ANÁLISIS DEL COMPORTAMIENTO DEL CIBERCRIMEN EN EL MUNICIPIO DE QUIBDÓ, DEPARTAMENTO DEL CHOCÓ.

RUTH YADIRA MOSQUERA PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD -
FACULTAD ESCUELA DE CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
QUIBDÓ – CHOCÓ
2018

ANÁLISIS DEL COMPORTAMIENTO DEL CIBERCRIMEN EN EL MUNICIPIO DE QUIBDÓ, DEPARTAMENTO DEL CHOCÓ.

RUTH YADIRA MOSQUERA PARRA

Monografía para optar al título de:
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Asesor: SALOMÓN GONZÁLEZ GARCÍA.
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD -
FACULTAD ESCUELA DE CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
QUIBDÓ – CHOCÓ
2018

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma de Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Quibdó, 20 de Febrero de 2018

DEDICATORIA

Primero a Dios que es la base de todo en mi vida, esposo, mis hijos; Wendy Yadira y Rodrigo Yadir, por su apoyo y comprensión en este proceso de mi vida, a familiares, quienes fueron el pilar en los primeros pasos de conocimientos adquiridos y lo hicieron con mucha sabiduría, con un gran amor incondicional en cada paso de mi vida, me enseñaron virtudes como ser perseverante, la cual permitió cumplir muchas metas en mi vida, Dios los bendiga.

Ruth Yadira Mosquera Parra

AGRADECIMIENTOS

Deseo expresar mis más sinceros agradecimientos a:

A la Universidad Nacional Abierta y a Distancia UNAD, como institución educativa fue un medio para conseguir este sueño, contribuyendo en mi crecimiento académico inspirador para la formación humana y profesional.

Ing. Salomón González, por ser una guía incondicional que plasmando perseverantemente en cada una de sus apreciaciones su gran inteligencia y valores propios del ser humano completo.

A los demás tutores involucrados en el transcurso de la Especialización, que me orientaron en cada uno de los cursos, y a los compañeros de postgrado, por cooperar y brindarme sus apreciables conocimientos, su profesionalismo, los que estuvieron en las dificultades, dejarnos experiencias permanentes que nos ayudaron a en la búsqueda de esta meta.

CONTENIDO

Pág.

LISTA DE ILUSTRACIONES

Pág.

LISTA DE TABLAS

Pág.

LISTA DE GRAFICAS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

Los ataques de cibercrimen que soportaran los sitio web, es una es una muestra de que ninguno(a) persona u organización está exenta de ser vulnerada. Dicho lo anterior, se destaca que el comportamiento humano es el primordial origen de una amenaza cibernética pasando al cibercrimen. Es transcendental conocer cuál es la el índice de educación que tiene cada persona que ingresa a Internet y si es consciente de los riesgos que este significa. La comisión significativa o importante es, que quien decide el nivel de inseguridad en el ingreso a web no corresponde al virus, Tiene que ver con el comportamiento humano que hace que esa agresión sea un exitoso. El objetivo de esta investigación consiste es como analizar cómo se comporta el cibercrimen en el municipio de Quibdó, partiendo de evidencias que permitan establecer las conductas de las buenas prácticas que se requieren para resguardar la información online, tanto en lo personal como en la vida profesional.

De allí que al no poseer de una habilidad de seguridad informática fuerte o solida se conviertan en objetivos perfectos de los cibercriminales, es importante enfatizar que las empresas y las personas en particular deben de reflexionar la forma en que tratan la información, el valor de contenida en la información y el eventual riesgo de perderla o que se vuelva pública. Frente a los delitos informáticos se hace evidente que hay que estudiar medidas de defensa que la población Quibdoseña reduzcan el ingreso a datos personales. El cibercrimen se entiende como una situación seria en esta ciudad, y aun que su índice todavía es bajo en comparación a otras ciudades del país, él no está orientado a algunas empresas o personas, sino que todos estamos expuestos. Es importante que esta monografía, llegue y se difunda para que cada uno de los habitantes de este municipio conozca y en la norma legal colombiana en todo su contexto en materia de derecho.

Palabras clave — Cibercrimen, Comportamiento, Ataque, riesgo, Sitios Web, Seguridad Informática, Norma Legal, Tecnologías de la Información, delitos informáticos.

ABSTRACT

The cybercrime attacks that support the website, is a sign that no person or organization is exempt from being violated. That said, it is emphasized that human behavior is the primary source of a cybercrime threat to cybercrime. It is transcendental to know what is the education index that each person who enters the Internet has and if he / she is aware of the risks that this means. The significant or important commission is that who decides the level of insecurity in the web entry does not correspond to the virus, It has to do with the human behavior that makes that aggression a success. The objective of this research is how to analyze how cybercrime behaves in the municipality of Quibdó, based on evidence that allows to establish the behaviors of good practices that are required to safeguard online information, both personally and professionally. .

Therefore, since they do not possess a strong or solid computer security skill, they become perfect targets for cybercriminals, it is important to emphasize that companies and individuals in particular must reflect on the way they treat information, the value of content. in the information and the eventual risk of losing it or that it becomes public. In the face of cybercrime, it is evident that defense measures must be studied to reduce the access to personal data for the Quibdoseña population. Cybercrime is understood as a serious situation in this city, and even though its index is still low compared to other cities in the country, it is not aimed at some companies or people, but we are all exposed. It is important that this monograph, arrive and be disseminated so that each of the inhabitants of this municipality knows and in the Colombian legal norm in all its context in the matter of law.

Keywords - Cybercrime, Behavior, Attack, risk, Websites, Computer Security, Legal Standard, Information Technology, computer crimes.

INTRODUCCIÓN

Las redes y las computadoras están en constate desarrollo, integrando a la sociedad e invitando a compartir recursos electrónicos utilizando una gran plataforma como lo es el internet, por eso es importante buscar tácticas para proteger los datos.

Resaltando lo importante que es la información siendo este un recurso de las compañías, y con esta ser competitivos esta misma forja a ser competidores, permitiendo esto volverse el blanco de los cibercriminales y ser atacados por este. Por ello la necesidad de implementar todas las practicas pertinentes, que permitan las medidas tendientes a reconocer riesgos y la vulnerabilidad de la red. Sin embargo los ataques del cibercrimen hacen parte de la vida cotidiana ya sea virtual o electrónica, esto consiente en intercambiar datos en las redes sociales y correos etc… puede ser vulnerada, conllevando a que al obtener el atacante información confidencial de las persona, esto puede afectar tanto su vida financiera y su integridad.

Con este estudio en la ciudad de Quibdó, se fundaría un poco de conciencia para que aprendan y conozcan las diferentes herramientas de protección y las puedan aplicar en su diario vivir.

1. TÍTULO DEL PROYECTO

ANÁLISIS DEL COMPORTAMIENTO DEL CIBERCRIMEN EN EL MUNICIPIO DE QUIBDÓ, DEPARTAMENTO DEL CHOCÓ.

2. PLANTEAMIENTO DEL PROBLEMA

Quibdó es un municipio del departamento del Chocó, tiene un clima húmedo y temperatura hasta de 38ºC, es una ciudad biodiversa; cuenta con una variedad de instituciones tanto públicas, privadas, comercio y con una población que no se queda atrás con el crecimiento tecnológicos en la actualidad; formando parte de esta sociedad consumista en entornos virtuales y electrónicos, estando expuesta a cibercrimenes, aunque son pocos, estos dañan claramente la integridad, la confidencialidad y seguridad de la información

En Quibdó, se han presentados sucesos de casos de delitos informáticos que han afectado la privacidad y moral de sus coterráneos, por ello ya se está temiendo por la integridad de los datos empresarial y personal.

Un principal problema es que hay un grado de ignorancia o desconocimiento en relación al cibercrimen y la ley que protege frente a este delito, hay que crear una misma línea de ayuda, cuando se juntan esfuerzo al combatir esta modalidad que tanto daño hace a la sociedad, con la realización de estudios o investigación que permita afianzar conocimientos y así aprender a reducir el número de víctimas de los posibles riesgos a que se está sometido tanto organizaciones como el usuario común en este mundo de tecnología.

La población Quibdoseña, También esta con una amenaza latente como lo es los delitos informáticos en todas sus características.

3. FORMULACIÓN DEL PROBLEMA

¿Al estudiar y analizar el comportamiento del cibercrimen en la ciudad de Quibdó a través de una monografía de investigación ayudaría a disminuir el impacto?

4. JUSTIFICACIÓN

Desde tiempos atrás, la información viaja a través de medios de comunicación denominadas redes de datos, las cuales requieren ser manejadas con un mínimo de criterios de seguridad, y a medida que se ha evolucionado la vulneración a que se ven sometidos los sistemas y redes informáticas, se presenta por los ineficientes filtros de seguridad con los que cuentan la mayoría de las empresas y las personas en su vida cotidiana, ya que no había conocimientos relacionados con la realización de un método de seguridad eficaz que resguardará los recursos informáticos de todas las existentes intimidaciones frecuentes del ciberciminal en el ciberespacio. A nivel general en el mundo de internet las redes de datos en todas las compañías han avanzado en todas las circunstancias en los cuales se desempeña el ser humano, son muchos los riesgos a los que se expone la información al viajar por la red, ya sea inalámbrica o cableada. El desarrollo del estudio en la ciudad de Quibdó que se planteó pone en evidencia la importancia de aplicar medidas de seguridad fiable y oportuna que permitan minimizar y neutralizar los riesgos como son los datos.

En Colombia se empieza a hablar de delitos informáticos a partir de la promulgación de la Ley 1273 de 2009. Esta nueva ley contiene dos tipos de conductas de delitos Informáticos: Los que atentan contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos como: Acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicaciones, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, Suplantación de sitios web y los atentados informáticos y otros, se encuentran dos delitos tipificados: Hurto por medios informáticos, transferencia no consentida de activos.

Actualmente es de suma necesidad conocer el funcionamiento, las potenciales vulnerabilidades y amenazas a que están expuesto los pobladores de la ciudad de Quibdó, cabe anotar que para contribuir el cibercrimen se debe tener una buena orientación, organización y enseñanza o preparación en el manejo de los sistemas y recurso, lo que garantizara la disminución a las vulnerabilidades que siempre están expuestas, permitiendo así que se contrarreste los riesgos.

El desarrollo de la presente investigación nos permitirá conocer cómo se comportan los diferentes tipos de delitos informáticos y las principales características de estos, que afectan de manera considerable la confiabilidad, integridad y disponibilidad de la información aprovechándose de las vulnerabilidades que presentan Internet, dispositivos y sistemas involucrados.

Para el caso de la ciudad de Quibdó, esta no ha sido ajena a este tipo de conductas, pues han empezado a aparecer delitos asociados al uso malintencionado de procesadores electrónicos de comunicación, lo que supone una alerta para nuestra sociedad en este sentido.

Con esta investigación, se pretende obtener información valiosa que contribuya a que los pobladores de Quibdó, puedan conocer de manera confiable, cuales con las principales tendencias de los delitos informáticos a nivel nacional, y cuales han empezado a cometerse en la ciudad. Cuáles son las principales caracterices de los delincuentes, los cuales ya no está en un determinado sitio geográfico, pues la globalización y el uso del internet convirtieron al mundo en una “aldea”; de modo tal, que nos enfrentamos a un enemigo cada vez más escurridizo ya que se mueve con la agilidad de la web.

Afrontar y conocer adecuadamente los contextos legales derivados del uso y desarrollo de la informática y de telecomunicaciones, propias del quehacer cotidiano.

Con este análisis se obtendrá un mayor conocimiento de las características y del impacto que este tipo de actividad maliciosa tiene sobre las personas y las entidades, afectando de manera negativa su patrimonio. Contribuirá a dimensionar adecuadamente el problema, y a establecer las acciones que se deben promover para minimizar el riesgo de ser víctima del delito informático a través de la formulación de recomendaciones.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Conocer el comportamiento del Cibercrimen en la ciudad de Quibdó, entre el año 2014 a 2017, por medio Investigación de campo y análisis de los casos presentados en la localidad.

5.2 OBJETIVOS ESPECÍFICOS

Identificar los diferentes casos de cibercrimen ocurridos en la ciudad de Quibdó y sus características.

Establecer cuál es la tendencia de la comisión de cibercrimenes en esta localidad.

Realizar encuestas para determinar el grado de conocimiento de la población frente a los delitos informáticos.

Proponer recomendaciones para contrarrestar la ocurrencia de la actividad maliciosa.

6. ALCANCE Y DELIMITACIÓN DEL PROYECTO

6.1 ESPACIAL

Reflexionando que este es un problema que afecta a todos, este proyecto analizará el comportamiento del Cibercrimen y se desarrollará en el Municipio de Quibdó, Departamento del Choco.

Este proyecto de investigación será desarrollado dentro de los estándares y normas de seguridad informática Nacionales e Internacionales, considerando las directrices institucionales de la Universidad Nacional Abierta y a Distancia – UNAD, y la asesoría de los tutores de la red de conocimiento.

6.2 TEMPORAL

Tomando como base de investigación, para el desarrollo de este proyecto, se estudiaran los años 2015 y 2016.

7. DISEÑO METODOLÓGICO

7.1 TIPO DE INVESTIGACIÓN

7.1.1 Investigación Exploratoria

En consecuencia al tipo de proyecto el cual se fundamenta en una monografía de tipo de investigación exploratoria, se indagara para realizar un análisis exacto del comportamiento del cibercrime en la ciudad de Quibdó, en donde resulta un tema poco explorado y mediante recolección de información se podrá realizar un estudio que brinde conocimientos sobre delitos informáticos en general.

El proyecto de investigación se desarrollara tomando como punto de partida los elementos o fases de la investigación cualitativa. Determinando un alcance de procedimientos exploratorios, y teniendo en cuenta los diferentes métodos y técnicas propias de cada una de las etapas que se abordaran en el estudio, incluyendo recolección, procesamiento y análisis de la información, además del seguimiento al cronograma de actividades.

Con esta monografía investigativa, se pretende dar cumplimiento a los objetivos específicos que se definieron con el propósito de poder alcanzar el objetivo general del proyecto, conocer casos y tendencia del cibercrimen, comenzando con una encuesta a la comunidad en general, organismos de investigación y control.

7.2 FASES DEL PROYECTO

La investigación se llevara a cabo en las siguientes fases o etapas que se describen a continuación:

Fase I: Identificación de las diferentes fuentes de información que permitirán ampliar la perspectiva del tema objeto de investigación**.**

Fase II: Desarrollo conceptual del tema.

Fase III: Análisis y clasificación de la información según su género, origen y categoría.

Fase IV: Elaboración y publicación de la encuesta sobre el cibercrimen y posterior análisis de resultados.

Fase V: Conclusiones y elaboración de un documento final.

8. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Con el propósito de obtener la mayor información posible para el desarrollo de la investigación se emplearan técnicas de recolección de la información cuantitativa y cualitativa, tales como:

8.1 FUENTES PRIMARIAS

Para acercarnos a la realidad, realizamos encuestas directas para recolectar información necesaria, dichas encuestas se realizaran con la finalidad de obtener los resultados más exactos con respecto a los problemas que se generan a través de las vulnerabilidades de los sistemas informáticos en la ciudad de Quibdó.

8.2 FUENTES SECUNDARIAS

Para complementar la información es necesario hacer uso de otras fuentes de información secundarias, como las consultas en internet, material multimedia, libros o textos que tengan relación con el tema y el problema planteado, inclusive todo material que aplique como fuente para el cumplimiento del objetivo.

8.3 TIPO DE ANÁLISIS

A la hora de hacer el análisis de la información obtenida, para establecer el comportamiento del cibercrimen en la ciudad de Quibdó, se aplicaran las técnicas cualitativas y cuantitativas, dado que los datos requieren representación gráfica o numérica.

9. MARCO REFERENCIAL

9.1 ANTECEDENTES

En este marco es importante describir que otros proyectos de grados que se parecen al Proyecto de Investigación de esta Monografía, con el objetivo de conocer las diferentes experiencias relacionadas con la seguridad de la información.

Proyecto de estudio Informe: Ciberdelito en América Latina y el Caribe una visión desde la Sociedad Civil.
Autor (es) de la investigación: Patricia Prandini y Marcia L. Maggiore
Fecha: Julio de 2013

El informe pretendía analizar y conocer el panorama de cada país y región a partir del aspecto de la acción ilegal de Internet, fundamentado en que los países de estudio eran el origen y resultado de sucesos de ataques malintencionados. Además reveló el comportamiento de los cibercrimen más repetidos, con un intento de proyección económica a raíz de la pérdida de esos ataques, una de sus conclusiones radica en que el informe recalcó el ranquin de las regiones con relación a los cibercriemen, coincidiendo con caídas económicas que aquejaban a los habitantes de cada región y las empresas en este extensión de riesgos.

Tesis: Delitos Informáticos-Caso de Estudio
Autor (es) de la investigación: Alicia Rubí Guerra Valdivia
Fecha: México D.F. Junio 2011.

El objetivo de esta investigación fue realizar un estudio de forma general en lo que tiene que ver con delitos informáticos con cada situación en diferentes países siendo México me exclusiva fuente de investigación, refiriéndose no solo a lo técnico, también los efectos con relación al llevar consigo el terreno jurídico.

Artículo: La Oportunidad Criminal en el Ciberespacio Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen.
Autor (es) de la investigación: Fernando Miró Llinares
Fecha: Julio de 2011

Se realiza un análisis sobre la cibercriminalidad, delitos perpetrados en el espacio virtual, por medio de la suposición del desarrollo de las tecnologías llevando esto a cambios fundamentales como lo es el cibercrimen. Con el artículo analizó lo exterior e interior del internet, concretando el nuevo riesgo como lo es ciberespacio, advierte el crecimiento del cibercrimen, semejante al avance de la cotidianidad diaria, ilustrando métodos que prevengan ser víctima de este flagelo.

Artículo: Contextualización del Cibercrimen en Colombia
Autor (es) de la investigación: Clara Lucía Guzmán A
Fecha: Octubre de 2009.

Es un trabajo de investigación, fundamentado para brindar una explicación frente al desconocimiento de los delitos informático en Colombia, y los alcances legales de las diferentes formas de delitos, esperando que los usuarios y las empresas enfrenten adecuadamente el contexto legal provenido del manejo de las telecomunicaciones de deferentes ámbitos en labores diarias.

9.2 MARCO CONTEXTUAL

Por informe de la Policía Nacional en donde refiere sobre resultados que trata sobre el Análisis del Cibercrimen 2016 y 2017 en Colombia, en donde permite conocer que en los últimos meses y por medio de escenarios se puede establecer que se acopiaron más de 15.000 casos informáticos. Esta monografía permite conocer cualesquiera representaciones e identificaciones del cibercrimen en tanto en la ciudad de Quibdó y en Colombia, se estableció son los ciberdelitos de mayor relevancia en años 2015, 2016 y 2017. En donde el phishing, es uno de los métodos que ataca a las personas común con engaños por vía internet.

Las transiciones por medios electrónicos, han sido el punto fácil para la exposición de malwares, por medio de esta realidad, se ha buscado varias alternativas que ayuden a contrarrestar, las habilidades o destreza de estos delincuentes informáticos, ejemplo como tal pudieron perpetuar correos, haciendo pasar por la Fiscalía General de la Nación, con la intensión de ser más fácil las victimas caer en sus trampas. Teniendo presente que para el año 2017 el ransonware, se creció significativamente, como la principal tendencias del cibercrimen, siendo los más azotadas la gente común, compañías tanto púbicas y privadas.

En la actualidad en la ciudad de Quibdó, la realidad sobre el cibercrimen es que hay mucha falta de educación o conocimientos de algunas personas con respecto a los mecanismos informáticos, con relación a lo que es legal o ilegal de algunos comportamientos. Como por ejemplo, descargar música y videos, se han transformado en efectivas acciones criminales “la piratería informática”.

Por medio de las redes ya se están robando datos a las en entidades e instituciones los ataques son más dirigidos a la bases de datos que contienen

información restringida, en esta ciudad ya se han cometido delitos informáticos, por ejemplo:

En el año 2015, la Universidad Tecnológicas del Chocó “Diego Luis Córdoba” UTCH, Facultad de Derecho, se presentó el escandalo más grande, que se registrado en los tiempos en el departamento del Chocó y especialmente en el municipio de Quibdó, en lo que se refiere a delitos informáticos.

Funcionarios internos y externos de esta Institución educativa, aprovechándose del conocimiento que tenían sobre la Institución Educativa y las falencias informáticas, concertaron para realizar fraude dentro de la plataforma educativa de la Universidad Chocoana, donde ellos podrían modificar Calificaciones para ganar las asignaturas, Tesis para obtener el grado de Profesional en Derecho, de manera fraudulenta, en averiguaciones perpetradas por la Fiscalía General de la Nación Seccional Chocó, están involucrados Docentes universitarios, Funcionarios de la misma Institución Educativa, Estudiantes de la Facultad de Derecho, Egresados.

Otro delito informático que en la actualidad azota al departamento Chocó y es especial a la capital de Quibdó es el Abuso de Confianza, el objetivo de realizar daño, el atacante se vale de alguna artimaña y se las ingenia para conseguir si generar sospecha información personal de mucha confidencialidad y hasta intimas, para difundirlas por la redes sociales, perjudicando la integridad y la imagen de la víctima.

Se vuelve un peligro general que reside en la escasa cultura sobre el CIBERCRIMEN, su manejo al interior de Colombia como en otros países, y por supuesto, la penalización de este comportamiento delictivo, que han tolerado toda una explotación ilegal en el mundo, como por ejemplo: lo que se perjudican

enormemente las casas disqueras y editoriales, a ellos les ha tocado realizar muchas acciones para disminuir o contrarrestar las grandes pérdidas de ganancias dados a los daños ocasionados por las personas que copian sin autorización los discos y obras colocadas en la red, para luego ser comercializadas como originales, este es también uno de los delitos informáticos que en el municipio de Quibdó se presenta habitualmente.

En el municipio de Quibdó, y se podría decir, que en Colombia, los empleados de la Justicia, como Fiscales, Jueces Investigadores no tienen la suficiente claridad sobre los comportamientos o conductas del Cibercrimen a través de la red o por medio de mecanismos informáticos, y tampoco el conocimiento de cómo tratar la investigación de estas conductas delictivas.

9.3 MARCO TEÓRICO

9.3.1 Cibercrimen

Cuando se refiere al término cibercrimen – cybercrimen, se piensa que se conoce como delitos realizados por medio de internet, con el uso de un ordenador o dispositivo similar a la Unidad de almacenamiento de datos, Smartphone, Tablet, entre otros, lo cual consiente en hacer usos de medios informáticos para comete ciberdelitos.

9.3.2 Cibercrimen Historia

A medida que inicio el manejo de internet para la realización de actividades o transiciones de tipo financieras, a la vez llegan los primeros delitos informáticos, junto con los delitos cibernéticos, con el fin de conseguir o robar su información la información más sensible y vulnerable. Es aquí cuando se hace necesario

implantar formas determinantes para resguardar el gran tesoro que es la información.

9.3.3 Cibercrimen en los últimos años

Con la afluencia de los sitios web y las redes sociales, los cibercriminales, han conseguido la ocasión de poder ingresar y sabotear datos personales sin escrúpulos. Por la falta de conocimiento e ignorancia le han puesto a sus pies todo lo que ellos necesitan para cometer fácilmente delitos informática trayéndolos con lo que más les gusta, técnica que está de moda llamada ingeniería social. Además está comprobado que los cibercriminales han aprendido a usar la psicología para este fin, que valiéndose de artes llegan hasta compañías que tienen información de gran relevancia y muy útil para sus propósitos criminales.

9.3.4 Cibercrimen y su crecimiento

Es un desarrollo constate el mundo de los delitos informáticos, cada día que pasa se observa las diferentes caras en las que se presenta el cibercrimen, a manera de ejemplo: las infecciones por ransomware, siendo una gran amenaza con el tema de seguridad a nivel mundial. De igual forma en los últimos años muchos individuos han dado su información personal a cinbercriminales, siendo el número uno por medio de las redes sociales. Es un tema de concientización tanto para los empleados de empresas y usuarios corrientes de como aprender a no ser víctima tan fácil de estos de atacantes.

9.3.5 Ataques de cibercriminales

Los delitos informáticos han crecido pero también la organizaciones que combaten estas forma. Todo esto se conjuga y lo hace más difícil la ignorancia que todavía existe en la actualidad, ayudando así al éxito de los ataques en conseguir y atravesar los sistemas y redes de empresas financieras, valiéndose de técnicas que han sido noticia hoy día.

9.3.6 Ciberdelitos

Con el esparcimiento global de Internet se ha demostrado que ésta provee la comisión de delitos, aunque su fortalecimiento ha permitido la llegada de nuevos comportamientos ilícitos. Así, una parte del sistema promueve a excluir inclusive el término delito informático para reemplazarlo como por ejemplo: cibercriminalidad ciberdelito, etc. La expresión cibercrimen se ha distinguido porque representa “el comportamiento de diferentes conductas referentes al ingreso, substracción, intercambio, practica o destreza de manejo de búsqueda en redes informáticas, logrando afectar a de manera grupal e individual. Se está frente a una nueva generación de delitos.

