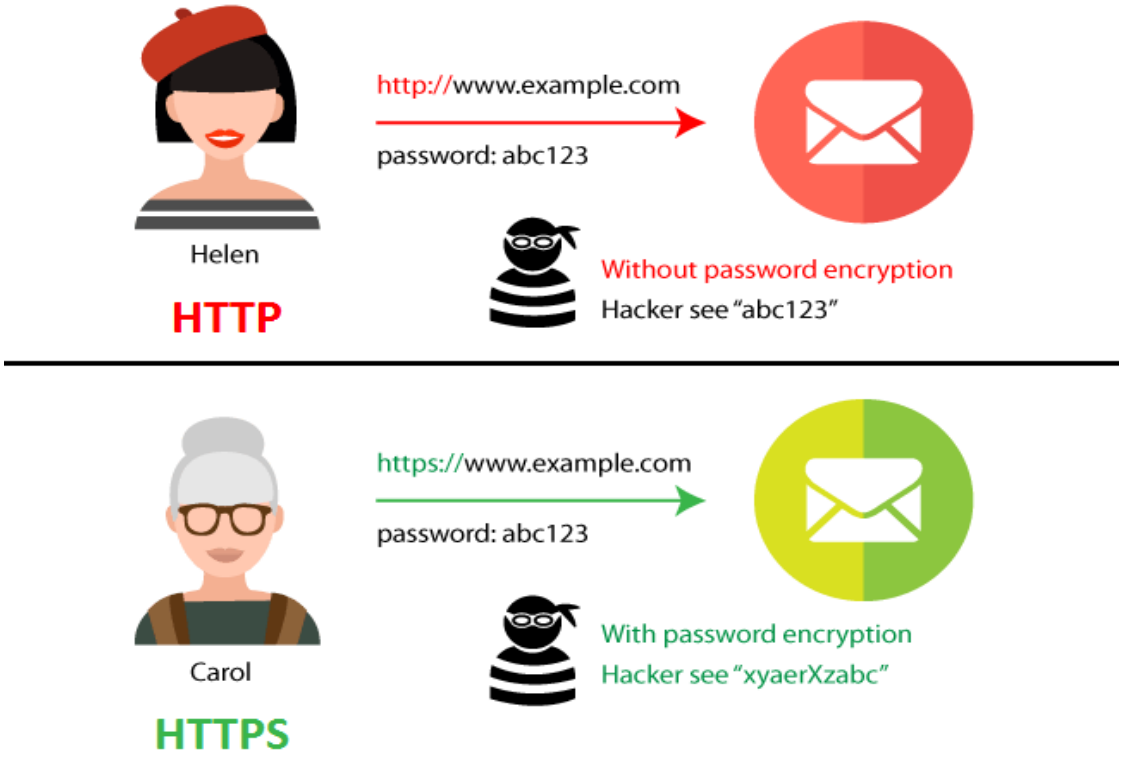
Basándose en la tabla, se puede definir que utilizar el protocolo HTTP, será igual a utilizar el protocolo HTTPS, es decir la comunicación será igual, sin embargo la seguridad no es la misma, y de ahí parte la diferencia abismal que existe entre ambos protocolos, mediante HTTP la comunicación entre el usuario y cualquier sitio web será de ida y vuelta sin seguridad, es decir que el usuario envía su información al sitio web y si algún hacker o persona mal intencionada intercepta la comunicación, no tiene que hacer mayor esfuerzo para ver que está enviando el usuario, y el problema es que en ese momento puede estar iniciando sesión en algún sistema bancario y por esa misma circunstancia el usuario puede estar en graves problemas, en cambio al utilizar el protocolo

HTTPS, funciona mediante el envío de la información y el sitio web la recibirá, sin embargo en ese momento que la información viajo mediante internet, si hubiese algún tipo de atacante que intercepte esa comunicación, aunque logre obtener los datos que se enviaron, no podrá descifrar lo que se está mandando, porque el protocolo habrá cumplido su trabajo y habrá sido haber enviado la información de una manera ilegible, y el sitio será el único que podrá decodificar la misma para saber qué es lo que está recibiendo.

