Incidentes informáticos y sus consecuencias en Colombia en los últimos 10 años

JAIR ANDRÉS GUERRERO GARZÓN

Universidad nacional abierta y a distancia - UNAD
Escuela de ciencias básicas, tecnología e ingeniería
Especialización en seguridad informática
Pitalito
2020

Incidentes informáticos y sus consecuencias en Colombia en los últimos 10 años

JAIR ANDRÉS GUERRERO GARZÓN

Monografía para oprta el título de
Especialista en Seguridad Informática

Ingeniero Gabriel Alberto Puerta Aponte
Asesor del Proyecto

Universidad nacional abierta y a distancia - UNAD
Escuela de ciencias básicas, tecnología e ingeniería Especialización en seguridad informática
Pitalito
2020

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado

Pitalito, Febrero 12 del 2020

Dedico esta monografía primero que todo a Dios, que es mi guía y fortaleza que me conforta y me brinda caminos hacia las oportunidades.

A mi familia que creyó en mí y me brindó su apoyo en todo momento.

Y a mis tutores, quienes con su enseñanza ayudaron a realizar este sueño de lograr ser un especialista en seguridad informática egresado de la Universidad Abierta y a Distancia.

Jair Andrés

AGRADECIMIENTOS

Agradezco a Dios por darme la fuerza y fortaleza de culminar esta nueva experiencia en mi formación académica y profesional.

Mi hija Ángel Sofia Guerrero Verdugo y a mi amada esposa Andrea Carolina Verdugo Benavides, que nuestros proyectos sigan creciendo y sigamos adelante a pesar de cualquier adversidad que se encuentre en nuestro camino.

Sinceros agradecimientos a mi familia en especial a mi Padre Segundo Guerrero y mi Madre Luz Marina Garzon, por brindarme la vida, y enseñarme que todo merito se puede lograr por esfuerzo propio, que solo necesitas esas personas que están cercanas y esperan triunfos de ti.

Completo agradecimiento al Ing. Gabriel Alberto Puerta Aponte por su guía, asesoramiento y sobre todo su paciencia; a los tutores, que con su conocimiento y vocación de igual forma agradecido con la Líder del programa de Especialización en Seguridad Informática la Ing. Sonia Ximena Moreno Molano, quienes me brindaron su apoyo incondicional, lo cual fue esencial para dar terminar mi monografía mis más sincero agradecimientos familia UNAD por hacer este sueño realidad.

CONTENIDO

LISTA DE IMÁGENES

Imagen 19: Cai Virtual 55

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

En los últimos tiempos y con la evolución de la tecnología, se habla contínuamente de procesos y procedimientos, basados en el ciclo deming PHVA, para establecer las responsibilidades y las respectivas auditorías, que permiten determinar la mayor evidencia fiable para hacer una medición a los incidentes cibernéticos, como uno del elemento que se han tenido en cuenta para dejar constancia del impacto que dejan en nuestra sociedad, abordando los temas de las delitos, modalidad y sector más afectado a lo de diez años.

La Universidad abierta a distancias UNAD es clave y relevante a la hora de ofrecer planes de estudios virtual a nivel nacional e internacional, lo que permite poder relacionarnos con diferentes tutores que tiene bastos conocimientos en todas las áreas de la informática y seguridad; áreas de gran envergadura e interés gracias a las nuevas tendencias de las tecnologías y campo en el cual se debe estar preparado para crear, prevenir y fortalecer nuestros conocimientos sobre la seguridad informática.

La presente monografía, se centra en dejar una relación de los incidentes informáticos que se han cometido en Colombia a lo largo de diez años, lo cual permite evaluar con certeza en que está fallando y pasando en el entorno a la seguridad informática en Colombia quienes son los más afectados y que sectores se ven seriamente perjudicados.

SUMMARY

In recent times and with the evolution of technology, processes and procedures, based on the PHVA deming cycle, are continually being discussed to establish the responsibilities and the respective audits, which allow determining the most reliable evidence to measure incidents. Cybernetics, as one of the elements that have been taken into account to record the impact they leave on our society, addressing the issues of crime, modality and sector most affected over ten years.

The University open at UNAD distances is key and relevant when offering virtual curricula at national and international level, which allows us to be able to relate to different tutors who have ample knowledge in all areas of computer science and security; Areas of great importance and interest thanks to the new trends in technologies and the field in which we must be prepared to create, prevent and strengthen our knowledge of computer security.

The present monograph, focuses on leaving a list of the computer incidents that have been committed in Colombia over ten years, which allows us to assess with certainty that it is failing and happening in the environment to computer security in Colombia who are the most affected and which sectors are seriously harmed.

INTRODUCCIÓN

La seguridad de la información ha desencadenado que se hable de diversos mecanismos para proteger la información de situaciones presentadas por terceros que puedan afectar la información valiosa o critica en nuestros sistemas informáticos, esta comienza por el individuo que la aplica. La norma ISO 27001, establece que la información es el activo fijo más importante en las empresas, pero sirve de base para salvagardar la información de las personas en los diferentes campos.

En lo referente a información, no se habla de accidentes, dado que no se desarrollan pérdidas humanas, pero sí la dignidad de las personas, es por ello que se identifica la necesidad de cada día mejorar la seguridad de los datos, la seguridad de la información relacionada con cada persona, sin embargo, cada instante se crean nuevas formas de quebrantar la seguridad, y de la misma manera las vulnerabilidades son mayores, una de ellas tienen mayor demanda las versiones libres que las poseen un valor, así no se posean las mismas características.

La revista infodir describe los principios fundamentales de la seguridad informática como principio de menor privilegio, la seguridad no se obtiene a través de la oscuridad, principio del eslabón más débil, defensa en profundidad, punto de control centralizado, seguridad en caso de fallo, participación universal y simplicidad. [1]. En ello, la posibilidad y oportunidad de realizar algún incidente,

[1] Heinekn Team, revista de información a directivos:Principios fundamentales de la Seguridad Informática

depende de la seguridad y la política en el sistema de seguridad de la información establecida para ello.

De acuerdo a un artículo publicado en welivesecurity “Los avances tecnológicos están progresando a pasos agigantados para ir a la vanguardia de las necesidades humanas, permitiendo así que las empresas puedan mejorar productivamente y mirar más posibilidades en el mercado tanto nacional como mundial, esto se ha logrado gracias a que ahora podemos comunicarnos entre redes y trabajar con ellas agiliza muchos procesos que le dan ventaja a una empresa”[2] , pero a pesar de los beneficios que trae la tecnología y sus novedosos inventos, hay amenazas que pueden llegar a afectar de manera leve o muy drástica a una empresa y la problemática radica en que gracias a las grandes oportunidades que traen las herramientas tecnológicas, hay compañías inescrupulosas que se dedican a aprovechar que personas ingenuas o incautas desconocen las trampas virtuales para robar o Hackear información que pueda perjudicar a la empresa, por esto se debe conocer los recursos se deben obtener para traer mayor seguridad en los sistemas informáticos, de acuerdo a lo recomendado por el especialista en seguridad informática Camilo Gutiérrez Amaya, el columnista del periódico El Espectador, Santiago la Rotta realizó un resumen detallado de las “amenazas de seguridad informática de las que se debe cuidar”[3], si bien, es claro en mencionar que la causas de ataques informáticos son el uso de equipos electrónicos sin debida cautela, nos aclara que básicamente los delitos informáticos suceden en

(http://www.sld.cu/sitios/infodir/temas.php?idv=1346).

[2] AMAYA GUTIERREZ, Camilo, "mportancia de la gestión de incidentes para la seguridad de la información". WeLiveSecurity by ESET.(https://www.welivesecurity.com/la-es/2013/01/07/importancia-gestion-incidentes-seguridad-informacion/)

[3] ROTTA, Santiago. Estas son las amenazas de seguridad informática de las que se debe cuidar. En: El espectador, Bogotá, 18, febrero,2016.

Colombia por que los habitantes de este país en su mayoría creen que este tipo de delitos suceden en el continente Asiático , Europeo y solo Norteamérica.

La seguridad informática está encargada de diseñar normas, métodos, técnicas y procedimientos, que permitan establecer en un individuo o empresa estándares de seguridad para el procesamiento de datos, es por ello, que de acuerdo a la investigación realizada dentro del marco de esta monografía, se puede evidenciar, que en los últimos diez años, Colombia ha sufrido una gran serie de cambios en el ámbito tecnológico que han impulsado la economía y en la redacción e implementación de normatividad que apoya la protección de los datos.

Con el crecimiento tecnológico e informático en el país y las múltiples denuncias presentadas en el ámbito de robo por medios tecnológicos, como se indica en el CaI virtual de la Policía Nacional de Colombia, herramienta de la Policía que viene funcionando desde el 2006, en Colombia a partir del 2009 se empezó a reglamentar que los delitos informáticos eran causal de multas y prisión, lo que ha ayudado en gran parte a investigar y mitigar este flagelo.

1. DEFINICIÓN DEL PROBLEMA

1.1 DEFINICIÓN DEL PROBLEMA

Al investigar los delitos informáticos en Colombia, se evidencia con información digital y acontecimientos esporádicos, los cuales no se conoce los tipos de delitos cometidos y solo quedan como noticia, lo cual genera que no sea reportado debidamente a las autoridades para que se tomen acciones al respecto.

Los incidentes informáticos, van a la vanguardia de la innovación tecnológica, tienen un modus operandi de técnicas, que permiten desarrollar y emplear funciones para cometer delitos informáticos tanto a personas como empresas, la efectividad de los delitos informáticos, se ve fundamentada básicamente en el bajo conocimiento de seguridad y confianza que tienen los operadores de dispositivos electrónicos, en lo cual el cibercrimen ha encontrado un nicho de negocio basto para explotar, para evitar que el ciudadano y empresas Colombianas se vean afectadas por este tipo de incidentes se recrea el escenario perfecto para presentar un estudio de los incidentes informáticos que se han presentado a lo largo de los últimos 10 años, obteniendo una información fiable a la hora saber que delitos se comete en Colombia, la modalidad y que sectores se ven afectados, tal como recalca la sabia frase del filósofo español Jorge Agustín Nicolás Ruiz de Santayana "Quién olvida su historia está condenado a repetirla"[4]

[4] GARCIA, Marcia. International Youth Coalition. 31,JULIO.2015. (https://iycoalition.org/quien-olvida-su-historia-esta-condenado-a-repetirla/)

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuáles son Incidentes informáticos en Colombia registrados en los últimos 10 años y que consecuencias tienen?

La amplificación de los efectos de la información por el uso de las nuevas tecnologías comporta un incremento paalelo de las oportunidades para su violación, con escasa o nula posibilidad de hacer revesible el daño causado y grandedificultades probatorias, que demanda un sistema de prevención real y efectivo.[5] En ello las definiciones solamente son entendidas por personas con conocimiento del ámbito de la tecnología, en ello se encuentran tres definiciones ataques informáticos, ciberataques y ciberdelincuentes, que aunque suenen similares, denotan caracteristicas diferenciales, la definición es relativamente nueva para aquellas personas que están entrando a la nueva era digital tratando de estar a la vanguardia tecnológica e informática.

Utilizando la herramienta Google trends, se obtuvo un promedio de búsqueda de los siguientes conceptos ciberdelincuencia, ciberataque y ataques informáticos desde el 1 de enero de 2010 al mes de noviembre de 2019; la relación de búsqueda en donce se evidencia, la necesidad de relacionar los riesgos de manera equitativa a nivel mundial, desarrollando y aplicando los protocolos de seguridad en todos los niveles de la información.

Tabla 1: Búsqueda de conceptos en google

Año	Ciberdelincuencia	Ciberataque	Ataques informáticos
2010	8	0	71

[5] Molina, M. J. M. (2000). *Seguridad de la información. criptología*. Retrieved from https://bv.unir.net:2056

Año	Ciberdelincuencia	Ciberataque	Ataques informáticos
2011	14	10	50
2012	12	7	41
2013	25	14	41
2014	13	9	29
2015	16	21	38
2016	19	17	35
2017	14	148	36
2018	17	31	35
2019	25	30	38
Total	163	287	414
Total, porcentual	19%	33%	48%

Fuente: elaboración propia - Goole trends - 2019

En donde las 5 regiones del pais que realizaron la búsqueda son en su orden Bogotá, Huila, Magdalena, César y Santander; y la palabra más buscada es ciberataque. Esto conlleva a las premisas de suponer, ¿la Capital de Colombia, por su congruencia nacional de empresas nacionales e internacionales, entidades estatales, es la ciudad más propensa a estos ataques, pero Medellín, al ser una ciudad tan mundialmente famosa y premiada, porque no aparece en la lista?, la respuesta es la seguridad y la innovación implementada en cada localidad antes mencionada.

La innovación siempre viene para ser adquirida a escalas de seguridad, a mayor nivel de seguridad, mayor estudios se realizan para obtener ese valor en el mercado y mayores las garantías de cada producto creado o innovado, como lo indica la revista Dinero en su columna del cibercrimen “Ya no se trata de aventuras individuales de un hacker, si no de bandas internacionales muy organizadas y poderosas”[6], lo que indica claramente que en Colombia se ve la necesidad de

[6] REVISTA DINERO. 02,02,2017. El apetitoso negocio del cibercrimen. (https://www.dinero.com/edicion-

asegurar los activos informáticos individuales o colectivos para prevenir ser atacado por una organización del cibercrimen, se debe aclarar que de esta forma la seguridad cuesta, y en ello según la prioridades que requiera se debe adquirir las herramientas necesarias para combatir la amenaza de un ataque informático con apoyo de estas herramientas, sin conocer de prevención informática; al analizar el panorama actual de amenazas, todas las personas que están en constante contacto con tecnología en el mundo, están expuestas a que nos suceda un ataque de virus informático especifico por la cantidad y variedad que hoy en día existe, queda claro que este es un problema que afecta a todas las personas, sin depender de su estratificación social y nivel de educación. Colombia, no es la excepción, el desconocimiento de medidas de seguridad, la necesidad de propender la enseñanza de la seguridad informática, la ineficacia de los controles de seguridad en empresas y hogares así como lo indica la publicación del articulo realizado por la revista dinero, “A pesar de quedar expuestas al secuestro de datos, fraude y otro tipo de delitos, las empresas colombianas aún siguen dejando de lado el tema de la seguridad informática”[7], lo que indica que el Colombiano promedio suele pensar, que nadie está expuesto a un cibercrimen y que vulneren sus derechos, pero en cierta manera, la realidad es que se confía de más en las nuevas tecnologías y esta confianza puede ser la excusa perfecta para que un ciberdelincunte pueda lograr su cometido.

El ciberdelito es rentable ya que se apropia de todo tipo información, tal como lo afirma Tecnosfera en una columna del periódico el Tiempo "Lo que buscan los criminales es obtener la mayor cantidad de usuarios infectados y a partir de eso

impresa/tecnologia/articulo/las-cifras-que-mueven-el-cibercrimen-a-nivel-global/241593)

[7] REVISTA DINERO. 02,02,2017. El apetitoso negocio del cibercrimen. (https://www.dinero.com/edicion-impresa/tecnologia/articulo/las-cifras-que-mueven-el-cibercrimen-a-nivel-global/241593)

mirar cuáles pagan para obtener una ganancia económica. Claro, las empresas son un blanco interesante porque por la información que manejan, existe mayor posibilidad de que efectúen el pago"[8] y para descubrir este infiltración o infección se debe poseer un cierto nivel de conocimiento del mundo de informática y tecnología, y conocer para que sirve la información.

Mientras en el mundo se conoce y se realiza la búsqueda de los términos ataque informáticos, el término ciberataque fue buscado en Google desde el mes de febrero 2008 y el término ciberdelincuencia desde el mes de mayo de 2009 (datos corroborados en Google trends). Colombia, en donde los niveles de inversión en seguridad informática crecen aceleradamente, al igual que la normatividad que las rige y las leyes de vulnerar la seguridad informática así lo ratifica la sección nación entregado por la revista Semana "Colombia tampoco estuvo libre de los grandes ataques cibernéticos a nivel mundial. Este año, el WannaCry, un malware que secuestraba los datos de los dispositivos que atacaba, afectó a más de 150 países y se convirtió en uno de los asaltos más famosos en la historia de la red. En Colombia, la Policía atendió a 52 víctimas de estos ataques globales y generó 59 alertas por posibles amenazas internacionales"[9].

Por todas estas modalidades del cibercrimen, las autoridades capturaron a 459 personas durante 2017 y desmantelaron 30 organizaciones dedicadas a estos delitos. Pero también le están apuntando a la prevención. En el año fueron capacitadas 1.192 personas en la materia, y las campañas adelantadas, según la

[8] EL TIEMPO, 28,06,2017. Tecnosfera. www.eltiempo.com. (https://www.eltiempo.com/tecnosfera/novedades-tecnologia/las-razones-por-las-que-el-secuestro-de-datos-se-esta-popularizando-103528)

[9] SEMANA, 28,12,2017. El cibercrimen en 2017: la amenaza crece sobre Colombia. Www.semana.com.co. (https://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2017/551979).

DIJÍN, habrían alcanzado a 3,6 millones de personas"[10]. Con ello se puede evidenciar la falta de prevención del ciudadano y la necesidad que tiene el país en invertir en capacitación a las empresas en el ámbito de seguridad informática, para minimizar al máximo los riesgos a los activos informáticos en las organizaciones.

1.3 OBJETIVOS

1.3.1 Objetivo general

Identificar los incidentes informáticos registrados en Colombia en la última década.