9.3.7 Delitos informáticos

Son acciones por medio del cual un delincuente por medio de mecanismos lo usa como herramienta con el fin de cometer una actuación delictiva, siendo actos delincuenciales que van al deterioro de la reserva, integridad y disponibilidad de los datos, relacionando formas de vías a causar perjuicios a un sistema informático. Estos influyen en la sociedad de manera negativa, porque en la actualidad donde haya acceso a un medio virtual que permite cambiar información, el riesgo y la vulnerabilidad este a la orden del día afectando la intimidad de una

persona y a las empresas. En síntesis se pueden definir los delitos informáticos son comportamientos ilícitos que pueden ser capaces de ser penalizados por la Ley, estos van evolucionando así como avanza la tecnología, razón por la cual el termino se puede extender a la inclusión de delito como el chantaje, violación de los derechos de autor, fraude, robo, perjuicio, falsificación y principalmente el manejo de cambios bancarios, pornografía infantil. Con los avances del ciberespacio, los ataques se han vuelto más habituales, porque el cibercriminal también se actualiza y con ello la posibilidad de pérdida de la información de las víctimas.

Otra teoría que se puede aplicar es definir los delitos informáticos de una forma genéricamente, como una manera característica el delito de infracción de datos informáticos, asemejando este comportamiento ilícito a la expresión Hacking informático, definiendo la palabra Hacking la forma de ingreso a sistemas informáticos, con o sin intención o propósito de realizar algún manejo fraudulento, perjuicio, o lesión. Según lo anteriormente dicho, podemos manifestar que su conducta es considerada nociva, pues traspasa toda reserva y con esto la integridad de un sistema informático. Los delitos informáticos más habituales en Colombia son:

- *Software malintencionado*

El objetivo principal de un troyano es ingresar a un dispositivo, y así poder tener control de forma remota para poder sustraer información persona y confidencial.

- *Trampas por medio de ventas en línea*

En los sitios web o internet, existe las ventas de productos ilegales, y el aumento de estas transacciones ha resultado un negocio muy beneficioso para los estafadores. En este medio se consigue cantidades de productos a precios muy

atractivos para las víctimas, volviéndose esto la trampa perfecta la para las personas que son fácil de engañar.

- *Publicidad fraudulenta de contenidos*

Son anuncios malintencionados que ofrecen en el internet, para así llegar a los posibles clientes, con fines ofensivos, amenazas y engaños.

- *Pornografía infantil en línea o en sitios Web.*

Los medios virtuales como foros, chats, o redes sociales los delincuentes utilizan internet con el objetivo de comercializar toda la información pornográfica que envuelve a menores de edad.

- *Quebrantamiento o violación derechos de autor*

Los delincuentes se han vueltos expertos usando colecciones en serie, para realizar cantidades de copias de software, obras, video y música.

9.3.8 Análisis de la informática

Es un saber que cada día distingue cambios y adelantos que nos exige a estar al pendiente de las nuevas creaciones que suceden en este tema, uno como estudiantes que nos formamos en esta especialidad del saber. Por eso es importante conocer los aspectos básicos y complejos que ofrece la tecnología. Hablando de estos temas nos encontramos con los puertos de comunicación del computador; que se han implantados debido al progreso tecnológico que han vivido con las computadoras en estos últimos tiempos, por medio de estos podemos recibir y enviar datos utilizando los medios periféricos que están conectados a ella. Entonces, los puertos son uniones que se utiliza para enlazar terminales de hardware, como por ejemplo: impresoras y mouse.

Hoy día los expertos que manejan estas plataformas se han convertido muy importantes y con muchas demandas y es ahí donde radica que las certificaciones IT, son tan la importancia por el tema de calidad. A nivel mundial existe una gran discusión si certificarse influye realmente, si esta efectivamente garantiza una mejora del demandante. Ese tema no es alcanzado por este artículo, pero sin embargo, la verdad es que muchos puestos de trabajos aparecen cada día y dentro de los requisitos piden algún tipo de especialización acreditada por una certificación.

La realidad actual es vivimos en el mundo de las IT, el cual está lleno de conocimientos, y las certificaciones son el único herramienta que las empresas tienen para seleccionar al mejor candidato. Tener altas certificaciones en las tecnologías en aumenta el prestigio, seguridad, oportunidades y estatus de todos los profesionales que la tengan. La nueva revolución de los sistemas de información ha hecho que manejemos y compartimos la información por el medio del ciberespacio, a diario recibimos cantidades de correos electrónicos, escribimos, trabajamos e intercambiamos un sin fin de documentos, conocemos a otras personas a través de internet, realizamos diferentes diligencias, nos conectamos a redes sociales o programa de mensajería instantánea creando todo tipo de relaciones; la lista es sinceramente interminable, lo que exterioriza que gran parte de nuestro día a día gira en torno a una red de datos, por esta razón es importante establecer la seguridad perimetral como técnicas posibles de defensa para una red, apoyándonos en unos firmes recursos que protejan el entorno de la red por donde se intercambia información sensible.

9.3.9 Los Sistemas Informáticos

Tiene como finalidad el afirmar que los datos almacenados en una computadora u ordenador se conserven libres de cualquier situación de riesgo, amenazas o vulnerabilidades, y que estos sistemas proporcionar mejor efectividad y sin interrupciones, pero más sin embargo la realidad es otra, es muy difícil que este objetivo se cumpla en su totalidad, porque en el mundo de la Informática existe un término que cada día incrementa más su popularidad como son los Ataques Informáticos, definidos como las técnicas que una persona (atacante) consigue manejar o utilizar para obtener que se le brinde Información o se le pueda dar facililllamente acceso a un Sistema restringido, pero resulta hasta normal que este atacante o delincuente informático pueda utilizar diferentes artimañas existentes, como por ejemplo: suplantación, chantaje o extorsión, presión psicológica, etc.

De acuerdo al objetivo o intención del delincuente informático hay diferentes tipos de ataques, unos más perjudiciales o peligrosos y que otros, entre los cuales podemos referirnos al ataque de denegación de servicios-DDoS. Este es un ataque de los dañinos y utilizados por los ciberdelincuentes, así como el ataque de intermediario- MiTM y el Phifhing entre otros.

Asumiendo que el agresión más frecuente es el malware o softwares de códigos maliciosos, los delincuentes informáticos recurren a implantar de diferentes métodos informáticos para penetrar de una forma más fácil posibles seguridades hachas a los sistemas, esta situación hace que se vuelvan más creativos inventado cantidades alternativas de formas y métodos de penetración; para ser más correctos con esta teoría esta como ejemplo: el ransomware, que en la actualidad se ha convertido uno de los ataques de un código malicioso del tipo troyano, siendo este una de las grandes amenazas que preocupa a la sociedad.

9.3.10 La Ingeniería Social

Es uno de los procedimientos que más manejan los ciberdelicuentes o atacantes para persuadir un ataque de virus informático, en los Sistemas de Información o en las redes, en lo que tiene que ver con la cadena de seguridad las personas es la más débil. Una protección exitosa obedece en tener en tener implementadas unas buenas políticas de seguridad y preparar a los empleados para que cumplan con estas políticas. En la actualidad, hay muchos programas y dispositivos o mecanismos que nos llevan al estudio de los movimientos en el tráfico de una red, entre esas están IDS, Nmap y el Kali Linux que contiene más de 300 herramientas para ejecutar pruebas de Penetración y Seguridad en los equipos informáticos de una red.

9.3.11 Seguridad en redes

Es salvaguardar la información sin riesgo y ofrecer servicios hacia un determinado objetivo final. También se puede decir, que Seguridad en redes es conservar bajo resguardo la información que tiene la red, a través de instrucciones establecidas con una política de seguridad que accedan el registro de lo operado.

Importancia: La seguridad de redes posee un gran valor en los sistemas informáticos porque aplicando las normas y políticas de seguridad aproximadamente estaríamos seguros de realizar servicios o transacciones de toda variedad, Es preciso que la seguridad en redes esté bien manejada para sacarle una mejor utilidad y evitar así evitarnos el mal uso de la misma, hay objetivos primordiales que debemos seguir para preservar la información en las rede son los siguientes:

- *Confidencialidad*

Es la protección de los datos ante no consentimiento de entrega de información a personas no permitidas. Es responsabilidad de las empresas en proteger su información.

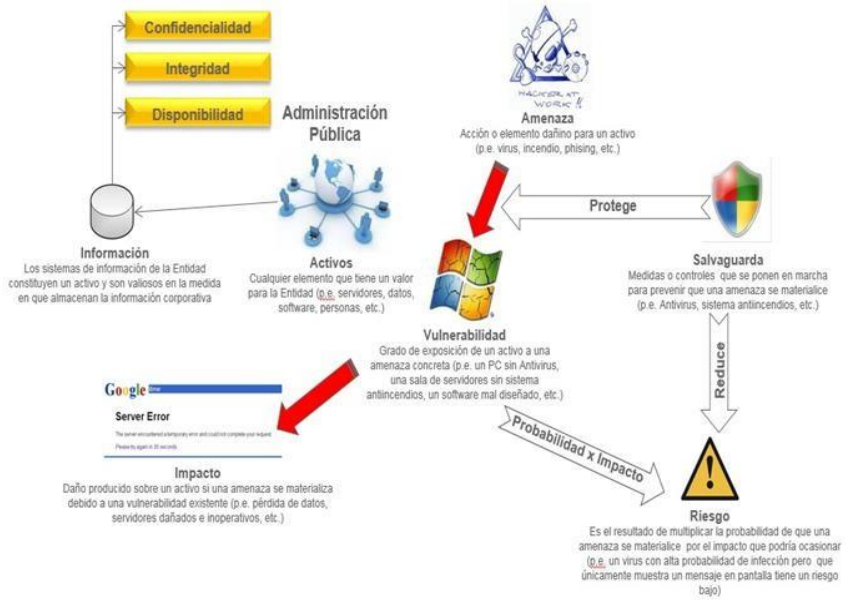
- *Integridad*

Esta representa que la información sea segura y no sea arruinada o destruida por individuos de una manera no autorizada.

- *Disponibilidad*

Se puede definir como el trabajo permanente de los sistemas de información. En la siguiente imagen nos muestra específicamente esta situación e introduce nociones muy significativas como son los activos, las vulnerabilidades, amenaza y lo más importante el riesgo.

Ilustración 1. Objetivos de Seguridad en Redes



Fuente: http://oscarpadial.com/objetivos-principales-de-la-seguridad-de-la- información-en-las-redes/

9.3.12 Seguridad en Bases de Datos

Son estrategias que se manejan para poder almacenar la información de forma tal que no se vea tan expuesta a la vulnerabilidad de las mismas, por ellos es importante manejar elementos de resguardo que ayuden a salvaguardar la información de intrusos.

Importancia: La seguridad en las bases de datos es alcanzar a avalar en un alto porcentaje la integridad de la información.

La atención universalmente se ha centrado en afirmar los perímetros de las redes por medio de: firewalls, IDS / IPS y antivirus, una buena configuración de estos medios es una gran defensa que bloquea la intrusión de perniciosos a nuestros sistemas. Las empresas cada vez más se están apuntando en la seguridad de las bases, resguardándolas de intrusiones y cambios no autorizados. Cada base de datos está cimentada con herramientas configurables para proteger los datos, no obstante, éstas igualmente tienen tipos similares y componentes idénticos para lograrlo.

*El objetivo primordial es que e*ste permite que las bases de datos puedan estar protegidas contra ingresos no autorizados.

9.3.13 Gestión de Sistema una Base de Datos – SGBD

Por medio del cual se realiza auditoria con el fin de inspeccionar los procedimientos que hacen los usuarios. Como las siguientes:

- Físicas: Inspecciona el ingreso acceso al equipo.

- Personal: ingreso solo del personal.
- Sistema Operativo: Seguridad a altura de sistema operativo.
- Limitaciones de visitas, Dispositivos de seguridad, perfiles del usuario.

9.3.14 Sistema Manejador de una Base de Datos – SMBD

Esta avala la seguridad y de la base de datos hacia el ingreso no autorizado. Como, por ejemplo: Métodos de cifrado, tratadas con ingreso por red o internet, credencial e Identificación de los usuarios, utilización de tablas para el usuario con su respectiva contraseña y código, características de cuentas con entrega de niveles de seguridad.

Ilustración 2. Bases de Datos

Fuente: http://mcristian2021.blogspot.com.co/2016/01/seguridad-y-base-de- datos.html

9.3.15 Seguridad en páginas web

Esta no obedece de la programación de ella, sino del tipo de negocio, el diseño, la plataforma de hospedaje y los varios funcionarios que toman al progreso y la transmisión del servicio.

Es por esta razón que la utilización de las páginas Web en las empresas y en las sociedad, han permitido el gran aumento de ataque, las técnicas de mejoramiento en sus herramientas los hace a los delincuentes del ciberespacio, más poderosos en penetraciones dañinas a los sistemas de información; por los que es importante proteger la seguridad de los sitios Web de forma definitiva.

9.3.16 Control de Acceso

Sistemas de firewall, Perimetral (firewalls, IDS, IPS,) y estar al pendiente de la disponibilidad, integridad de la confidencialidad de la información.
Una conspiración tiene los siguientes objetivos:

- Acceso a datos personales, bases de datos, hurto y corrupción.
- Cambiar el código de un sitio web con el objetivo de modificar lo que los usuarios están viendo.
- Conseguir los datos personales, sensibles y delicados.
- Ataques de denegación de servicio (DoS), que apagan la disponibilidad de los servicio.

Ilustración 3. Seguridad en Páginas Web

Fuente: https://www.nexica.com/es/blog/importancia-de-la-seguridad-en-las- p%C3%A1ginas-web

9.3.17 Seguridad en Sistemas Operativos

Los sistemas operativos permiten interactuar con el computador y que las aplicaciones se ejecuten. Este radica en estar libre de riesgo, y seguro, en otras palabras es que garantice que sea integro, confiable y esté disponible la información. Un administrador de sistemas operativos, debe de cumplir con una buena seguridad externas, porque lo que sí es real con la apenas seguridad física resulta escasa ante la eventualidad de ingreso por medio de equipos remotos conectados. Por eso la importancia de identificar las posibles amenazas que pueden resultar de fuentes maliciosas o no. Entre las funciones principales podemos agrúpalas de la siguiente manera:

Los SO deben asegurar que cada proceso consiguiendo una parte del tiempo del procesador, y que este a su vez sea usando de una forma eficaz. Además especifica los métodos por los cuales el operativo determina la memoria a los

procesos, permite gestionar de los datos de una forma segura, las entradas y salida facilitando interactuar con las aplicaciones, el usuario y mecanismos hardware, y por último el SO debe admitir la comunicación en red de las diferentes aplicaciones.

9.3.18 Funciones Principales de un Sistema Operativo

Entre las funciones primordiales que tiene un SO, están las siguientes:

Gestión del Procesador y la Memoria*:* el Sistema Operativo debe que afirmar que cada paso consigue una fracción del tiempo del procesador y que este sea utilizado de manera eficiente.
Gestión de los Sistemas de Almacenamient*o*: se detalla cómo son almacenados los datos de una forma íntegra.
Gestión de la Entrada/Salida: El Sistema Operativo debe poder tramitar cómo interactúan los dispositivos hardware, tanto como con el usuario y las aplicaciones.
Gestión de la Red: El Sistema operativo debe consentir la comunicación en red de diferentes aplicaciones.

9.3.19 Seguridad y Criptografía

Con la utilización de la computadora, y el aumento del uso de Internet, fue necesario el manejo de equipos automatizados para el resguardo de registros y toda la información guardada en los ordenadores, en los cuales tememos herramientas muy importantes como los Sistemas Detectores de Intrusos (IDM), cortafuegos y la utilización de los métodos criptográficos. Estos sistemas no únicamente permiten preservar la información, también protegen los Sistemas Informáticos.

9.3.20 Criptografía

Es el mecanismo que se emplea para la protección de los datos mediante cifrado o códigos que permiten mantener en secreto la información de manera segura, salvaguardando que la información sea integra y confiable, evitando el acceso a datos privados y sobre todo generando la prevención de algunos atacantes de ordenadores.

9.3.21 Usos de la Criptografía

Esta se usa para esconder mensajes de los usuarios con el objetivo de garantizar la integridad, autenticidad y así poder resguardar la confidencialidad de la información.

9.3.22 Tipos de criptografía.

Criptografía simétrica, también llamada (llave privada) o criptografía clásica. Es aquella que se manejó antes de esta la época, y se puede analizar como la criptografía no automatizada. Es una forma para esconder un mensaje, especialmente en los que se utilizan los gráficos o códigos en letras desde la A hasta la Z, utilizando métodos a mano o con aparatos mecánicos muy sencillos.

Criptografía asimétrica, también llamada (llave pública) o criptografía moderna, fue desarrollada en los años 70 y maneja complicados cifrados matemáticos relacionados con curvas elípticas y números primos, su objetivo es ser más rápida usando claves más cortas que las técnicas antiguas.

9.3.23 Objetivos de la criptografía

El objetivo de la criptografía es crear, implementar, establecer, y hacer uso de las técnicas criptográficos para conceder una manera de seguridad. En la actualidad, la criptografía ha crecido de manera enorme al ser utilizada en la informática con el objetivo de proteger la seguridad de los datos y también toda aquella información que se comparte principalmente a través de internet.

9.3.24 Análisis Forense

El análisis forense consiente en reestablecer lo que ha ocurrido en un sistema después de un acontecimiento de seguridad. Por medio de este análisis se establece quién, cómo, cuándo, desde dónde. También se puede decir que son métodos predestinados a sacar información importante de discos, sin modificar el estado de los datos.

Hay varias etapas que definen el método a llevar en una investigación, como primera medida se debe identificar las fuentes de datos a examinar y aquello que se quiere encontrar, luego se realiza el análisis de lo conseguido para extraer información confidencial y posteriormente se establecer los resultados del análisis y se presentan, de tal modo que resulten.
A continuación se explican las principales fases para su ejecución, en lo que se refiere a un análisis forense:

Identificación: esta fase nos permite reconocer que huellas o sospechas nos deja el agresor según sea el caso.

Recopilación de las pruebas: son todas las evidencias que se pueden conseguir como documento o información que sirve para el impulso de escudriñamientos, de memorias o discos.

Preservación de la evidencia: Este punto es muy importante, antes de iniciar el procedimiento de análisis hay que realizar copias de seguridad y aplicar buenas técnicas para el etiquetado de las evidencias.

Análisis de las pruebas o evidencias objeto de investigación: En esta fase se realizará la línea de tiempo del suceso, conseguir la identificación del atacante, como cometió la acción, y el daño originado a los datos o al sistema.

Resultados Ejecutivos, Técnicos y documentación: se realiza la entrega de la investigación, presentándola en los formatos correspondientes o establecidos.

9.3.25 Riesgo y Control Informático

Consiste en identificar los riesgos que ejecuta la valoración independiente del sistema de control para esta forma poder prevenir y detectar vulnerabilidades en los sistemas de información en general. Para entender el concepto de riesgo, explicaré los siguientes conceptos de los siguientes elementos más preciso posible.

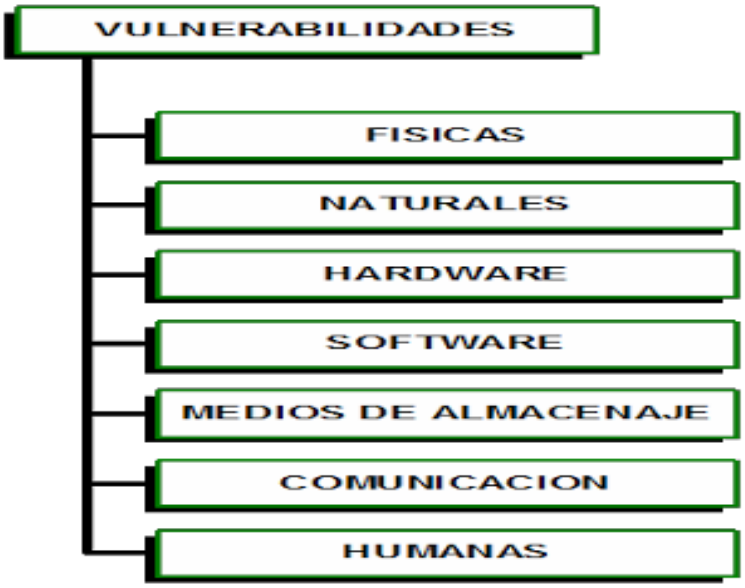
Probabilidad: Se puede crear de forma cuantitativa o cualitativa teniendo claro la posibilidad de que la amenaza se presente sin importar que se presente o no.
Amenaza: Esta situación pueden producir las siguientes situaciones:
El usuario: Es un riesgo de un sistema informático, dado a que unas veces comete errores con intención y otras por desconocimiento.

Programas maliciosos: creados para hacer daño o manejo ilegal de los recursos del sistema. Estos pueden llegar hacer grandes virus informáticos.
Intruso: quien ingresa a un sistemas informático sin tener permitido el acceso.
Siniestro: estos pueden ser incendio, inundación, temblor, robo, un mal manejo, provocando la pérdida del material y archivos importantes.
Personal interno del sistemas: la competencia por querer llevar los análisis entre las secciones y presentándose inconformidades para la seguridad informática.
Activos: Son los recurso para que la empresa funcione correctamente los sistema de información o dando importancia los objetivos propuestos por una organización.
Vulnerabilidades: son situaciones que intervienen negativamente en un activo y que facilita la realización de una amenaza.

9.3.26 Análisis y administración de riesgos

Está fundamentada en la caracterización de fallas de seguridad que demuestren vulnerabilidades que pueden ser utilizadas por las amenazas, presentándose impactos en los negocios de la organización, el objetivo de este análisis es identificar los peligros de los activos. Luego de tener la información necesaria y las herramientas para el manejo de las vulnerabilidades y un análisis general sobre la situación, desde ese momento se establecen las políticas de orden preventivo, correctivo, para corregir los problemas conseguidos.

Ilustración 3. Sitios Débiles de la Información



Fuente: http://www.cabinas.net/informatica/analisis_riesgos_informaticos.asp

9.3.27 Ámbitos del análisis de riesgos

Es fundamental que toda empresa u organización tenga implementada herramienta que le permitan un buen análisis de los riesgos, en donde estén involucrados todos los procesos de informática.

Controles: Es un conjunto de prácticas ordenadas, con el objetivo de vigilar las funciones y la manera cómo funcionan las empresas u organización y para eso se debe revisar que todo se haga de acuerdo a los parámetros establecidos.

Gestión de Riesgos: Son pasos realizados por el Consejo de administración u organización, creado para identificar sucesos posibles que logren minimizar, y suministrar una seguridad para el logro sus objetivos.

9.3.28 Aspectos Éticos y Legales

El derecho y la ética, juntas conforman un solo objetivo que consiente en fortalecer la ejecución de estrategias de seguridad informática. La ética se manifiesta en el compromiso de hacer parte de un proceso que tiene como objetivo preservar y conservar la integridad y buen uso de la información; y la seguridad radica en que un sistema informático sea seguro, entonces para que estas situaciones ocurran, se deben de tener en cuenta tres condiciones fundamentales como lo es la integridad, disponibilidad y la confidencialidad, y para que esto y para que esto suceda hay reglamentos que seguir, es aquí donde ingresa la ISO 27001, donde nos enseña a cumplir normas y procedimientos que se deben de colocar en práctica para la seguridad de la empresa o en particular.

9.3.29 Características de algunos ataques

Agresiones, repudio de servicio - DDoS: Este método de ataque es estableciendo una recopilación de aparatos electrónicos como computador, cámara web, impresoras, grabadoras de video digital, refrigeradores, enlazados a internet, contagiados con un troyano para ser manipulados en un ciberataque sin la noción del propietario del dispositivo, esto es, que esta forma de ataques se pueden topar tres partes, el hacker o atacante, una persona manejado vía (dueño de los aparatos infectados) y la victima a quien va encaminado el ataque (página o servidor), acá el hacker trae el ancho de banda del módulo infectado, el cual hemos citado “medio” , y de esta manera viene a la víctima quien es en al final es el objetivo del hackers, formando como secuelas en el “medio” (dueño del aparato), lentitud y que se obstaculice la enlace a internet continuamente.

Las derivaciones que tiene para la victima final este forma o manera de ataques, son muchas para que su página web se vuelva enormemente lenta aunque tenga

bastante amplio de banda, además que por esto la sobre carga formada por los pedidos que se transportan desde los dispositivos electrónicos de la persona que fue manipulada como medio, la página web de la víctima se desplome continuamente y en muchas veces de modo permanente (denegación de servicios), produciendo perjuicio grandes que los clientes y/o usuarios de aquellas página de internet, se fastidien de la contexto y resuelvan retirarse y en el peor de los casos desafiliarse de los servicios allí suministrados, produciendo detrimento o pérdidas de ingresos para la empresa u organización y hasta su quiebra.