Esto puede sonar algo confuso, pero en términos simples es, que al utilizar HTTP el usuario mandará la información y recibirá respuesta, y ahí habrá terminado todo, en cambio al utilizar HTTPS, es como si el usuario todo lo que vaya a enviar al sitio, se lo mandará en una caja fuerte, y únicamente el sitio tendrán la llave, es por ello que el sitio será el único que podrá ver el contenido que manda el usuario y el usuario podrá ver el contenido que envía el sitio.

Cabe destacar que el protocolo HTTPS es configurado por parte del sitio web, es decir no depende del usuario, y acá puede surgir más dudas, pero no es tan complicado, porque lo único importante en este caso es que si el usuario verifica que el sitio no es completamente seguro al no utilizar el protocolo, el mismo usuario será el encargado de permanecer o salir de ese sitio, nadie lo obliga a permanecer en el, y es por ello que siempre se hace énfasis a que en la mayoría de ciberataques, es por complicidad del usuario.

Figura 15. **HTTP y HTTPS gráficamente**



Fuente: *Jeffth. HTTP vs HTTPS: The Difference And Everything You Need To Know.* https://seopressor.com/blog/http-vs-https/. Consulta: abril de 2019.

La imagen anterior muestra cómo es que funciona el protocolo HTTPS, y claramente se puede observar que cuando Helen envía su información para iniciar sesión en algún sitio, la contraseña va exactamente como ella la ha ingresado, sin embargo, cuando Carol envía su información de inicio de sesión, esta va ilegible, de tal forma que si alguien intercepta su navegación, no podrá entender que es lo que en este caso Carol ha escrito y enviado.

4.4.2. Redes gratuitas y sus riesgos

El hecho de ir a un lugar nuevo y no querer perderse ni un segundo del mundo cibernético implica buscar comercios que cuenten con redes inalámbricas de acceso gratuito o libre, pero a todo esto las personas no magnifican que riesgos puede implicar estas conexiones que aparentemente son gratuitas y no esperan nada a cambio, que simplemente los comercios son bondadosos y regalan algo por lo que ellos si pagan. De estos puntos los usuarios deben tener presente que muchas veces para conectarse a dichas redes se solicita llenar un pequeño formulario, en este no parece nada grave o que no implica nada, pero porque solicitan correo electrónico, número telefónico, tu nombre y más datos sensibles, los cuales simplemente no son necesarios para conectarse a internet, entonces he ahí donde viene otro tipo de situaciones que debe tomar en cuenta el usuario.

Los factores a tomar en cuenta para hacer conciencia al usuario y pueda tener un mayor panorama de todos los riegos y situaciones suscitadas al conectarse a una red gratuita son los siguientes:

- No todo lo que brilla es oro: cuando una red a la que aparentemente puedes conectarte sin necesidad de pagar o hacer algo adicional, generalmente tendrán lo que se le conoce como truco, y esto puede resaltar que quien distribuye gratuitamente este tipo de redes, es un comercio o persona particular que en algún momento puede interferir en las comunicaciones de los usuarios y los sitios web, es decir, que el administrador de esa red o propietario, puede monitorear el uso que se le da a la red mediante los dispositivos conectados, y peor aún, si el monitoreo se realiza puede suceder que solamente un simple monitoreo, pueda tener un método para capturar la información que el usuario envía,

entonces esto implica que el administrador de la red, pasa de ser la persona o comercio caritativo, a un atacante que únicamente quiere adueñarse de los datos del usuario para poder utilizarlos como mejor les convenga.