1.3.2 Objetivos específicos

a. Gestionar Recolectar información relacionada con la tipificación de delitos informáticos.

b. Identificar la repercusión de los incidentes informáticos bajo la aplicación de la normatividad Colombiana en lo referente a seguridad informática.

c. Mitigar los riesgos de seguridad, mediante la entrega de recomendaciones

1.4 JUSTIFICACIÓN

La necesidad de seguridad en todos los aspectos de la vida diaria es intrínseca de todos los seres humanos, la naturaleza al defenderse propende su existencia; este principio se aplica en cierta medida en la información que guardamos en las aplicaciones electrónicas, es así como la aplicación correo electrónico se ha vuelto

[10] SEMANA, 28,12,2017. El cibercrimen en 2017: la amenaza crece sobre Colombia. Www.semana.com.co. (https://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2017/551979)

parte fundamental de innovación en el entorno de la comunicación laboral, varios sitios de seguridad informática respaldan dicha afirmación, tal es el caso de B'Secure que ratifica "El correo electrónico es posiblemente la herramienta de trabajo más usada y una de las más importantes para las empresas debido a los múltiples beneficios que trae la comunicación por este medio"[11], es por ello que las empresas necesitan mayor seguridad ante las posibles amenazas que puedan acarrear el hecho de recibir archivos de información maliciosa.

Es por ello que se pretende dar a conocer las diferentes formas como se podrían llegar a desarrollar los incidentes informáticos, ayudaría a establecer protocolos de vigilancia y control, protocolos de concientización en el uso y/o abuso de estos, aprender que la seguridad tiene un valor, que cada día se incrementa este es un objetivo principal.

En Colombia, el 69% de las personas invierten más de $ 750.000 en la adquisión de equipos electrónicos y de ellos el 41%, lo cambian en menos de un año; el uso con más de 60% de popularidad es pago de productos, transferencias de dineo, estudio, streaming de series o películas[12]. Con ello, al hablar de delitos informáticos, se puede evidenciar más las personas están al alcance de elementos tecnológicos que permiten la comunicación y facilitan los trabajos, por consiguiente en Colombia las personas y las empresas están empezando a llevar información valiosa en los programas que la nueva tecnología nos proporciona, pero de una manera no segura, por la confianza que la persona deposita en el medio

[11] B´SECURE. Pasión por la seguridad. S.f. Protección de correo electrónico. www.b-secure.co. (https://www.b-secure.co/estrategias/infraestructura/proteccion-de-correo-electronico)

[12] NEIRA MARCIALES, Laura. 28,08,2019. Cinco de cada 10 colombianos cambian el celular cada dos años. LA REPÚBLICA. Www.larepublica.com.co. (https://www.larepublica.co/empresas/cinco-de-cada-10-colombianos-cambian-el-celular-cada-dos-anos-2902128)

informático sin tocar las debidas precauciones de seguridad informática, tal vez por desconocimiento del área o por no asumir gastos o costos en la implementación de un programa de seguridad. Ahora bien, ¿cómo determinar cuando una persona o empresa está sufriendo un delito informático, un ataque o incidente?. Los términos, aúnque parezcan iguales, poseen diferencias; un delito informático según el convenio sobre la ciberdelincuencia del Consejo de Europa, suscrito en Budapest, el 23 de noviembre de 2001, son los actos que pongan en peligro la confidencialidad, la integridad, y la disponibilidad de los sistemas, redes, y datos informáticos, así como el abuso de dichos sistemas redes y datos garantizando la tipificación como delito de dichos actos[13].

El ataque informático, se encuentra bastante contenido al respecto en la web, uno de los conceptos más claros para comprender el tema se explica en el blog Consulthink por parte de la ingeniera Lucia D'Adamo, la cual expresa: “Un ataque informático se puede describir como una actividad hostil contra un sistema, un instrumento, una aplicación o un elemento que tenga un componente informático. Es una actividad que aspira a conseguir un beneficio para el atacante a costa del atacado. Existen diferentes tipologías de ataque informático que dependen de los objetivos que se quieren alcanzar, de los escenarios tecnológicos y de contexto.”[14] lo que lleva a concluir, son aquellos causados únicamente por medios que la tenologia moderna brinda, en donde se pretende adquirir un bien por medio de hurto de la información, para apoyar la veracidad del anterior concepto, los incidentes informáticos con forme a gestión de incidentes de seguridad de la

[13] CONVENIO SOBRE LA CIBERDELINCUENCIA. (23, OCTUBRE, 2001: Budapest, Hungría). Serie de tratados Europeos. 26 p. (https://www.oas.org/juridico/english/cyb_pry_convenio.pdf)

[14] D´ADAMO, Lucia. Qué es y en qué consiste un ataque informático {En línea}.{18 de julio de 2017} disponible en : (https://www.consulthink.it/es/que-es-y-en-que-consiste-un-ataque-informatico/).

información son indicados por un único o una serie de eventos indeseados o inesperados de seguridad de la información que tiene una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información[15].

El término de seguridad informática, las comunicaciones son el punto estratégico, un punto de acceso, puede generar la destrucción total de la información sensitiva, Andrés Valcárcel, manifestó en la Universidad Santiago de Cali, en el desarrollo del II Simposio Nacional e Internacional de Delitos Informáticos “Dejen de publicar todo lo que tienen y todo lo que hacen, es el punto de partida para la delincuencia digital”[16], con lo cual se aclara que cualquier persona puede ser víctima en la intromisión de sus datos. En el año de 1985, Nidia Callegari publicó el artículo “Oficina eficiente”, en donde expresa en unos de sus apartes, “a medida que se generaliza el uso de la informática se tipifican una serie de delitos cometidos en esta área, los cuales no se hayan contemplados en nuestro régimen penal vigente”[17], han pasado tres décadas, en lass cuales la normatividad impone graves penas a quienes las incumplan, pero estas nacieron después de suscitados hechos, donde la pérdida de información es creciente.

El desarrollo de la presente monografía pretende recopilar información sobre los distintos tipos de incidentes informáticos y analizar su funcionamiento de intrusión para luego poner en conocimiento su impacto en nuestro sistema, como disminuir

---

[15] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. GTC-ISO/IEC 27035. Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Bogotá. ICONTEC. 2012

[16] LARRAHONDO, Daniela. Delitos informáticos, una amenaza creciente. {En línea}. { 8 de noviembre de 2017} disponible en: (https://www.usc.edu.co/index.php/noticias/item/3693-delitos-informaticos-una-amenaza-creciente)

17 CALLEGARI, Nidia. Delitos informáticos y legislación. {En línea}. Septiembre - Octubre, 1985. Disponible en: (https://revistas.upb.edu.co/index.php/derecho/article/viewFile/6054/5551)

y mitigar este tipo de incidencia.

Al tener conocimiento en las formas de cómo se realiza los incidentes informáticos se asegura que haya una implementación en materia de seguridad y la creación de plan de seguridad, lo cual tiene un mayor impacto a contrarrestar y disminuir el daño a los cuales está expuesta una persona u organización cada día, esta afirmación se respalda con el informe de amenazas del Cibercrimen en Colombia 2016-2017, entregado por la Policía Nacional en la cual se aclara: " La transnacionalización del delito y los nuevos escenarios determinados por los procesos de globalización, plantean nuevos desafíos en materia de seguridad digital que generan la necesidad de implementar y desarrollar de estrategias bajo el principio de corresponsabilidad con el ánimo de hacer frente a los requerimientos nacionales y globales que enfrentamos"[18]. La seguridad de los sistemas de información, es costosa y reglamentaria, depende de dos factores importantes: El conocimiento de las personas en pretender la seguridad de los datos y el reconocimiento de las empresas en salvaguardar los datos de las personas, como valor agregado a sus servicios orecidos.

[18] Centro Cibernético Policial. Amenaza del Ciberrimen en Colombia 2016 -2017. Policía Nacional de Colombia. (https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf)

2. MARCO REFERENCIAL

2.1 MARCO TEÓRICO

El uso de equipos electrónicos se ha convertido en un problema social, y al hablarse del tema, se convierte en un riego psicosocial, en ello los jóvenes en Colombia son más propensos a ser víctimas de delitos en internet , los riesgos que conllevan al estar a merced de la tecnología, es un debededebemos preocuparnos de los sistemas de seguridad para los usuarios, clientes y personas se deber colectivo medir las consecuencias contra este tipo de acciones que se realizan. Aunado a ello, la tipificación de los delitos informáticos, encarna la relación entre normatividad y realidad de aplicación de las mismas y la tramitología a aplicar. En ello, ¿Qué es un delito informático?.

Se detalla definición de phising, como aquella en donde se suplanta la identidad del sujeto (llámese personas o empresas), con el propósito de menoscabar el buen nombre de la persona o apoderarse de su bienes y/o capital. La información es recolestada mediante mensajes de email o al celular.

En Colombia, la primera ley que se debe aplicar y concientizar a las empresas, es la ley 1581 de 2012, protección de datos personales, entendiendo como dato personal, cualquier información vinculada o que puede asociarse a una o varias personas naturales que, dependiendo de su grado de utilización y acercamiento con la intimidad de las prsonas podrá ser pública, semiprivada o privada. Sumado a ello, el registro Nacional para la Base de Datos, reglamentado por el Decreto Nacional 886 de 2014, en donde enfatiza “Serán objeto de inscripción en el Registro Nacional de Bases de Datos, las bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al Responsable del Tratamiento o al Encargado

del Tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales”[19].

Los delitos informáticos, “se entiende como toda acción culpable realizada por un ser humano que cause un perjuicio a personas sin que necesariamente se beneficie el autoro que por el contrario produzca un beneficio ilícito a su autoraunque no perjudique en forma directa o indirecta a la víctima. Actitudes ilícitas en qe se tiene a las computadoras como instrumentos o fin. Cualquier compartamiento criminal en que la computadora está involucrada como material objeto de medio”[20]. En ello, cada persona poseedora de un equipo electrónico, es la responsable del manejo y utilización del mismo, de las publicaciones en las redes.

Édison Raúl Serrano Buitrago , en su ensayo “ La práctica de delitos informáticos en Colombia” afirma que “con el desarrollo e implementación de la programación y el internet, los delitos se han vuelto frecuentes y han tenido un nivel sofisticado”[21], esto implica que su detección sea más difícil y con ello comprobar que no existe la seguridad completa, dado que cuando se presenta un incidente informático, el usuario toma medidas para contrarrestar esta amenaza dado que al mismo tiempo este método deja de ser efectivo ya que el ciberdelincuente cambia la estructura y forma de ataque dando la probabilidad de una nueva intrusión.

---

[19] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. Decreto 886 (13 de mayo de 2014). Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos. Bogotá, El Ministerio, 2014.

[20] García, de la Cruz, Juan Manuel. Delitos informáticos, El Cid Editor | apuntes, 2009. ProQuest Ebook Central, https://bv.unir.net:2056/lib/univunirsp/detail.action?docID=3180494.

[21] SERRANO BUITRAGO, Edison Raul. La práctica de los delitos informáticos en Colombia. Universidad Militar Nueva Granada. Bogotá, 2014. 26 p.

En la defición del Modelo Ontológico de los Ciberdelitos: Caso de estudio Colombia, determina los tipos de ataque y la tipificidad en el código penal; compuestos así:

- Los ciberataques, se desglosan el acceso físico, interceptación de comunicaciones, denegación de servicio, intrusiones, ingeniería social y puertas trampa.

- Los delitos informáticos, se definen delitos como delitos contra la conficencialidad y atentados informáticos.

Si bien, la normatividad Colombiana, posee grandes vacios, por el desconocimiento y la falta de instrumentalización física y electrónica en el mismo campo, es necesario comenzar la documentación y la aplicabilidad rigurosa de la ley.

El convenio sobre ciberdelincuencia (Computer Forensic, 2015) , del primero de noviembre de 2001 celebrado en Budapest, los divide en 4 grupos:

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de delitos.

Ciberdelincuencia del Consejo de Europa" que incluye, entre otros aspectos, las medidas que se deben tomar en casos de:

- Difusión de material xenófobo o racista.
- Insultos o amenazas con motivación racista o xenófoba.
- Negociación, minimización burda, aprobación o justificación del genocidio o

de crímenes contra la humanidad.

Clasificación

Dentro de las acciones legales en contra de los ciberdelincuentes existe dos categorías de crímenes los cuales tiene como finalidad:

1- Con fin u objetivo: Los incidentes informáticos que tiene como objetivo deshabilitar, modificar o eliminar servicios informáticos ejemplo, ataques masivos a servidores de internet, creación de virus, spam.

2- Como instrumento o medio: crímenes que se efectúan atreves de computadores e internet ejemplo espionaje, fraude y robo entre otros.

3- Colombia es uno de los 7 países que están penalizando los delitos informáticos, esto permite que los habitantes de Colombia y usuarios de tecnologías informáticas en el país puedan hacer valer sus derechos si se llegan a ver vulnerados en cuanto a carácter informático según la ley 1273 de 2009.

4- Las estafas que realizan los ciberdelincuentes siempre van a estar presentes y a la vanguardia tecnológica, hay que ser precavido, leer más sobre este tipo de fraudes y sobre todo ayudar a la ciudadanía en general haciéndoles saber que este tipo de delitos existen y que no caigan fácilmente en ellos.

5- En Colombia se entiende como delito informático todo aquello que atente contra los sistemas informáticos, de comunicaciones y entre otras disposiciones relacionadas que perjudiquen información y datos personales o de entidades (empresas, industrias entre otras), con forme a la ley 1273 de 2009, los delitos informáticos que se relacionen con los siguientes artículos, son causales de prisión de hasta 120 meses y multas de hasta 1000 salarios mínimos legales vigentes:

- Artículo 269A: Acceso abusivo a un sistema informático

- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación
- Artículo 269C: Interceptación de datos informáticos
- Artículo 269D: Daño informático
- Artículo 269E: Uso de software malicioso
- Artículo 269F: Violación de datos personales
- Artículo 269G: Suplantación de sitios web para capturar datos personales
- Artículo 269H: Circunstancias de agravación punitiva
- Artículo 269I: Hurto por medios informáticos y semejantes
- Artículo 269J: Transferencia no consentida de activos

6- La Ley 1273 de 2009 es necesaria por la cantidad de tecnología que contiene información para los usuarios en Colombia ya que gracias a esta se puede clasificar las actividades criminales informáticas que se relacionan en el acceso sin autorización a las bases de datos o información de un sistema, esta ley pretende proteger los bienes informáticos.

7- Además de la anterior ley también está la ley 1341 del 2009 por la cual se definen los principios y conceptos sobre la sociedad de la información y organización de las tecnologías de la información y las comunicaciones TIC, en la cual se puede destacar lo siguiente:

- Elimino la clasificación de servicios públicos domiciliarios y no domiciliarios
- Conservo el carácter de servicio público de los servicios de Telecomunicaciones.

- Consagro el principio de neutralidad Tecnológica

Consagro el principio de los derechos de los usuarios

2.2 MARCO CONCEPTUAL

Es necesario reconocer las diferentes características de las definiciones de seguridad informática, y sus aspectos diferenciadores. En ello el consejo Nacional de Política Económica y Social, perteneciente al Departamento Nacional de Planeación - DNP- junto al Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC -, Ministerio de Defensa Nacional Dirección Nacional de Inteligencia; implementaron el 11 de abril de 2016 el documento CONPES 3854, articulado con el CONPES 3701, en donde el objetivo fundamental es fortalecer las capacidades del estado para enfrentar las amenazas que atentan contra la defensa y seguridad nacional en el ámbit cibernético; con tres objetivos específicos[22]:

1. Implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional.

2. Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad.

3. Fortalecer la legislación en materia de ciberseguridad y ciberdefensa, la cooperación internacional y adelantar la adhesión de Colombia a los

[22] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. CONPES 3854 (11 de abril de 2016). Política Nacional de Seguridad Digital. Bogotá, El Ministerio, 2016

diferentes instrumentos internacionales en esta temática.

La Organización para la Cooperación y Desarrollo Económico, institución que tiene como objetivo objetivo principal promover políticas para mejorar el bienestar social, cooperar para responder a los desafíos económicos, sociales, medioambientales y de buen gobierno, los desafíos acentuados con la globalización y a su vez aprovechar mejor las oportunidades que surgen de la misma. Más en concreto los objetivos de la OCDE son los siguientes[23]:

- Lograr la más fuerte expansión posible de la economía y del empleo, y aumentar el nivel de vida en los países miembros, manteniendo la estabilidad financiera y contribuyendo así al desarrollo de la economía mundial.
- Contribuir a una sana expansión económica en los países miembros y en los no miembros en vías de desarrollo.
- Contribuir a la expansión del comercio internacional.

Determidas los objetivos de la OCDE, los pilares fundamentales en términos son:

1. Riesgo: es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.

2. Riesgo de seguridad digital: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad

[23] MINISTERIO DE ASUNTOS EXTERIORES , UNIÓN EUROPEA Y COOPERACIÓN. ¿Qué es la OCDE?. {En línea}. {11 de diciembre de 2018}. (http://www.exteriores.gob.es/RepresentacionesPermanentes/OCDE/es/quees2/Paginas/default.aspx)

territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan.

3. Gestión de riesgos de seguridad digital: es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

La OCDE propone los siguientes principios generales:

- Conocimiento, capacidades y empoderamiento: las múltiples partes interesadas deben entender los riesgos de seguridad digital. Deben ser conscientes de que el riesgo de seguridad digital puede afectar el logro de sus objetivos económicos y sociales, y el de otros. Deben estar educados al respecto, poseer las habilidades necesarias para entender el riesgo, administrarlo y evaluar su impacto.

- Responsabilidad: las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales.