- Ataque de intermediario (Man-in-the-Middle, MitM)

En este procedimiento se introduce un intermediario (persona en el medio), un cibercriminal o un arma maliciosa, entre el origen y la víctima y transfiere mensajes entre ellos, haciéndoles pensar que están conversando directamente entre sí a través de un enlace privado, situación que en realidad es otra, toda la comunicación es inspeccionada por el atacante, estos ciberdelincuente son capaces de interceptar todos los mensajes que van entre las dos víctimas e introducir nuevos.

En el ataque MitM el ciberatacante manipula un router wifi configurándolo como genuino, para interceptar las comunicaciones del usuario y si este se enlaza a páginas bancarias o adquieres en línea, el delincuente (ciberatacante) podrá robar los documentos de la víctima para subsiguientemente utilizarlas él. Actualmente es muy escuchado ese tipo de ataque, ya que los adelantos tecnológicos y el ritmo de vida que lleva la humanidad actual, hace que se averigüe la manera más posible, rápida y práctica de cumplir con deberes como pagos, con lo cual, es muy tradicional que se manejen sitios del ciberespacio y registren cuentas bancarias, para llenar sus necesidades; así se maneje la red pública o privada se está en vulnerabilidad de que le pase un ataque de intermediario. Esta particularidad de

ataque le genera a la víctima un enorme daño, debido que, como secuela tiene el hurto de los dineros que se hallen en su cuenta bancaria y para el ciberdelincuente, es un delito penal según el código penal colombiano.

- Ataque Ransomware

Esta forma de ataque se presenta transmitiendo un virus malicioso, al computador de la víctima le da al ciberdelincuente de tener la forma de poder bloquear el computador desde un lugar distante y encriptándole los archivos despojándolo del manejo de toda la información y datos almacenados. Para desactivar el virus manda una ventana emergente en la que pide el desembolso de una liberación.

Según los investigadores del software antivirus McAfee, el ransomware “Locky” es una de las más gigantescas amenazas de seguridad informática del 2016 y 2017. Se prevé que afecto ordenadores domésticos y actividades comerciales por igual, pues a los delincuentes no les importa más nada sino el pago del secuestro; no buscan robar información, ejemplo de esto es cuando la víctima le llaga un correo electrónico de una dirección desconocida, el cual va en un archivo unido como documento de Word comprimido y al abrirlo se ejecuta el virus, bloqueando información de la víctima.

- Ataque Phishing

Actualmente se expresa que este ataque radica en una técnica para atraer información bancaria de los usuarios a través de la uso de la imagen de una entidad financiera y al meter el usuario la información pedida, esta va directo al estafador, acarreando como resultado para el dueño de la cuenta bancaria perdida de dinero del usuario y, para la entidad bancaria perdida de la producción, gasto del ancho de banda, lentitud en el desarrollo de los procesos bancarios. El ataque

phishing reside en la llegada a los equipos correos electrónicos que simulan venir de sitios confiables como entidades bancarias, los atacantes tratan de conseguir información confidencial del usuario, que después utilizan para para cometer alguna forma de fraude.

- Los principales daños provocados por el phishing

Esto puede hace que el usuario tenga pérdidas económicas y no poder entrar a sus propias cuentas.
Pérdida de producción, Robo, uso inadecuado de los correos electrónicos y redes.
Una de las características muy peligrosas del phishing es el pharming. Esta habilidad que tienen con la víctima a página web falsa.

Ataque Vishing. Es una forma de estafa informática, parecida al phishing, donde el delincuente por vía telefónica llama a su víctima, le hace pensar que la llamada es de un origen fiable y engaña a sus víctimas con el objetivo de robar los datos personales y posteriormente su información bancaria.

Ataque Pharming. Es otra práctica de sustitución de identidad unida al phishing, pero con significativas diferencias. El Pharming reside en el atacante consiga dañar o alterar el servidor DNS- Domain Name System, el que convierte las direcciones IP de los lugares web a dominios .com, .net, etc. que manejas con el propósito de enviarte a páginas web malintencionadas, para robarla Informacion de su víctima.

El Pharming es más dañino que el Phishing, porque fue creado como soporte de malware, cuando te atacan la primera vez, continúa el atacante controlando el DNS, con esto el usuario se halla más indefenso, porque a diferencia del Phishing,

con el Pharming se sigue consiguiendo con la URL auténtica del sitio web, y en el camino sería falsificado.

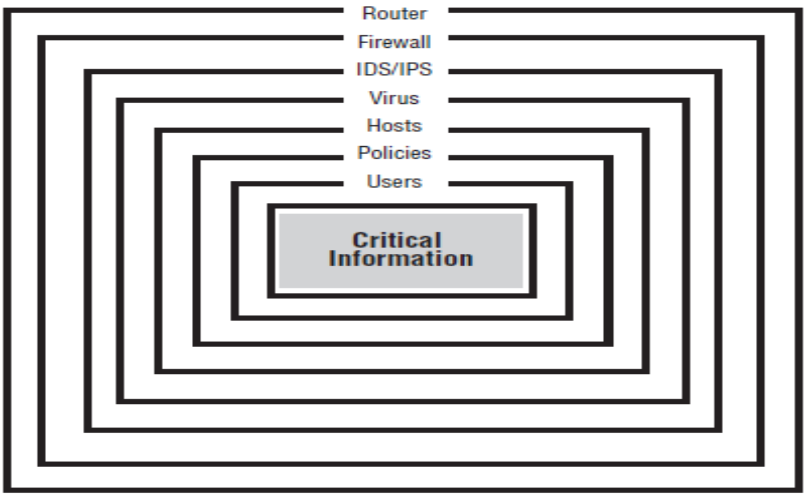
Ataq***ue Botnets.*** Este ataque se identifica porque el ciberdelincuente, crea pequeños eventos que se introducen en las terminales con el objetivo de tener el control sin la aprobación del usuario y así poder robar datos bancarios, enviar correos basura (Spam), atacar programas determinados.

Ataque Hijacker. Este ataque es muy parecido al Ransomware, por ser también se coge la información del usuario, con la diferencia que este procede sobre los navegadores de internet, intercambiando la página de inicio bloqueándolas, exponiendo algunas páginas o incluso impedir la realización de un antivirus.

9.3.30 Niveles de Defensa en la Seguridad Informática

El objetivo es que se presente una protección creada para cada uno de los niveles, esto quiere decir, que si se presenta un ataque este sea bloqueado y al mismo tiempo realice una alerta de seguridad.

Ilustración 4. Niveles de Defensa



Fuente: http://www.mauriciomatamala.net/SAD/fundamentos-de- seguridad.php

9.3.31 Niveles de Seguridad Informática

Los niveles se refieren diferentes características de seguridad del Sistema Operativo y van desde la más baja a la más alta en cuanto a seguridad se refiere. Estos niveles han sido e asiento de progreso de estándares como la (ISO/IEC).
Los niveles de seguridad son tratados según el sistema operativo que esté manejando sobre la red una empresa o institución, en la siguiente tabla se pueden identificar:

Tabla 1. Niveles de seguridad Informática

Nivel D1	El sistema entero no es seguro, no ofrece defensa para el hardware; el sistema operativo es vulnerable, en relación a los usuarios no hay garantías para poder ingresar a la información guardada en la computadora.
Nivel C1	Hay cierro grado de seguridad para el hardware, los usuarios ingresan al sistema, identificándose con su login y password.
Nivel C2	Soluciona problemas del nivel C1. El nivel C2 limita más a los usuarios con el ingreso a algunos archivos, y niveles de autorización.
Nivel B1	Llamada protección de seguridad sellada, es el primer nivel con base para seguridad confidencial.
Nivel B2	Este nivel es llamado Seguridad Estructurada, demanda que todos los objetos estén marcados o rotulados, los dispositivos como por ejemplo :discos duros, memorias etc.
Nivel B3	Dominio de Seguridad Este nivel requiere también que la terminal del usuario esté conectada al sistema por medio de una ruta de ingreso confidencial segura.
Nivel A	Diseño y ejecución, ente es el nivel de seguridad legal más alto. El uso debe de ser confidencial; significa que tanto el hardware y el software estén protegidos durante su transferencia para impedir infracciones a los sistemas de seguridad.

Fuente el autor

9.3.32 Hackers

- Hackers de sombrero blanco

Son profesionales expertos en seguridad informática, son especialmente llamados por las empresas; para que descubran vulnerabilidades de seguridad en el software. Su motivación es ofrecer seguridad, investigar, hallar y corregir los posibles errores de seguridad.

- Hackers de sombrero negro

Son expertos buscando vulnerabilidades (exploits, gusanos, troyanos, malware) de seguridad en los sistemas del software, para manipularlas en beneficio propio, personas con habilidades de robar claves de tarjetas de créditos, correos electrónicos, datos confidenciales, etc. Con un simple objetivo el de hacer daño.

9.3.33 Sujetos de los delitos informáticos

Es importante ates de seguir con el tema de delitos informáticos o cibercrimen, saber un poco sobre la definición de que es un sujeto activo y pasivo.

El sujeto activo poseen la habilidad para usar los sistemas de información, también utilizan datos que tienen información confidencial y el sujeto pasivo es aquel comportamiento, en donde de se establece el sujeto activo. Las víctimas pueden establecimientos financieros, empresa e instituciones y persona etc.

9.4 MARCO LEGAL

9.4.1 Normas Nacional Ley 1273 de 2009

El 5 de enero de 2009, el Congreso de la República de Colombia difundió la Ley 1273 “Por medio del cual se cambia el Código Penal, se crea un nuevo bien legal defensor – llamado “De la Protección de la información y de los datos”- y se resguardan integralmente los sistemas que manejen las tecnologías de la información y las comunicaciones, entre otras prácticas”.[1]

Ley normalizó como delitos una serie de normas que tienen que ver con el uso de datos personales, por lo que es fundamental que todas las personas y las empresas se recubran legalmente para protegerse y no caer en alguno de estas características criminales.[2]

Esta ley se agrega al Código Penal colombiano el Título VII BIS escogido "De la Protección de la información y de los datos" que fracciona en dos capítulos, que son: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras contravenciones”.[3]

9.4.2 Capítulo I

- *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

[1] Ley 1273 de 2009 Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[2] Ibídem.

[3] Ibídem.

del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.[4]

- *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, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.[5]

- *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 trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.[6]

- *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, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.[7]

---

[4] Ibídem.

[5] Ibídem.

[6] Ibídem.

[7] Ibídem.

- 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, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.[8]

- *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, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.[9]

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien “sustraiga” e “intercepte” dichos datos a pedir autorización al titular de los mismos.[10]

- *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,

[8] Ibídem.

[9] Ibídem.

[10] Ibídem.

enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.[11]

9.4.3 Capítulo II

- *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, incurrirá en las penas señaladas en el artículo 240 del Código Pena, es decir, penas de prisión de tres (3) a ocho (8) años.[12]

- *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, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.[13]

Así mismo, la Ley 1273 agrega como circunstancia de mayor punibilidad en el artículo 58 del Código Penal el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos o telemáticos. Como se puede apreciar, la Ley

[11] Ibídem.

[12] Ibídem.

[13] Ibídem.

1273 es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea y las personas como seres individuales en apoyarse y no dejarse vulnerar por los delincuentes informáticos, que viven pendiente de la oportunidad de hacer un ataque sin importar las consecuencias dañinas de este.[14]

9.4.4. Ley 1581 de 2012 Protección de Datos Personales

Esta es reajustada o actualizada con la idea de proteger dato persónales.

¿Qué es un dato personal?
Es cualquier información vinculada o que pueda asociarse a una o varias personas naturales que, dependiendo de su grado de utilización y acercamiento con la intimidad de las personas podrá ser pública, semiprivada o privada.[15]

DATO PERSONAL PÚBLICO: Son aquellos datos personales que las normas y la Constitución han determinado expresamente como públicos y, para cuya recolección y tratamiento, no es necesaria la autorización del titular de la información. (Ej. Dirección, teléfono, datos contenidos en sentencias judiciales ejecutoriadas, datos sobre el estado civil de las personas, entre otros.).[16]

DATO PERSONAL SEMIPRIVADO: Son datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no

---

[14] Ibídem.

[15] Tomado de ABC DE LA Ley 1581 de 2012 Protección de Datos Personales - Colombia. GENERALIDADES. La ley de protección de datos personales – Ley 1581 de 2012 – es una ley que complementa la regulación vigente. [En línea] http://www.colcob.com/web1/images/pdf-word/el_abc_Ley_1581_2012.pdf.

[16] Ibídem.

solo a su titular, sino a un grupo de personas o a la sociedad en general. Para su tratamiento se requiere la autorización expresa del titular de la información. (Ej. Dato financiero y crediticio).[17]

DATO PERSONAL PRIVADO: Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización expresa. (Ej. *Nivel de escolaridad).*[18]

DATO PERSONAL SENSIBLE: Es aquel dato personal de especial protección, por cuanto afecta la intimidad del titular y su tratamiento puede generar discriminación. NO puede ser objeto de tratamiento a menos que sea requerido para salvaguardar un interés vital del titular o este se encuentre incapacitado y su obtención haya sido autorizada expresamente. (Ej. Origen racial o étnico, orientación política, convicciones religiosas, datos biométricos, relativos a la salud, entre otros.).[19]

¿A cuales datos no se aplica la ley de protección de datos personales?
No aplica a bases de datos o archivos que contengan:
Información de uso personal o doméstico.
Información que tiene por finalidad la seguridad y defensa nacional
Información que tiene por finalidad la prevención, detección, monitoreo y control del lavado de activos y financiación del terrorismo.
Información que tiene por finalidad de inteligencia y contrainteligencia.[20]

¿Los datos personales de los niños, niñas y adolescentes tienen alguna protección especial?

---

[17] Ibídem.

[18] Ibídem.

[19] Ibídem.

[20] Ibídem.

Si, los datos personales de los menores de edad tienen una especial protección y por lo tanto su tratamiento podrá realizarse siempre y cuando no se vulnere o se ponga en peligro alguno de sus derechos fundamentales y se busque la protección de sus intereses y su desarrollo armónico integral.[21]

TITULARES DE LA INFORMACIÓN

¿Quién es el titular de los datos personales? Todas las personas naturales son titulares de sus datos personales. En el caso de los menores de edad, sus representantes legales tendrán la facultad de autorizar o no el tratamiento de sus datos personales.[22]

¿Cuáles son los derechos del titular de los datos personales?
Conocer, actualizar y rectificar sus datos personales.
Solicitar la prueba de su autorización para el tratamiento de sus datos personales.
Ser informado respecto del uso que se le da a sus datos personales.
Revocar la autorización y/o solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo considere, siempre y cuando no se encuentren vigentes con el Banco los servicios o productos que dieron origen a dicha autorización. Presentar quejas ante la entidad administrativa encargada de la protección de los datos personales.[23]

¿Cómo debe ser la autorización del titular para el tratamiento de sus datos personales?
Debe ser previa, informada y expresa. Debe especificar la finalidad para la cual se busca la obtención de los datos personales.

---

[21] Ibídem.

[22] Ibídem.

[23] Ibídem.

La autorización puede obtenerse por cualquier medio escrito, físico o electrónico, que permita su consulta posterior.[24]

¿En qué casos no se requiere autorización del titular?

Cuando se trata de datos personales públicos.

Cuando los datos personales son requeridos por una entidad pública en ejercicio de sus funciones.

Cuando se está frente a casos de urgencia médica o sanitaria.

Cuando son tratados para para fines históricos, estadísticos o científicos.

Cuando el dato se relaciona con información contenida en el registro civil. [25]

RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DE LA INFORMACIÓN

El Responsable del tratamiento de los datos personales es una persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros decida sobre la base de datos y/o el tratamiento de los mismos. El Encargado es el que realice el tratamiento de los datos personales por cuenta del Responsable.[26]

¿Qué información debe indicar el responsable y/o encargado del tratamiento de los datos personales al titular?

Debe indicar la finalidad con la que es recaudado el dato personal.

Los derechos del titular.

Los medios por los cuales el titular puede ejercer sus derechos.

La No obligatoriedad de suministro de los datos personales que requieran autorización.[27]

---

[24] Ibídem.

[25] Ibídem.

[26] Ibídem.

[27] Ibídem.

¿Cuáles son los deberes de los responsables y/o encargados del tratamiento de los datos personales?

Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.

Tramitar las consultas, solicitudes y reclamos.

Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran.

Respetar las condiciones de seguridad y privacidad de información del titular.

Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.[28]

¿Se pueden transferir datos personales a terceros países?

Sí, siempre y cuando los datos personales a transferir cumplan con los estándares fijados por la SIC.

En todo caso los datos personales podrán ser objeto de transferencia cuando:

Su titular lo haya autorizado expresamente.

La transferencia se haga por razones de interés médico.

Se trate de operaciones bancarias o bursátiles conforme a la legislación que les resulte aplicable.

La transferencia se encuentre enmarcada dentro de un Tratado Internacional en el cual Colombia es parte.

La transferencia se justifique en atención a la salvaguarda del interés público o a la defensa de un proceso judicial.[29]

¿Cuáles son las entidades administrativas de control a la aplicación de normas de protección de datos personales?

La entidad administrativa encargada de velar por el cumplimiento de las normas sobre protección de datos personales es la Superintendencia de Industria y

---

[28] Ibídem.

[29] Ibídem.

Comercio (SIC), a través de la Delegatoria para la Protección de Datos Personales.[30]

¿Cómo, cuándo y dónde debo registrar mis bases de datos?

Deberán inscribir en el Registro Nacional de Bases de Datos aquellas bases automatizadas y/o jurídicas pública o privadas. El registro se deberá realizar por cada una de las bases de datos manejadas por la entidad presentando como mínimo la siguiente información: Datos de identificación, ubicación y contacto del Responsable del Tratamiento de la base de datos; 2. Datos de identificación, ubicación y contacto del o de los Encargados del Tratamiento de la base de datos; 3. Canales para que los titulares ejerzan sus derechos; 4. Nombre y finalidad de la base de datos; 5. Forma de Tratamiento de la base de datos (manual y/o automatizada), y 6. Política de Tratamiento de la información. La inscripción de la base de datos se deberá realizar ante la Superintendencia de Industria y comercio por parte de Los Responsables del Tratamiento dentro del año siguiente a la fecha en que la Superintendencia de Industria y Comercio habilite dicho registro, de acuerdo con las instrucciones que para el efecto imparta esa entidad.[31]

[30] Ibídem.

[31] Ibídem.

Tabla 2. Ley de Delitos Informáticos en Colombia

CAPITULO	ARTICULO	DESCRIPCION
CAPÍTULO I: **"De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos"**	Artículo 269A: Acceso abusivo a un sistema Informático.	**Se explota alguna vulnerabilidad en el acceso a los sistemas de información o debilidades en los procedimientos de seguridad.**
	Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.	**Se bloquea de forma ilegal un sistema o se impide su ingreso o acceso a cuentas de correo electrónico de otras personas, sin el debido consentimiento.**
	Artículo 269C: Interceptación de datos informáticos.	**Se interceptan o captan datos transmitidos de forma ilegal o sin la debida autorización.**
	Artículo 269D: Daño Informático.	**Se destruye, borra o altera los datos o un activo tangible sin estar facultado para ello.**
	Artículo 269E: Uso de software malicioso.	**Se vende, instala o distribuye software malicioso o programas dañinos para los activos informáticos.**
	Artículo 269F: Violación de datos personales.	**Se intercepte, venda, cambie, trafique o sustraiga información personal de los archivos o bases de datos sin la debida autorización.**
	Artículo 269G: Suplantación de sitios web para capturar datos personales.	**Se diseñen, implementen o redireccionen sitios web fraudulentos con el objetivo de capturar datos sensitivos de las personas.**
CAPÍTULO II: **" De los atentados informáticos y otras infracciones"**	Artículo 269H: Circunstancias de agravación punitiva.	**Se revele información confidencial de las empresas o pongan en riesgo la seguridad nacional.**
	Artículo 269I: Hurto por medios informáticos y semejantes.	**Se superen las barreras de seguridad informáticas y se extraigan de manera ilegal los activos, así como suplantar las identidades de las personas.**
	Artículo 269J: Transferencia no consentida de activos.	**Se extraiga y transmita información con ánimo de lucro en perjuicio de un tercero.**

Fuente: CONGRESO DE LA REPÚBLICA. "Ley 1273 de 2009"

9.4.5 Estrategia de Gobierno en Línea

Esta práctica está normalizada en el ***Decreto 2573 de 2014***, este fundan los trazos de Metodologías del Gobierno en línea, estableciendo temporalmente ***la Ley 1341 de 2009***. Lo que significa causar el ingreso eficientemente y en equidad de oportunidades a todos los pobladores del territorio nacional.[32]

9.4.6 Ley 1266 de 2008 Habeas Data en Colombia

Esta se creó con el objeto de que todas las personas puedan conocer a sus derechos legales, permitiendo actualizar y rectificar todo los datos que las entidades financieras en Colombia hayan recogido.

Entre sus artículos, esta Ley busca que sea aplicable a todos los datos registrados en bancos de datos, sin importar si éstos son administrados por entidades públicas o privadas, estableciendo que la información registrada debe ser autentica, fiel y entendible. Esta ley también permite entre otras cosas que el titular de la información solicite la modificación de datos en el momento que lo requiera.[33]

---

[32] DECRETO 2573 DE. 2014. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. [En línea] 12 de Dic. de 2014. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60596.

[33] LEY ESTATUTARIA 1266 DE 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dicta. [En línea] 31 de Dic de 2008. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488.

9.4.7 Decreto 1377 de 2013

Este Decreto expedido el 27 de junio de 2013, en síntesis hace referencia a aquellas actividades inscritas en la vida privada o familiar de las personas. También describe la manera como se realiza la recolección de los datos personales y aclara que ésta no se podrá realizar sin autorización.[34]

9.5 MARCO CONCEPTUAL

Se presentan algunas definiciones importantes relacionadas con el tema de investigación de esta Monografía y es fundamental para el lector poner un contenido actualizado y resumido del tema cibercrimen, se un expone un grupo de conceptos que se usan como marco conceptual en el análisis investigación con la intención comprender el tema de estudio, Las definiciones han sido conseguidas a partir de la investigación y el desarrollo propio de esta investigación de monografía y se muestra en orden alfabético de la siguiente manera:

Cibercrímen: Son un conjunto de ataques ilegales vinculados con los métodos de los sistemas y las Comunicaciones, y el mundo web, con un fin específico.[35]

Ciberterrorismo: el objetivo es generar terror en los sistemas de información y en la web, logrando que las personas aceden a entregar la información que ellos quieren.[36]

---

[34] DECRETO 1377 DE 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. [En línea] 27 de Junio de 2013. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646.

[35] Abogados Portaley Madrid penal, civil e Internet (2015). Qué es y como combatir el cibercrimen Recuperado de: http://portaley.com/2015/04/que-es-y-como-combatir-el-cibercrimen/#

[36] REYES, JOSÉ ALBERTO CRUZADO. Delitos Informaticos y Ciberterrorismo, Fundamentos de Investigación. Libres, Puebla, Octubre 2011. [En línea] https://beorlegui.files.wordpress.com/2011/10/delitos-informaticos-y-ciberterrorismo.pdf

Los delitos informáticos: Son comportamientos ilícitos que pueden ser capaces de ser penalizados por la Ley. Siendo actos delincuenciales que van al deterioro de la disposición, reserva y que los datos estén disponibles.[37]

Sistema de Información: Conjunto de software, hardware y el factor humano para usar el sistema y sostenerlo.[38]

Disponibilidad: Se describe en tener la información o se logre recuperar en el tiempo que sea necesaria.[39]

Confidencialidad: Reserva o secreto de la información.[40]

Integridad: Evidenciar que la información no haya sufrido modificaciones.[41]

Ataque cibernético: operaciones ejecutadas de con el objetivo de causar daño a un sistema a través del Internet.[42]

Control de accesos: Este controla el ingreso no autorizado a las computadoras y sistemas de información. De igual forma, detecta actividades no autorizadas.[43]

Amenaza: visión de un escenario donde se presente la posibilidad realizar un ataque cibercriminal contra una persona, región, país, empresa y grandes organizaciones.[44]

Vulnerabilidad: Es lo que facilita la acción de una amenaza para la información, servicios y activos.[45]

---

[37] TELLEZ VALDÉS, Julio. —Los Delitos informáticos. Situación en Méxicoll, Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996

[38] CONSULTORES, CSI. 2016. Seguridad Informática vs Seguridad de la Información. [En línea] 22 de Sep. de 2016. https://www.maestrodelacomputacion.net/seguridadinformatica-seguridad-de-la-informacion/.

[39] INFORMATICA, MONOGRAFIA INTRODUCCION A LA SEGURIDAD. 2012. observatorio Tecnológico. [En línea] 26 de Mar. de 2012. http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica.

[40] Ibídem.

[41] Ibídem.