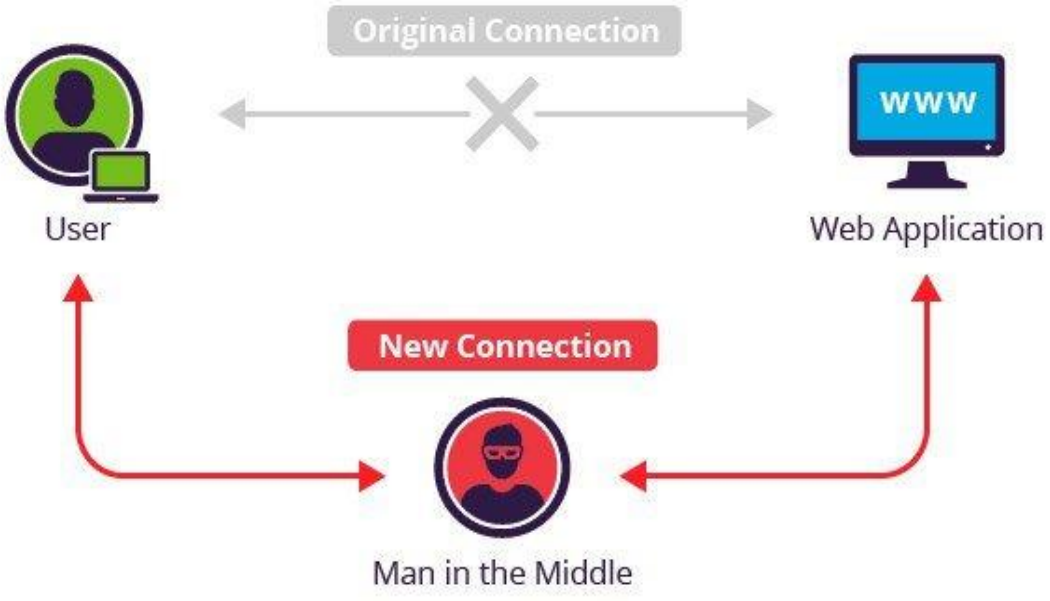
- Redes con inicio de sesión: una red libre o gratuita permite conectarse pero para poder utilizar el internet, solicita información de registro, es decir que le pide al usuario que cree un usuario es decir, que ingrese datos como nombres, números telefónicos y/o correos electrónicos, pero la pregunta que muchos usuarios se plantean es, ¿En verdad son necesarios estos datos?, y la respuesta es, no son necesarios. Entonces surge una interrogante adicional y es, ¿Para que el comercio me solicita datos de registro para conectarme gratuitamente?, He ahí donde viene el truco, y es que la información de los usuarios es lo más importante para el usuario en cuanto a lo digital, es decir, los usuarios están pagando por conectarse a internet gratuito con su información personal, y hasta ciertos comercios permiten seleccionar una opción de suscripción a ofertas o boletines informativos, y posterior a ello, se tiene la bandeja de correo electrónico saturada con ofertas de estos comercios debido a que el usuario fue el único que permitió que eso sucediera. Este es el punto primordial para entender que el internet gratuito no lo es.

- Toda navegación gratuita puede ser interceptada sin salir al internet: este concepto es poco comprensible para los usuarios, pero lo que se quiere dar a entender es que un ataque a la seguridad del usuario y robo de información puede darse entre el propio usuario y los distribuidores del internet gratuito, esto quiere decir que no hay necesidad de conectarse a una página web y establecer conexión, porque la información puede ser interceptada antes de llegar al sitio web y ser robada.

- Virus en la red: si un dispositivo que este en la red contiene algún tipo de virus o lo contrae en su navegación, este puede replicarse de manera rápida que es imperceptible por el usuario, esto quiere decir que todos los dispositivos conectados pueden estar en riesgo porque desde un origen puede llegarse a todos los destinos que serán los dispositivos conectados a la red.

- Evite la comunicación donde sea indispensable el uso de información sensible del usuario: este factor debe ser el fundamental, debido a que los usuarios no deberán iniciar sesión en redes sociales, sistemas bancarios y realizar alguna compra utilizando redes públicas y gratuitas, debido a que toda la información estará desprotegida, y es por ello que se recomienda por ningún motivo realizar estas acciones, por más indispensables que parezca, será mejor siempre utilizar redes seguras.

Figura 16. **Man in the middle (hombre en el medio)**



Fuente: PÉREZ FERNÁNDEZ, Daniel. *Punto de acceso inalámbrico Man-in-the-middle dentro de un contenedor docker.* https://tecnonucleous.com/2018/02/09/punto-de-acceso-inalambrico-man-in-the-middle-dentro-de-un-contenedor-de-docker/. Consulta: abril de 2019.