- Derechos humanos y valores fundamentales: las múltiples partes interesadas deben gestionar los riesgos de seguridad digital de manera transparente y compatible con los derechos humanos y los valores fundamentales. La implementación de la gestión de riesgos de seguridad digital debe ser compatible con la libertad de expresión, el libre flujo de la información, la confidencialidad de la información, la protección de la privacidad y los datos personales. Las organizaciones deben tener una política general de transparencia acerca de sus prácticas y procedimientos para la gestión de riesgos de seguridad digital.

- Cooperación: las múltiples partes interesadas deben cooperar, incluso más allá de sus fronteras, a nivel regional e internacional.

A continuación, los principios operativos recomendados por la OCDE:

- Evaluación de riesgos y ciclo de tratamiento: la evaluación de riesgos debe llevarse a cabo de manera sistemática y continua, evaluando las posibles consecuencias de las amenazas y las vulnerabilidades digitales en las actividades económicas y sociales en juego. El tratamiento del riesgo debería tener como objetivo reducir el riesgo a un nivel aceptable en relación con los beneficios económicos y sociales.

- Medidas de seguridad: los líderes y tomadores de decisiones deben asegurarse de que las medidas de seguridad sean apropiadas y proporcionales al riesgo, y deben tener en cuenta su potencial impacto, negativo o positivo, sobre las actividades económicas y sociales que tienen por objeto proteger. La evaluación de riesgos de seguridad digital debe guiar la selección, operación y mejora de las medidas de seguridad para reducir el riesgo a niveles aceptables.

- Innovación: los líderes y tomadores de decisiones deben asegurarse de que

la innovación sea considerada como parte integral de la reducción del riesgo de seguridad digital. Esta debe fomentarse tanto en el diseño y funcionamiento de la economía, y de las actividades sociales basadas en el entorno digital, como en el diseño y el desarrollo de las medidas de seguridad. Preparación y continuidad: con el fin de reducir los efectos adversos de los incidentes de seguridad, y apoyar la continuidad y la capacidad de recuperación de las actividades económicas y sociales, deben adoptarse preparaciones y planes de continuidad. El plan debe identificar las medidas para prevenir, detectar, responder y recuperarse de los incidentes y proporcionar mecanismos claros de escalamiento.

Así mismo, en Colombia la Norma Técnica Colombiana NTC-ISO-IEC 27001 Tecnología de la información, Técnicas de seguridad, Sistemas de Gestión de la seguridad de la Información, la cual especifica requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. La presente Norma incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización[24], determina los siguientes conceptos:

- Análisis de riesgo: uso sistemático de la información para identificar las fuentes y estimar el riesgo.

- Confidencialidad: propiedad que determina que la información no esté

[24] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. NTC-ISO/IEC 27001. Tecnología de la información, Técnicas de seguridad, Sistemas de Gestión de la seguridad de la Información. Requisitos. Bogotá. ICONTEC. 2013

disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- Declaración de aplicabilidad: documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.

- Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

- Evaluación del riesgo: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

- Evento de seguridad de la información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

- Incidente de seguridad de la información: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.

- Sistema de gestión de la seguridad de la información SGSI: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

- Tratamiento del riesgo: proceso de selección e implementación de medidas para modificar el riesgo.

- Valoración del riesgo: proceso global de análisis y evaluación del riesgo

2.3 ANTECEDENTES

El ser humano está utilizando la tecnología desde la primaria infancia, los niños aprenden a manipular un equipo electrónico, pero no saben por qué y para qué sirve, los padres a veces de manera involuntaria crean la necesidad de un vínculo adictivo de los infantes hacia los aparatos tecnológicos ya que optan muchas veces a estos medios tecnológicos para entretenerlos y ocuparlos, de esa manera se comienzan los riesgos en la casa; cuentas de Facebook en menores de 10 años debería ser prohibido y normalizado, la pregunta es ¿Cómo logarlo?. La deficiente infraestructura en América Latina, crean la inquietante posibilidad de intromisión en las comunicaciones, en ello la afectación de los sistemas informáticos, crece a cada instante y se desarrollan habilidades para el manejo y la intrusión, su víctima puede ser individuos, instituciones, gobiernos, empresas, personas hasta incluso países con el fin de ver, modificar y eliminar la información, En un artículo de información general publicado por el Banco BBVA se enfatiza que los ciberdelincuentes ven más atractivo los países latinos por débil seguridad informática, escribiendo lo siguiente: “Estos delincuentes han ampliado el negocio a América Latina porque ven que las infraestructuras son deficientes o inexistentes y las entidades normalmente actúan de manera reactiva, con lo cual los esfuerzos preventivos son escasos. Además, existe una gran capacidad de inventiva y creatividad (en el sentido negativo) que provoca mucho daño al cliente de banca”, (BBVA, 2017), con ello se pretende ayudar a las demás empresas a encaminarse en el tema de seguridad informática , ya que la plataforma de BBVA es robusta y es una empresa ejemplo a nivel mundial en seguridad de la información de sus

clientes.

El foro de gobernanza en internet en el 2003 en Ginebra y 2005 en Túnez, describe la diferencia entre derecho informático, informática jurídica, derecho de la informática, da a cada término la definición concreta para evitarnos confusiones, “Si bien es difícil dar una definición de la informática jurídica, como suele suceder con las disciplinas de reciente surgimiento, cabe decir que se trata, en última instancia, de la utilización de las computadoras en el ámbito jurídico y el derecho informático es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática)[25]. En la cumbre mundial de información de Ginebra en el 2003, establecen como partes interesadas a los gobiernos, sector privado y sociedad civil de estas formas todas las partes interesadas son los directamente responsables de su protección[26].

Sin embargo, al hablar de delitos informáticos en Latinoamérica se toma como referencia la legislación vigente aplicable a cada país, para en caso de Colombia se determinan las leyes 1273 de 2009 y ley 1366 de 2009, en las cuales se establece la confidencialidad e integralidad de los datos.

2.4 MARCO LEGAL

[25] TELLEZ VALDEZ, Julio. Derecho informático. {En línea}. {2008}. (https://clauditha2017.files.wordpress.com/2017/09/derecho-informatico-cuarta-edicion-julio-tc3a9llez-valdc3a9z.pdf)

[26] BETANCUETH, Valeria.La cumbre mundial sobre la sociedad de la información (CMSI) proceso y temas debatidos. (https://www.apc.org/sites/default/files/wsis_process_ES.pdf)

Tenemos los delitos más comunes y que se presentaron con una mayor incidencia en cada año con su mes respectivamente, en el 2008 no se presentó ninguna denuncia, por lo anterior el delito que se cometió con una mayor incidencia fueron los siguientes:

- 2009 artículo 134 B – Hostigamiento por motivos de raza, religión, ideología, política u origen nacional, étnico o cultura, en el mes de diciembre con una cantidad reporte de 1 con un total 1 denuncia en el año que equivale al 100% de denuncias en el año transcurrido.

- 2010 artículo 269 A – acceso abusivo a un sistema informático, en el mes de marzo y junio una cantidad reporte de 1 cada uno con un total 2 denuncias en el año que equivale al 100% de denuncias en el año transcurrido.

- 2011 artículo 269 A – acceso abusivo a un sistema informático, en el mes de junio y diciembre una cantidad reporte de 1 cada uno con un total 2 denuncias en el año que equivale al 100% de denuncias en el año transcurrido.

- 2012 artículo 269 A – acceso abusivo a un sistema informático, en el mes de julio con una cantidad reporte de 106 con un total 183 denuncia en el año que equivale al 58% de denuncias en el año transcurrido.

- 2013 artículo 246 – Estafa, en el mes de febrero y abril con una cantidad reporte de 96 con un total 648 denuncia en el año que equivale al 15% de denuncias en el año transcurrido.

- 2014 artículo 246 – Estafa, en el mes de octubre con una cantidad reporte de 284 con un total 2842 denuncia en el año que equivale al 10% de denuncias en el año transcurrido.

- 2015 artículo 246 – Estafa, en el mes de noviembre con una cantidad

reporte de 220 con un total 3935 denuncia en el año que equivale al 6% de denuncias en el año transcurrido.

- 2016 artículo 269 A – acceso abusivo a un sistema informático, en el mes de enero con una cantidad reporte de 388 con un total 5036 denuncia en el año que equivale al 8% de denuncias con fecha de corte de julio 2018.

- 2017 artículo 246 – Estafa, en el mes de agosto con una cantidad reporte de 341 con un total 7621 denuncia en el año que equivale al 4% de denuncias en el año transcurrido.

- 2018 artículo 246 – Estafa, en el mes de marzo con una cantidad reporte de 402 con un total 7621 denuncia en el año que equivale al 7% de denuncias en el año transcurrido.

3. GESTIONAR RECOLECTAR INFORMACIÓN RELACIONADA CON LA TIPIFICACIÓN DE DELITOS INFORMÁTICOS.

3.1. SKIMMING- FRAUDE CON TARJETAS DEBITO Y CREDITO

Para poder indicar un claro concepto de Skimming o como su traducción indica “desnatar”, se recopilo información de la presentación proporcionada por VISA (Rivero, 2014) en la cual da a entender que este tipo de delito es el robo de la información de las tarjetas crédito o débito al momento en el que el usuario realiza una transacción, esto lo realizan clonando la tarjeta copiando la banda magnética, para después realizar las actividades fraudulentas. En Colombia los usuarios se han visto afectados en lugares como restaurantes, gasolineras, bares y cajeros automáticos que previamente han sido vulnerados por los delincuentes (para un usuario del cajero automático es muy poco probable que detecte que este siendo víctima del fraude).

¿Cómo funciona el skimming?

El delincuente utiliza un dispositivo para copiar y robar la información de la banda magnética de las tarjetas créditos o débitos, luego pasa la información a una nueva tarjeta y procede a cometer el delito.

¿Cómo combatir el Skimming?

Actualmente se está llevando a cabo el manejo de sistemas anti-skimming, estos sistemas permiten bloquear el ingreso de las tarjetas cuando detectan un dispositivo en la entrada del lector de tarjetas, también hay sensores ópticos e infrarrojos que detectan y anulan una tarjeta cuando alrededor de la misma se esté usando dispositivos fraudulentos.

¿Qué hacer para evitar el Skimming?}

1- Si va a realizar transacciones, debe asegurarse de que el teclado del cajero este en buenas condiciones, verificar que no este flojo, ya que podría estar ante un dispositivo que lea sus datos.

2- Si usted observa que la ranura para insertar la tarjeta está más ancha o presenta alteraciones que no son normales, notifique al banco y evite usar ese cajero.

3- Si la ranura donde inserta la tarjeta esta floja puede que tenga insertado un lazo libanés el cual es un metal que no permite la salida de la tarjeta.

4- Las cámaras que usan las entidades bancarias no son tan evidentes o visibles, si observa una que le genere dudas evite usar el cajero ya que dicha cámara puede capturar su clave.

5- No acepte ayuda de extraños en el cajero ya que puede ser víctima de robo aprovechando su distracción.

6- Se recomienda utilizar las tarjetas de chip inteligente ya que hasta el momento no han sido clonadas.

7- Aplicando SNCP (Sistema Nacional de Cifrado de Pistas), se reduce el riesgo en los comercios relacionado con acceso no autorizado a datos de tarjetas de pago gracias a la encriptación punto a punto.

Imagen 1: FLUJOGRAMA DE SKIMMING

Fuente: https://www.pcihispano.com/que-es-sncp-sistema-nacional-de-cifrado-de-pistas

Imagen 2: RECOMENDACIÓN – PREVENCIÓN DE SKIMMING

Fuente: https://usa.visa.com/dam/VCOM/download/merchants/Webinar-Preventing-ATM-Skimming-Spanish-021914.pdf

3.2 ESTAFA

Esta es una de las modalidades más variadas y utilizadas por los ciberdelincuentes en Colombia, se realizan principalmente vía correo electrónico, redes sociales y teléfonos móviles , la estafa que más daño puede causar a la víctima es el phishing, pero -¿Qué es el phishing?- proviene de la palabra en ingles Fishing que refiere a pesca (Significados, 2014), lo cual quiere decir que los ciberdelincuentes realizan intentos de que los usuarios piquen la trampa o anzuelo quien ellos dejan, luego de tener una víctima tratan de obtener toda la información posible que luego utilizan para cometer estafa.

Como mencione anteriormente hay variadas modalidades de estafas utilizadas por estos delincuentes en red, ejemplo de ellas son:

- Fraude en subasta: Se causa cuando el usuario quiere acceder a un producto subastado que se ve de excelente calidad, paga lo acordado y recibe un producto totalmente diferente al pactado o en ocasiones no recibe nada.

Oportunidad de negocio “Trabaje desde casa”: Es muy usual encontrar dicho mensaje en redes sociales, en la cual promete ganar mucho dinero, la única condición es dar tus datos personales al supuesto empleador y esperar tu pronta afiliación a un sistema falso.

- Fraude en Viajes: En Colombia se vivió recientemente el caso del robo de millas a Avianca por parte de Jaime Alejandro Solano Moreno, el cual prometía a sus víctimas viajes a sitios turísticos a menor precio y con mejores prestaciones, realizando el proceso con millas que les correspondían a famosos de la farándula

colombiana (Justicia, 2015).

• Ventas de productos tecnológicos desde tiendas online falsas: Para este caso, hay variedad de páginas que a simple vista son falsas, por la facilidad en acceder al producto y los costos tan bajos de los mismos, pero hay personas incautas que deciden creer en estos sitios y son estafadas.

Este tipo de estafas es que por el monto del fraude o por la pena que siente la victima de la estafa muchas veces no se denuncia ante las entidades pertinentes.

¿Cómo combatir la estafa informática?

Para indicar formas efectivas para combatir la estafa informática, se tomo en cuenta los aportes del blog Internet Ya[27] los cuales están a la vanguardia de la prevención de delitos informáticos y recomiendan:

1- Solicitar o utilizar una tarjeta solo para compras en internet, para el caso de Colombia los bancos BBVA y Bancolombia ya cuentan con esta modalidad y no permiten generar excesivos gastos en línea ya que lo ven como sistema de alarma o posible fraude al usuario.

[27] Blog escrito por Andrea Sánchez el 06/09/2016-en el cual se aclara la relación de la prevención d ellos delitos informáticos con la protección de la información, obtenido de:

https://www.internetya.co/como-prevenir-compras-fraudulentas-en-una-tienda-en-linea/

2- Estar pendiente de los movimientos que se realizan en su cuenta bancaria, ahora las entidades bancarias para mayor seguridad utilizan para otorgarle de información real y momentánea a su correo electrónico y su número de celular

3- Verificar la página web donde pretende realizar la compra y sobre todo no dejarse deslumbrar por los precios bajos a comparación del mercado estándar.

4- Una manera de evitar ser timado es verificar el sistema de rastreo de lo que compro y verificar los procedimientos a realizar si lo que recibe no es lo deseado, modalidad que emplea Mercado libre en Colombia.

5- Verifique el candado verde que aparece junto a las siglas htpps de la página web donde indica que es seguro navegar ahí.

6- No utilice redes Wi-Fi públicas o de acceso fácil para comprar cosas en línea, ya que se desconoce el sistema de seguridad que contengan dichas redes.

3.3 MALWARE

El Malware son aquellos programas creados por ciberdelincuentes con el fin de obtener de un usuario información valiosa, modificar un sistema o llegar a tomar control total de un equipo.

Con forme a la revista Seguridad 101 (Kaspersky, 2018) los tipos de malware son:

- Virus clásicos. Programas que infectan a otros programas por añadir su código para tomar el control después de ejecución de los archivos infectados. Gusanos de red. Este tipo de malware usa los recursos de red para distribuirse. Lo hacen por medio de correo electrónico, sistemas de mensajes instantáneos, redes de archivos compartidos (P2P), canales IRC, redes locales, redes globales, etc. Su velocidad de propagación es muy alta.

- Troyanos. Esta clase de programas maliciosos incluye una gran variedad de programas que efectúan acciones sin que el usuario se dé cuenta y sin su consentimiento: recolectan datos y los envían a los criminales; destruyen o alteran datos con intenciones delictivas, causando desperfectos en el funcionamiento del ordenador o usan los recursos del ordenador para fines criminales, como hacer envíos masivos de correo no solicitado.

- Spyware. Software que permite colectar la información sobre un usuario/organización de forma no autorizada. Pueden colectar los datos sobre las acciones del usuario, el contenido del disco duro, software instalado, calidad y velocidad de la conexión, etc.

- Phishing: Es una variedad de programas espías que se propaga a través de correo. Los emails phishing están diseñadas para parecer igual a la correspondencia legal enviada por organizaciones bancarias. Tales emails contienen un enlace que redirecciona al usuario a una página falsa que va a solicitar entrar algunos datos confidenciales, como el número de la tarjeta de crédito.

- Adware: Muestran publicidad al usuario, la mayoría de los programas adware son instalados a software distribuido gratis. La publicidad aparece en la interfaz. A veces pueden colectar y enviar los datos personales del usuario.

- Riskware: No son programas maliciosos, pero contienen una amenaza potencial. En ciertas situaciones ponen sus datos a peligro. Incluyen programas de administración remota, marcadores, etc.

- Bromas: Este grupo incluye programas que no causan ningún daño directo a los equipos que infectan. Pueden ser mensajes advirtiendo a los usuarios de que los discos se han formateado, que se ha encontrado un virus o se han detectado síntomas de infección. Las posibilidades son limitadas sólo por el sentido del humor

del autor del virus.

- Rootkits: Un rootkit es una colección de programas usados por un hacker para evitar ser detectado mientras busca obtener acceso no autorizado a un ordenador. Esto se logra de dos formas: reemplazando archivos o bibliotecas del sistema; o instalando un módulo de kernel.

- Otros programas maliciosos: Son una serie de programas que no afectan directamente a los ordenadores, pero que se usan para crear virus, troyanos o para realizar actividades ilegales como ataques DoS y penetrar en otros ordenadores, etc.