[42] Seguridad cibernética | NEC, Gestión de la información. ¿Qué constituye un ataque cibernético?:. [En línea] [Citado el: 12 de 05 de 2027.] http://mex.nec.com/es_MX/solutions/security/safety/info_management/cyberattack.html.

[43]Ibídem.

[44]Erb, M. (2009). Amenazas y vulnerabilidades. Recuperado de http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades

Riesgos: Posibilidad de que una situación sea peligrosa.[46]

Violación de datos personales: Individuo sin autorización adquiera beneficio y agrupen, despojen, brinden, cedan, comercien, remitan, obtengan, intercepten, publiquen, alteren o usen códigos personales, datos personales que se estén en archivadores y registros similares.[47]

Acceso abusivo a un sistema informático: Es cuando se irrumpe a un sistema protegido por encima de quien tiene genuino poder de la información.[48]

Obstáculo ilegítimo de una Red de comunicación: Impedir el buen funcionamiento de una red y a la información que ahí reposa. [49]

Interceptación de datos informáticos: persona sin disposición legal, tome en su origen datos informáticos.[50]

Daño informático: Individuo quien comete acto sin autorización y perjudique, arruine, elimine, estropee, modifique, perturbe datos de un sistema informático o sus partes o mecanismos lógicos.[51]

Fraude Electrónico: Esta forma delito se caracteriza por el robo identidad, por medio del cual se realizan en engaños o con la utilización de herramienta de punta como Software y Hardware, el atacante consigue descubrir los datos financieros privados de su víctima, para después realizar transacciones Bancarias.[52]

---

[45] Universidad Nacional Abierta y a Distancia. Dateca. Riesgos y control informático. Lección 1: Conceptos de Vulnerabilidad, Riesgo y Amenaza recuperado de http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

[46] Universidad Nacional Abierta y a Distancia. Dateca. Riesgos y control informático. Lección 1: Conceptos de Vulnerabilidad, Riesgo y Amenaza recuperado de http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

[47] Ley 1273 de 2009 Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[48] Ibídem.

[49] Ibídem.

[50] Ibídem.

[51] Ibídem.

[52] KROW, SHAILYNN. Qué es lo que constituye el fraude electrónico. [En línea] http://www.ehowenespanol.com/constituye-fraude-electronico-info_349315/.

Malware: Es un virus infeccioso creado por cibercriminales con el único fin de hacer a sus víctimas, realizando cambio al sistema operativo, instalar y robo.[53]

Phisihnig: Será penalizado quien, quien ilícitamente y sin estar con permiso para ello, cree, desarrolle, diseñe, negocie, comercialice, elabore, proyecte o remita páginas electrónicas. Además quien cambie el sistema de identidades de dominio, permitiendo ingresar al usuario a una dirección IP diferente para poder acceder a un banco o a otro lugar personal o de seguridad.[54]

Ciber-sexting: Es la práctica de intercambió de videos fotografías o "íntimos" con información sexual, usando medios tecnológicos. Se da de modo privado pero acontece que todo lo que se sube a web, no sabe cuál es el rumbo que va a tomar y es allí cuando se muestra la problemática del ser víctimas del cibersexting, porque al subir videos o fotografías, estas va a estar guardadas no solo en un teléfono, no en el correo, no en una red social, es en un sitio de libre ingreso a cualquier usuario de ciberespacio o web. La generación joven es la más propensa a este riesgo y es donde cada padres de familia deben de aprender qué es este ciberdelito, y qué resultados podría traer. Por qué hablar del cibercrimen, el conocimiento de ciber-sexting, y ante la falta de legislaciones, es una práctica que pasa de ser algo totalmente gustoso a ser un acto ilícito, y en la mayoría de las ocasiones con fines de un beneficio. Las víctimas del ciber-sexting no contemplan los riesgos que puede acarrear realizar esta práctica.[55]

Las redes sociales son el lugar principal de conocimiento y practica del ciber-sexting y en esto es importante manifestar que el ciber-sexting puede empezar desde una simple foto sensual que se toman en vacaciones, en la privacidad de tu

---

[53] SEMANA, PELIGROS INFORMÁTICOS. 2014. ¿Qué es un Malware y cómo se puede prevenir? [En línea] 30 de de Ene. 2014. http://www.semana.com/tecnologia/tips/articulo/que-malware-como-puede-prevenir/372913

[54] UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO (2009). Eduteca. Manual para identificar y notificar phishing scam. Pharming [En línea] [19 de Noviembre de 2016] Disponible en http://www.seguridad.unam.mx/usuario- casero/eduteca/main.dsc?id=194

[55] NACIÓN, PABLO A. GÓMEZ MAROTO LA. 2013. Los peligros de la práctica del ciber-sexting. [En línea] 12 de Abril de 2013. http://www.nacion.com/archivo/peligros-practica-emciber-sextingem_0_1335066516.html

casa. La foto casualmente fue subida al Facebook o Twitter y se expandió que sin aprobación muchos descargaron y compartieron, entre otros suceso.

Robo de identidad: Provecho particulares para simular ser otra persona, con el propósito de obtener ganancias y realizar delitos informáticos, como datos confidenciales, claves de ingreso, recibos, identidades, etc. Prácticamente este infracción tiene por objeto el obtener acceso a recursos y patrimonios que se consiguen o que están a nombre de la víctima, como por ejemplo propiedades, tarjetas de crédito, préstamos financieros, etc.[56]

Piratería Informática:

Es quien patrocina por acción la falsificación o duplicación, usurpación y comercialización con objetivos rentables información películas, música, software, de la cual no tiene licencia o autorización de su autor, habitualmente usando su computador.[57]

---

[56] Ley 1273 de 2009 Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[57] SORIANO, LUZ ARIDIA ESTRELLA. 2014. La Piratería. ¿Qué es la piratería? tipos, causas, consecuencias y persistencia de la piratería. [En línea] 04 de Nov de 2014. https://www.google.com.co/search?q=consecuencias+de+la+pirateria+informatica&sa=X&ved=0ahUKEwjw1dCSmprXAhUHQyYKHRydDvcQ1QIIiAEoAA.

10. PRODUCTO RESULTADO A ENTREGAR

- Casos de delitos informáticos cometidos en la ciudad Quibdó e identificados
- Casos de cibercrimen analizados
- Tendencia del cibercrimen identificada
- Recomendaciones formuladas
- Identificado el grado de conocimiento en la ciudad de Quibdó frente a los delitos informáticos.

11. RECURSOS Y PRESUPUESTO

Para este análisis de investigación, se requieren de los siguientes recursos y presupuesto:

Tabla 3: Recursos y Presupuesto

ÍTEM / ACTIVIDAD	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
1**. Personal**			
Investigador	1	3.500.000	3.500.000
2. Equipos			
Computador	1	1.500.000	1.500.000
Impresora Láser	1	500.000	500.000
Internet	3 Meses	95.000	285.000
3. Desplazamientos			
Transporte	1	380.000	380.000
Combustible	3 Meses	100.000	300.000
4. Materiales			
Memorias USB	1	50.000	50.000
Papelería (Lapiceros, CD, etc.)	1	70.000	70.000
Fotocopias	10	30.000	300.000
Tóner de impresora	1	300.000	300.000
5. Servicios Técnicos			
Transcripción de encuestas	1	100.000	100.000
6. Otros			
Imprevistos	1	1.000.000	1.000.000
7. Total		$ 7.625.000	$ 8.285.000

Fuente: El autor

12. CRONOGRAMA DE ACTIVIDADES

A continuación se describen las fases de desarrollo del proyecto

Tabla 4: Cronograma de Actividades

Fases	Septiembre				Octubre				Noviembre				Diciembre			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
I	X	X	X	X												
II					X	X	X	X								
III									X	X	X					
IV													X	X		
V															X	X

Fuente: El autor

13. DESARROLLO DEL PROYECTO

Levantamiento de la información

En el levantamiento de la información requerida, se efectuó mediante visitas a entidades, verificando con el método de observación inicialmente, y mediante entrevistas verbales con algunos empleados sobre el manejo de la mismas, es allí cuando me di cuenta que en algunas de ellas nunca han tenido seguridad, también se realizó encuesta a los habitantes de la ciudad, sin distinción alguna para poder evaluar que tanto conocen o saben de seguridad informática y en cuanto al cibercrimen se refiere.

Para esta investigación se va a empezar con el primer objetivo y después de algunas entrevistas realizadas a la población, a algunas entidades y en especial a la Fiscalia General de la Nación, donde se recurrió al Fiscal que esta destacado para llevar este casos sobre delitos informáticos en todas sus modalidades, con estas entrevistas se pudo extraer de manera más segura la información necearía identificando los diferentes casos de cibercrimen que están ocurriendo con mayor frecuencia en nuestra región y en donde ya hay personas que han sido identificadas, capturadas e imputadas por delitos informáticos.

Se debe de mencionar que en el municipio de Quibdó, por ser un pueblo pequeño la cantidad de delitos informáticos o cibercrimenes no son en un porcentaje alto en comparación a las demás regiones o municipios de Colombia. En esta investigación se trató de señalar los delitos que ya han sido conocidos a nivel Departamental y a nivel Nacional, sin desconocer que pueden estar ocurriendo con alguna frecuencia pero por la falta de conocimientos y hasta pena, no registran dichos hechos. Se pudo establecer que los delitos que se exponen a

continuación son los que se pudieron identificar que el cibersexting, piratería informática, usurpación, extorsión, Ingreso abusivo a un sistema informático, violar datos personales y hurto por cualquier medio informático o similares.

14. IDENTIFICACION CASOS DE CIBERCRIMEN OCURRIDOS EN EL MUNICIPIO DE QUIBDÓ DEPARTAMENTO DEL CHOCÓ

A continuación se expondrá casos de cibercrimen de connotación, denunciados en la Fiscalía General de la Nación Seccional Quibdó, departamento del Chocó, con sus respectivas características:

Delito: *VIOLACION DE DATOS PERSONALES ART 269F, LEY 1273 DE 2009, AGRAVADO POR REVELAR O DAR A CONOCER EL CONTEDIDO DE LA INFORMACION EN PERJUICIO DE OTRO:*

La utilización de información personal se ha convertido en una modalidad en personas de la población Quibdoseña, y especialmente en personas despechadas por lo general hombres, que toma información confidencial de la expareja y al rehusarse de no volver con esta persona, el inicia la extorsión a través de llamadas telefónica, como es claro que la víctima no quiere continuar con la relación, el objetivo del victimario es que ella entregue el dinero por las fotos y videos que él tienen en su poder, y así evitar que las suba a la redes sociales. El delito informático se ejecuta cuando el victimario no consigue su objetivo, y procede a revelar o da a conocer por medio de la web, todo el contenido, como videos y fotos intimas ocasionando perjuicio al otro.

Este otro caso tuvo su génesis con los hechos que se están presentando en la ciudad de Quibdó – Chocó, donde un grupo de estudiante en el año 2015, crearon

dos grupos en WhatsApp, donde uno se llamaba Fiesta y el otro exámenes, se pensaría que lo usarían para darle la utilización como estudiantes algo sano, realmente ellos hicieron un compromiso que los que estaban en esos grupos debían de subir toda clase de información personal y de otras personas, realizaban diariamente publicaciones en las redes sociales, más exactamente en la aplicación WhatsApp, crearon esos grupos en las cuales dicha publicación dañan el prestigio de diferentes personas de la comunidad de Quibdó, afectando así, su buen nombre y moral, ya que estas imágenes y videos contienen archivos íntimos de cada persona afectada.

La Fiscalía 7 Seccional de Delitos contra la Administración Pública, por estos casos radicó las audiencias de legalización de captura, fórmula e imputa y se impone medida intramuros, y en la actualidad están algunas de estas personas ya están pagando condena en centro carcelario de la ciudad de Quibdó por delitos informáticos.

Otro caso presentado en la ciudad de Quibdó y es entrar a las redes sociales y con la información que sube los usuarios por ejemplo las fotos que comparten en la web, el delincuente las baja, y las envía por todos los medios como WhatsApp, Facebook, y en momento de la publicación crean memes destructivos, que terminan dañando amistades, matrimonios, perder hasta el trabajo etc. Destruyen el prestigio, la integridad y moral diferentes personas de la comunidad de Quibdó.

Delito: *DAÑO INFORMÁTICO - Artículo 269D.*

ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO - Artículo 269A

Caso 1. En la Universidad Tecnológica del Chocó “Diego Luis Córdoba, Facultad de Derecho, se ejecutaron casos de delitos informáticos como lo es daño informático e ingreso abusivo a los sistema informático. El fundamento radica al

interior de la entidad personal administrativo, docentes, alumnos de la institución educativa, conformaban un banda organizada de delitos informáticos dedicada a la penetración, robo, falsificación, eliminación y modificación de los datos confidenciales o sensibles que se encuentran en la plataforma universitaria.

Este cartel interno de la institución le exigía dineros entre un valor de dos y tres millones de pesos por estudiante, con el objetivo de colocarles la nota del trabajo de grado, falsificando firmas de los jurados, inventaban sustentación que no existían, ingresando ilegalmente al sistema informático y así poder realizar lo prometido, siendo esto es una pequeña descripción de las irregularidades de este plantel educativo.

Se realizó denuncia bajo Noticia Criminal Nro. 270016001100201502048, caso asignado a la Fiscalía 7° Seccional de Administración Pública, después de realizada labores investigativas, se procede realizar allanamiento, a una vivienda de la ciudad de Quibdó, plenamente identificada de donde presuntamente desde ahí se estaba cometiendo el delito informático, la penetración al sistema informático de Universidad; esta labor permitió arrojar registros de materiales probatorios contundentes para la desarticulación de la banda organizada de delitos informáticos, quienes fueron descubiertos en flagrancia en el momento en que accedían en la plataforma académica falsificando o adulterando los datos de registro académicos y financieros de estudiantes universitarios y particulares.

La habitación de Sistemas donde se cometía el delito informático es paralela a la de la Universidad, conservaba un permanente funcionamiento, prestaba sus servicios a diferentes personas, estudiantes o no, consiguiendo organizar, en confabulación con varios funcionarios y exfuncionarios de la misma institución, desde la matricula financiera y académica, las calificaciones y hasta las tesis con el proceso de graduación de cualquier programa académico de la universidad.

En el ejercicio de las autoridades, decomisaron o incautaron tres ordenadores, varios discos duros, diferentes memorias USB, $4 millones y una impresora láser la cual era manejada para imprimir recibos de matrículas, sabanas de calificaciones, certificados de paz y salvo y todo tipo de documentación universitaria falsificada, también confiscada.

Hasta la actualidad, se pudo establecer, por parte de las autoridades, que solo en el año 2016, un total de 208 diplomas referentes a la facultad de derecho fueron entregados, de forma fraudulenta y que no poseerían ningún valor por cuanto fueron adquiridos sin el lleno de los requisitos académicos.

La Fiscalía 7 Seccional de Delitos contra la Administración Pública, legalizo captura, formuló de imputación de cargos y medida carcelaria hoy en días a más de 100 personas de las cuales ya están pagando su condena tanto por delitos informáticos como de administración pública.

Las averiguaciones o investigaciones siguen su trayectoria porque presuntamente hay más de 400 profesionales del derecho en específico, y personas involucradas en este desfalco a la institución educativa de formación superior más importante del departamento de Chocó.

Delito: *HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES - Artículo 269I*

Casos 1. En este caso por lo general ocurren con personas que se encuentran fuera del departamento del Chocó, en donde el atacante dispone de un war dialing para hacer llamadas a números telefónicos en una región cualquiera. Cuando le responden a la llamada, una grabación de alerta que a la víctima que su tarjeta de crédito está manejando de forma fraudulenta y llame al número que se le indiaca que es una entidad financiera que se pretende simular.

Luego le contestada una grabación que le indica a la persona que su cuenta necesita ser verificación esto es para que le dé la clave de la tarjeta de crédito, Después que entrega los datos, la victima queda a merced del vishing tiene todo lo que necesita para hacer cargos engañosos a la tarjeta de la víctima. También pueden hacer la llamada para sacar datos importantes como el PIN de seguridad, la fecha de expiración, el número de cuenta.

Casos 2. Es que se presenta la siguiente situación, llaman de cualquier región de Colombia más que todo de barranquilla y Cali según víctimas en el municipio de Quibdó, y se hacen pasar por entidades bancarias conocidas, como por ejemplo BBVA, AVVILLA, BANCOLOMBIA, y empresa de celular como CLARO, y otras más… haciendo creer que son funcionarios de dichas entidades, les dicen sus nombres completo en la ciudad que residen y empiezan a ofrecer productos que según los delincuente las víctimas tienen derecho o se han ganado un premio, ofrecen productos tentativos, el objetivo es sacarle toda la información de puedan a la víctima, en donde le piden validar sus datos por seguridad y se esa forma muchos caen y terminan robados.

Delito: *Sexting*

Casos que suceden con frecuencia y esta en práctica en nuestro medio, se está realizando o presentando en la población de jóvenes que en medio de sus relaciones de parejas o intimas, terminan tomándose fotos desnudas y teniendo relaciones sexuales, registros o imágenes que quedan guardadas en mecanismos informáticos, terminando en manos de personas mal intencionadas y ese producto de pacer o mutuo acuerdo lo suben a redes sociales sin el consentimiento de la persona que va ha ser dañada en su moral e integridad personal.

Caso1. La víctima, una mujer de 35 años de edad, sostuvo una relación sentimental con el hoy indiciado, quien en su momento tomó fotografías intimas

bajo consentimiento de los dos. Posteriormente, y en razón de la ruptura de la relación sentimental, este presiona a su expareja con el fin de una reconciliación bajo la manera de hacer públicas las imágenes privadas por la tomada. Debido a que la víctima no cede ante esa coerción, el victimario finamente pública mediante la plataforma técnologica de whatsapp, la serie de imágenes que comprometen la intimidad de su excompañera sentimental, estas fueron multiplicadas por las diferentes medios informáticos, perjudicando la honra, integridad moral y social de la víctima.

Caso que fue radicado con Noticia Criminal N° 270016001099201500135, asignado a la fiscalía 6° Local de Quibdó, al indiciado se le realizó la imputación de cargos e imposición de medida de aseguramiento, actualmente está pagando su pena.

Caso 2. Mujer de 25 años de edad, estudiante universitaria; para el año 2014 fue víctima del delito Sexting. En su relación de pareja sentimental tenía por costumbre tomarse fotos desnudas y videos haciendo el amor con su novio, para posteriormente observar lo que hacían, esto lo realizaban con pleno consentimiento de ambos, pues ello les resultaba bastante excitante y lo tenían como práctica en cada encuentro que sostenían, ella guardaba las fotos y videos en memoria USB, la cual compartía con él, dado que eran estudiantes de la misma facultad. La victima decide acabar con la relación sentimental, pero al principio el novio no aceptaba que la relación se había acabado y a raíz de esa situación ambos sostenían fuertes discusiones, finalmente la expareja decide de buena forma aceptar que la relación terminó y se lo hace saber a la víctima, luego se encuentran en la facultad y él le pide el favor que le preste la memoria USB para sacar la documentación de estudio que él tenía almacenada en ese dispositivo, ella accede a prestársela, procede el exnovio y toma la memoria y pasa la información a su portátil y luego se la devuelve, días siguiente la expareja

sentimental inicia a llamar para amenazarla, que si no siguen con los encuentros íntimos ella se va arrepentir de haberse tomado fotos y videos con él, la victima dice que no lo va hacer que es una decisión definitiva. Luego amistades la contactan y le informan que por el Facebook, hay videos y fotos circulando en las redes sociales de ella y con hoy día el indiciado.

Pero para el victimario no fue suficiente, creo un perfil en Facebook con el nombre de la víctima, donde escribían palabras feas y publicaban fotos de ella y hombres desnudos haciendo el amor, dentro de esas publicaciones daban la dirección de la casa y el número telefónico, y efectivamente varios hombres la llamaban o llegaran a la casa a preguntarle que si era la mujer de la prostitución y de las publicaciones que hacían de la cuenta de Facebook.

La victima realizó la respectiva denuncia en contra de su expareja sentimental por el delito de Sexting, por utilizar los medios informáticos con el único objetivo de dañar su moral, mujer que se sintió vulnerada en todos los aspectos de su vida, nunca se pudo imaginar, que con una persona que en su momento sentía que era de confianza le pudiera realizar este daño, son los arrepentimiento que les deja este tipo de prácticas a sus víctimas.

Caso radicado con la Noticia Criminal N° 270016100628201400165, el señor Juan fue condenado a pagar condena por este delito, se allanó a los cargos.

Delito: *Piratería Informática*

En este aspecto, se debe analizar con más profundidad, la piratería de Cd, DVD, Música Software etc. Es el pan de cada día, el tema no consiste en justificar las acciones delictivas, pero en la ciudad de Quibdó, departamento del Chocó, el índice del desempleo es muy alto y resulta normal, conseguir los andenes de

muchos jóvenes distribuyendo, las últimas películas, música, y hasta libros, claro todo esto es un mercado pirata que se mueve, en frente de todos los pobladores, y de las respectivas autoridades, este si es un delito patrocinado y consentido de la misma población, ¿porque expresar esta teoría?, si es muy cierto la misma comunidad Quibdoseña en medio de su desconocimiento está financiando de alguna forma este delito que tanto daño le ha hecho y le sigue haciendo a la población Colombiana desde todas las esfera con que se analice y observe.

Cuando una persona se acerca y comprar cualquiera de estos productos está contribuyendo con la delincuencia informática y aportando con su granito de arena para que este suceso siga aumentando, porque el individuo entre más le compren, más va a seguir infringiendo la norma.

Este es un caso muy preocupante, porque ni las autoridades están colaborando con esta situación, es tanto la piratería informática, que las personas encargan las últimas películas, los libros que desean obtener de forma ilegal, música, software, en fin un mercado que día a día crece y no se ve la forma de como detenerlo.

14.1 ANÁLISIS DE LAS CARACTERÍSTICAS

Se indago y como resultado son varios casos pero muy pocas las denuncias, con lo referente a esta investigación en esta ciudad, todo ello por la falta de conocimientos y reglas por parte algunos jueces y fiscales, cabe anotar que en la ciudad de Quibdó, son comportamiento que simbolizan conductas de cibercrimenes, mientras se determina la cantidad de personas afectadas por esta causa, es importante realizar capacitaciones o ejercicios ocupacionales, para llegar a esa población de alguna manera están siendo víctima de estos ciber delincuentes o personas mal intencionadas.

Podemos mencionar que estas acciones ilícitas son de oportunidad, logrando que se aproveche de un momento, situaciones en donde se puede mencionar que se ven vulnerados las entidades, así como las personas por medio del sistema tecnológicos, sin necesidad de hacer presencia física para poder comunicarse.

Al realizar un análisis preciso de las características de los casos de **cibercrimen**, es significativo señalar que se debe de proceder de la forma más eficaz para impedir que estos tipo de delitos no se continúen realizando y de manera impune, se debe de establecer de una modo serio y honesto, apelando a las diferentes personas que poseen el conocimiento, como técnico relacionado en seguridad informática, y en lo legal como es la rama del Derecho, porque si no se aprende aspectos básicos de la materia, dificultosamente se lograrán utilizar y tipificar sanciones justas a las personas que ejecutan este tipo de actividades de forma habitual.

15. TENDENCIA DE LA COMISIÓN DE CIBERCRIMENES EN EL MUNICIPIO DE QUIBDÓ, DEPARTAMENTO DEL CHOCÓ

La tendencia del *Cibercrimen,* será un desafío, además de saber cuáles son las amenazas, los pobladores de esta localidad deben de capacitarse en la utilización de herramientas de seguridad que les permitirá conservar segura la información. De lo contrario, el aumento de las amenazas y ataques seguirán siendo una preferencia por los delincuentes informáticos en esta región.

Según el análisis que se realizó en esta monografía, se puedo establecer que durante los próximos años se alcanzaran más estafas por medio de celulares a través de WhatsApp, redes sociales, más ransomware, aplicaciones y códigos maliciosos.

Los atacantes continuarán buscando la forma de causar daño a través de Internet, y seguirán sucediendo más casos de delitos informáticos al correr de los meses.