En la imagen anterior se muestra como ocurre una interceptación de el envío de información que puede ocurrir en una red pública o gratuita, esta forma de interceptar viene dada a que el administrador o distribuidor de internet gratuito, interceptan la comunicación con internet, y siempre accederás al sitio que andes buscando, y podrás interactuar, pero la persona que está en medio sabrá todo lo que realices pudiendo interceptar tu información robarla y hacer uso de ella posteriormente.

4.5. Qué hacer si se es víctima de un ataque o hackeo

Cuando una persona detecta que existe algo sospechoso en sus redes sociales, correos electrónicos, cuentas bancarias, o cualquier situación, puede ser porque ha sido víctima de un ataque o hackeo, y las medidas principales a tomar en cuenta serán las siguientes:

- Cuando el usuario detecta que es víctima o tiene sospechas, deberá realizar una actualización de datos de acceso, esto implicando cambios de claves, actualizaciones de usuarios y todo tipo de información que pueda haber sido obtenida por los atacantes, este mecanismo, permite tener acceso simplemente por el usuario quien es propietario de las cuentas, sin embargo, sería ideal revisar que no se haya alterado nada y no haya sido robada más información.

- Si el usuario vincula un ataque a sus credenciales bancarias y este tipo de información, deberá inmediatamente contactar al servicio al cliente de su banco para realizar los bloqueos de las cuentas así como una actualización de sus credenciales de acceso lo antes posible, para evitar que los atacantes sigan utilizando su información para cometer algún tipo de robo.

- Conservar la calma, ya el ataque habrá sido concretado, y por ende se deberán realizar las acciones pertinentes, alterarse o realizar alguna acción precipitada, solo puede conllevar a seguir agrandando el problema, y por eso es que hay que ser cuidadoso en cuanto a los sitios que se visita y mediante que redes se conecta a internet.

4.6. Factores a tomar en cuenta si se desea desarrollar un sistema informático

Muchas empresas o usuarios están conscientes que se necesita un cambio radical del papel a lo digital, y por ello pretenden dar el salto que les permita realizar ese cambio, sin embargo deben tomar en cuenta muchos factores para poder garantizar el éxito en sus desarrollos y por ende, un cambio completamente positivo y útil.

Los principales factores que los usuarios deberán tomar en cuenta para realizaciones de nuevos proyectos en cuanto a desarrollo de nuevos sistemas o actualizaciones de algunos existentes deben ser:

- Medidas de seguridad y vulnerabilidades verificadas: este es el principal factor, debido a que las empresas muchas veces no toman en cuenta todos los riesgos que pueda llevar el desarrollar un proyecto simplemente funcional, sin medidas de seguridad necesarias, y es por ello que se propone una verificación previa a desarrollar de todas las posibles vulnerabilidades así como detalles de seguridad que puedan tomarse en cuenta para que cuando se desarrolle un sistema, todo este contemplado y no existe algún tipo de situaciones que lamentar posteriormente.

- La seguridad también se debe aplicar físicamente: los sistemas siempre estarán en sistemas físicos es decir, servidores o computadores convencionales con el papel de servidores, quienes tienen el papel fundamental te albergar los sistemas que serán utilizados por los usuarios, y es por ello que se debe garantizar que dichos servidores tengan las medidas de seguridad necesarias y los sistemas utilizados también las tengan, debido a que siempre debe existir una dependencia

entre lo tangible y lo intangible en un sistema informático, es por ello que se debe configurar todo lo necesario para garantizar ello; tomando como base que actualmente existen los sistemas en la nube, se debe realizar todas las configuraciones necesarias en los sistemas en la nube y por ende se debe tener el personal adecuado para la realización de esto debido a que siempre la seguridad será primordial y por ende es mejor invertir en seguridad y tener algo sólido y no estar posteriormente con problemas.

- Poseer los sistemas actualizados y utilizar software genuino: esto es fundamental debido a que se habló de las vulnerabilidades que pueden poseer los sistemas al no estar actualizados y también los riesgos de utilizar software pirata o que no es original, y es por ello que las empresas o usuarios deberán tener el cuidado de utilizar todos los sistemas originales así como actualizar los mismos para poder estar en todo momento garantizando un nivel mayor de seguridad en el sistema en desarrollo o desarrollado.