- Spam: Los mensajes no solicitados de remitente desconocido enviados en cantidades masivas de carácter publicitario, político, de propaganda, solicitando ayuda, etc. También hay emails dedicados a robo de contraseñas o números de tarjetas de crédito, cartas de cadena, etc.

¿Cómo combatir los Malware?

Como lo indica la Universidad Politécnica de Cartagena en su plataforma InfoWiki (UPCT, 2018) las principales medidas de prevención para combatir este tipo de incidentes son:

1- Como principal medida instalar un sistema de antivirus y tenerlo actualizado

2- Ser precavido, evitar al máximo descargar programas desconocidos.

3- No seguir enlaces desconocidos que le sugieran dirigirse a servicios bancarios.

4- Dudar de emails sospechosos y no acceder a ellos.

5- Tener un cortafuegos, filtros antispam, mantener actualizados los programas

instalados confiables.

Imagen 4: Malware WhatsApp

Fuente: https://caivirtual.policia.gov.co/sites/default/files/untitled_infographic_7.png

Imagen 5: Malware pago de facturas

Fuente: https://caivirtual.policia.gov.co/sites/default/files/cmenes6woaatfdw.png

3.4 SMISHING

En Colombia desde el 2010 se empezó a incrementar el número de víctimas de esta modalidad de delito informático tal como lo afirma el periódico el Tiempo en conjunto con el Caí Virtual de la Policía Nacional, argumentando lo siguiente: “Cifras de la Policía Nacional indican que en el 2010 por el delito de 'hurto por medios informáticos y semejantes', consagrado en la Ley 1273 del 2009, hubo 486 casos en todo el país. A estos se sumaron otros casos de 'acceso abusivo a un sistema informático', 'interceptación de datos', 'violación de datos personales' y 'transferencia no consentida de activos' para sumar en conjunto 2.953 millones de pesos” (Gonzalez, 2011).

De acuerdo al concepto aportado por la UniColombia “El smishing consiste en una estafa por medio de mensajes de texto que llegan a móviles al azar, en el cual se solicitan datos personales o seguir un link para acceder a un premio o recompensa con el fin de luego utilizar la información dada por el usuario para cometer fraude por parte de los ciberdelincuentes”. (UniColombia, 2018)

Además, el smishing usa varias de las actividades de atracción que genera el phishing, pero usa la ingeniería social por medio de mensajes de texto dirigidos solamente a usuarios de telefonía móvil.

¿Cómo combatir el smishing?

Una de las plataformas confiables en el término de seguridad informática público un blog del Ingeniero Lucas Paus en la cual da pautas sobre la prevención de este tipo de delito y menciona: “Ten especial cuidado con mensajes que dicen provenir de entidades financieras o promociones que incluyan un enlace web, una petición urgente o que te induzcan a compartir ese enlace. Mayormente son estafas, pero

puedes comunicarte con la entidad para confirmarlo, Revisa tus cuentas periódicamente, tanto tu factura telefónica, que puede incrementarse rápidamente por suscripción a servicios de SMS Premium, como los gastos de tu tarjeta, que pueden aumentar si lograron robarte tus credenciales mediante un software espía." (Paus, 2017)

En mención de lo anterior se recomienda lo siguiente:

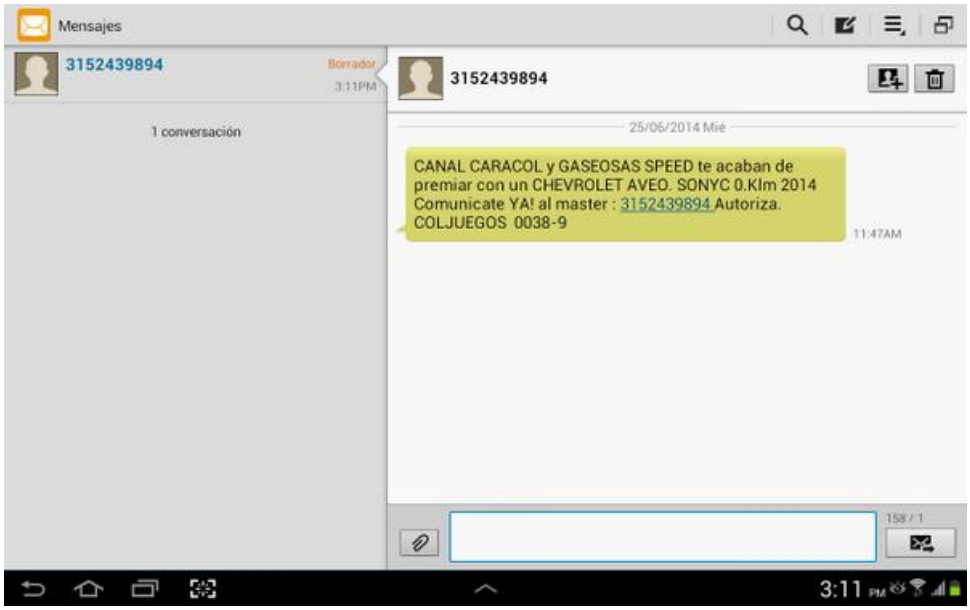
1- Después de recibir un mensaje igual o parecido al que indican las imágenes anteriores, evitar responder el mensaje de texto o tratar de llamar a dicho número.

2- Si el mensaje es alusivo o con carácter financiero que relacione directamente con el banco con el cual uses servicios, es mejor contactar directamente con la entidad financiera y asegurarse preguntando sobre dicho mensaje para verificar su procedencia.

3- Los bancos en Colombia no solicitan información personal y de servicios por medios telefónicos.

4- Es mejor ignorar dichos mensajes y ayudar a alerta a conocidos para que eviten ser víctimas.

Imagen 8: Smishing Carcel



Fuente: https://caivirtual.policia.gov.co/sites/default/files/prem.png

3.5 CARTA NIGERIANA

También conocida como ”Fraude 419” recibe su nombre ya que este tipo de estafas en su mayoría proceden de este país, se ejecuta por medio de correos electrónicos no solicitados, consiste en hacerle creer al usuario incauto que es acreedor de una fortuna (inexistente) y tratar de hacerle creer que para acceder a dicho dinero debe pagar un traslado como seguro de su bien, la cantidad de dinero solicitada es elevada pero a comparación con la dichosa fortuna a entregar es casi nada, por esta razón muchas víctimas caen en la estafa, como lo menciona Claudia Florentina en su tesis fraudes en internet: “Se le conoce bajo el nombre de estafa nigeriana porque estos correos electrónicos provienen de Nigeria. Este fraude viola el artículo 419 del Código Penal nigeriana, y por este motivo también se le denomina fraude 419. Lo más frecuente es prometer a la víctima un porcentaje de

los millones de dólares que el remitente está tratando de transferir fuera de Nigeria supuestamente de forma legal. Se le solicita a la víctima datos personales como nombres de bancos y número de cuentas bancarias, así como enviar dinero al remitente de estos correos electrónicos en forma de pagos parciales. Se le promete al destinatario el reembolso de estos gastos que debe pagar, que evidentemente nunca se efectuará". (Dinca, 2016)

Las modalidades de dicha carta son muchas, a continuación, un ejemplo otorgado por la página Hijos Digitales.es (Hijos Digitales, 2014) del hecho en mención:

"Donación de la señora. Ruth Hamson

obispo [38 rue des mártires cocody

Abidjan, costa de marfil.

Más querido en Cristo,

Soy de kuwait. Estoy casada con el sr. Richead Hamson, quien trabajó con la embajada de kuwait en costa de marfil durante nueve años antes de morir en 2004. Nos casamos por once años sin un niño. Murió después de una breve enfermedad que duró sólo cuatro días.

Antes de su muerte, tanto cristiano nacido de nuevo. Desde su muerte he decidido no volver a casarse o tener un hijo fuera de mi hogar conyugal que está en contra de la biblia. Cuando mi marido estaba vivo él depositó la suma de ($ 2,5 millones) en el banco aquí en abidjan cuenta de suspenso. Actualmente, el fondo se encuentra todavía en el banco. Recientemente, mi doctor me dijo que tengo enfermedad grave que es problema del cáncer. Lo que más me molesta es mi enfermedad del movimiento. Sabiendo que mi condición decidía donar este fondo a la

iglesia o los que usan este dinero la manera que se lo recomendaría aquí. Quiero una cola iglesia utilice este fondo para los orfanatos, las viudas, para promover la palabra de dios y la cola esfuerzo la casa de dios se mantiene.

La biblia es para nosotros entender que bendito el lado da. Tomé esta decisión porque no tengo cualquier niño que heredará este dinero y mi marido familiares no son cristianos y no quiero que mi marido para ser utilizados por los incrédulos. No quiero una situación donde este dinero será utilizado en una manera impía. Es por eso que estoy tomando esta decisión. No tengo miedo de la muerte, así que sé a dónde voy. Sé que voy a estar en el pecho del hombre. Éxodo 14 vs 14 dice que el señor luchará que mi caso y me callaré. No necesito una comunicación del teléfono en este respeto debido a mi salud por lo tanto la presencia de los parientes de mi marido alrededor de mí siempre, y yo no quiero que sepan acerca de este desarrollo. En dios todas las cosas son posibles. Tan pronto como consiga una respuesta le daré el contacto del banco aquí en abidjan. Quiero que tú y la iglesia rogaran siempre para mí porque el señor es mi pastor. Mi felicidad es que viví una vida digna cristiana. El que quiera servir al señor le debe servir en espíritu y en verdad. Siempre orando por sus vidas enteras. Responda yo para más información, en su respuesta me dará el sitio en sourcing otra iglesia o una persona con el mismo fin. Aseguro que me dejas que van a actuar en consecuencia a las especificadas. La esperanza de obtener una respuesta."[28]

[28] Hijos Digitales/ 20 Octubre/2014- Ejemplo timo Nigeriano; Obtenido en su totalidad de: https://www.hijosdigitales.es/es/2014/10/ejemplo-de-timo-nigeriano-la-donacion-de-la-senora-ruth-

Envíame la siguiente información, según abajo.
Su nombre completo .....
Abordar .....
Actúa .....
La ocupación .....
Fotos .....
siendo bendecido en usted.

Suyo en cristo, Hermana
Ruth Hamson.

¿Como combatir la Carta Nigeriana?

Además de dar uso adecuado al correo electrónico, la plataforma de Premier Consumer (Premier Consumer, 2016) indica pautas de seguridad para evitar ser víctima de este tipo de incidente informático, entre los cuales están:

1- No abra correos de spam o ventanas emergentes

2- Sea más analítico y centrado, a esto me refiero a que, si usted no tiene familiares en Nigeria y ni siquiera ha oído del tema, no sea incauto y sea más razonable es obviamente una trampa.

3- Actualmente los correos electrónicos cuentan con una opción en la cual uno puede descartar correos o reportarlos como spam, es la mejor opción para este tipo de mensajes.

---

hamson/

4- No compartir bajo ninguna medida información personal en red.

5- Sea más cuidadoso con lo que publica en redes sociales ya que estas a veces son las principales promotoras de información para los ciberdelincuentes.

Imagen 9: Carta Nigeriana

---------- Mensaje reenviado ----------
De: **PATRICK** <fa606045@skynet.be>
Fecha: 21 de junio de 2015, 15:48
Asunto: FW: tr: Re: Mensaje Muy Important
Para: ma132534@skynet.be
Cc: uc.lac@hotmail.com

Hola me gustò,

Excusa yo soy de esta manera que usted contactar porque no sabemos, sòlo he visto tu perfil y me han dicho que usted es la persona que me necesitan. En definitiva, mi nombre es Sr. **OLIVIER GIRROUX** nació el 14 de enero de 1944, nacionalidad canadiense.Te envío este mensaje a buscar su consentimiento a un proyecto de donaciòn que quiero hacer durante mucho tiempo.

Tengo la suma de **850.000 Euros** como un regalo. Te pido que aceptar esa suma porque puede muy bien eres muy útil. Es necesario que me contestes si acepto mi oferta directamente por mi correo

correo electrónico : Olivier.girroux@outlook.com

Me siento muy mal y estoy muy asustada, casi no puedo dormir por la noche como el día. No puedo morir sin haber donado esta cantidad lo contrario creo que sería un desastre.

Que Dios está con usted.

Sr. **OLIVIER GIRROUX**

--
Juan Diego López Medina

Lo que no te mata, te fortalece -Nietzsche

CENTRO CIBERNÉTICO POLICIAL

Fuente: https://caivirtual.policia.gov.co/sites/default/files/untitled_infographic_7.png

3.6 PHISHING

En el pasado año 2017 se presenta en Colombia el caso de Phishing a los usuarios de la entidad bancaria Bancolombia, el banco privado más grande del país con sede principal en la ciudad de Medellín.

De acuerdo a las declaraciones que hizo el grupo de investigadores de seguridad informática de la empresa eslovaca ESET, el fraude comenzó con un correo electrónico proveniente de la cuenta informacion@bancolombia.com.co que eran enviados a las cuentas de correo de los usuarios de este banco en el que se le informaba a los clientes que por motivos de seguridad los servicios contratados por este habían sido suspendidos temporalmente y que para volver a hacer uso de estos canales virtuales debían hacer clic en un enlace proporcionado en el cuerpo del correo. Una vez el cliente ingresaba a la página fraudulenta, se le solicitaba que ingresara los datos correspondientes al usuario, contraseña y preguntas de seguridad con el fin de obtener en una base de datos toda la información necesaria a la hora de realizar una transferencia de dinero. Para darles sensación de seguridad a los usuarios, los delincuentes diseñaron el teclado virtual que usa realmente el banco y hacían que para ingresar la contraseña solo se pudiera por medio de este teclado virtual. Así, el cliente no sospechaba que estaba entregándoles información valiosa a personas sin escrúpulos.

Fraude en viajes:

Según la revista Semana para el año 2017, más de 5.000 colombianos han perdido cerca de 60.000 millones de pesos en diferentes fraudes cibernéticos. Tan solo en venta de pasajes aéreos la cifra llegó a 22.000 millones. Estas son algunas modalidades.

Una de las modalidades más comunes por estos días es la conocida como ‘turinet’. Consiste en que una persona recibe por WhatsApp, mensaje de texto o en su Facebook un mensaje en donde le ofrecen tours turísticos o alquiler de lujosas fincas a precios aparentemente favorables. Lo remiten incluso a páginas web perfectamente diseñadas, en donde hay un teléfono de contacto de una supuesta empresa en donde efectivamente alguien contesta y suministra los datos. Para obtener el descuento le informan al interesado que debe cancelar por medio de giros el 50 por ciento del valor del plan o finca que quiere. Una vez ocurre esto

sencillamente no vuelven a aparecer, y el estafado descubre que la dirección de la supuesta empresa solo existe en el mundo virtual. Los criminales también usan esta modalidad para ‘vender’ por internet productos que van desde una silla hasta un carro. En estos casos ocurre algo similar. El incauto consigna una parte y queda a la espera de pagar el saldo una vez reciba lo que adquirió. Obviamente ese producto nunca llega.

Otra forma de estafa virtual tiene que ver con los tiquetes aéreos. Por medio de redes o páginas de ventas de productos se ofrecen pasajes a diferentes destinos nacionales y en el exterior a unos precios muy llamativos. Es así como los criminales ofrecen un vuelo Bogotá a Madrid (España), que puede costar un poco más de 2 millones de pesos, hasta en la mitad o menos. Pero a diferencia del ‘turinét’, en este caso el producto sí existe. En efecto, los criminales previamente han comprado los tiquetes por medio de tarjetas de crédito clonadas o robadas y al revenderlo, a precios muy inferiores, están obteniendo efectivo, ya que una de las condiciones es que el cliente debe pagar mediante empresas de giros para evitar ser rastreados. Quien compra efectivamente recibe un tiquete, pero cuando lo va a usar puede ser eventualmente vinculado a un proceso por formar parte de una cadena criminal. En lo que va de este año a más de 50 personas se les impidió subir al avión al detectar que compraron por esos canales.

Ventas de productos tecnológicos desde tiendas online oficiales y falsas:

Para poder aclarar de mejor manera esta situación que se incrementa cada vez más en los portales de compra y venta cono Mercado Libre OLX Amazon entre otros tome en cuenta que el sitio web VICE y su investigación sobre esta estafa publicaron lo siguiente:

Ejemplo de estafa web vivida en Colombia

Usted pone a la venta un producto en una página de compraventas. Suele ser un

portátil, un celular de alta gama, una consola de videojuegos. Aunque también ha pasado con muebles, perros, un aire acondicionado. Un comprador (muchas denuncias coinciden en que es un tipo de acento costeño) se muestra interesado en su producto. Lo contacta amablemente, no regatea el precio, se comporta como el cliente perfecto. Usted y el comprador arreglan los detalles de lo que será su futuro infierno. El tipo le manda una foto de un recibo de consignación, muchas veces incluso parece en efectivo. Le dice que revise su cuenta bancaria, revise que todo está en orden y, de ser así, le envíe el producto. Usted va, coge su celular o su computador, abre la sucursal virtual de su banco y ve que efectivamente aparece un ingreso nuevo: un millón, lo que había pedido por su computador usado. Debajo de ese valor, aparece subtítulo que dice "consignación en canje". Usted lo ignora. Envía el producto. Un rato después entra de nuevo a la sucursal, quizás con ganas de gastarse la plata que acaba de ganar. Pero ve, con sorpresa, que la consignación no aparece. Ya no está su millón. Se quiere pegar un tiro. Llama al comprador, que por supuesto ya no contesta. Llama desesperado al banco. Le explica de mil formas al asesor. Y él, mucho más calmado que usted, le dice que lo robaron.