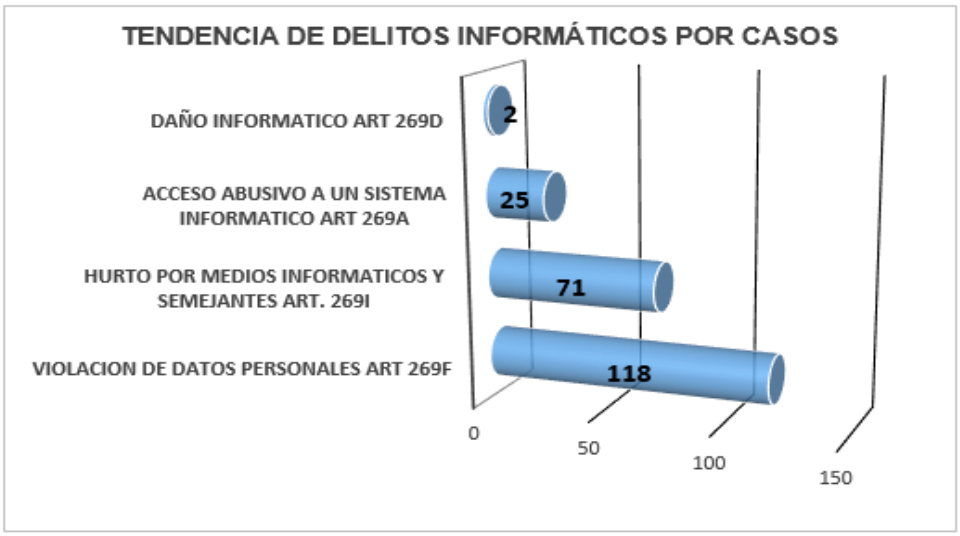
Es fundamental que los usuarios sean personal, empresa o entidades educativas, conozcan los ataques que permiten causar daño, este puede ser de una estafa por correo electrónico, hasta la violación o robo de información, por ello es necesario realizar todas las formas de concientización para impedir, que estos hechos sucedan.

Habitualmente, se debe al no conocimiento de las características de seguridad, la falta de información sobre la consecuencia de las amenazas informáticas y el cuidado que se debería tener.

Un reto importante y necesario para los pobladores de la ciudad de Quibdó, es sean capaces de educarse para aprender cómo protegerse de los delitos informáticos, qué información publicar y cuáles son los métodos de protección a utilizar.

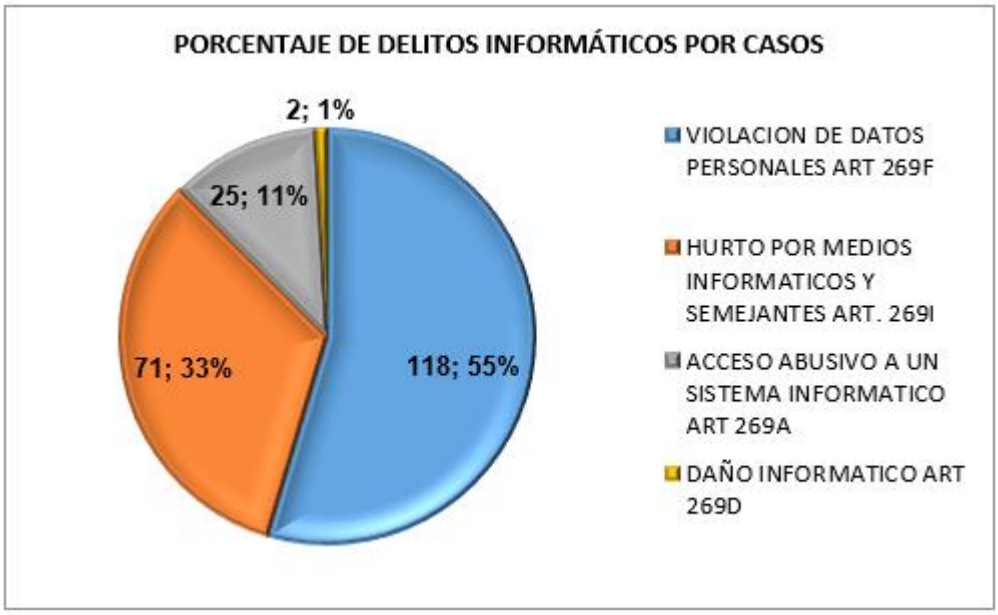
A continuación se en las siguientes ilustraciones de muestra la tendencia de los delitos informáticos por casos y años.

Ilustración 5. Tendencia de los delitos informáticos por casos



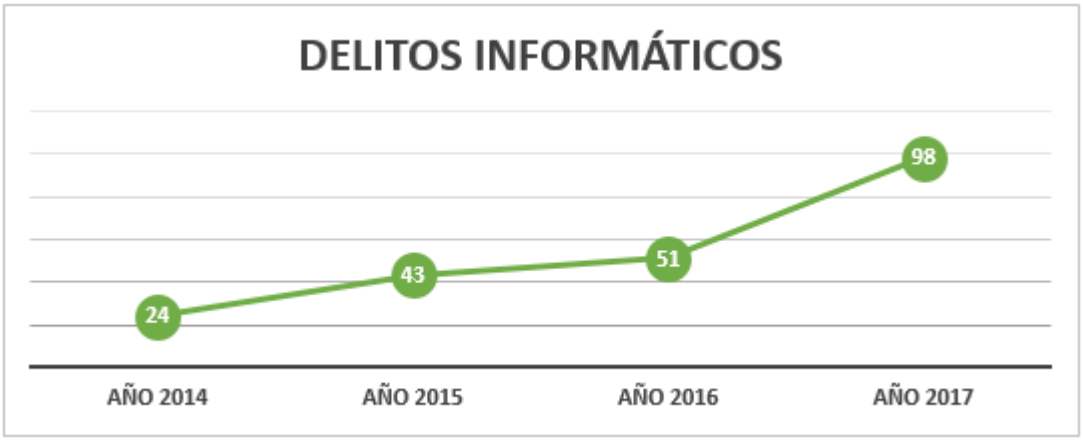
Fuente: El autor. Datos obtenidos del sistema de información SPOA, Fiscalía General de la Nación Seccional Chocó.

Ilustración 6. Porcentaje de los delitos informáticos por casos



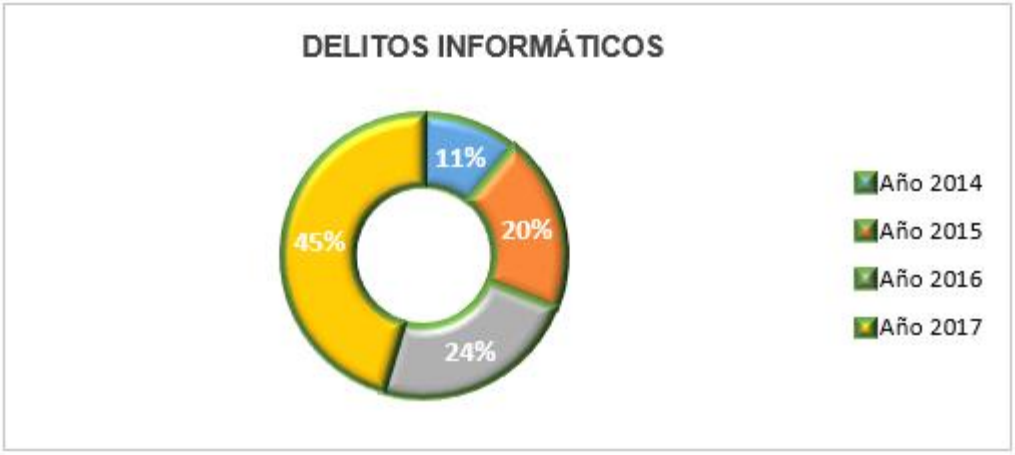
Fuente: El autor. Datos obtenidos del sistema de información SPOA, Fiscalía General de la Nación Seccional Chocó.

Ilustración 7. Tendencia de los delitos informáticos por años



Fuente: El autor. Datos obtenidos del sistema de información SPOA, Fiscalía General de la Nación Seccional Chocó.

Ilustración 8. Porcentaje comparativo años 2014 - 2017



Fuente: El autor Datos obtenidos del sistema de información SPOA, Fiscalía General de la Nación Seccional Chocó.

Tabla 5. Porcentaje comparativo años 2014 - 2017

Año	Porcentaje de aumento
2014	11%
2017	45%

Fuente: El autor.

Durante los años 2014, 2015, 2016 y en lo que va corrido del 2017, se han recibido 216 denuncias por violación a la ley 1273 de 2009. En el estudio que se realizó para establecer la tendencia del cibercrimen, este arrojó un indicador que nos muestra el aumento de los casos de delitos informáticos en la ciudad de Quibdó, departamento del Chocó, que violaron integridad, disponibilidad y confidencialidad de las víctimas.

Por ello, el análisis que se realizó después de la recolección de información nos informa que los casos de Violación de datos personales Artículo 269F, tiene un mayor índice de denuncia con una equivalente al 55%, seguido del Hurto por medios informático Artículo 269I con un porcentaje de 33%, luego Acceso abusivo a un sistema informático Artículo 269A con el porcentaje de 11% y por ultimo Daño a un sistema informático 269D con el 2%, siendo este el de menor tendencia de comisión del delito de la región.

Todo lo anterior es el resultado de cifras de las modalidades de casos de delitos informáticos más comunes y que se han denunciado y que se hallan tipificados en el código penal colombiano, siendo la de más tendencia la Violación de datos personales Articulo 269F, con el 55% de los casos más denunciados en la comunidad.

Nota: En la ciudad de Quibdó a partir de este año se empieza a tener un control estadístico preciso que permita determinar los indicadores del cibercrimen.

16. ENCUESTA NO. 1

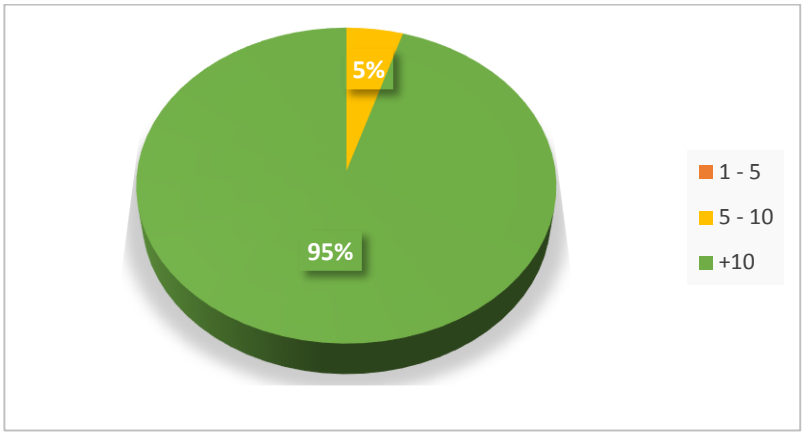
ENCUETAS REALIZADA A ALGUNAS ENTIDADES O EMPRESAS DEL MUNICIPIO DE QUIBDÓ, DEPARTAMENTO DEL CHOCÓ SOBRE LA SEGURIDAD INFORMÁTICA

¿De cuántos ordenadores dispone su entidad?

1-5 5-10 +10

Valor ponderado	Frecuencia	Porcentaje %
1-5	0	0%
5-10	1	5%
+10	20	95%
Total	21	100%

Grafico 1. ¿De cuántos ordenadores dispone su entidad?



Fuente: El autor

En la visita realizada a algunas entidades, se pudo establecer no tienen el mismo número de funcionarios se aprecia que la mayor parte de los procesos cuenta con

más de 10 computadores representando el 95% y la dependencia que posee menos equipos entre 5 a 10 corresponde al 5%.

¿Los aparatos de cómputo de la empresa, ¿tienen antivirus?

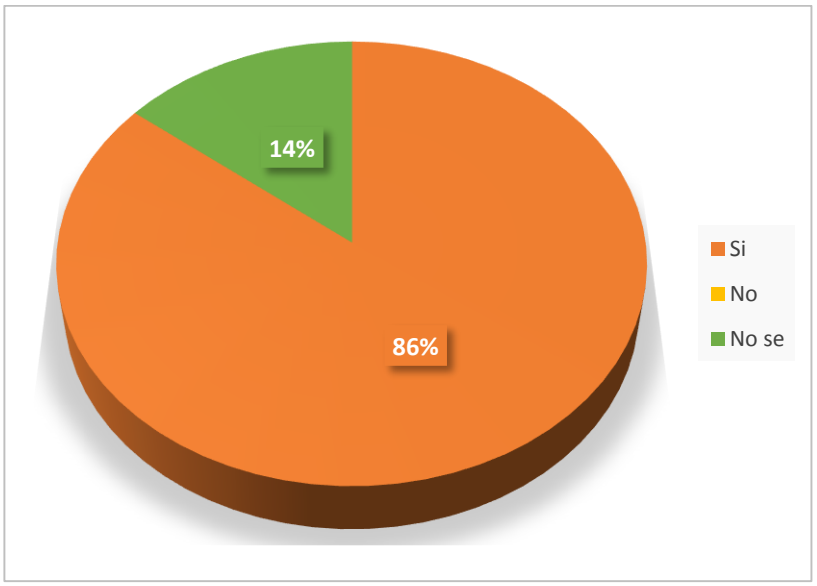
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	18	86%
No	0	0%
No se	3	14%
Total	21	100%

Grafico 2. ¿Los aparatos de cómputo de la empresa, ¿tienen antivirus?



Fuente: El autor

Se observa que el 86% de los empleados tienen instalado un antivirus como medida de protección contra amenazas de un virus que pueda afectar el normal funcionamiento del equipo y un 14% no tiene conocimiento al respecto.

¿Si tienen antivirus en los equipos de la empresa, ¿está actualizado?

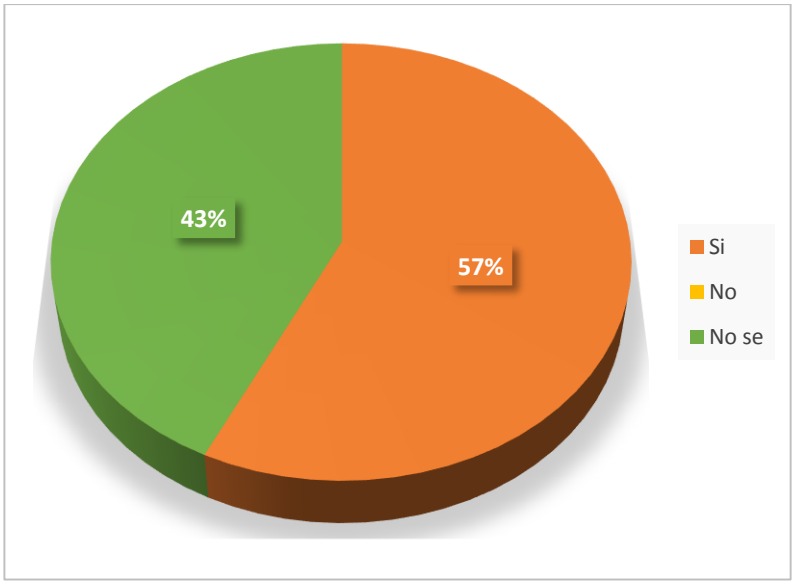
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	12	57%
No	0	0%
No se	9	43%
Total	21	100%

Grafico 3. ¿Si tienen antivirus en los equipos de la empresa, ¿está actualizado?



Fuente: El autor

Una vez formulada las dos preguntas enunciadas anteriormente a los entrevistados, se evidencia que el 57% respondieron afirmativamente que el antivirus está actualizado de acuerdo a las últimas definiciones.

Tan solo un 43% manifestó no saber si este era actualizado de acuerdo a los requerimientos establecidos.

¿La empresa le hace mantenimiento periódicamente a los computadores?

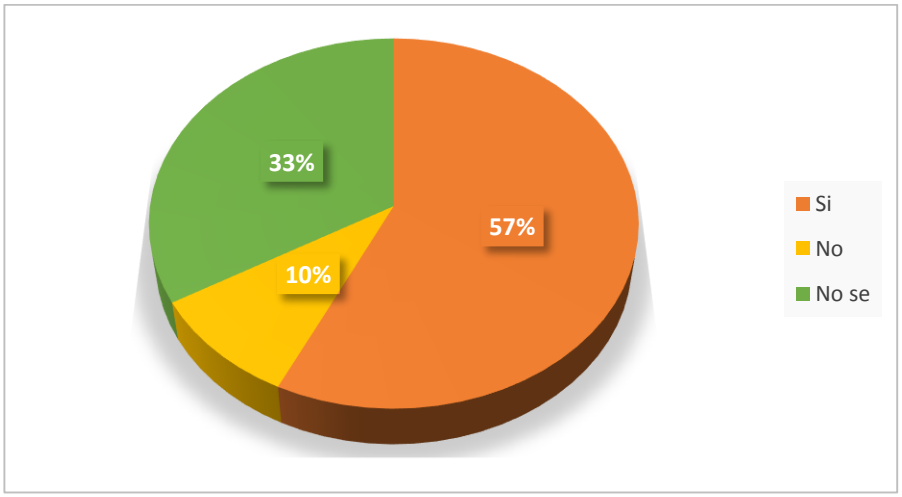
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	12	57%
No	2	10%
No se	7	33%
Total	21	100%

Grafico 4. ¿La empresa le hace mantenimiento periódicamente a los computadores?



Fuente: El autor

El 57% de la población entrevistada afirmo que se realiza cada 6 meses el mantenimiento preventivo a los equipos de cómputo, esto de acuerdo a un cronograma previamente definido y un 33% manifiestan no tener conocimiento al respecto. Dicho mantenimiento toma aproximadamente 1 horas por equipo.

¿Se utilizan programas de descarga de archivos de usuario (música, películas, programas...)?

¿Tienen por costumbre realizar descargar de programas o aplicaciones de internet?

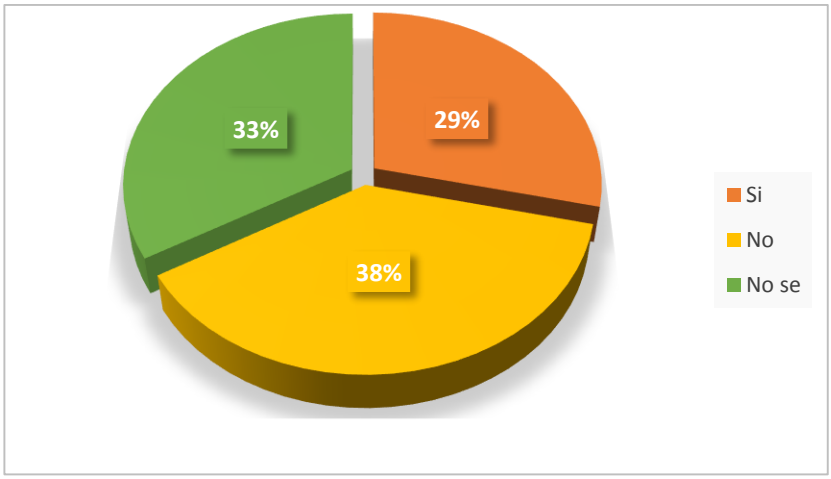
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	6	29%
No	8	38%
No se	7	33%
Total	21	100%

Grafico 5. ¿Tienen por costumbre realizar descargar de programas o aplicaciones de internet?



Fuente: El autor

En este caso el 38% indico que no era posible instalar programas que no fueran autorizados por la oficina de sistemas, mucho menos si estos eran de uso gratuito. Por su parte el 29% declararon que si se hacía uso de aplicaciones de uso gratuito para descargar no solo música sino otro tipo de archivos multimedia a pesar de que se esté incurriendo en el incumplimiento de la "CARTA DE COMPROMISO DE LICENCIAMIENTO, USO DE SOFTWARE Y CUMPLIMIENTO DE POLÍTICAS INFORMÁTICAS", en tanto a las personas que indicaron no saber si este tipo de descargas se estaban efectuando al interior del área coincidieron en que no era posible hacerlo dado que le habían explicado que no es correcto caer en esa mala conducta dentro de una empresa o entidad

¿Sabe si la empresa tiene un servidor central de datos?

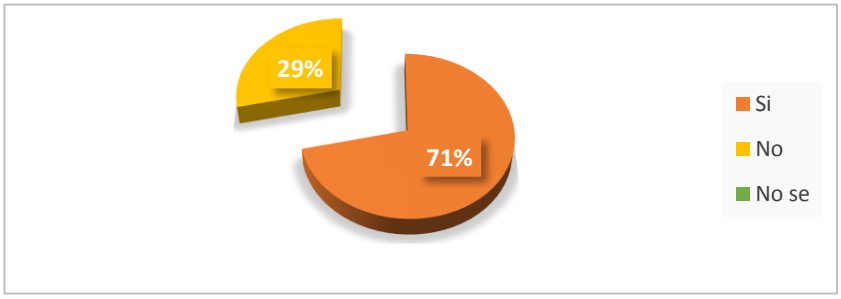
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	15	71%
No	6	29%
No se	0	0%
Total	21	100%

Grafico 6. ¿Sabe si la empresa tiene un servidor central de datos?



Fuente: El autor

Como se puede apreciar en el gráfico el 71% de los empleados de las entidades tienen noción de que en la entidad se cuenta con un servidor central de datos y un 29% no sabe la existencia de un servidor.

¿Si la empresa tiene servidor se le realiza mantenimiento constante?

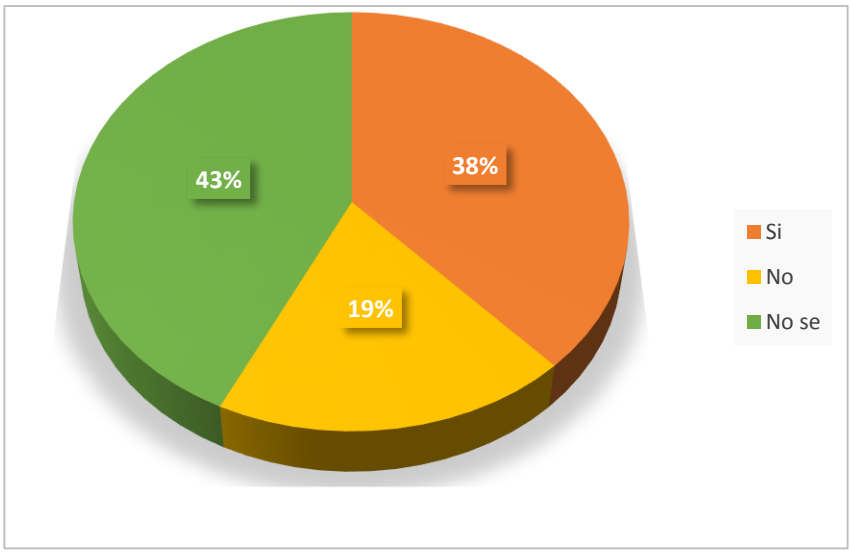
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	8	38%
No	4	19%
No se	9	43%
Total	21	100.00%

Grafico 7. ¿Si la empresa tiene servidor se le realiza mantenimiento constante?



Fuente: El autor

Para este cuestionamiento las respuestas no coincidieron en cuanto a saber si existía o no un servidor central de datos puesto que un 43% asumieron no saber nada del mantenimiento de un servidor central debido a que no conocen la existencia del mismo y un 38% afirman que si se realiza mantenimiento informático periódico al servidor central de datos. Es de notar que hay desconocimiento en cuanto a los activos informáticos y su manejo.

¿La empresa realiza su labor desde algún computador externo, o por sitio web?

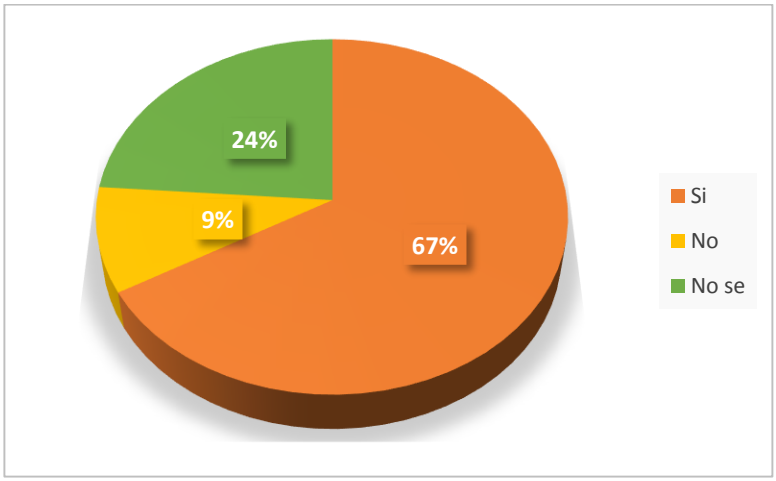
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	14	67%
No	2	9%
No se	5	24%
Total	21	100%

Grafico 8. ¿La empresa realiza su labor desde algún computador externo, o por sitio web?



Fuente: El autor

Con un 67% la respuesta SI tiene la mayor representación; es por esto que se evidencia que hay conocimiento por parte de los funcionarios de proceso, en las entidades visitadas, tan solo el 24% de los entrevistados respondió no saber que se gestionan procesos desde fuera de las instalaciones.

¿Si la empresa se conecta utilizando red WIFI, y si lo hace utilizan los medios de seguridad adecuados?