4.7. Consejos y recomendaciones para los usuarios que navegan en internet

Los usuarios conociendo las bondades de internet, siempre harán uso del mismo, por ello se sabe que ellos deciden que hacer y cómo hacerlo, pero para evitar caer en situaciones incomodas, se ha considerado una serie de consejos que deben tomar en cuenta, debido a que ellos son los responsables de lo que realicen.

- Utilizar siempre navegadores de confiabilidad, no todos los navegadores garantizan la seguridad de los usuarios, pero hay otros que velan por la

seguridad de los mismos y es por ello que se debe utilizar navegadores de proveedores confiables, así como los navegadores que estén en constate actualizaciones, eso habla de que los mismos siempre están buscando mejorar para que la experiencia de usuario sea la mejor, y no dejar al usuario en segundo plano.

- Si se va a utilizar un computador que no sea propiedad del usuario, lo más recomendable es navegar en modo incognito, es decir, que la mayoría de navegadores permiten la navegación de manera incógnita y la finalidad de la misma es no dejar rastro de lo que se realizó por parte del usuario a nivel local, es decir no se sabrá a que sitios accedió, ni nada de eso, debido a que de esa forma estará mejorando su navegación y no exponiendo su información que pueda quedar guardada si no se utiliza el modo incognito; tomando en cuenta también que la navegación en modo incognito implica no dejar rastro local como se comentó, sin embargo la empresa distribuidora de internet y los sitios a donde se accedió si saben del usuario que está haciendo uso, porque la comunicación existe, pero localmente es como si no hubiese pasado nada; esto ayuda muchas veces a que los usuarios que utilizan computadores de amigos o alquilan computadores temporalmente.

- Evitar guardar información en los navegadores de uso público, puede catalogarse de uso público el computador familiar, así como un computador de alquiler, esto debido a que lo utilizará más de una persona, y al guardar la información (los navegadores permiten guardar credenciales de acceso), cualquiera que utilice dichos navegadores, podrán hacer uso de estos credenciales de manera libre, es por ello que se recomendable si es computador para el hogar, tener usuarios

diferentes en los sistemas operativos, para poder tener los datos resguardados por usuario y no se comparta la información.

- Controlar a los más vulnerables en el hogar, los usuarios más vulnerables siempre serán los niños; esto ocurre mediante la falta de información y madurez de los mismos, siendo los niños las victimas más fáciles de manipular, mediante anuncios, y cosas llamativas, las cuales siempre serán algo novedoso para los niños, es por ello que los adultos deben supervisar siempre lo que los niños realizan cuando navegan por internet.

- No utilizar software pirata, este problema es el mayor fracaso del usuario, en su gran mayoría los usuarios hacen uso de software alterado, es decir con un comportamiento casi igual pero con cambios que pueden parecer imperceptible, que pueden generar problemas posteriores, los cuales llegan a resultar hasta en pérdida total de la información el usuario si se tratase del sistema pirata, pero si se utiliza juegos, aplicaciones interesantes con los denominados parches, los cuales sustituyen una licencia original por algo similar pero pudiendo estar afectando al usuario, porque puede estar robando información o simplemente teniendo algún tipo de beneficio por parte de la entidad encargada de la modificación de dicho software, es poco probable que las personas realicen el trabajo de hacer todos los cambios necesarios para que el usuario utilice de manera fraudulenta los programas no obtengan algún tipo de beneficio, es por eso que nunca es recomendable la piratería de software.