Daniel Puerta, una víctima de este robo en Medellín, dice que así perdió su cámara. Nos relata un reflejo del arquetipo de estafa: "Puse a la venta, por OLX, mi cámara Canon T2i porque quería una mejor. Lo puse un día por la noche y al día siguiente muy temprano me llamó un señor llamado Fernando. Me pareció confiable, no noté nada raro. El man quería concretar la compra rápido y me dijo que quitara la publicación de la plataforma. Me mandó de una foto de un recibo de consignación y yo revisé en la página de Bancolombia y aparecía la plata. No me fijé en lo de "en canje". No vendo cosas así normalmente. La plata se desapareció al día siguiente y el celular del man ya sonaba apagado. Luego alguien me explicó por qué había pasado y me sentí como una güeva. Puse el denuncio en la Fiscalía, pero no ha pasado nada con eso". La explicación que le han dado a Daniel y a todas las víctimas es breve: la consignación en canje, esas tres palabras que usted

pasó por alto, indican que su comprador pagó con un cheque. Lo que usted no sabía (y por lo que cayó en la trampa) es que el cheque tiene un periodo de canje de tres días, en el que quien lo depositó puede revertir el pago. O bien puede ser un cheque sin fondos: el popular cheque chimbo. Ahora lo sabe las consecuencias de la carencia de protección en los sistemas de información y por la ausencia de claridad en su utilización, en el Boletín de análisis de ciberseguridad financiera, del 23 de agosto de 2017 entre los años 7117 denuncias clonación de tarjetas de débito y crédito (skimming), (Centro Cibernético Policial, 2017); muchos de estos casos es la violencia contra las mujeres, el sexting, que incrementa cada día.

En el informe de la Policía Nacional, amenazas del Cibercrimen en Colombia 2016-2017, los apartes Aunque han pasado ya más de treinta años desde que comenzó a hablarse de la criminalidad informática, y más de veinte desde que se acuñó el término Cibercrimen, parece que el fenómeno de la criminalidad relacionada con el uso de las Tecnologías de la Información y la Comunicación sigue siendo totalmente novedoso y por ello, parcialmente incomprendido por la sociedad en general y, en particular, por las instituciones encargadas de la prevención de esta amenaza. El Cibercrimen forma parte ya de la realidad criminológica de nuestro mundo, pero en muchas ocasiones se exagera la amenaza que el mismo supone y en otras no se percibe el riesgo real al que el uso de las TIC conlleva. La lógica de que esta «novedad» dure tanto, es la revolución de las TIC, como concepto amplio, abierto y dinámico que engloba todos los elementos y sistemas utilizados en la actualidad para el tratamiento de la información, su intercambio y comunicación en la sociedad actual, en la que se enmarca el fenómeno del Cibercrimen. No ha terminado todavía, ni lo hará en mucho tiempo, lo que supone que la cibercriminalidad o delincuencia asociada al ciberespacio seguirá expandiéndose y evolucionando en las próximas décadas. (Centro Cibernético Policial, 2017) .

Las empresas colombianas deben seguir una serie de recomendaciones que

permitan implementar medidas de protección contra delitos informáticos, tales como:

- Evitar riesgos al momento de almacenar información de la empresa: Los entes quieren tener en lo posible toda su información con respaldo y actualmente la tecnología ofrece medios como almacenamiento en nube, por tal razón se debe contar con los medios tecnológicos y humanos de calidad, que sean fiables, que permitan salvaguardar la información para beneficios de la empresa.

- Contar con una gestión de riesgos y manejo de la información: Para permitir que las empresas alcancen sus metas y objetivos, se debe realizar una adecuada gestión de la información ya que permite examinar los procesos de comunicación y la protección d ellos sistemas informáticos para analizar las consecuencias de un posible ataque que cause perdida parcial o vulnerabilidad d ellos servicios.

- Herramientas especializadas: En el mercado actual se pueden encontrar herramientas que sirvan específicamente para detectar amenazas en los sistemas operativos o en los sitios web que se consultan.

- Verificar las direcciones d ellos sitios Web que se visita: Por medio de la verificación del URL, con mayor razón si son para realizar transacciones electrónicas, por seguridad no se debe seguir enlaces que lleguen al correo electrónico o que se enlacen a paginas desconocidas.

- Proteger los datos de los empleados y dictar capacitaciones del tema a estos: Es importante mantener la información de los empleados solo con miembros de la compañía, estar al pendiente que en los sitios donde se guarde la información de estos no sufra daños o posibles infiltraciones por parte de terceros ya que se puede ocasionar una suplantación que ocasione robos de datos e información valiosa para el ente.

¿Qué clases de riesgos justifican estas medidas de protección?, se debe definir

desde diferentes puntos de vista:

1- Riesgos personales: acoso laboral y conflictos laborales

2- Riesgos operativos: mala calidad del producto, errores en el desarrollo, desacierto en el diseño, fraude, deterioro de la maquinaria, error de diseño, fallas de las maquinas, acceso ilegal, omisiones, inexactitud.

3- Riesgos estratégicos: fuga de información, espionaje industrial, actos malintencionados de terceros, sabotaje, retiro de personal estratégico. (Mejía Quijano, 2013) .

Existe una cuarta definición de riesgos, los riesgos físicos (inundación, incendio, terremoto, cortocircuito, humedad y contaminación ambiental), que, por su condición de suceder sin causar perjuicios adicionales, no se describe en el presente documento.

La auditoría, para la seguridad en el trabajo, no solamente corresponde a Seguridad y Salud en el trabajo, uno de los enfoques importantes es el puesto de trabajo del trabajador, cuando se habla de seguridad de la información el enfoque desarrollado pertenecen a las inversiones de seguridad de mejoramiento y renovación, en donde los costos son elevados. (Ramírez Cavassa, 2005)

Los riesgos empresariales son innegables y de manera decisiva se debe disponer de estrategias para minimizarlos, de esta manera se puede definir que la capacidad para establecer estrategias que socorran estos impases, comenzando por estrategias directivas, habilidades directivas que se vinculan a una tarea, implican un entorno, se demuestran en la realización de tareas con regularidad y eficacia, esto implica romper paradigmas. (Madrigal Torres, 2009)

Si, se basa la necesidad de protección contra los riesgos y la necesidad de

habilidades directivas propias al principio de protección, llegamos a la pregunta ¿En Colombia existen personas con la preparación académica adecuada y los principios éticos necesarios para solventar los incidentes informáticos en su mayoría?, ¿Cómo se evaluaría a las personas para ocupar cargos que conlleven el tratamiento de estos incidente informáticos?, ¿El tratamiento de los incidente informáticos en Colombia debe estar a cargo con personas de conocimiento tecnológico y programación y principios humanitarios?, los riesgos se deben evaluar desde el momento mismo en que se diligencia un documento, un formato, ya que son los soportes de la información registrada en los sistemas de información. El otro extremo de la moneda es hacking ético, profesionales de seguridad con fines éticos, los siete valores dominantes de la sociedad red y de la ética protestante son el dinero, el trabajo, la optimización, la flexibilidad, la estabilidad, la determinación y la contabilidad de resultados. Ahora podemos resumir los siete valores de la ética hacker que han desempeñado un papel significativo en la formación de nuestra nueva sociedad y que representan un desafiante espíritu alternativo del informacionalismo. Una vez más conviene recordar que sólo aquellos hackers informáticos comparten esos valores en su integridad, aunque deben ser considerados colectivamente debido a su interrelación lógica y social (Himanen, 2001)

Imagen 11: Phishing Banco Falabella

Fuente: https://caivirtual.policia.gov.co/sites/default/files/c9o0llrxcae8gia.jpg

3.7. CIBERBULLYING

El ciberacoso denominado acoso virtual o acoso cibernético, se ven presente en el uso de las redes sociales que se usan para acosar a una persona o grupo de personas, mediante ataques personales, divulgación o creación de información personal y sensible lo cual afecta la vida cotidiana de la persona o grupo de persona. Existe varios métodos como acosos electrónicos, acosos sms, acoso móvil, acoso en línea, acoso en internet entre otros, que se usen herramientas informáticas.

¿Como combatir el ciberbullying?

1- Utilizar internet con responsabilidad limitando la información sensible que uno comparte para no ser una víctima en potencia.

2- Cuidar la privacidad de los elementos que se comparten en redes sociales.

3- Denunciar este tipo de actividades con las herramientas de denuncio para que tomen correcciones correspondientes a la medida del caso.

Imagen 12: CiberBullying

Fuente: https://kidshelpline.com.au/sites/default/files/bdl_image/Teen%20girl%20being%20cyberbullied_3.png

3.8 VISHING

El termino Vishing es la combinación de dos palabras claves " Voice" y "Phishing" la cual se trata de tipo de amenazas que combinan llamada telefónicas fraudulenta con información antes recaudada en internet para tener una mayor tasa de éxito a la hora de robar datos financieros entre otros datos sensibles

¿Como combatir la Vishing?

1- Evitar proporcionar información financiera a través de llamadas telefónicas.

2- No ingresas datos personales en sitios web dudosos

3- No responder mensajes de algún número sospechoso

4- Conocer de antemano que ninguna entidad financiera solicita datos personales a través de llamada telefónica

Imagen 13: Vishing

Fuente: https://www.bbva.com/wp-content/uploads/2018/11/smishing-1024x427.png

3.9 RANSOMWARE

Es un malware de rescata conocido común mente como Ransomware su función que impide acceder al sistema y archivos ya que encripta todos los archivos, exige un pago por el rescate de la información que se encuentra nuestro computador, dispositivos de almacenamiento y servidores

Tipos de Ransomware

Hay tres tipos principales de métodos Ransomware, cuya escala va desde un spam hasta cifrar tu información:

- Scareware: Se instala bajo programa de seguridad falsos y ofertas falsas de soporte técnico, ataca con emitiendo pantalla emergente que se ha detectado malware y que única forma de liberar el equipo es pagando un rescate, la mayoría de estos rescates se pagan BTC “Bitcoin” una moneda virtual que no se puede rastrear. En este caso nuestros archivos se encuentran a salvo

- Bloqueadores de pantalla: Pasamos a otro tipo de secuestro de equipo el cual es ocupar parte de nuestra pantalla para emitir una imagen con logotipos oficiales de FBI o entidad seguridad lo cual nos indica que hemos cometido una infracción con diferentes delitos cibernéticos y por lo tanto debemos pagar una multa para recuperar el control de nuestro equipo.

- Ataque Ransomware: Es una aplicación maliciosa que la podemos encontrar en páginas o sitios web como publicidad engañosa también cuando se nos envié correo de personas desconocidas con finalidad que ejecutemos el software que nos envía para infectar nuestro pc, lo cual encripta en su mayor parte el equipo, y nos solicita pagar un rescate para liberar nuestro equipo

¿Como combatir el Ransomware?

1- Comprobar que nuestro software de nuestro equipo este actualizado en todo momento, como nuestro sistema operativo, navegador y complementos de seguridad que tengamos instalados.

2- Prever herramientas para su detección temprana como antirransomware que evite que código se ejecute con normalidad

Imagen 14: Ransonware

Fuente: https://tecnokratix.net/wp-content/uploads/Ransomware-pic-770x433.jpg

3.10 DDOS

Conocido como ataque de denegación de servicio es un ataque aun sistema de computadores o red que causa que el servicio o recurso sea ralentizar o sea vuelva inaccesible para los usuarios, provocando una perdida de conectividad total con la red por la sobrecarga del número de peticiones haga.

¿Como combatir el DDOS?

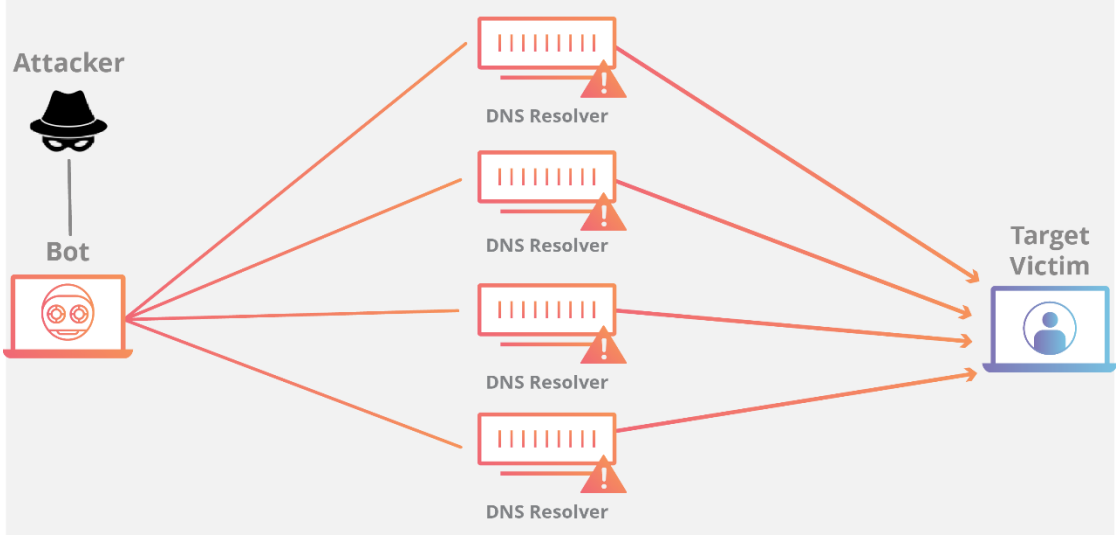
1- Revisar quienes nos están enviando solicitudes cada 5 segundos exactos, lo cual es eviten que es un "bot" por lo cual con las reglas que creemos en nuestros sistemas le prohibiéremos el ingreso mediante ip, o mac,

2- Mirar nuestros proveedores de internet y hosting donde se aloja nuestro sitio

web o servicio, tenga plenamente filtros y herramienta para evitar el DOS

3- Contratar servicios especializados contra ataques de DDoS ya que se van innovando con el tiempo nuevo métodos como hacer ataques de DDoS

Imagen 16: Ataque DDos



Fuente: https://www.testdevelocidad.es/app/uploads/2018/03/ntp-amplification-botnet-ddos-attack.png

3.11 SPOOFING

Es conocidos en la seguridad redes, ya con la herramienta adecuada se puede hacer prácticas técnicas de hacking ético, pero hay personas que generalmente lo usan con sentido malicioso y malintencionado, lo usan para hacer daños a través de la red haciendo una suplantación a nuestra IP, ARP, DNS, Sitio web, Correo electrónico y GPS:

- Suplantación de IP: Por lo general consiste en cambiar la ip para tener acceso y que el sistema lo reconozca como un usuario verdadero.

- Suplantación de ARP: Condiciona a la víctima con un envenenamiento de ip y mac lo cual hace que el equipo que es atacado solo se pueda comunicar y forzarla a que envié los paquetes al host atacan en lugar de hacerlo con el host legítimo

- Suplantación de DNS: Se trata de falsear la relación entre el dominio y la ip, con este método obtener en unos de los dos casos, la ip o nombre del DNS.

- Suplantación de web: Hacer creer que esta página web real, con la cual hará que la víctima le revele la información en los formularios de la página web en este método se inyecta estos códigos con el fin de obtener todos los datos sensibles.

- Suplantación de correo electrónico: Esta técnica para hacernos simular nos envían un correo supuestamente legítimo y con dominio parecido al verdadero. Lo cual muchas personas caen en este tipo de suplantación por no saber verificar las fuentes de donde proviene este correo electrónico

- Suplantación de GPS: Con herramientas alteran la medición del GPS haciendo creer que se encuentra en otro lugar.

¿Como combatir el spoofing?

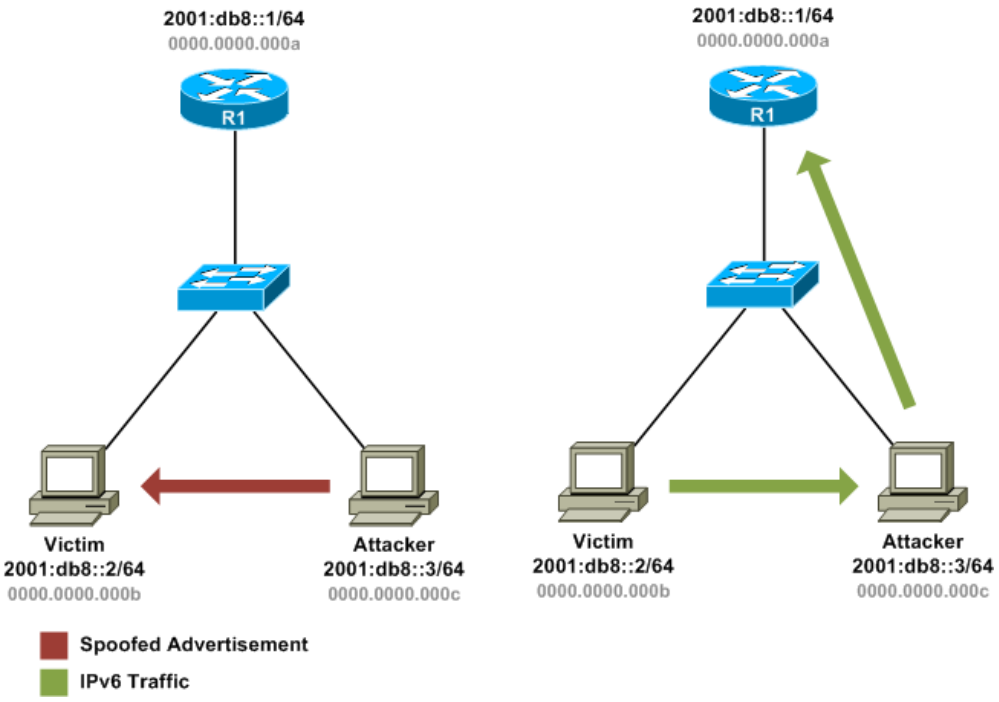
1- Establecer solución integral en la cual el filtrado de paquete de tu router o firewall, analice y descarte aquellos paquetes que no provenga de la red.