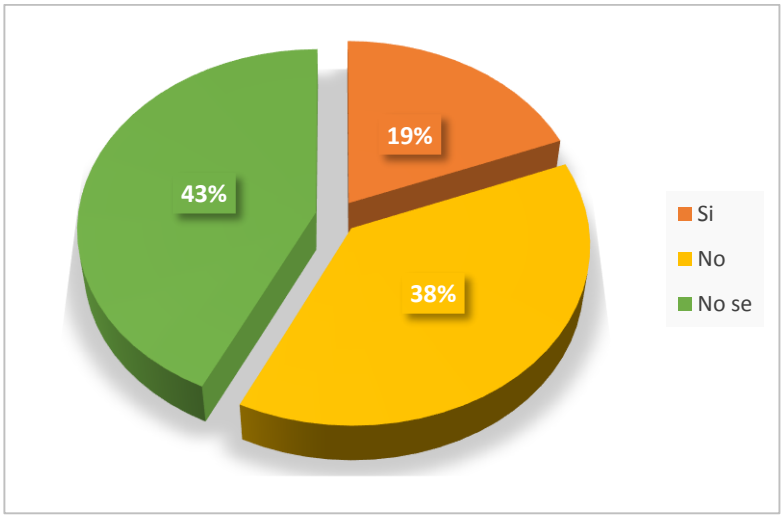
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	4	19%
No	8	38%
No se	9	43%
Total	21	100%

Grafico 9. ¿Si la empresa se conecta utilizando red WIFI, y si lo hace utilizan los medios de seguridad adecuados?



Fuente: El autor

En este aspecto, se puede observar que el 43% desconocen el hecho de haber conexión de esta forma y, sin embargo, el 38% informa que no tienen conexión WI-FI y por su parte el 19% indica que sí tiene conexión WI-FI en las entidades y que cuenta con las medidas pertinentes.

¿Los dispositivos de la empresa almacenan la información en el disco duro?

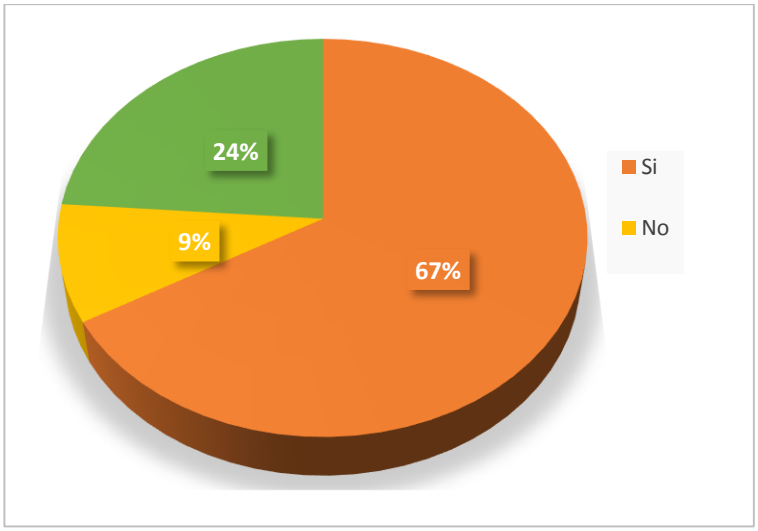
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	14	67%
No	2	9%
No se	5	24%
Total	21	100%

Grafico 10. ¿Los dispositivos de la empresa almacenan la información en el disco duro?



Fuente: El autor

En base a la encuesta y cómo podemos observar en el gráfico el 67% de los entrevistados afirmaron que efectivamente la mayoría de la información de la entidades entrevistadas reposa en cada uno de las estaciones de trabajo por seguridad. Por otro lado un 24% desconocen si se realiza copia de segurida.

¿La información que maneja la empresa se le realiza periódicamente copia de seguridad?

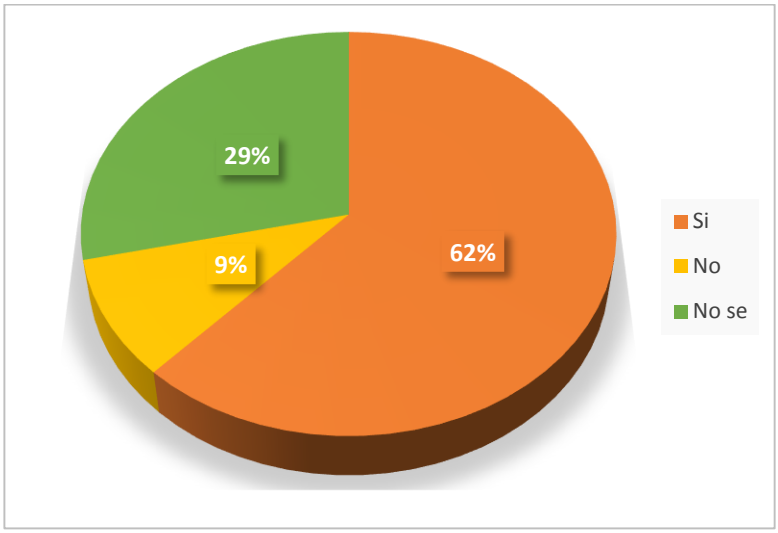
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	13	62%
No	2	9%
No se	6	29%
Total	21	100%

Grafico 11. ¿La información que maneja la empresa se le realiza periódicamente copia de seguridad?



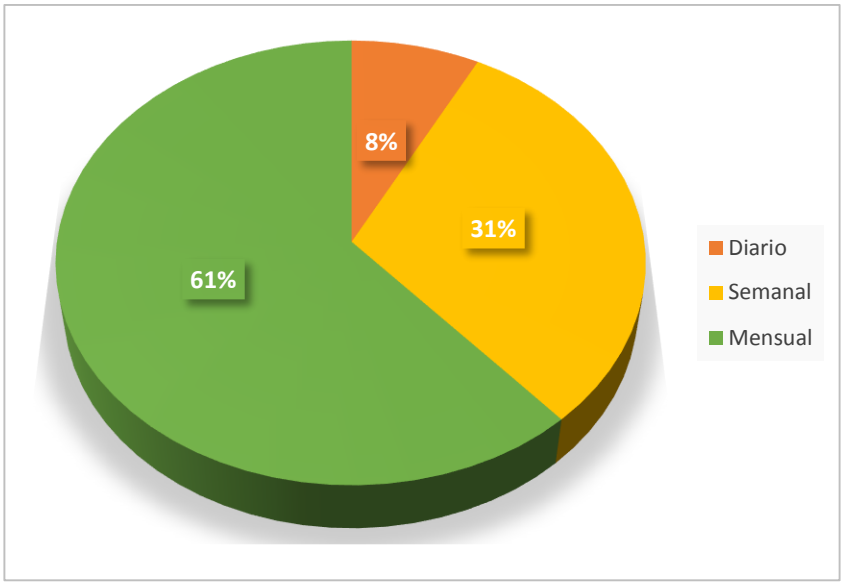
Fuente: El autor

¿Con qué frecuencia?

Diaria semanal otro

Valor ponderado	Frecuencia	Porcentaje %
Diario	1	8%
Semanal	4	31%
Mensual	8	61%
Total	21	100%

Grafico 12. ¿Con qué frecuencia?



Fuente: El autor

El 62% de los entrevistados coincidieron en que se realizan copias de seguridad con el fin de respalda la disponibilidad de la información, esta práctica esta apropiada por los funcionarios más por ser una exigencia que por el sentido mismo de su importancia a la hora de mantener la información dispuesta cuando esta se requiera y un 29% no saben realizar dicho proceso. En tanto a la frecuencia con la que se realizan las copias de seguridad el 61% indica que esta se realiza mensualmente debido a la importancia de la información, el 31% indica

que lo hace semanalmente debido a la sensibilidad de los datos manejados por la entidad y por su parte solo el 8% responde que estas se llevan a cabo diariamente según sea la necesidad.

¿Usted o sus colaboradores a cargo poseen alguna copia de seguridad (USB / DVD / Otro) fuera de la empresa?

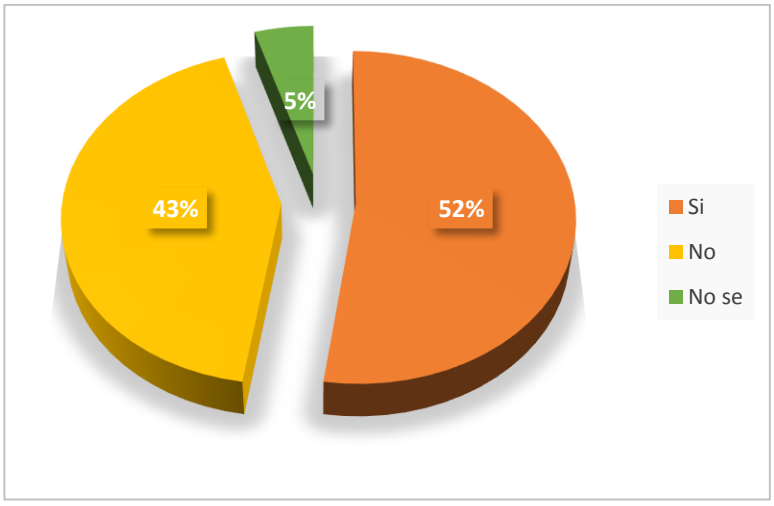
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	11	52%
No	9	43%
No se	1	5%
Total	21	100%

Grafico 13. ¿Usted o sus colaboradores a cargo poseen alguna copia de seguridad (USB / DVD / Otro) fuera de la empresa?



Fuente: El autor

El 52% revela que por su seguridad realizan copias de seguridad en dispositivos extraíbles por su tranquilidad debido a que no tienen la certeza de que la información haya sido guardada. El 43% revela que no es posible guardar copias de seguridad en dispositivos extraíbles, esto debido a que no cuentan con dichos dispositivos. El restante 5% aclaro desconocimiento del tema en cuestión.

¿Se realiza un mantenimiento de las copias de seguridad de su entidad o empresa?

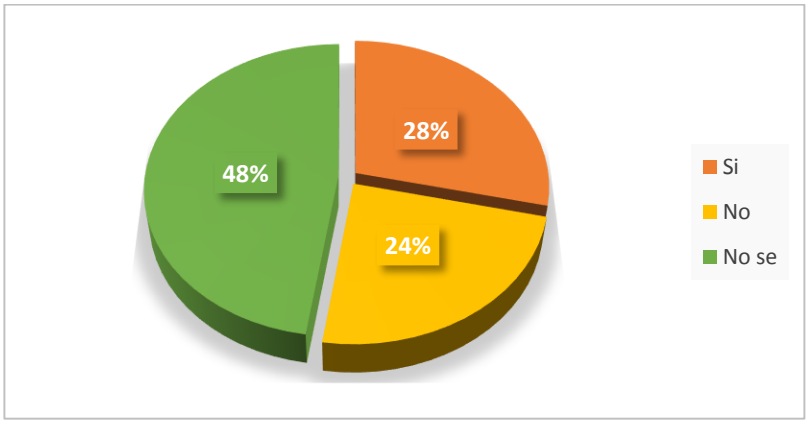
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	6	28%
No	5	24%
No se	10	48%
Total	21	100%

Grafico 14. ¿Se realiza un mantenimiento de las copias de seguridad de su entidad o empresa?



Fuente: El autor

Se aprecia que en este sentido el 48% de los entrevistados desconocen los procesos que se realizan a las copias de seguridad de su entidad o empresa, para el 28% de los interrogados afirman tener conocimiento de los mantenimientos que se realiza a la copia de seguridad de la entidad y un 24% responde que no se le realiza este proceso a las copias de seguridad.

¿Los programas y aplicaciones usados, cumplen con las características de seguridad informática?

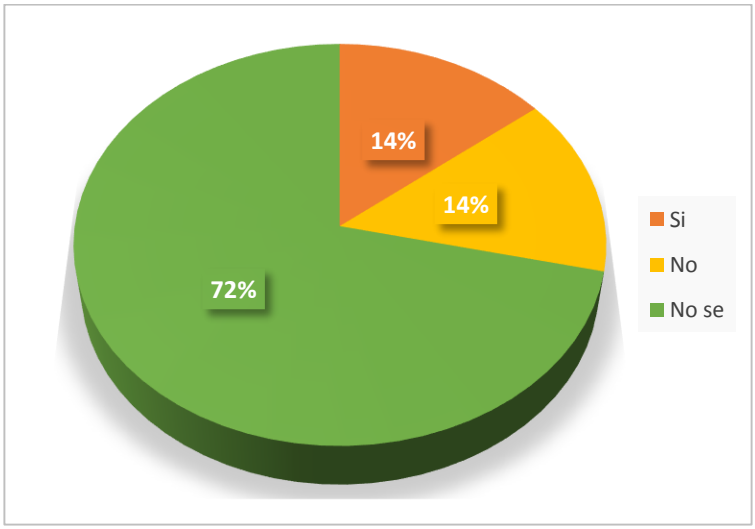
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	3	14%
No	3	14%
No se	15	72%
Total	21	100%

Grafico 15. ¿Los programas y aplicaciones usados, cumplen con las características de seguridad informática?



Fuente: El autor

El 72% no tener conocimiento de la seguridad informática y si las aplicaciones y programas lo aplican, Solo algunos o pocos funcionarios que equivale al 14% afirman que los sistemas de información cuentan con parámetros de seguridad que garantizan la confiabilidad, integridad y disponibilidad de la información, aunque en si no tiene políticas claramente definidas en materia de software y un 14% niegan que las aplicaciones y programas cuente con los parámetros que requiere de acuerdo a la seguridad informática.

¿Hay algún encargado de instalar/desinstalar los programas y aplicaciones informáticas?

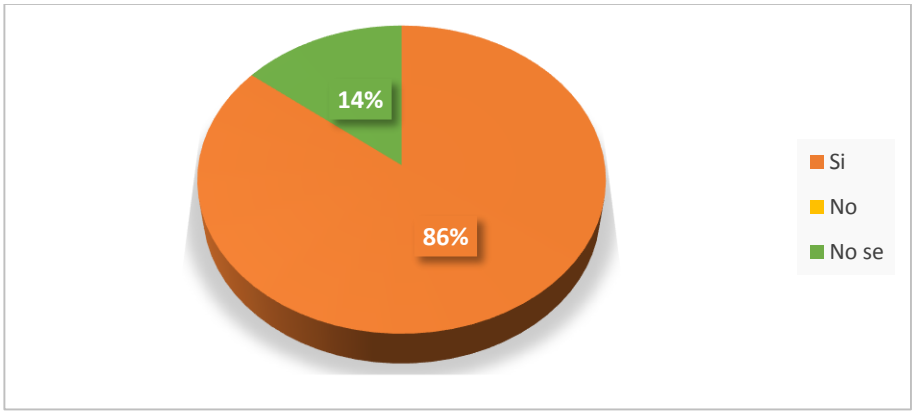
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	18	86%
No	0	0%
No se	3	14%
Total	21	100%

Grafico 16. ¿Hay algún encargado de instalar/desinstalar los programas y aplicaciones informáticas?



Fuente: El autor

Es claro que las entidades o empresas cuentan con firmas externa encargada de realizar las configuraciones pertinentes de acuerdo a la necesidad del proceso que se gestiona. El 86% de los entrevistados afirma conocer que los encargados de esta labor directivos. Un 14% manifiestan no saber quién es el encargado de dicho proceso.

¿Conoce usted algo referente a la seguridad informática?

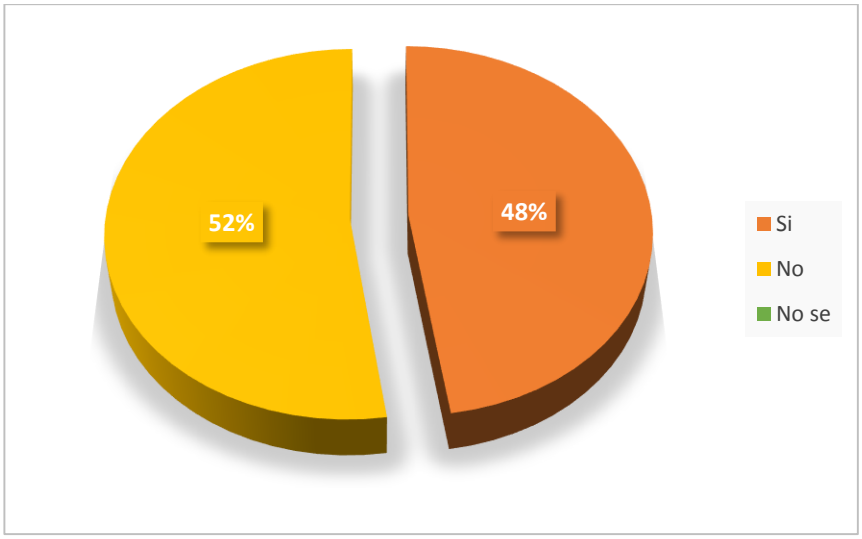
Sí

No

No se

Valor ponderado	Frecuencia	Porcentaje %
Si	10	48%
No	11	52%
No se	0	0%
Total	21	100%

Grafico 17. ¿Conoce usted algo referente a la seguridad informática?



Fuente: El autor

Siendo la seguridad un factor muy importante en el manejo de información en las entidades, es indudable que el desconocimiento es un ingrediente muy común en las organizaciones, como se puede notar el 52% no tienen idea de lo que es la seguridad informática y un 48% afirman saber algo de seguridad informática debido a sus experiencias en otras entidades o por su formación académica.

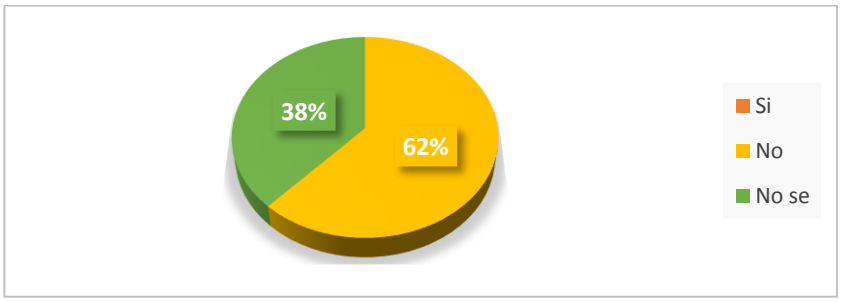
¿Qué sabe al respecto?

Lo que indicaron los encuestados de la que era la seguridad informática para ellos son:
La seguridad informática es muy esencial para los datos manejados en la entidad
Es con lo que se protege la información que manipulamos diariamente
Es la protección que cada uno debemos de darle a la información que manipulamos
La verdad no mucho, pero hay una persona en la entidad que se encarga de revisar los equipos
Es el manejo adecuado que le damos a la información
Proceso mediante el cual se protege todo la información que tiene que ver por vía de redes de datos
Es la seguridad que debe tener la empresa evitando ataques
Es la seguridad que todos debemos tener para evitar la pérdida de la información
Es la protección que se brinca a los equipos

¿La compañía ha dispuesto políticas de seguridad para el manejo de herramientas para la gestión de su proceso?
Sí
No
No se

Valor ponderado	Frecuencia	Porcentaje %
Si	0	0%
No	13	62%
No se	8	38 %
Total	21	100%

Grafico 18. ¿La compañía ha dispuesto políticas de seguridad para la gestión de su proceso?



Fuente: El autor

Como se puede observar en la gráfica el 62% niegan el hecho de que en la entidad hayan políticas de seguridad, y un 38% desconocen por completo este tema.

17. ENCUESTA NO. 2

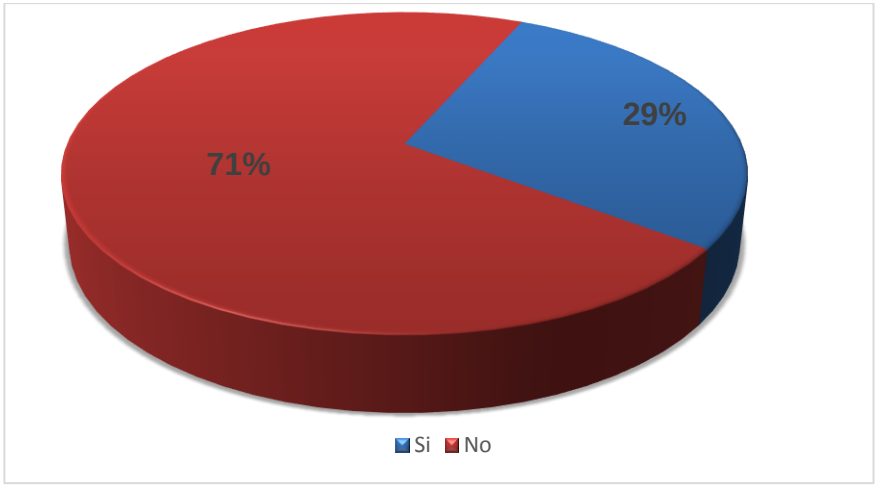
CUESTIONARIO DE SEGURIDAD INFORMÁTICA EN EL MUNICIPIO DE QUIBDÓ – CHOCÓ

1. ¿Tiene usted equipos informáticos en su hogar o en su lugar de trabajo?

SI

NO

Grafico 19. ¿Tiene usted equipos informáticos en su hogar o en su lugar de trabajo?



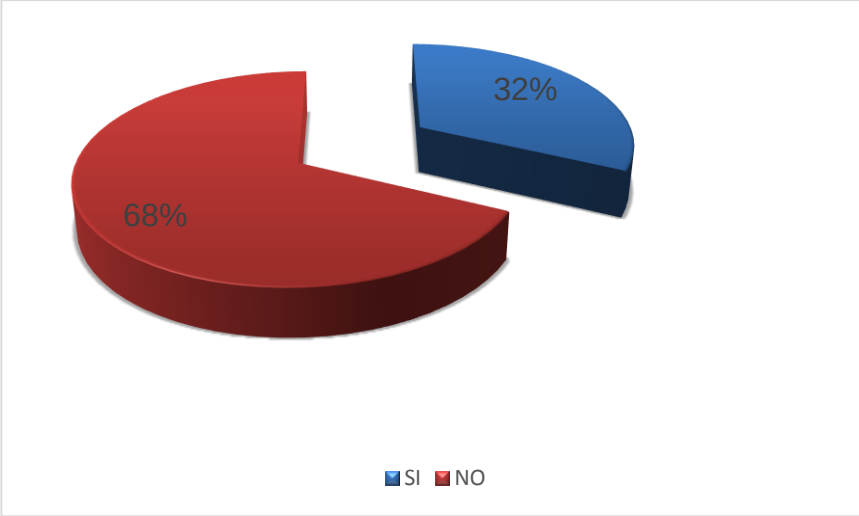
Fuente: El autor

2. Si tienen antivirus en el equipo, ¿este se encuentra actualizado?

SI

NO

Grafico 20. Si tienen antivirus en el equipo, ¿este se encuentra actualizado?



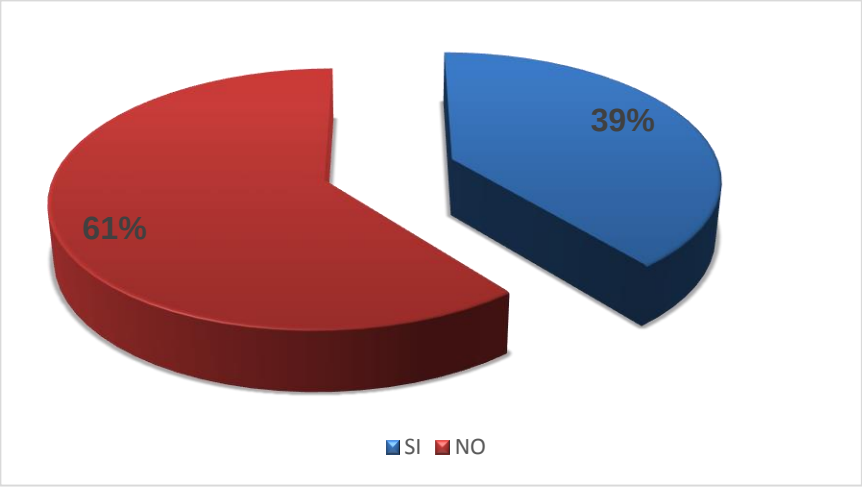
Fuente: El autor

3. ¿Sabe usted sabe que es un delito informático o Cibercrimen?

NO

SI

Grafico 21. ¿Sabe usted sabe que es un delito informático o Cibercrimen?