- Una frase encontrada en muchos sitios cita: “Cuando el producto es gratis, el producto eres tú”; muchas personas no terminan de comprender el trasfondo de esta frase, debido a que el ser humano por naturaleza se

ve atraído por todo lo que se le presente como libre o gratuito, es decir, siempre el proveedor del producto gratuito obtendrá de cualquier forma algún tipo de beneficio, por los usuarios es ignorado, y tal es el caso de las redes sociales, aparentemente son gratuitas, pero ¿En verdad lo son?, esta pregunta redunda por todos lados, y la respuesta lamentablemente para muchos es que no, no es gratuito, pero muchos usuarios defensivamente siempre tendrán algo que responder y será similar, que ellos nunca han realizado algún pago, y es más nunca se solicitó detalles bancarios o de tarjetas de crédito o débito para poder utilizar dicha red social o sitio web, pero hay algo que desconocen y es lo que siempre está pero todos ignoran conscientemente, y son las políticas de privacidad. Las políticas de privacidad amparan a las empresas que proveen productos gratuitos en utilizar todo tipo de información que ellos recaben de tal forma que es vital saber por parte del usuario que lo más valioso de un usuario en internet es su información, entonces ahora deberás pensar dos veces si en verdad es gratuito. Muchas empresas generan grandes cantidades de información, la cual pueden vender, y realizar todo tipo de pruebas o situaciones con la misma, debido a que el usuario en todo momento aceptó sin darse cuenta que su información fuese de uso público.

CONCLUSIONES

1. Al tomar en cuenta todas las medidas preventivas que se deben tener para navegar por internet, es notable que siempre existirá un factor muy elevado de que las amenazas estén y sean más fuertes, pero con dichas medidas se habrá logrado tener una barrera de protección elevada, la cual no podrá ser violada tan fácilmente.

2. Las personas tendrán mayor conciencia de los riesgos que existen en internet y por ello se sabe a lo que se exponen, pero teniendo las herramientas a la mano, el factor de fallo esta reducido grandemente.

3. Que los usuarios tengan la conciencia plena de que es mucho mejor y más barato prevenir que corregir, es decir, siempre será mejor protegerse, mantener el sistema actualizado y los dispositivos en óptimas condiciones para evitar todo este tipo de situaciones que corregir posterior a que el atacante haya logrado su objetivo.

4. Los mayores ataques a sistemas informáticos lograron generar pérdidas millonarias, debido a que con el pasar de los días las amenazas y/o atacantes siempre buscarán vulnerar de diferentes maneras, por ese motivo los sistemas siempre deben busca una mejora continua para garantizar al usuario una navegación segura.

RECOMENDACIONES

1. Para garantizar la máxima seguridad en un sistema informático es necesario tener conciencia de prevención, porque los desastres cibernéticos existen, y logran muchas veces notarse hasta que se tiene una medición exacta de lo que se perdió, de lo contrario las personas no toman las medidas necesarias.

2. Tomar en cuenta que al navegar siempre se está expuesto, pero siempre depende del usuario el permitir dejar las puertas abiertas a los atacantes o tenerlas cerradas para evitar todo este tipo de situaciones.

3. Es importante tener instalados los programas que garanticen una mayor seguridad, para proteger los archivos e información, porque es lo más preciado de una persona.

4. Visitar sitios que tengan certificados de seguridad y evitar acceder a los que no lo tengan, debido a que muchas veces estos sitios pueden parecer confiables pero no lo son, y peor aún, pueden ser sitios que suplanten los originales y sin darse cuenta se puede ser víctima de una estafa.

BIBLIOGRAFÍA

1. AGUDO, Sergio. *¿Por qué es importante HTTPS y qué implica no usarlo?* [en línea]. <https://www.genbeta.com/a-fondo/por-que-es-importante-https-y-que-implica-no-usarlo>. [Consulta: 15 de abril de 2019].

2. ARES SÁNCHEZ, Rubén. *Cuando el producto es gratis, el producto eres tú.* [en línea]. <https://blogs.deusto.es/master-informatica/cuando-el-producto-es-gratis-el-producto-eres-tu/>. [Consulta: 29 de marzo de 2019].

3. ARTEAGA, Sandra. *Los 10 peores ataques hacker de la historia.* [en línea]. <https://computerhoy.com/listas/tecnologia/10-peores-ataques-hacker-historia-277193>. [Consulta: 12 de febrero de 2019].

4. BAHILLO, Luis*. Historia del internet: ¿Cómo nació y cuál fue su evolución?* [en línea]. <https://marketing4ecommerce.net/historia-de-internet/>. [Consulta: 21 de noviembre de 2018].