2- Evitar el método de autenticación basado en el host

3- Crear reglas confiables a la hora de administrar nuestra red con los nuevos protocolos que se recomienda nuestros proveedores

4- Comprobar la autenticidad de los correos

Imagen 17: Spoofing



Fuente: http://packetlife.net/media/blog/attachments/338/neighbor_spoofing.png

4. IDENTIFICAR LA REPERCUSIÓN DE LOS INCIDENTES INFORMÁTICOS BAJO LA APLICACIÓN DE LA NORMATIVIDAD COLOMBIANA EN LO REFERENTE A SEGURIDAD INFORMÁTICA.

4.1 CASOS DE ESTAFA INFORMÁTICA EN COLOMBIA

En Colombia los casos de estafa Informática se están presentando de manera creciente desde el año 2008, tal como lo indica la Policía Nacional con el reporte de Caí Virtual, además desde que se implementa la ley 1273 de 2009 se puede evidenciar el incremento de denuncias por parte de los ciudadanos víctimas de este tipo de delitos y los casos que han sorprendido a los incautos Colombianos, en la página de la Fiscalía General de la Nación se pueden encontrar los Delitos informáticos que han sido procesados y judicializados[29], entre los más mencionados se encuentran los de modalidad de estafa informática.

Entre las estafas más conocidas en Colombia están los fraudes en compras en línea por plataformas reconocidas y el fraude de subasta:

4.1.1 Fraude Compras en Línea:

De acuerdo al la pagina Dinero en su publicación en la sección de Empresas, publicó un articulo en el cual indica que los fraudes por compra en línea son cada vez mas comunes, cayendo en la trampa de los “productos fantasma” (Dinero, 2017) de la siguiente manera: “Es uno de los fraudes más típicos en la era de

---

[29] Fiscalía General de la Nación-Delitos Informáticos, Fuente: https://www.fiscalia.gov.co/colombia/tag/delitos-informaticos/

internet -y al mismo tiempo más difíciles de detectar- y ocurre cuando creemos que estamos comprando algo muy barato pero nos están engañando: en realidad, no existe. Ocurre con todo tipo de bienes y servicios, desde vuelos hasta muebles, seguros de viaje o teléfonos móviles que, en apariencia, son una ganga.”

Este tipo de delito afecta tanto a vendedores como a compradores, para entender este tipo de delito a continuación se citan dos ejemplos que ocurren en cada caso (al vendedor o al comprador de dicho producto o servicios) por esta modalidad:

“Un comprador perfecto y un vendedor incauto:

Esta estafa, a diferencia de las más conocidas, hace parecer que el vendedor tiene ventaja sobre su cliente. Luego de leer gran cantidad de denuncias, se llega a la conclusión que esta persona o este grupo de personas ataca a los vendedores ocasionales. Esto significa que las personas que vendan por primera vez en internet son los blancos más fáciles.

La estafa sucede más o menos así:

1. Al publicar un artículo en plataformas como OLX o Ebay, aparece el 'cliente perfecto'. Esta persona lo contacta amablemente, no busca una rebaja del producto y le pide que retire el anuncio de la plataforma.

2. Normalmente, este 'cliente' se encuentra en otra ciudad del país, esto significa que no se podrán ver personalmente para acordar el trato. Por esta razón le dice que envíe el producto a una dirección, y que él, o ella, realizarán la respectiva consignación.

3. El supuesto cliente, le envía una foto del recibo de consignación y le pide que revise su cuenta bancaria. Luego de que usted revisa su sucursal virtual, notará que la transacción fue realizada 'correctamente', y que el dinero está en su cuenta.

4. Usted le envía el producto, y al día siguiente, el dinero desaparece de su cuenta bancaria. El estafador no responde los mensajes, ni las llamadas". (Tamayo, 2016)

En este caso la víctima es el vendedor del producto o servicios, por desconocimiento del cheque en canje que se utiliza en las entidades financieras, a continuación una respuesta del banco Davivienda a una incógnita de su cliente en su sección de preguntas frecuentes:

"Consigné un cheque en mi cuenta, ¿En cuánto tiempo tengo disponible mi dinero?

Si consignó el cheque de lunes a viernes de 9:00 a.m. a 4:00 p.m., su dinero estará disponible al siguiente día hábil después de las 7:00 p.m. Si realizó la consignación después de las 4 p.m. o un sábado tendrá disponible su dinero en los siguientes dos días hábiles después de las 7:00 p.m." (Banco Davivienda, 2016)

Entonces, el cheque se encuentra en canje durante el tiempo en que la entidad financiera valide que este tenga fondos, es por ello que el dinero se refleja en la cuenta de ahorros del vendedor durante un lapso de tiempo y después dicho dinero ya no se evidencia en la cuenta.

El otro tipo de fraude se ejecuta cuando la victima es el comprador, un ejemplo claro de este tipo de delito lo publicó el periódico El Tiempo en su sitio web en la parte de Blogs Lectores la cual dice:

"Hace como un mes a un primo lo tumbó un man por Mercado Libre, diciéndole que trabajaba en la Aduana y que tenía LCD's, pc portátiles, cámaras digitales,etc, decomisados por contrabando y que le vendía lo que quisiera casi a mitad de precio, ¡obviamente a mi primito se le abrieron las pepas! El man le dio un número de cuenta, y le dijo que le consignara 500 mil de adelanto por un TV LCD Sony de 46" que se lo "vendía" en 2 millones y que lo fuera a recibir al aeropuerto y que

después le consignara el resto.

Mi primito, creyendo que se había hecho el negocio de la vida, le consignó los 500 mil. El man le dio un número de guía y se fue al aeropuerto a esperar el paquetico…. y como ya se imaginarán el paquete nunca llegó y en los números con que se comunicaba con el tipo jamás le volvieron a contestar.” (Carbez, 2008)

A pesar de que el anterior ejemplo sucedió en Colombia en el 2008, aún en el 2018 los delincuentes practican este tipo de delito, con el mismo modus operandi y van a la vanguardia de los medios tecnológicos con el fin de hacer mas certeros sus golpes criminales.

4.1.2 Fraude Subasta

Se genera cuando usted después de enviar el dinero para comprar el producto o bien que le indicaban, recibe un producto cuyas características no corresponden con las indicadas en web o incluso un producto que no tiene ningún valor.

Un caso que se vive en Colombia y lo ha reflejado el periódico el Heraldo es el siguiente:

BARRANQUILLA 18 de diciembre de 2016

“La subasta de casas embargadas se ha convertido en foco de acción de organizaciones delictivas. EL HERALDO averiguó con expertos y afectados cómo operan estas redes y recabó recomendaciones para evitar ser víctima de engaños.

Las capturas de 16 funcionarios de la empresa Global Bróker, entre directivos y empleados en Barranquilla y Valledupar, dejó al descubierto una nueva modalidad de estafa en el sector inmobiliario, con el falso ofrecimiento de la venta de casas en remate, que afectó a más de 370 personas en el Atlántico. Las estafas superan los 15 mil millones de pesos, según cálculos de la Fiscalía.

Las de esta empresa fueron las primeras denuncias que se conocieron en el Atlántico en esta modalidad de estafa, que fue descubierta en 2011, pero por la que solo este año se materializaron las primeras capturas. Los implicados se encuentran a las puertas de enfrentar un juicio oral, cuya audiencia de acusación quedó programada para llevarse a cabo los primeros días de enero."

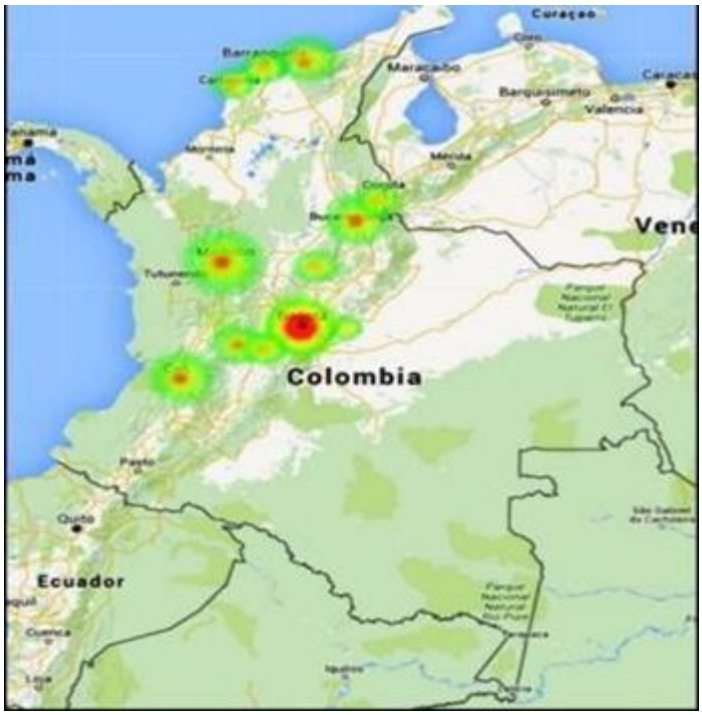
Casos cómo lo anteriores son coloquialmente "el pan de cada día" en Colombia y a pesar de que se han tomado las medidas en tema de legislación y por parte de la Policía Nacional son muchos los ciudadanos victimas que no denuncian estos hechos, la única manera de combatirlos es la educación acerca de este flagelo.

5. MITIGAR LOS RIESGOS DE SEGURIDAD, MEDIANTE LA ENTREGA DE RECOMENDACIONES

De acuerdo con el objetivo general de la presente monografía y para tener mayor respaldo en el proceso de investigación, se procede a realizar una recolección de información desde la página del CAI virtual de delitos informáticos de la Policía Nacional, para poder obtener así una información confiable y precisa de los delitos informáticos en Colombia en los últimos 10 años.

Según el mapa de calor de los incidentes informáticos, se puede observar que Bogotá es la ciudad del país con el mayor número de incidencias informáticas, seguida de Medellín, Cali, Barraquilla y Bucaramanga, registrado por las denuncias registradas en el CAI virtual de la Policía Nacional.

Imagen 18: Amenazas cibercrimen



Fuente:https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Año	Total, Delitos
2008	0
2009	1
2010	2
2011	2
2012	183
2013	648
2014	2842
2015	3935
2016	5036
2017	7621
2018	5842
Total	26112

Tabla 1. Total, Delito en los años 2008 a 2018

Con las herramientas obtenidas del centro cibernético policial podemos hacer un mapa virtual a tiempo real de los delitos que ha sido registrado a lo largo con datos como el tipo de delito, la modalidad y el sector afectada con lo genera el reporte para centralizar cual es la incidencia informática más común entre la fecha 1/1/2008 al 31/07/2018. Los cuales se detallan en cantidad en la tabla 1.

Imagen 19: CaiVirtual

Fuente: https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real

Tabulación de la información de las siguientes tablas demostraron lo siguiente:

Que en la fecha de 1/1/2008 al 31/07/2018 se reportaron cantidad delitos los cuales indican que cada vez hay un mayor impacto en la sociedad por el crecimiento de las tecnologías. De las cuales encontramos los siguientes delitos que se usan y por lo cual nombraremos los más comunes que se presentaron a lo largo de estas fechas ya mencionadas en la siguiente tablas 2 y 3.

Delito	Año	Mes	Cantidad	Total	Equivale
	2008	-	0	0	0
Artículo 134 B – Hostigamiento por motivos de raza, religión, ideología, política u origen nacional, étnico o cultura	2009	diciembre	1	1	100%
Artículo 269 A – acceso abusivo a un sistema informático	2010	Marzo y junio	2	2	100%
Artículo 269 A – acceso abusivo a un sistema informático	2011	Junio y diciembre	2	2	100%
Artículo 269 A – acceso abusivo a un sistema informático	2012	Julio	106	183	58%
Artículo 246 – Estafa	2013	Febrero y Abril	96	648	15%
	2014	Octubre	284	2842	10%
	2015	Noviembre	220	3935	6%
Artículo 269 A – acceso abusivo a un sistema informático	2016	Enero	388	5036	8%
Artículo 246 – Estafa	2017	Agosto	341	7621	4%
	2018	Marzo	402	5842	7%
Total	2009-2018			26112	

Tabla 2. Delito mayor reportado por mes y año

Delito	Total	Porcentaje
Artículo 246 – Estafa	9689	37%

Delito	Total	Porcentaje
Artículo 269 E – uso de software malicioso	2855	11%
Artículo 269 F – Violación de datos personales	2831	11%
Artículo 269 G – suplantación de sitios web para capturar datos personales	2427	9%
Artículo 269 A – acceso abusivo a un sistema informático	2008	8%
Artículo 269 I – Hurto por medios informáticos y semejantes	1150	4%
Artículo 220 – Injuria y/o calumnia a través de internet	1069	4%
Artículo 347 – Amenazas	901	3%
Artículo 244 – Extorsión	747	3%
Artículo 218 – Pornografía con personas menores a 18 años	746	3%
Artículo 134 B – Hostigamiento por motivos de raza, religión, ideología, política u origen nacional, étnico o cultura	691	3%
Artículo 221 – Calumnia	387	1%
Artículo 269 D – Daño informático	154	1%
Artículo 268 F – Violación de datos personales	130	0%
Artículo 269 J – Transferencia no consentida de activos	126	0%
Artículo 182 – Constreñimiento legal	109	0%
Artículo 269 B – Obstaculización ilegítima de sistema informático o red de telecomunicación	85	0%
Artículo 211 – Calumnia	9	0%
Artículo 269 C – Intercepción de datos informáticos	8	0%
TOTAL	26122	100%

Tabla 3. Delitos 1/1/2008 a 31/07/2018

Adicional a ello en las tablas 2 y 3 se tipifica cuáles son los delitos que se usan y reportan en Colombia, se observa una mayor tendencia al Artículo 246 – Estafa con un total de denuncias 9689 de 26122 que son 37% lo largo de 01/01/2008 al 31/07/2018.

AÑO	Total, Modalidad
2008	0
2009	1
2010	2
2011	2
2012	183
2013	643
2014	2621
2015	3760
2016	4698
2017	7865
2018	5673
Total	25448

Tabla 4. Total, Modalidad en los años 2008 a 2018

Que en la fecha de 1/1/2008 al 31/07/2018 se reportaron la modalidad que usan los delincuentes informáticos los cuales indican que cada vez hay un mayor impacto en la sociedad por el crecimiento de las tecnologías, como se demuestra en la tabla 4. De las cuales encontramos que la modalidad que se usa y cuáles son las practicas más comunes que se presentaron a la de las fechas ya mencionadas en la siguiente tabla.

Modalidad	Año	Mes	Cantidad	Total	Equivale
	2008		0	0	
Ciberbullying	2009	Diciembre	1	1	100%
Defacement y Estafa por compra y/o venta a través de internet	2010	Marzo y junio	2	2	100%
Skimming y Defacement	2011	Junio y Diciembre	2	2	100%
Defacement	2012	Julio	106	183	58%
Estafa por compra y/o venta a través de internet	2013	Febrero	40	643	6%
Estafa por compra y/o venta a través de internet	2014	Octubre	259	2621	6%
Estafa por compra y/o venta a través de internet	2015	Noviembre	153	3760	10%
Defacement	2016	Enero	378	4698	26%
Vishing	2017	Agosto	1221	7865	4%
Malware	2018	Junio	301	5673	5%
Total	2009-2018			25448	

Tabla 5. Modalidad mayor reportado por mes y año.

En la tabla 5, se detalla la modalidad que se comete y que se presentaron con una mayor incidencia en cada año con su mes respectivamente, en el 2008 no se presentó ninguna denuncia que da exento de esta tabla, por lo anterior la modalidad que se cometió con una mayor incidencia en los meses de los presente años fueron los siguientes:

- 2009 ciberbullying, en el mes de diciembre con una cantidad reporte de 1 con un total 1 denuncia en el año que equivale al 100% de denuncias en el año transcurrido

- 2010 Defacement y Estafa por compra y/o venta a través de internet, en el mes de marzo y junio una cantidad reporte de 1 cada uno con un total 2 denuncias en el año que equivale al 100% de denuncias en el año transcurrido

- 2011 Skimming y Defacement, en el mes de junio y diciembre una cantidad reporte de 1 cada uno con un total 2 denuncias en el año que equivale al 100% de denuncias en el año transcurrido

- 2012 Defacement, en el mes de julio con una cantidad reporte de 106 con un total 183 denuncia en el año que equivale al 58% de denuncias en el año transcurrido

- 2013 estafa por compra y/o venta a través de internet, en el mes de febrero con una cantidad reporte de 40 con un total 643 denuncia en el año que equivale al 6% de denuncias en el año transcurrido

- 2014 estafa por compra y/o venta a través de internet, en el mes de octubre con una cantidad reporte de 259 con un total 2621 denuncia en el año que equivale al 6% de denuncias en el año transcurrido

- 2015 estafa por compra y/o venta a través de internet, en el mes de noviembre con una cantidad reporte de 153 con un total 3760 denuncia en el año que equivale al 10% de denuncias en el año transcurrido

- 2016 Defacement, en el mes de enero con una cantidad reporte de 378 con un total 4698 denuncia en el año que equivale al 26% de denuncias con fecha de corte de julio 2018

- 2017 Vishing, en el mes de agosto con una cantidad reporte de 1221 con un total 7865 denuncia en el año que equivale al 4% de denuncias en el año transcurrido

- 2018 malware, en el mes de junio con una cantidad reporte de 301 con un total 5673 denuncia en el año que equivale al 7% de denuncias en el año transcurrido.