Fuente: El autor

4. ¿De las siguientes Normas sabe usted cuál es la ley que sanciona a las personas que realizan delitos informáticos? Seleccionar una opción

a. Ley 136 de 1994

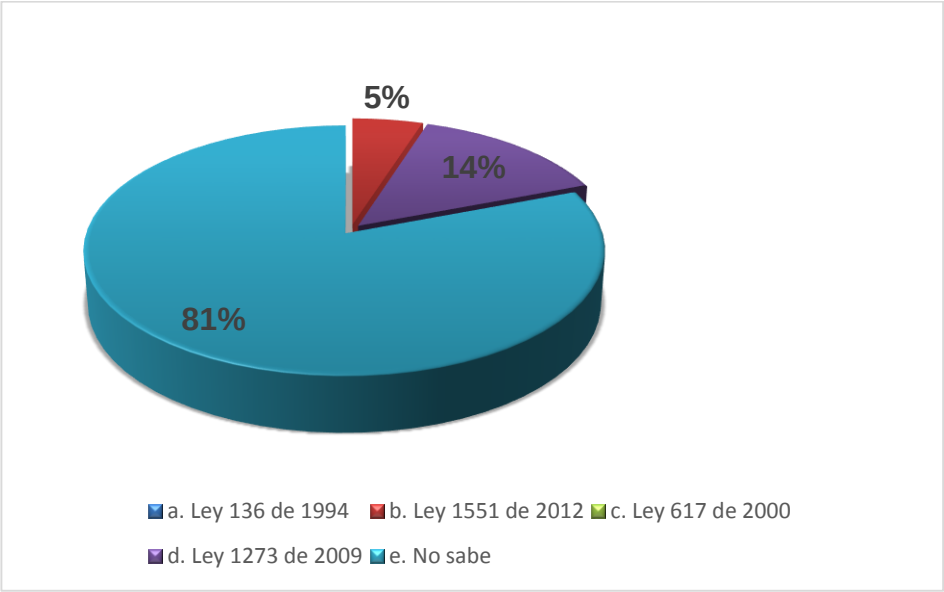
b. Ley 1551 de 2012

c. Ley 617 de 2000

d. Ley 1273 de 2009

e. No sabe

Grafico 22. ¿De las siguientes Normas sabe usted cuál es la ley que sanciona a las personas que realizan delitos informáticos?



Fuente: El autor

5. ¿Qué tan habitualmente utiliza las redes sociales?

Siempre

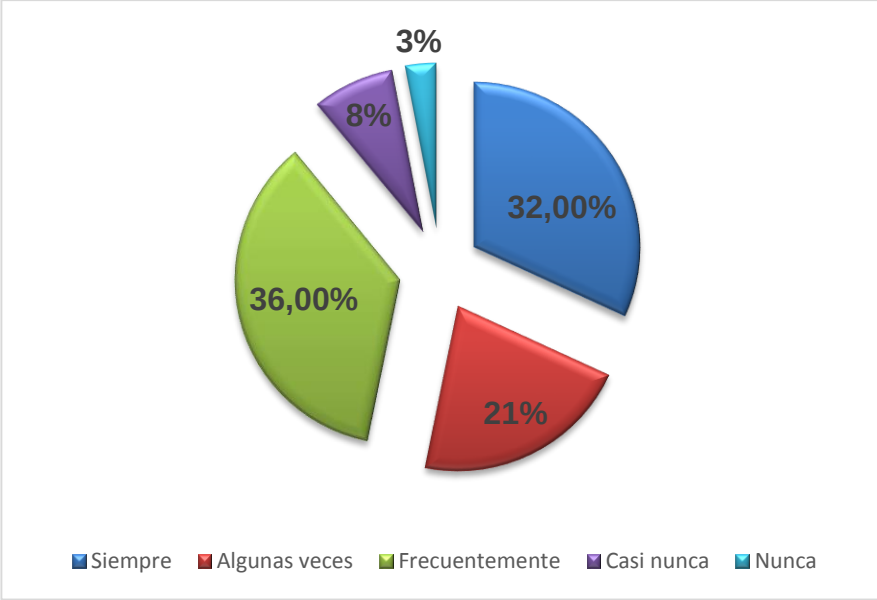
Algunas veces

Frecuentemente

Casi nunca

Nunca

Grafico 23. ¿Qué tan habitualmente utiliza las redes sociales?



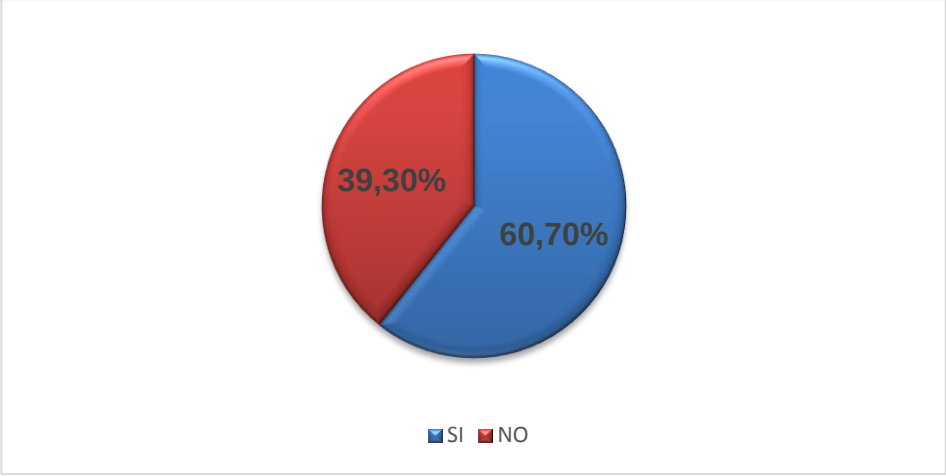
Fuente: El autor

6. ¿Sabe que es el ciberespacio, o la web?

SI

NO

Grafico 24. ¿Sabe que es el ciberespacio, o la web?



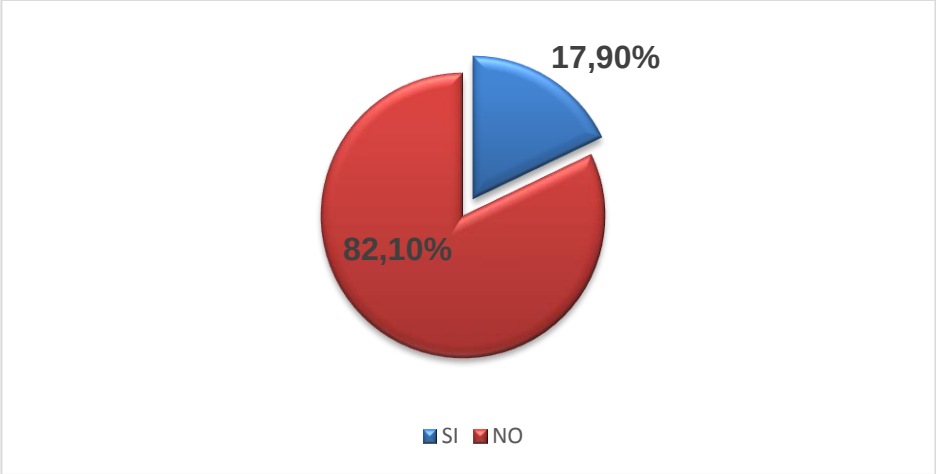
Fuente: El autor

7. ¿Cuándo entra a una página web sabe usted si es segura?

SI

NO

Grafico 25. ¿Cuándo entra a una página web sabe usted si es segura?



Fuente: El autor

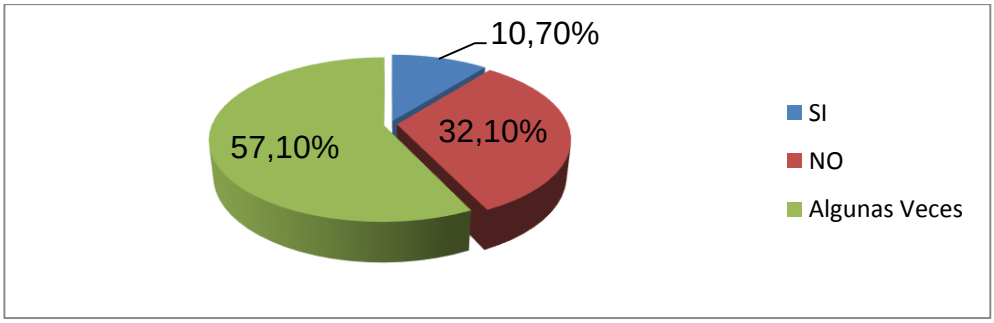
8. ¿Siempre cierra su correo electrónico o redes sociales al instante de finalizar sesión en los equipos?

SI

NO

Algunas veces

Grafico 26. ¿Siempre cierra su correo electrónico o redes sociales al instante de finalizar sesión en los equipos?



Fuente: El autor

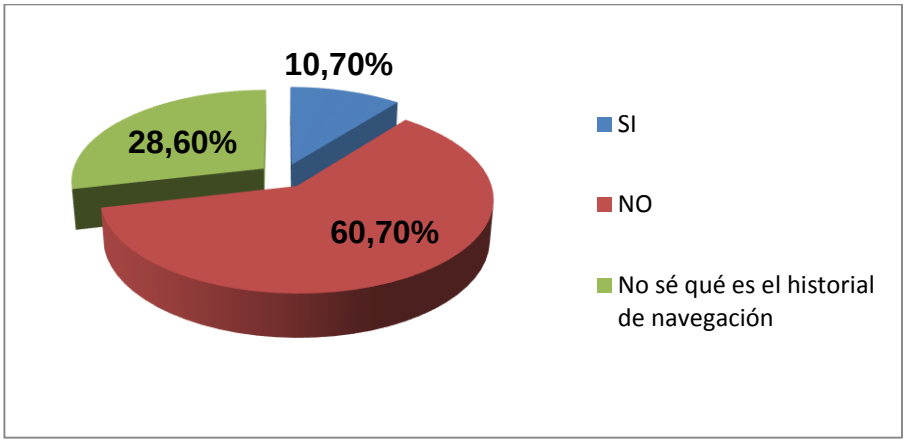
¿Al finalizar de navegar en internet acostumbra borrar el historial de navegación?

SI

NO

No sé qué es el historial de navegación

Grafico 27. ¿Al finalizar de navegar en internet acostumbra borrar el historial de navegación?



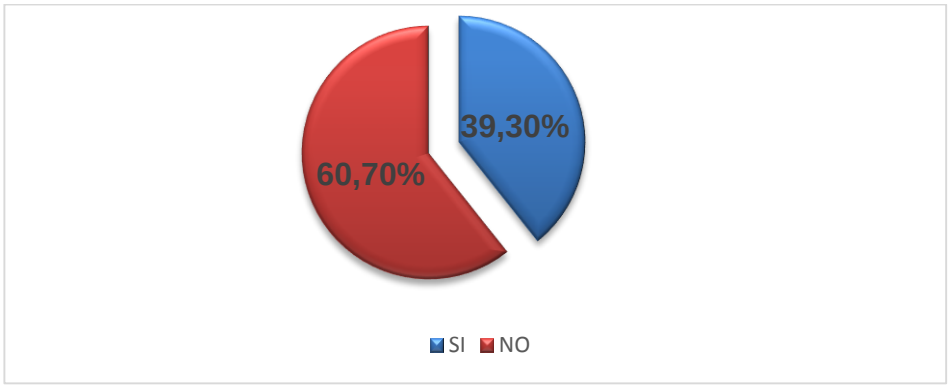
Fuente: El autor

10. ¿Ha sido usted víctima de algún tipo de delito informático?

SI

NO

Grafico 28. ¿Ha sido usted víctima de algún tipo de delito informático?



Fuente: El autor

11. ¿De la siguiente lista de delitos informáticos, Cuál de estos usted conoce?

a. Robos de datos personales, robo de computadores, hackers, robo en los bancos

b. Los sabotajes a empresas, uso fraudulento de Internet, fugas de información, espionaje informático

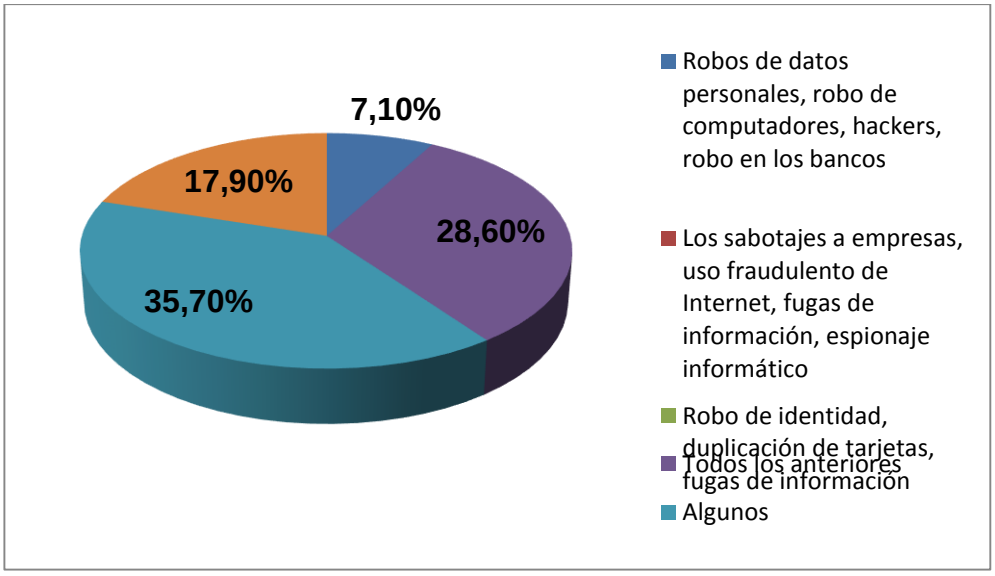
c. Robo de identidad, duplicación de tarjetas, fugas de información

d. Todos los anteriores

e. Algunos

f. Ninguno

Grafico 29. ¿De la siguiente lista de delitos informáticos, Cuál de estos usted conoce?



Fuente: El autor

12. ¿Cuándo fue la última vez que cambio su contraseña del correo electrónico y de su equipo?

Entre 1 y 3 meses

Entre 2 y 6 meses

Entre 8 meses

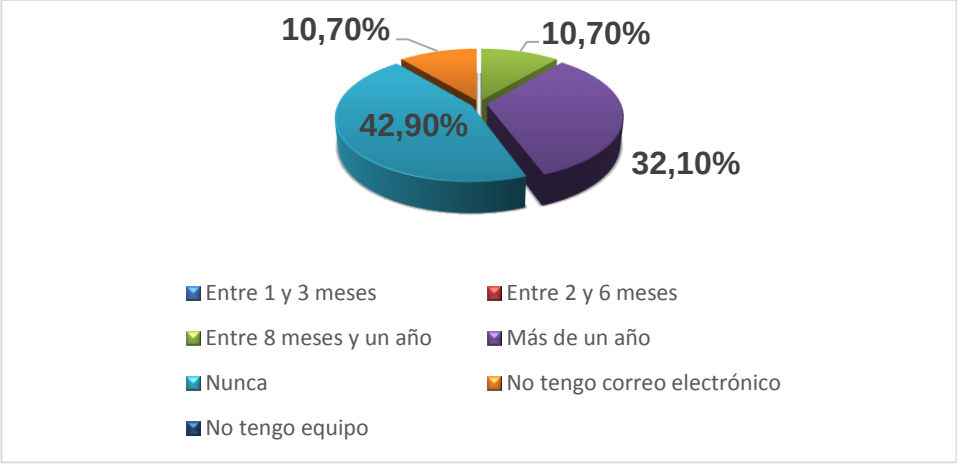
Más de un año

Nunca

No tengo correo electrónico

No tengo equipo

Grafico 30. ¿Cuándo fue la última vez que cambio su contraseña del correo electrónico y de su equipo?



Fuente: El autor

13. ¿Cree usted que hacer compras a través de Internet es seguro?

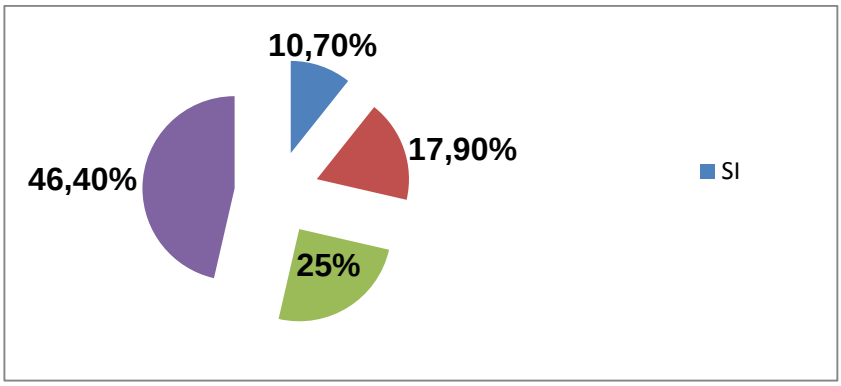
SI

NO

Depende la situación

No sabe

Grafico 31. ¿Cree usted que hacer compras a través de Internet es seguro?



Fuente: El autor

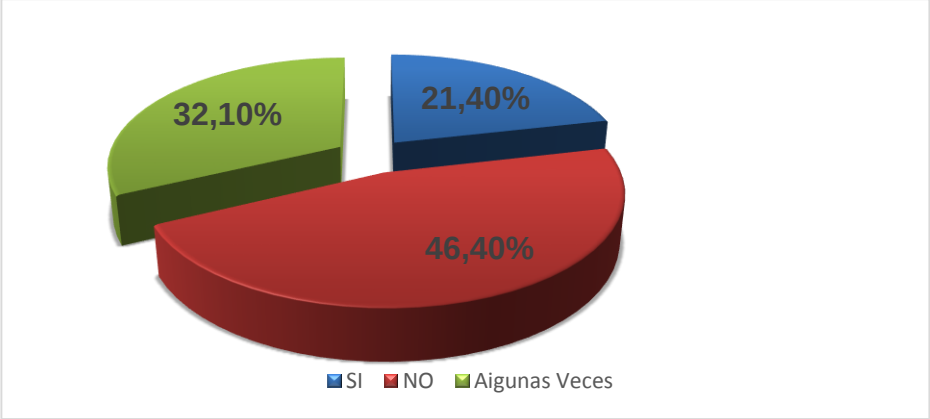
14. ¿utiliza usted los servicios de internet (virtuales) que ofrecen los bancos?

SI

NO

Algunas veces

Grafico 32. ¿Utiliza usted los servicios de internet (virtuales) que ofrecen los bancos?



Fuente: El autor

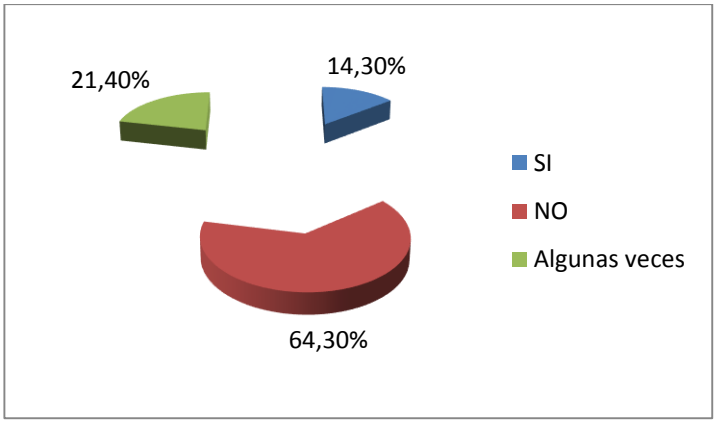
15. ¿Entrega información bancaria a través del internet?

SI

NO

Algunas veces

Grafico 33. ¿Entrega información bancaria a través del internet?



Fuente: El autor

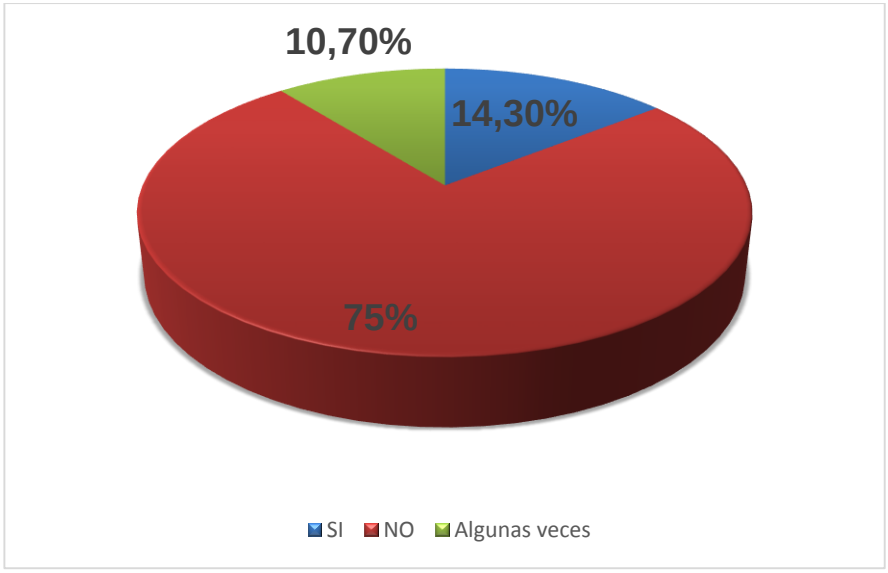
16. ¿Proporciona información personal a terceros para que tramiten formatos de transacciones bancarias por usted por medio de internet?

SI

NO

Aganas veces

Grafico 34. ¿Proporciona información personal a terceros para que tramiten formatos de transacciones bancarias por usted por medio de internet?

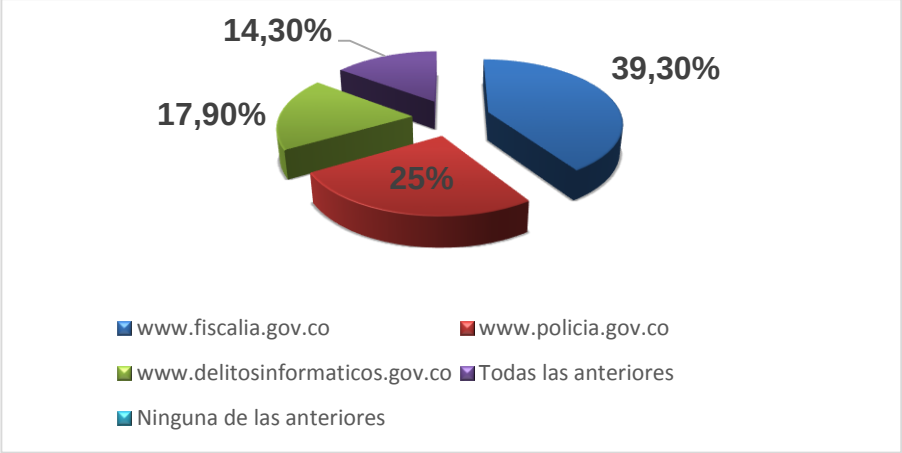


Fuente: El autor

17. ¿Sabe usted dónde se pueden hacer las denuncias de un delito informático?

www.fiscalia.gov.co
www.policia.gov.co
www.delitosinformaticos.gov.co
Todas las anteriores
Ninguna de las anteriores

Grafico 35. ¿Sabe usted dónde se pueden hacer las denuncias de un delito informático?



Fuente: El autor

18. RECOMENDACIONES

Actualmente, los ciberdelincuentes no se restringen en el momento de ejecutar sus delitos. Para esta monografía es importante dejar plasmadas o asentada algunas recomendaciones básicas e importantes, que le puedan permitir al ciudadano de esta localidad, conocer cómo prevenirse frente a la situación global que se está presentando en estos tiempos y que está afectando al mundo entero, como lo es el CIBERCRIMEN.

Con estas recomendaciones se puede evitar el robo de identidad y al mismo tiempo se busca contrarrestar los delitos de cibercrimen en la sociedad del Chocó:

Hay que ser prudente al momento de abrir correos electrónicos, teniendo en cuenta que en la actualidad es un medio muy utilizado para cometer robos de identidad, concretamente empleando una técnica muy utilizadas por estos ciber delincuentes llamada phishing, y así, poder lograr conseguir los datos confidenciales de sus víctimas. Adema es bueno saber, que cuando llegan enlaces que se reciben por correos electrónicos hay que evitar darles clic, por la gran posibilidad de que pueden provenir de sitios engañosos.

Siempre deben crear contraseñas que se consideren fuerte y que sean difíciles de penetrar por los delincuentes informáticos, por seguridad hay que evitar enviar información confidencial o contraseñas por correo electrónico y mucho menos por mensajería instantánea.

Tener activado el Firewall en los computadores, es fundamental habituarse a cerrar todas secciones después de finalizar, para mayor seguridad es importante el resguardo de los datos personales confidenciales.

Antes de desechar algunos documentos como ejemplo tarjetas de crédito y débito pres - aprobados y las que ya expiraron, estados de cuenta bancarios, los cheques de tarjeta de créditos, es importante destruirlos antes de tirarlos a la basura.

Existe personas que se hacen pasar por vendedores, asesores comerciales o representantes de entidades financieras, con el objetivo de robar los datos, por eso se debe evitar dar información confidencial, como número de seguro social, licencia, tarjetas de crédito y débito, cedula de ciudadanía, dirección de residencia, fecha de nacimiento, etc…, a estas personas que contactan a los usuarios por vía telefónica solicitando esta información.

Es importante tener cuidado con los sitios, porque es usual conseguirse con aplicaciones que ofrecen auto instalación de dudosa reputación. Estas aplicaciones normalmente son barras con funcionalidades que se sitúan en el explorador, cuando una aplicación pretenda ubicarse sin autorización, hay que desconfiar, como ejemplo los sitios pornográficos, ellos contienen grandes contenidos de programas perjudiciales que se aprovechan de la vulnerabilidad de algunas computadoras, permitiendo que se puedan instalar con facilidad. Estos programas dañinos se desarrollan rápidamente, por ello la importancia de tener un buen antivirus y actualizado, con capacidad para revelar cuando estas estas aplicaciones quieran instalarse en el computador y a su vez impedirlo.