5. BIRYUKOV, Vladislav. *5 amenazas que afectan el hardware.* [en línea]. <https://latam.kaspersky.com/blog/5-amenazas-que-afectan-el-hardware/5218/>. [Consulta: 10 de febrero de 2019].

6. CAD. *Historia del internet.* [en línea]. <http://www.cad.com.mx/historia_del_internet.htm>. [Consulta: 20 de noviembre de 2018].

7. CLULEY, Graham. *Evernote hackeado – casi 50 millones de contraseñas restablece después de fallo de seguridad.* [en línea]. <https://nakedsecurity.sophos.com/es/2013/03/02/evernote-hacked-almost-50-million-passwords-reset-after-security-breach/>. [Consulta: 11 de febrero de 2019].

8. COLLAZO, Andrea. *Como realizar compras seguras por internet.* [en línea]. <https://profesoradeinformatica.com/como-realizar-compras-seguras-por-internet/>. [Consulta: 29 de marzo de 2019].

9. DUARTE, Eugenio. *Las 12 amenazas más peligrosas en Internet.* [en línea]. <http://blog.capacityacademy.com/2012/06/21/las-12-amenazas-mas-peligrosas-en-internet/>. [Consulta: 10 de diciembre de 2018].

10. ESET Security. *11 errores de seguridad que probablemente sigues cometiendo.* [en línea]. <https://www.welivesecurity.com/la-es/2015/07/22/11-errores-de-seguridad-sigues-cometiendo/>. [Consulta: 1 de marzo de 2019].

11. GLOBALFINANZ. *Empresas expuestas a ataques informáticos y cibernéticos.* [en línea]. <https://www.responsabilidadconsejerosydirectivos.com/ataques-ciberneticos-en-las-empresas/>. [Consulta: 20 de diciembre de 2018].

12. INCIBE*. Amenazas vs Vulnerabilidad. ¿sabes en qué se diferencian?* [en línea]. <https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian>. [Consulta: 11 de diciembre de 2018].

13. Kaspersky*. Amenazas web | Malware de navegadores de Internet | Kaspersky Lab Es*. [en línea]. <https://www.kaspersky.es/resource-center/threats/web>. [Consulta: 10 de diciembre de 2018].

14. MARQUES, Luciana. *Mapa de los ataques cibernéticos en Latinoamérica 2018.* [en línea]. <https://blog.f-secure.com/es/mapa-de-los-ataques-ciberneticos-en-latinoamerica-2018/>. [Consulta: 19 de marzo de 2019].

15. MARTÍNEZ, Emmanuel. *7 de los ciberataques más famosos de la historia.* [en línea]. <http://www.icorp.com.mx/blog/ciberataques-mas-famosos/ >. [Consulta: 12 de febrero de 2019].

16. ReasonWhy*. Qué consecuencias puede tener un ciberataque para tu empresa.* [en línea]. <https://www.reasonwhy.es/actualidad/digital/que-consecuencias-puede-tener-un-ciberataque-para-tu-empresa-2017-05-15>. [Consulta: 12 de diciembre de 2018].

17. RODRÍGUEZ GARCÍA, Elías. *Los riesgos que corres al conectarte a una red Wi-Fi pública.* [en línea]. <https://omicrono.elespanol.com/2017/07/riesgos-redes-wifi-publicas-gratis/. [Consulta: 15 de abril de 2019].

18. SALDANA, Gustavo. *Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina.* [en línea]. <https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-ataques-ciberneticos-en-america-latina/13266/>. [Consulta: 19 de marzo de 2019].

19. SCHREIBER, Christian. *Cybersecurity Challenges for Latin America.* [en línea].<http://www.seguridadinternacional.es/?q=es/content/cybersecurity-challenges-latin-america>. [Consulta: 19 de marzo de 2019].

20. ZAHUMENSZKY, Carlos. *Así fueron los mayores ataques informáticos de la historia.* [en línea]. <https://es.gizmodo.com/los-10-mayores-ataques-informaticos-de-la-historia-1580249145>. [Consulta: 11 de febrero de 2019].