Modalidad	Total	Porcentaje
Estafa por compra y/o venta a través de internet	5308	21%
Suplantación de identidad	3229	13%
Vishing	2967	12%
Phishing	2851	11%
Malware	2264	9%
Injuria y/o calumnia a través de internet	1535	6%
Smishing	1287	5%
Amenazas a través de internet	1108	4%
Defacement	1051	4%
Sextorsión	734	3%
Ciberbullying	581	2%
Ransomware	580	2%
Carta Nigeriana	469	2%
Publicación de imágenes/videos con menores de 18 años	404	2%
Ingeniería social	395	2%
Grooming	260	1%
Skimming	175	1%
Spoofing	80	0%
DDOS	69	0%
Suplantación de sitios web para capturar datos personales	53	0%
Turinet	48	0%
TOTAL	25448	100%

Tabla 6. Modalidad 1/1/2008 a 31/07/2018

La tabla 6, se tipifica cual es la modalidad que se usa y reportan en Colombia, se observa una mayor tendencia a los Modalidad Estafa por compra y/o venta a través de internet con un total de denuncias 5308 de 25448 que son 21% lo largo de 01/01/2008 al 31/07/2018.

AÑO	Total, Sector
2008	0
2009	1
2010	2
2011	2
2012	183

AÑO	Total, Sector
2013	648
2014	2846
2015	4086
2016	5355
2017	7989
2018	6354
TOTAL	27466

Tabla 7. Total, Sector en los años 2008 a 2018

En la fecha de 1/1/2008 al 31/07/2018 se reportaron los sectores que se vieron afectados por los delincuentes informáticos, la tabla nos indica que cada vez hay un mayor impacto en la sociedad por el crecimiento de las tecnologías. De las cuales encontramos los sectores que se ven afectados tras cometerse estos delitos informáticos y la por lo cual nombraremos los sectores que han reportado un mayor número de casos dentro de las fechas anteriormente ya mencionadas. (tabla 7 y 8).

Sector	año	Mes	Cantidad	total	Equivale
	2008			0	
Menor de edad	2009	Diciembre	1	1	100%
Ciudadano y Gobierno	2010	Marzo y Junio	2	2	100%
Ciudadano y Gobierno	2011	Junio y Diciembre	2	2	100%
Gobierno	2012	Julio	29	183	16%
Ciudadano	2013	Abril	96	648	15%
Ciudadano	2014	Octubre	463	2846	16%
Ciudadano	2015	Agosto	438	4086	11%
Ciudadano	2016	Septiembre	591	5355	11%
Ciudadano	2017	Agosto	936	7989	12%
Ciudadano	2018	Junio	687	6354	11%
Total	2009-2018			27466	

Tabla 8. Sector mayor reportado por mes y año.

Con la siguiente tabla podemos decir que los sectores que se vieron afectados y cuales ha sido mayor mente afectado cada año con su mes respectivamente, en el 2008 no se presentó ninguna denuncia que da exento de esta tabla, por lo

anterior el sector que se cometió con una mayor incidencia en los meses de los presente años fueron los siguiente tabla 9:

- 2009 menor de edad, en el mes de diciembre con una cantidad reporte de 1 con un total 1 denuncia en el año que equivale al 100% de denuncias en el año transcurrido

- 2010 ciudadano y Gobierno, en el mes de marzo y junio una cantidad reporte de 1 cada uno con un total 2 denuncias en el año que equivale al 100% de denuncias en el año transcurrido

- 2011 ciudadano y Gobierno, en el mes de junio y diciembre una cantidad reporte de 1 cada uno con un total 2 denuncias en el año que equivale al 100% de denuncias en el año transcurrido

- 2012 gobierno, en el mes de julio con una cantidad reporte de 29 con un total 183 denuncia en el año que equivale al 16% de denuncias en el año transcurrido

- 2013 ciudadano, en el mes de abril con una cantidad reporte de 96 con un total 648 denuncia en el año que equivale al 6% de denuncias en el año transcurrido

- 2014 ciudadano, en el mes de octubre con una cantidad reporte de 463 con un total 2846 denuncia en el año que equivale al 16% de denuncias en el año transcurrido

- 2015 ciudadano, en el mes de agosto con una cantidad reporte de 438 con un total 4086 denuncia en el año que equivale al 11% de denuncias en el año transcurrido

- 2016 ciudadano, en el mes de septiembre con una cantidad reporte de 591 con un total 5355 denuncia en el año que equivale al 11% de denuncias con

fecha de corte de julio 2018

- 2017 ciudadano, en el mes de agosto con una cantidad reporte de 936 con un total 7989 denuncia en el año que equivale al 12% de denuncias en el año transcurrido

- 2018 ciudadano, en el mes de junio con una cantidad reporte de 687 con un total 6354 denuncia en el año que equivale al 11% de denuncias en el año transcurrido

Sector	Cantidad	Porcentaje
ciudadano	17.998	65,53%
Financiero	3.913	14,25%
Educación	1.269	4,62%
Industrial	1.218	4,43%
Gobierno	912	3,32%
Tecnología	761	2,77%
Menor de edad	735	2,68%
Medios de comunicación	589	2,14%
Salud	71	0,26%
Total	27.466	100,00%

Tabla 9. Sector 1/1/2008 a 31/07/2018.

De acuerdo al análisis de las gráficas consultadas y analizadas mes a mes, de la página del CAI virtual, de los delitos informáticos reportados en los últimos 10 años en Colombia, se puede observar que el delito con mayor repercusión e impacto en el país está asociado al área Bancaria, para esta conclusión se tiene de apoyo la investigación realizada por la asociación Colombiana de Ingenieros de Sistemas (Acis),los cuales realizaron en el año 2017 la encuesta nacional de seguridad informática, en donde de manera aleatoria e interactiva se demuestran las tendencias en el sector de servicios financieros y banca, obtuvo el porcentaje de mayor de participación en el desarrollo de la encuesta, con un 20% y las fuerzas armadas cero, es ilógico que el último sector no posea intereses en seguridad, se podría tomar como conclusión que el sector de las

fuerzas armadas no participó en el desarrollo de la encuesta. En relación con los cargos de la persona que desarrolla la encuesta el 29%, la diligenció la persona de sistemas, pero la sumatoria de en todo el proceso, el 76% de la encuesta lo desarrollaron personas conocedoras de tecnología, se concluye que la seguridad toma el valor que debió poseer desde hace años atrás. (Junco, 2017) Según la Superintendencia Financiera de Colombia, los datos obtenidos en el último informe mensual de octubre vs septiembre de 2017 (Colombia, 2017) , se obtuvo: La Diferencia entre los meses de octubre y noviembre de tarjetas (débito y crédito) en Colombia, es diferencial en todos los bancos, las tarjetas vigentes a la fecha de cohortes y vigentes durante el mes, son positivas; pero las canceladas y bloqueadas durante el mes son negativas, ¿En qué afecta estos resultados a la seguridad?, una de ellas es:

1- Una sola tarjeta (débito y/o crédito) puede contener la capacidad de mínimo 15 tarjetas.

2- Las tarjetas pueden ser empresariales, lo que el saldo es elevado.

3- Las transacciones empresariales poseen niveles de seguridad y auditoría, igual que las de las personas naturales

El Center for Financial Inclusion afirma que, gracias al acceso omnipresente, los bajos costos, altos niveles de seguridad, y las mejoras en la productividad, la tecnología se convierte en un aliado estratégico para lograr inclusión financiera, puesto que permite el diseño de herramientas que pueden llegar a población que actualmente se encuentra excluida y por lo tanto trae beneficios en términos de desarrollo económico a todo un país. Vale la pena decir que la tecnología no necesariamente significa nuevos productos o servicios; también implica el mejoramiento y/o transformación de canales y productos existentes (ASOBANCARIA, 2015) . La seguridad es, de por sí, la necesidad de los usuarios para invertir en servicios bancarios.

- Posee los requisitos Delito informático: Es el termino genérico para aquellas acciones ilícitas realizadas por medio de internet o que tiene como objetivo destruir y dañas computadores

- Computador: Llamado común mente ordenador, computador, laptop, es una maquina electrónica que recibe y procesa datos para convertirlos en información

- Código Malicioso: Códigos maliciosos que tiene la capacidad de auto duplicarse y contagiar a otros programas, tiene tres características las cuales son producir daño al sistema, auto reproducirse en el mismo y es estar estado oculto para dificultar su búsqueda

El gobierno con el MINTIC ha dado el visto bueno para fortalecimiento de las gestiones de las TI en el estado mediante seguridad informática cumpliendo con los siguientes objetivos los cuales serían aumentar los niveles de madurez y fortalecer las capacidad en la apropiación de aspectos de seguridad y privacidad de la información, crear un modelo de gestión de TI para el estado, articulando que se creen normas de seguridad y privacidad de la información, crear confianza e interés en las empresas y ciudadanos respecto al uso apropiado de las TI en el estado.

El Ingeniero Camilo Gutiérrez asegura:

“La educación en seguridad, una responsabilidad a nivel social”

- Cambia las amenazas, pero la propagación se mantiene

- Ciber crimen: Una actividad despiadada y eficiente

- La educación no es solo cuestión de edad

- La paradoja actual: más información, menos sensación de seguridad
- Pequeños cambios hacen grandes diferencias
- La educación hace la diferencia

6. **CONCLUSIONES**

Recolectar información para observar la tendencia de la siguiente monografía era saber que incidentes informáticos y en qué cantidad se miraba afectado Colombia en los últimos 10 años, al ver los resultados dejan un nivel preocupación alto. Ya que se observa que tiene un incremento a medida que avanza la tecnología, por lo cual en las tabla de recolección de datos se pudo tipificar los delitos, modalidad y sector que se afectan cada año, de lo cual es importante fortalecer nuestra seguridad a la hora de comprar dispositivos electrónicos, así como transmitir nuestro conocimiento de una forma simple pero eficaz que ayude a evitar la proliferación de estos incidentes informados, se deben adoptar medidas antes esta problemática afecte aún más personas y a empresas a nivel nacional, lo cual generan pérdidas millonarias.

Por otro lado, se observa la seguridad informática para contrarrestar este mal, pero la ausencia de elementos y medios de comunicación hacen que el conocimiento no llegue a todas las personas, así mismo como la falta de interés de las personas para salva guarda su información personal.

La confianza de creer que no me va pasar por qué sucedió en otro lugar y creer que tiene dominado las tecnologías, al saber que como parte de la misma los incidentes informáticos van evolucionando y adaptándose al entorno que se encuentra para explotar todo tipo de vulnerabilidad, aunque podemos evitarlos ya que algunos incidentes necesitas algunos requisitos mínimos para poder realizar su actividad, si los podemos detectar a tiempo podemos corregir y disminuir en gran medida los incidente informáticos que se comente a diario en Colombia.

7. **RECOMENDACIONES**

Las recomendaciones se entregan en relación en tres aspectos, aquellos que forman parte de los sistemas informáticos. En el capítulo 5 del presente trabajo se desarrollan recomendaciones informáticas.

7.1 RECOMENDACIONES LOGÍSTICAS

Las recomendaciones logísticas están basadas en las características de la empresa, ellas son:

1. Abastecer un buen proveedor de servicios de conectividad.
2. Realizar una encuesta de seguimiento a proveedores.
3. Aplicar evaluación a proveedores, con peridiocidad definida. El desarrollo de evaluación como lista de chequeo,

7.2 RECOMENDACIONES USUARIOS

Los usuarios son en realidad los mayores beneficiarios de los servicios de la empresas, pero depende de ellos la seguridad primaria de todo sistema de información. Las recomendaciones básicas serán:

1. Evaluación de las necesidad es de información de los ususarios finales.[30]

[30] KOTLER, Philip; ARMSTRONG, Gary. *Fundamentos de marketing*. Pearson Educación, 2016.

2. Crear contraseñas seguras y no compartirlas, cambiar la clave cada 90 días (máximo).

3. No compartir la contraseña.

7.3 RECOMENDACIONES ADMINISTRATIVAS

Entre ellas se tiene:

1. Plan de auditorías bimensuales, semestrales y anuales.

2. La implementación de incadores de éxito.

3. Realizar procesos y procedimientos conformes a las necesidades y misionalidades de la empresa.

4. Los mercadólogos obtienen puntos de vista (insight) de los clientes y mercado[31], con ello la empresa logra un posicionamiento en el campo.

5. Comunicación directa con el cliente.

6. Segmentación del mercado de consumo, en donde se establece las capacidades emrpesariales.

7. Formlación de la declaración de la misión empresarial, siendo el llamado general de la acción y de be partir del supuesto de la organización como un todo se comprometerá a cumplir esa misión.[32]

---

[31] KOTLER, Philip; ARMSTRONG, Gary. *Fundamentos de marketing*. Pearson Educación, 2016.

[32] CHIAVENATO, Idalberto; SAPIRO, Arao. *Planeación estratégica*. McGraw-Hill Interamericana,

8. Designar permisos a los usuarios en cierto nivel para el uso de la información.

2017.

8. BIBLIOGRAFIA

1. AMAYA GUTIERREZ, Camilo, {en línea}, "importancia de la gestión de incidentes para la seguridad de la información".7 de enero de 2013 WeLiveSecurity by ESET.(https://www.welivesecurity.com/la-es/2013/01/07/importancia-gestion-incidentes-seguridad-informacion/).

2. B´SECURE. Pasión por la seguridad. {en línea} .Protección de correo electrónico. S.f. www.b-secure.co. (https://www.b-secure.co/estrategias/infraestructura/proteccion-de-correo-electronico).

3. BBVA. { En línea}. Crecen los atracos cibernéticos. S.f. (https://www.bbva.com/wp-content/uploads/2018/11/smishing-1024x427.png)

4. BETANCUETH, Valeria.La cumbre mundial sobre la sociedad de la información (CMSI) proceso y temas debatidos. {En línea} (https://www.apc.org/sites/default/files/wsis_process_ES.pdf).

5. CAI VIRTUAL POLICIA NACIONAL. 10,10,2019. Ciberincidentes.{En línea}.(https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real).

6. CALLEGARI, Nidia. Delitos informáticos y legislación. {En línea}. Septiembre - Octubre, 1985. Disponible en: (https://revistas.upb.edu.co/index.php/derecho/article/viewFile/6054/5551).

7. CHIAVENATO, Idalberto; SAPIRO, Arao. Planeación estratégica. McGraw-Hill Interamericana, 2017.

8. CONVENIO SOBRE LA CIBERDELINCUENCIA. (23, OCTUBRE, 2001: Budapest, Hungría). Serie de tratados Europeos. 26 p. (https://www.oas.org/juridico/english/cyb_pry_convenio.pdf)

9. D´ADAMO, Lucia. Qué es y en qué consiste un ataque informático {En línea}.{18 de julio de 2017} disponible en : (https://www.consulthink.it/es/que-es-y-en-que-consiste-un-ataque-informatico/).

10. DAVIVIENDA. 20,08,2015. Consigné un cheque en mi cuenta, ¿En cuánto tiempo tengo disponible mi dinero?. .{En línea}. (http://davivienda.custhelp.com/app/answers/detail/a_id/226/~/consign%C3%A9-un-cheque-en-mi-cuenta%2C-%C2%BFen-cu%C3%A1nto-tiempo-tengo-disponible-mi-dinero%3F).

11. DINCA, Claudia Florentina. Fraudes en internet. 14,06,2016. .{En línea}. (http://repositori.uji.es/xmlui/bitstream/handle/10234/161252/TFG_2016_DincaClaudia.pdf?sequence=1&isAllowed=y).

12. EL HERALDO. 18,12,2016. Casas de remate, una mina para los estafadores. .{En línea}. (https://www.elheraldo.co/barranquilla/casas-de-remate-una-mina-para-los-estafadores-312237).

13. EL TIEMPO, 06,02,2011 . Crecen los 'ciberatracos'. Www.eltiempo.com.co (https://www.eltiempo.com/archivo/documento/MAM-4381268) .

14. EL TIEMPO, 25,06,2015. El ciberdelincuente que viajó por el mundo con millas de los famosos. .{En línea}. Www.eltiempo.com.co (https://www.eltiempo.com/archivo/documento/CMS-16006809) .

15. EL TIEMPO, 28,06,2017. Tecnosfera. www.eltiempo.com. (https://www.eltiempo.com/tecnosfera/novedades-tecnologia/las-razones-por-las-que-el-secuestro-de-datos-se-esta-popularizando-103528).

16. GARCIA, Marcia. International Youth Coalition. 31,JULIO.2015. (https://iycoalition.org/quien-olvida-su-historia-esta-condenado-a-repetirla/).

17. INFORMATICA FORENSE COLOMBIA, 28,11,2019. www.informaticaforense.com. .{En línea}. (https://www.informaticaforense.com.co/smishing/).

18. KASPERSKY. Tipos de amenazas conocidas. {En línea}.{1 de febrero de 2019. (https://support.kaspersky.com/sp/614).

19. kidshelpline. 2019. (https://kidshelpline.com.au/sites/default/files/bdl_image/Teen%20girl%20being%20cyberbullied_3.png).

20. KOTLER, Philip; ARMSTRONG, Gary. Fundamentos de marketing. Pearson Educación, 2016.

21. LARRAHONDO, Daniela. Delitos informáticos, una amenaza creciente. {En línea}. {8 de noviembre de 2017} disponible en: (https://www.usc.edu.co/index.php/noticias/item/3693-delitos-informaticos-una-amenaza-creciente).

22. Mejia Quijano, R. M. (2013). Identificación de Riesgos. Medellín: Colección Académica – EAFIT.

23. MINISTERIO DE ASUNTOS EXTERIORES , UNIÓN EUROPEA Y COOPERACIÓN. ¿Qué es la OCDE?. {En línea}. {11 de diciembre de 2018}. (http://www.exteriores.gob.es/RepresentacionesPermanentes/OCDE/es/quees2/Paginas/default.aspx).