Se invita a la población Quibdoseña que realice una exploración, investigación, analizar la ley, normas, decretos, con el objetivo de que puedan conocer, comprender y aprender a proteger la misma y descubrir métodos o estrategias para evitar ser víctimas de delitos informáticos, así mismo es importante que en las empresas del departamento del Chocó y sus municipios, se socialicen e implementen las políticas de seguridad informática, capacitando a todos sus

funcionarios sobre seguridad, que más allá de realizar las actividades diarias dentro de la empresa, su obligación es proteger la información confidencial de esta y así poder ayudar a evitar, reducir, prevenir los perjuicio que trae los delitos informáticos en el municipio de Quibdó.

19. CONCLUSIONES

El presente proyecto investigativo, permitió realizar un análisis para establecer una idea del comportamiento, acontecimientos del Cibercrimen en las personas, empresas e instituciones educativas en la ciudad de Quibdó.

De esta investigación, se pudo observar el desarrollo del arte del cibercrimen permitiendo abrir la puerta a las técnica de los delitos como el hurto, estafa y suplantación y demás que logren estar puntualizados entre los casos de comportamientos de cibercrimenes más frecuentes que violan la integridad, confidencialidad y disponibilidad de las personas que llegan hacer víctimas de estos ataques.

En el proyecto se pudo identificó y analizó los diferentes casos que tuvieron mas relevancia en cuento al cibercrimen en la ciudad de Quibdó, teniendo en cuenta el crecimiento del mundo de las tecnologías en la actualidad.

Se estableció cuál es la tendencia de la comisión de cibercrimen en el departamento del Chocó y sus municipios, este análisis se realizó tomando como referencia las denuncias realizadas a la Fiscalía General de la Nación Seccional Quibdó, entre los años 2014, 2015, y 2017, permitiendo determinar que el delito informático que más incidencia tiene es el delito de violación de datos personales - Articulo 269F, con el 55% siendo este más denunciado por la población del Chocó.

Dentro de este contexto se consiguió identificar y determinar el grado de conocimiento de la población frente a los delitos informáticos, realizando encuestas a la población de Quibdó, sin importar su género y cultura; las cuales

arrojaron como conclusión un alto índice de ignorancia en lo que tiene que ver con el tema de delitos informático tipificados dentro de la Ley 1273 de 2009.

Es fundamental para los pobladores del municipio de Quibdó, entender que los delitos informáticos van progresando de manera incontrolable, esto manifiesta que el cibercrimen se ha convertido en la sociedad un reto que se debe de atacar.

La importancia de este estudio está, en que si se tiene un mayor conocimiento sobre la actividad dañina en el municipio de Quibdó, en los que tiene que ver con los delitos informático y en el uso de internet, esto ayudaría o permitiría a dimensionar apropiadamente el problema, es decir, como primera conclusión es que la falta de noción de datos sobre el cibercrimen, en cuanto a su forma como en sus características está haciendo más difícil saber su real magnitud, y las verdaderas consecuencias.

Por otro lado en la región del Chocó, hay una situación que no ayuda a contrarrestar este flagelo, es que la mayoría de las víctimas de delitos informáticos no denuncian porque les da temor que se vea a afectada la integridad moral y social, y además porque las autoridades o entidades judiciales no hacen nada al respecto.

Esta investigación que se realizó pudo mostrar que el cibercrimen posee características cambiantes, esta situación es evidente, dado a que los delincuentes informáticos se van adecuando según la forma del entorno, siendo cada día más hábiles realizando ataques cada vez más sofisticados, por ello, se hace necesario la creación de estrategias o recomendaciones que permitan y muestren la posibilidad de crear ambientes más seguros y así poder reducir los riesgos que se presentan en el departamento del Chocó.

20. DIVULGACIÓN

El presente proyecto de investigación monografía llamado — ANÁLISIS DEL COMPORTAMIENTO DEL CIBERCRIMEN EN EL MUNICIPIO DE QUIBDÓ, DEPARTAMENTO DEL CHOCÓ, tendrá como única fuente de publicidad en la Universidad Nacional Abierta y a Distancia - UNAD, en donde estará disponible para todas las personas que quieran conocer información del comportamiento de los delitos informáticos *(Cibercrimen)*.

21. BIBLIOGRAFÍA

LUZARDO, ANA MARÍA. 2017. Periodista. El nuevo blanco de los cibercriminales en Colombia son las empresas. [En línea] 03 de 31 de 2017. [Citado el: 12 de 09 de 2017.] http://www.enter.co/chips-bits/seguridad/empresas-el-nuevo-blanco-de-los-cibercriminales-en-colombia.

GUTIÉRREZ, JAVIER ARRIETA. 2013. Educación. Medidas para aumentar la seguridad informática en su centro de trabajo. [En línea] 15 de Oct. De 2013. [Citado el: 14 de 09 de 2016.] https://es.slideshare.net/mariorafaelquirozmartinez/medidas-para-aumentar-la-seguridad-informatica-en-su-centro-de-trabajo.

CARRASCO, F. 2011. 90 % de las empresas han sido víctimas de vulnerabilidades de Seguridad. CIO América Latina. [En línea] 30 de 11 de 2011. http://www.cioal.com/2011/06/30/90-de-las-empresas-han-sido-victimas-de-vulnerabilidades-de-seguridad/.

DAVID A. FRANCO, JORGE L. PEREA & LUIS C. TOVAR. (2013). 2016. Herramientas para la Detección de Vulnerabilidades basada en la identificación de servicios. [En línea] 14 de Ene. De 2016. [Citado el: 26 de Oct. de 2016.] http://www.scielo.cl/scielo.php?pid=S0718-07642013000500003&script=sci_arttext.

MEDINA, ÉDGAR. 2016. Periodista. *El Cibercrimen se volvió una profesión.* [En línea] 23 de Mayo de 2016. [Citado el: 30 de Abril de 2017.] http://www.eltiempo.com/archivo/documento/CMS-16601202.

ESCRIVÁ, G. G., ROMERO, S. R. M., & RAMADA, D. J. (2013). 2017. Seguridad Informática. Madrid, ES: Macmillan Iberia, S.A... [En línea] 19 de 02 de 2017. [Citado el: 03 de 05 de 2017.] http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10820963&p00=seguridad+inform%C3%A1tica. .

FERREYRO, A., & LONGHI, A. D. (2014). e-Biblioteca de la UNAD. Metodología de la investigación. Córdoba, Argentina: Encuentro Grupo Editor. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?user=proveedor&pass=danue0a0&url=http://bibliotecavirtual.unad.edu.co:2051/.

ISO (INTERNATIONAL ORGANIZATION OF ESTANDARDIZATION). ISO/IEC 27001:2005. Tomado de: http://www.iso.org/iso/catalogue_detail?csnumber=42103.

ISO / IEC 27000: 2009 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Información general y vocabulario. Recuperado de https://www.iso.org/standard/41933.html.

MYERSON, J. (2012). 2012. Servicios en la nube: mitigar riesgos, mantener la disponibilidad. *IBM.* [En línea] 24 de Dic. De 2012. http://www.ibm.com/developerworks/ssa/cloud/library/cl-cloudservicerisks. .

PURBA, NARINDER. 2016. Educación, Periodista. *El crecimiento del cibercrimen es "despiadado" según Europol.* [En línea] 28 de Sep. De 2016. https://www.welivesecurity.com/la-es/2016/09/28/crecimiento-del-cibercrimen-despiadado/. .

27032, NORMA ISO/IEC. 2012. Noticias. *Nuevo Estándar de Ciberseguridad.* [En línea] 17 de Octubre de 2012. http://cso.computerworld.es/alertas/norma-isoiec-27032-nuevo-estandar-de-ciberseguridad. .

DIGITAL, CORPORACIÓN COLOMBIA. 2017. Los dispositivos conectados caminan como un ejército en manos de los cibercriminales. [En línea] 24 de Abril. De 2017. https://colombiadigital.net/actualidad/noticias/item/9654-los-dispositivos-conectados-caminan-como-un-ejercito-en-manos-de-los-cibercriminales.html.

CASABONA, CARLOS MARÍA ROMEO. 2006. Los datos de carácter personal como bienes jurídicos penalmente protegidos. *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político criminales.* ESPAÑA: Granada: Comares.

UNAD. Riesgos y control informático. Conceptos de Vulnerabilidad, Riesgo y Amenaza. [En línea] [Citado el: 21 de Sep. de 2017.] http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html.

BUITRAGO, JOHNNATAN. 2016. Seguridad Informatica Ataques y Vulnerabilidades. [En línea] 01 de Agos. De 2016. [Citado el: 13 de Sep. de 2017.] http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades.

MIERES, JORGE. 2009. Ataques informáticos. *Debilidades de seguridad comúnmente explotadas.* [En línea] Enero de 2009. [Citado el: 09 de Sep. de 2017.] http://www.coreoneit.com/tipos-de-ataques-informaticos/.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO (2009). Eduteca. Manual Para identificar y notificar phishing scam. Pharming {En línea} {19 de Noviembre de 2016} Disponible en http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=194

NTC-ISO/IEC, NORMA TÉCNICA. 2006. TECNOLOGÍA DE LA INFORMACIÓN. *Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).* [En línea] 03 de Abril de 2006. http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf.

MÉNDEZ., VÍCTOR. 2017. Diario Pontevedra. El c*ibercrimen provoca 300 denuncias en lo que va de año en la ciudad.* [En línea] 30 de Abril de 2017. [Citado el: 03 de Mayo de 2017.] http://diariodepontevedra.galiciae.com/noticia/696064/el-cibercrimen-provoca-300-denuncias-en-lo-que-va-de-ano-en-la-ciudad.

AL., JOSÉ. 2015. cibercrimen. *Qué es y cómo combatir el cibercrimen.* [En línea] 16 de Abril de 2015. http://portaley.com/2015/04/que-es-y-como-combatir-el-cibercrimen/.

SERNA, ISRAEL MACEDO. 2014. DEEP WEB: EL LADO OSCURO DE INTERNET. [En línea] 30 de Junio de 2014. http://expansion.mx/economia/2014/06/27/como-opera-la-deep-web-en-mexico.

LEY 1273 DE 2009 (Enero. 2009. Propiedad de la Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C. *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen*

las tecnologías de la información y las comunicaciones. [En línea] 05 de Enero de 2009. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

DECRETO 2573 DE. 2014. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. [En línea] 12 de Dic. De 2014. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60596.

LEY ESTATUTARIA 1266 DE 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dicta. [En línea] 31 de Dic de 2008. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488.

DECRETO 1377 DE 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. EL PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. [En línea] 27 de Junio de 2013. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646.

ABC DE LA Ley 1581 de 2012 Protección de Datos Personales - Colombia. GENERALIDADES. La ley de protección de datos personales – Ley 1581 de 2012 – es una ley que complementa la regulación vigente. [En línea] http://www.colcob.com/web1/images/pdf-word/el_abc_Ley_1581_2012.pdf.

INFORMATICA, MONOGRAFIA INTRODUCCION A LA SEGURIDAD. 2012. observatorio Tecnológico. [En línea] 26 de Mar. de 2012. http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica.

DUARTE, EUGENIO. 2012. 7 Tipos De Hackers Y Sus Motivaciones. [En línea] 11 de Julio de 2012. http://blog.capacityacademy.com/2012/07/11/7-tipos-de-hackers-y-susmotivaciones/.

CONSULTORES, CSI. 2016. Seguridad Informática vs Seguridad de la Información. [En línea] 22 de Sep. De 2016. https://www.maestrodelacomputacion.net/seguridadinformatica-seguridad-de-la-informacion/.

SEMANA, PELIGROS INFORMÁTICOS. 2014. ¿Qué es un Malware y cómo se puede prevenir? [En línea] 30 de Ene. 2014. [Citado el: 19 de Sep de 2017.] http://www.semana.com/tecnologia/tips/articulo/que-malware-como-puede-prevenir/372913

A, CLARA LUCÍA GUZMÁN. 2009. Contextualización del cibercrimen en Colombia. [En línea] 23 de 10 de 2009. https://www.google.com.co/search?ei=Gp_2WbmgLsHLmwH0yIHgCA&q=cibercrimen+en+colombia&oq=cibercrimen&gs_l=psy-ab.1.1.0i67k1j0j0i67k1l2j0i10k1j0l4j0i67k1.2311799.2314847.0.2317557.11.11.0.0.0.0.190.1460.0j9.9.0....0...1.1.64.psy-ab..2.9.1456...0i131k1.0.PIy.

NACIÓN, PABLO A. GÓMEZ MAROTO LA. 2013. Los peligros de la práctica del ciber-sexting. [En línea] 12 de Abril de 2013. http://www.nacion.com/archivo/peligros-practica-emciber-sextingem_0_1335066516.html

DR. SANTIAGO ACURIO DEL PINO, Profesor de Derecho Informático de la PUCE. Delitos Informáticos: Generalidades. [En línea] [Citado el: 04 de 11 de 2016.] www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.

ROMERO, JUAN DIEGO MEDINA. 2017. Generalidades. Factores que contribuyen al crecimiento del Cibercrimen. [En línea] repository.unimilitar.edu.co/bitstream/10654/15765/.../MedinaRomeroJuanDiego2016.p....

REYES, JOSÉ ALBERTO CRUZADO. Delitos Informáticos y Ciberterrorismo, Fundamentos de Investigación. *Libres, Puebla, Octubre 2011.* [En línea] https://beorlegui.files.wordpress.com/2011/10/delitos-informaticos-y-ciberterrorismo.pdf

NEC. Mexico Gestión de Información. Seguridad Cibernética ¿Qué constituye un ataque cibernético? [En línea] [Citado el: 12 de Mayo de 2017.] http://mex.nec.com/es_MX/solutions/security/safety/info_management/cyberattack.html.

SORIANO, LUZ ARIDIA ESTRELLA. 2014. La Piratería. ¿Qué es la piratería? tipos, causas, consecuencias y persistencia de la piratería. [En línea] 04 de Nov de 2014. https://www.google.com.co/search?q=consecuencias+de+la+pirateria+informatica&sa=X&ved=0ahUKEwjw1dCSmprXAhUHQyYKHRydDvcQ1QIIiAEoAA.

BRADANOVIC, TOMÁS. Conceptos Básicos de Seguridad Informática. [En línea] http://www.bradanovic.cl/pcasual/ayuda3.htm

TELLEZ VALDÉS, Julio. —Los Delitos informáticos. Situación en Méxicoǁ, Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996.

22. ANEXOS

ANEXO A. ENCUETAS No. 1

REALIZADA A ALGUNAS ENTIDADES O EMPRESAS DEL MUNICIPIO DE QUIBDÓ, DEPARTAMENTO DEL CHOCÓ SOBRE LA SEGURIDAD INFORMÁTICA

¿De cuántos ordenadores dispone su entidad?

5-10 +10

¿Los aparatos de cómputo de la empresa, ¿tienen antivirus?

Sí

No

No se

¿Si tienen antivirus en los equipos de la empresa, ¿está actualizado?

Sí

No

No se

La empresa le hace mantenimiento periódicamente a los computadores?

Sí

No

No se

¿Tienen por costumbre realizar descargar de programas o aplicaciones de internet?

Sí

No

No se

¿Sabe si la empresa tiene un servidor central de datos?

Sí

No

No se

¿Si la empresa tiene servidor se le realiza mantenimiento constante?

Sí

No

No se

¿La empresa realiza su labor desde algún computador externo, o por sitio web?

Sí

No

No se

¿Si la empresa se conecta utilizando red WIFI, y si lo hace utilizan los medios de seguridad adecuados?

Sí

No

No se

¿Los dispositivos de la empresa almacenan la información en el disco duro?

Sí

No

No se

¿La información que maneja la empresa se le realiza periódicamente copia de seguridad?

Sí

No

No se

¿Con qué periodicidad?

Diaria semanal otro

¿Usted o sus colaboradores a cargo poseen alguna copia de seguridad (USB / DVD / Otro) fuera de la empresa?

Sí

No

No se

¿Se realiza un mantenimiento de las copias de seguridad de su entidad o empresa?

Sí

No

No se

¿Los programas y aplicaciones usados, cumplen con las características de seguridad informática?

Sí

No

No se

¿Hay algún encargado de instalar/desinstalar los programas y aplicaciones informáticas?

Sí

No

No se

¿Conoce usted algo referente a la seguridad informática?

Sí No No se

¿Qué sabe al respecto?

¿La compañía ha dispuesto políticas de seguridad la gestión de su proceso?

Sí

No

No se

ANEXO B. ENCUESTA No. 2

CUESTIONARIO DE SEGURIDAD INFORMÁTICA EN EL MUNICIPIO DE QUIBDÓ – CHOCÓ

Esta encuesta es únicamente de manera investigativa. Su participación es importante es voluntaria y anónima, con el siguiente cuestionario se pretende analizar los conocimiento que posean sobre delitos informáticos o el cibercrimen a los habitantes del municipio de Quibdó. Por favor conteste las siguientes preguntas.

1. ¿Tiene usted equipos informáticos en su hogar o en su lugar de trabajo?
SI
NO

2. Si tienen antivirus en el equipo, ¿este se encuentra actualizado?
SI
NO

3. ¿Sabe usted sabe que es un delito informático o Cibercrimen?
NO
SI

4. ¿De las siguientes Normas sabe usted cuál es la ley que sanciona a las personas que realizan delitos informáticos? Seleccionar una opción
a. Ley 136 de 1994
b. Ley 1551 de 2012
c. Ley 617 de 2000

d. Ley 1273 de 2009

e. No sabe

5. ¿Qué tan habitualmente utiliza las redes sociales?

Siempre

Algunas veces

Frecuentemente

Casi nunca

Nunca

6. ¿Sabe que es el ciberespacio, o la web?

SI

NO

7. ¿Cuándo entra a una página web sabe usted si es segura?

SI

NO

8. ¿Siempre cierra su correo electrónico o redes sociales al instante de finalizar sesión en los equipos?

SI

NO

Algunas veces

9. ¿Al finalizar de navegar en internet acostumbra borrar el historial de navegación?

SI

NO

No sé qué es el historial de navegación

10. ¿Ha sido usted víctima de algún tipo de delito informático?

SI

NO

11. ¿De la siguiente lista de delitos informáticos, Cuál de estos usted conoce?

a. Robos de datos personales, robo de computadores, hackers, robo en los bancos

b. Los sabotajes a empresas, uso fraudulento de Internet, fugas de información, espionaje informático

c. Robo de identidad, duplicación de tarjetas, fugas de información

d. Todos los anteriores

e. Algunos

f. Ninguno

12. ¿Cuándo fue la última vez que cambio su contraseña del correo electrónico y de su equipo?

Entre 1 y 3 meses

Entre 2 y 6 meses

Entre 8 meses y un año

Más de un año

Nunca

No tengo correo electrónico

No tengo equipo

13. ¿Cree usted que hacer compras a través de Internet es seguro?

SI

NO

Depende la situación

No sabe

14. ¿utiliza usted los servicios de internet (virtuales) que ofrecen los bancos?

SI

NO

Algunas veces

15. ¿Entrega información bancaria a través del internet?

SI

NO

Algunas veces

16. ¿Proporciona información personal a terceros para que tramiten formatos de transacciones bancarias por usted por medio de internet?

SI

NO

Aganas veces

17. ¿Sabe usted dónde se pueden hacer las denuncias de un delito informático?

www.fiscalia.gov.co

www.policia.gov.co

www.delitosinformaticos.gov.co

Todas las anteriores

Ninguna de las anteriores

ANEXO C. RESUMEN ANALÍTICO ESPECIALIZADO (RAE)

Título de Documento	ANÁLISIS DEL COMPORTAMIENTO DEL CIBERCRIMEN EN EL MUNICIPIO DE QUIBDÓ, DEPARTAMENTO DEL CHOCÓ.
Autor	Mosquera Parra Ruth Yadira
Director	González García Salomón
Publicación	Quibdó. Universidad Nacional Abierta y a Distancia, 2017.
Palabras Claves	Cibercrimen, Comportamiento, Ataque, riesgo, Sitios Web, Seguridad Informática, Norma Legal, Tecnologías de la Información, delitos informáticos.
Descripción	Monografía para optar el título de especialista en seguridad informática. La actual investigación se realiza con el objetivo de Analizar el Comportamiento del Cibercrimen en el municipio de Quibdó, departamento del Chocó.
Resumen	El objetivo de esta investigación consiste es como analizar y se comporta el cibercrimen en el municipio de Quibdó, partiendo de evidencias que permitan establecer las conductas de las buenas prácticas que se requieren para resguardar la información online, tanto en lo personal como en la vida profesional. Es importante que esta monografía, llegue y se difunda para que cada uno de los habitantes de este municipio conozca y se eduquen en todo lo relacionado con la seguridad informática, y en la norma legal colombiana en todo su contexto en materia de derecho.
Fuentes	A, CLARA LUCÍA GUZMÁN. 2009. Contextualización del cibercrimen en Colombia. [En línea] 23 de 10 de 2009. https://www.google.com.co/search?ei=Gp_2WbmgLsHLmwH0yIHgCA&q=cibercrimen+en+colombia&oq=cibercrimen&gs_l=psy-ab.1.1.0i67k1j0j0i67k1l2j0i10k1j0l4j0i67k1.2311799.2314847.0.2317557.11.11.0.0.0.0.190.1460

	.0j9.9.0....0...1.1.64.psy-ab..2.9.1456...0i131k1.0.PIy. AL., JOSÉ. 2015. cibercrimen. Qué es y cómo combatir el cibercrimen. [En línea] 16 de Abril de 2015. http://portaley.com/2015/04/que-es-y-como-combatir-el-cibercrimen/. LEY 1273 DE 2009 (Enero. 2009. Propiedad de la Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá D.C. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. [En línea] 05 de Enero de 2009. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. DECRETO 2573 DE. 2014. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. [En línea] 12 de Dic. De 2014. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60596.
Objetivos	Objetivo General Conocer el comportamiento del Cibercrimen en la ciudad de Quibdó, por medio Investigación de campo y análisis de los casos presentados en la localidad. Objetivos Específicos Identificar los diferentes casos de cibercrimen ocurridos en la ciudad de Quibdó y sus características. Establecer cuál es la tendencia de la comisión de cibercrimenes en esta localidad. Realizar encuestas para determinar el grado de conocimiento de la población frente a los delitos

	informáticos. Proponer una serie de recomendaciones para contrarrestar la ocurrencia de la actividad maliciosa.
Metodología	El proyecto de investigación se desarrollara tomando como punto de partida los elementos o fases de la investigación cualitativa. Determinando un alcance de procedimientos exploratorios, y teniendo en cuenta los diferentes métodos y técnicas propias de cada una de las etapas que se abordaran en el estudio, incluyendo los procedimientos, recolección, procesamiento y análisis de la información, además del seguimiento al cronograma de actividades. El desarrollo de este proyecto se llevó a cabo en 5 Fases según los objetivos planteados: Fase I: Identificación de las diferentes fuentes de información que permitirán ampliar la perspectiva del tema objeto de investigación. Fase II: Desarrollo conceptual del tema. Fase III: Análisis y clasificación de la información según su género, origen y categoría. Fase IV: Elaboración y publicación de la encuesta sobre el cibercrimen y posterior análisis de resultados. Fase V: Conclusiones y elaboración de un documento final.
Recomendaciones	Se invita a la población Quibdoseña que realice una exploración, investigación y análisis a las leyes, normas y decretos frente a la resguardo de la información y datos, con el objetivo de que puedan conocer, comprender y aprender a proteger la misma y descubrir métodos o estrategias para evitar ser víctimas de delitos informáticos.
	El presente proyecto investigativo, permitió realizar un análisis para establecer una idea del comportamiento del Cibercrimen en el municipio de Quibdó, departamento del Chocó, y con sus respectivas características. Análisis e identificación de los diferentes casos de cibercrimen que se cometen con más frecuencia en la ciudad de Quibdó, igualmente

Conclusiones	se estableció cuál es la tendencia de la comisión de cibercrimen en el departamento del Chocó y sus municipios, tomando como referencia las denuncias realizadas por las víctimas. En la investigación se realizó encuestas a la población de Quibdó, sin importar su género y cultura; las cuales arrojaron como conclusión un alto índice de ignorancia en lo que tiene que ver con el tema de delitos informático tipificados dentro de la Ley 1273 de 2009. También se pudo mostrar que el cibercrimen posee características cambiantes, por ello, se hace necesario la creación de estrategias o recomendaciones que permitan y muestren la posibilidad de crear ambientes más seguros y así poder reducir los riesgos que se presentan en el departamento del Chocó.

Elaborado por:	Mosquera Parra Ruth Yadira
Revisado por:	González García Salomón

Fecha de elaboración del Resumen:	17	12	2017