24. MINISTERIO DE ASUNTOS EXTERIORES , UNIÓN EUROPEA Y COOPERACIÓN. ¿Qué es la OCDE?. {En línea}. {11 de diciembre de 2018}. (http://www.exteriores.gob.es/RepresentacionesPermanentes/OCDE/es/quees2/Paginas/default.aspx).

25. MINISTERIO DE ASUNTOS EXTERIORES , UNIÓN EUROPEA Y COOPERACIÓN. ¿Qué es la OCDE?. {En línea}. {11 de diciembre de 2018}. (http://www.exteriores.gob.es/RepresentacionesPermanentes/OCDE/es/quees2/Paginas/default.aspx).

26. NEIRA MARCIALES, Laura. 28,08,2019. Cinco de cada 10 colombianos cambian el celular cada dos años. LA REPÚBLICA. Www.larepublica.com.co. (https://www.larepublica.co/empresas/cinco-de-cada-10-colombianos-cambian-el-celular-cada-dos-anos-2902128).

27. PACKETLIFE. Templating configuraciones de dispositivos. 8,10,2019. .{En línea}. (http://packetlife.net/media/blog/attachments/338/neighbor_spoofing.png).

28. PEREZ, JM. Ejemplo de timo nigeriano, la donación de la señora Ruth Hamsonhttps. {En linea}. {20,10,2014}(https://www.hijosdigitales.es/es/2014/10/ejemplo-de-timo-nigeriano-la-donacion-de-la-senora-ruth-hamson/).

29. PREMIERE CONSUMER. La Estafa Nigeriana: Conózcala y Protéjase.

30. REVISTA DINERO. 02,02,2017. El apetitoso negocio del cibercrimen. .{En línea}. (https://www.dinero.com/edicion-impresa/tecnologia/articulo/las-cifras-que-mueven-el-cibercrimen-a-nivel-global/241593).

31. REVISTA DINERO. 7,2,2017. ¿Cómo evitar caer en las estafas de productos fantasma por internet?. .{En línea}. (https://www.dinero.com/empresas/articulo/evite-estafas-de-productos-fantasma-por-internet/247161).

32. RIVERO,Mario. GOOTTSCHALK, Franz. Los Ataques de Skimming en Cajeros Automáticos y Cómo Prevenirlos. {En línea}. {2014}. (https://usa.visa.com/dam/VCOM/download/merchants/Webinar-Preventing-ATM-Skimming-Spanish-021914.pdf).

33. ROTTA, Santiago. Estas son las amenazas de seguridad informática de las que se debe cuidar. En: El espectador, Bogotá, 18, febrero,2016.

34. SANCHEZ, Andrea Sánchez. ¿Cómo prevenir compras fraudulentas en una tienda en línea?, {En línea}. {20 de agosto de

2019}.(https://www.internetya.co/como-prevenir-compras-fraudulentas-en-una-tienda-en-linea/).

35. SEMANA, 28,12,2017. El cibercrimen en 2017: la amenaza crece sobre Colombia. Www.semana.com.co. .{En línea}. (https://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2017/551979).

36. SERRANO BUITRAGO, Edison Raul. La práctica de los delitos informáticos en Colombia. Universidad Militar Nueva Granada. Bogotá, 2014. 26 p.

37. TECNOKRATIX. Ransonware. .{En línea}. (https://tecnokratix.net/wp-content/uploads/Ransomware-pic-770x433.jpg).

38. TELLEZ VALDEZ, Julio. Derecho informático. {En línea}. {2008}. (https://clauditha2017.files.wordpress.com/2017/09/derecho-informatico-cuarta-edicion-julio-tc3a9llez-valdc3a9z.pdf).

39. TEST DE VELOCIDAD. .{En línea}. (https://www.testdevelocidad.es/app/uploads/2018/03/ntp-amplification-botnet-ddos-attack.png).

40. WELIVESECURITY. 8,08,2017.Engaños reinventados: phishing, smishing y archivos adjuntos ahora trabajan en equipo. .{En línea}. (https://www.welivesecurity.com/la-es/2017/08/08/phishing-smishing-adjuntos-combinados/).

41. XATAKA. 26,08,2016. Así están robando a los vendedores por internet en Colombia.{En línea}. (https://www.xataka.com.co/seguridad/asi-estan-robando-a-los-vendedores-por-internet-en-colombia)

9. WEBGRAFÍA

10. ANEXOS

ANEXO A

1. CIRCULAR 01 de diciembre 15 del 2000[36] DERECHOS DE AUTOR

El derecho de autor es una forma de propiedad privada que reconoce una protección jurídica especial al autor como creador de una obra literaria o artística, entendida como tal, toda expresión personal de la inteligencia manifestada en forma perceptible y original.

A esos efectos, la Dirección Nacional de Derecho de Autor, Unidad Administrativa Especial adscrita al Ministerio del Interior, en desarrollo de su objeto de brindar asesoría general en materia de derecho de autor y derechos conexos o afines a éste; ejercer la inspección y vigilancia sobre las sociedades de gestión colectiva de los mencionados derechos; inscribir en el registro las obras literarias y artísticas, los contratos y actos vinculados con el derecho de autor y los derechos conexos; propender por la difusión y la promoción de esa rama de la propiedad intelectual; y fijar las políticas gubernamentales, que en torno a esa disciplina jurídica, requiere nuestro país, se permite ilustrar a las sociedades comerciales y civiles en el cumplimiento de la Ley 603 del 27 de julio de 2000, por la cual se modifica el artículo 47 de la Ley 222 de 1995, que establece como una de las obligaciones de los representantes legales de las sociedades, incluir dentro de su informe de gestión, el grado de cumplimiento de la legislación referente al derecho de autor, en los siguientes términos:

_____

"Artículo 1º. El artículo 47 de la Ley 222 de 1995, quedará así:

"Artículo 47. Informe de gestión. El informe de gestión deberá contener una

exposición fiel sobre la evolución de los negocios y la situación económica, administrativa y jurídica de la sociedad.

"El informe deberá incluir igualmente indicaciones sobre:

1. Los acontecimientos importantes acaecidos después del ejercicio.

2. La evolución previsible de la sociedad.

3. Las operaciones celebradas con los socios y con los administradores.

4. El estado de cumplimiento de las normas sobre propiedad intelectual y derechos de autor por parte de la sociedad.

"El informe deberá ser aprobado por la mayoría de votos de quienes deban presentarlo. A él se adjuntarán las explicaciones o salvedades de quienes no lo compartieren.

"Artículo 2º. Las autoridades tributarias colombianas podrán verificar

El estado de cumplimiento de las normas sobre derechos de autor por parte de las sociedades para impedir que, a través de su violación también se evadan tributos."

Según la disposición legal, corresponde a los representantes de las sociedades comerciales o civiles elaborar dentro de su informe de gestión un panorama del cumplimiento de las normas de propiedad intelectual, específicamente, del derecho de autor.

En consideración a lo señalado por la Ley 603 de 2000, y de conformidad con el marco de protección cimentado por los acuerdos internacionales y la normatividad colombiana vigente en materia de derecho de autor, esta Dirección ha advertido la relevancia de emitir unas recomendaciones de orden práctico a fin de que sean

tenidas en cuenta por parte de las sociedades, en los siguientes términos:

1. El principio fundamental del derecho de los creadores de obras literarias y artísticas, tales como programas de computador, bases de datos, libros, obras fotográficas, obras audiovisuales, obras musicales, etc., consiste en que toda utilización de aquellas requiere ser autorizada de manera previa y expresa por sus autores o legítimos titulares;

2. Las interpretaciones o ejecuciones de los artistas, las fijaciones sonoras de los productores fonográficos y las emisiones de los organismos de radiodifusión (radio y televisión) se encuentran protegidas como derechos conexos al derecho de autor. Tales prestaciones requieren de la respectiva autorización por parte de sus legítimos titulares para poder ser utilizadas;

3. Para hacer uso de obras protegidas por el derecho de autor o de las interpretaciones o ejecuciones de artistas intérpretes o ejecutantes, de las grabaciones fonográficas y de las emisiones de los organismos de radiodifusión, protegidas por los derechos conexos al derecho de autor, es necesario contar con las autorizaciones debidamente soportadas en contratos de licencia de uso, para así entender dichas utilizaciones como legales;

4. Para la adquisición de derechos de autor, de obras realizadas mediante encargo por parte de las sociedades, bien sea mediante contratos de prestación de servicios o bajo contratos laborales, es necesario que se observen las formalidades prescritas por el artículo 183 de la Ley 23 de 1982, que establece que la transferencia de los derechos, vía cesión, debe constar en escritura pública o en documento privado con diligencia de reconocimiento de firma y contenido ante notario (artículo 183 de la Ley 23 de 1982);

5. Para que los contratos, en virtud de los cuales se negocia la adquisición o uso de derechos de autor o de derechos conexos, tengan efectos

ante terceros, deben ser inscritos en el Registro Nacional de Derecho de Autor de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor; sin embargo, la omisión de este requisito no invalida la negociación entre las partes (artículo 183 Ley 23 de 1982 y artículo 6 de la Ley 44 de 1993);

6. la sociedad hace uso de obras musicales, aún en el ámbito privado, se encuentra obligada a cumplir con el pago por concepto de comunicación pública de la música ante las sociedades que administran, recaudan y distribuyen dichos derechos, como son la Sociedad de Autores y Compositores de Colombia, SAYCO, y la Asociación Colombiana de Intérpretes y Productores Fonográficos, ACINPRO;

7. En materia de utilización de programas de computador (software), las sociedades deben contar con las respectivas licencias de uso para el número de equipos de computador permitidos por la licencia. Los usos o explotación de los programas deben ser no más que los autorizados expresamente en el contrato de licencia de uso y la licencia debe estar vigente al momento de la utilización de los programas;

8. Si la sociedad ha adquirido legalmente los derechos patrimoniales de autor sobre una obra, no le es dable desconocer los créditos de quién la creó, puesto que debe mencionarse el nombre del creador con cada utilización (paternidad); tampoco es posible entrar a modificar, mutilar, deformar o alterar el contenido de la obra (integridad), conforme a los postulados del derecho moral de autor de la obra;

9. La responsabilidad en materia de violaciones al derecho de autor y derechos conexos, está regulada en su parte civil, por el artículo 242 y ss. de la Ley 23 de 1982, que remite a las disposiciones del Código Civil en lo atinente a la indemnización por daños y perjuicios dentro del régimen de responsabilidad civil extracontractual (artículo 2.341). En lo pertinente a la

responsabilidad penal, se encuentra determinada por el artículo 51 y ss. de la Ley 44 de 1993 que señala penas de prisión e imposición de multas.

Tales sanciones, así como los trámites procesales jurídicos, se encuentran igualmente contemplados en los nuevos Código Penal y Código de Procedimiento Penal (Ley 599 y 600 de 2000 respectivamente), los cuales entrarán en vigencia en el mes de julio del año 2001.

ANEXO B

Se entrega Caracterización Caí Virtual Delitos-Incidencias-Sector fecha 01-01-2008 al 31-0-2018 en formato .xls a la dirección que sea solicitada para su repositorio.

ANEXO C

Normatividad sobre delitos informáticos

CÓDIGO PENAL COLOMBIANO LEY 599 DE 2000

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones. 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para sí o para un tercero. 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave.

1. **TITULO:** Incidentes informáticos y sus consecuencias en Colombia en los últimos 10 años

2. **AUTOR:** Jair Andrés Guerrero Garzón

3. FUENTE BIBLIOGRÁFICA

AMAYA GUTIERREZ, Camilo, {en línea}, "importancia de la gestión de incidentes para la seguridad de la información".7 de enero de 2013 WeLiveSecurity by ESET.(https://www.welivesecurity.com/la-es/2013/01/07/importancia-gestion-incidentes-seguridad-informacion/).

B´SECURE. Pasión por la seguridad. {en línea} .Protección de correo electrónico. S.f. www.b-secure.co. (https://www.b-secure.co/estrategias/infraestructura/proteccion-de-correo-electronico).

BBVA. { En línea}. Crecen los atracos cibernéticos. S.f. (https://www.bbva.com/wp-content/uploads/2018/11/smishing-1024x427.png)

BETANCUETH, Valeria.La cumbre mundial sobre la sociedad de la información (CMSI) proceso y temas debatidos. {En línea} (https://www.apc.org/sites/default/files/wsis_process_ES.pdf).

CAI VIRTUAL POLICIA NACIONAL. 10,10,2019. Ciberincidentes.{En línea}.(https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real).

4. RESUMEN

En los últimos tiempos y con la evolución de la tecnología, se habla contínuamente de procesos y procedimientos, basados en el ciclo deming PHVA, para establecer las responsibilidades y las respectivas auditorías, que permiten determinar la mayor evidencia fiable para hacer una medición a los incidentes cibernéticos, como uno del elemento que se han tenido en cuenta para dejar constancia del impacto que dejan en nuestra sociedad, abordando los temas de las delitos, modalidad y sector más afectado a lo de diez años.

5. PALABRAS CLAVES

Ciberdelincuencia, ciberataque, ataques informáticos, riesgo de seguridad digital, auditoría de sistemas.

6. CONTENIDOS

Los temas tratados son skimming- fraude con tarjetas debito y credito, estafa, malware, smishing, carta nigeriana, phishing, ciberbullying, vishing, ransomware,ddos, poofing. Identificar la repercusión de los incidentes informáticos bajo la aplicación de la normatividad colombiana en lo referente a seguridad informática

7. DESCRIPCIÓN DEL PROBLEMA DE INVESTIGACIÓN

Los incidentes informáticos, van a la vanguardia de la innovación tecnológica, tienen un modus operandi de técnicas, que permiten desarrollar y emplear funciones para cometer delitos informáticos tanto a personas como empresas, la efectividad de los delitos informáticos, se ve fundamentada básicamente en el bajo conocimiento de seguridad y confianza que tienen los operadores de dispositivos electrónicos, en lo cual el cibercrimen ha encontrado un nicho de negocio basto para explotar, para evitar que el ciudadano y empresas Colombianas se vean afectadas por este tipo de incidentes se recrea el escenario perfecto para presentar un estudio de los incidentes informáticos que se han presentado a lo largo de los últimos 10 años, obteniendo una información fiable a la hora saber que delitos se comete en Colombia, la modalidad y que sectores se ven afectados.

8. OBJETIVO

8.1 GENERAL

Identificar los incidentes informáticos registrados en Colombia en la última década.

8.2 ESPECÍFICOS

Gestionar Recolectar información relacionada con la tipificación de delitos informáticos.

Identificar la repercusión de los incidentes informáticos bajo la aplicación de la normatividad Colombiana en lo referente a seguridad informática.

Mitigar los riesgos de seguridad, mediante la entrega de recomendaciones

9. METODOLOGÍA

El proceso de investigación será de tipo descriptivo, el cual permite el estudio de una situación o fenómeno con el uso de variables cuantitativas y cualitativas, debido a que este estudio busca especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno. Haciendo énfasis en el estudio independiente de cada característica, con el fin de determinar cómo es y cómo se manifiesta la situación. El método de investigación a utilizar será el inductivo, pues este analiza casos particulares, cuyos resultados son tomados para extraer conclusiones de carácter general.

10. PRINCIPALES REFERENTES TEÓRICOS Y CONCEPTUALES

En Colombia, la primera ley que se debe aplicar y concientizar a las empresas, es la ley 1581 de 2012, protección de datos personales, entendiendo como dato personal, cualquier información vinculada o que puede asociarse a una o varias personas naturales que, dependiendo de su grado de utilización y acercamiento con la intimidad de las prsonas podrá ser pública, semiprivada o privada. Sumado a ello, el registro Nacional para la Base de Datos, reglamentado por el Decreto Nacional 886 de 2014, en donde enfatiza “Serán objeto de inscripción en el Registro Nacional de Bases de Datos, las bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al Responsable del Tratamiento o al Encargado del Tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales”[1].

[1] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES. Decreto 886 (13 de mayo de 2014). Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.

11. RESULTADOS Y CONCLUSIONES

Recolectar información para observar la tendencia de la siguiente monografía era saber que incidentes informáticos y en qué cantidad se miraba afectado Colombia en los últimos 10 años, al ver los resultados dejan un nivel preocupación alto. Ya que se observa que tiene un incremento a medida que avanza la tecnología, por lo cual en las tabla de recolección de datos se pudo tipificar los delitos, modalidad y sector que se afectan cada año, de lo cual es importante fortalecer nuestra seguridad a la hora de comprar dispositivos electrónicos, así como transmitir nuestro conocimiento de una forma simple pero eficaz que ayude a evitar la proliferación de estos incidentes informados, se deben adoptar medidas antes esta problemática afecte aún más personas y a empresas a nivel nacional, lo cual generan pérdidas millonarias.

Por otro lado, se observa la seguridad informática para contrarrestar este mal, pero la ausencia de elementos y medios de comunicación hacen que el conocimiento no llegue a todas las personas, así mismo como la falta de interés de las personas para salva guarda su información personal.

La confianza de creer que no me va pasar por qué sucedió en otro lugar y creer que tiene dominado las tecnologías, al saber que como parte de la misma los incidentes informáticos van evolucionando y adaptándose al entorno que se encuentra para explotar todo tipo de vulnerabilidad, aunque podemos evitarlos ya que algunos incidentes necesitas algunos requisitos mínimos para poder realizar su actividad, si los podemos detectar a tiempo podemos corregir y disminuir en gran medida los incidente informáticos que se comente a diario en Colombia.

Bogotá, El Ministerio, 2014.