UNIVERSIDAD RAFAEL LANDÍVAR
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE

"EVOLUCIÓN DE LA INVESTIGACIÓN CRIMINAL EN EL ROBO DE INFORMACIÓN PERSONAL (PHISHING), ACOSO PEDERASTA (GROOMING) Y SUPLANTACIÓN DE IDENTIDAD (SPOOFING)"

TESIS DE GRADO

KENET VENANCIO ARMANDO CHAC COTUC
CARNET 16789-15

QUETZALTENANGO, MAYO DE 2021
CAMPUS DE QUETZALTENANGO

UNIVERSIDAD RAFAEL LANDÍVAR

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE

"EVOLUCIÓN DE LA INVESTIGACIÓN CRIMINAL EN EL ROBO DE INFORMACIÓN PERSONAL (PHISHING), ACOSO PEDERASTA (GROOMING) Y SUPLANTACIÓN DE IDENTIDAD (SPOOFING)"

TESIS DE GRADO

TRABAJO PRESENTADO AL CONSEJO DE LA FACULTAD DE

CIENCIAS JURÍDICAS Y SOCIALES

POR

KENET VENANCIO ARMANDO CHAC COTUC

PREVIO A CONFERÍRSELE

EL TÍTULO Y GRADO ACADÉMICO DE LICENCIADO EN INVESTIGACIÓN CRIMINAL Y FORENSE

QUETZALTENANGO, MAYO DE 2021

CAMPUS DE QUETZALTENANGO

AUTORIDADES DE LA UNIVERSIDAD RAFAEL LANDÍVAR

RECTOR:	P. MYNOR RODOLFO PINTO SOLÍS, S. J.
VICERRECTORA ACADÉMICA:	DRA. MARTHA ROMELIA PÉREZ CONTRERAS DE CHEN
VICERRECTOR DE INVESTIGACIÓN Y PROYECCIÓN:	LIC. JOSÉ ALEJANDRO ARÉVALO ALBUREZ
VICERRECTOR DE INTEGRACIÓN UNIVERSITARIA:	MGTR. MYNOR RODOLFO PINTO SOLÍS
VICERRECTOR ADMINISTRATIVO:	MGTR. JOSÉ FEDERICO LINARES MARTÍNEZ
SECRETARIO GENERAL:	DR. LARRY AMILCAR ANDRADE - ABULARACH

AUTORIDADES DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

DECANO:	DR. HUGO ROLANDO ESCOBAR MENALDO
VICEDECANA:	MGTR. HELENA CAROLINA MACHADO CARBALLO
SECRETARIO:	LIC. CHRISTIAN ROBERTO VILLATORO MARTÍNEZ

NOMBRE DEL ASESOR DE TRABAJO DE GRADUACIÓN

LIC. MOISÉS FRANCISCO LÓPEZ GARCÍA

TERNA QUE PRACTICÓ LA EVALUACIÓN

LIC. LUIS EDUARDO ESCOBAR DE LEÓN

AUTORIDADES DEL CAMPUS DE QUETZALTENANGO

DIRECTOR DE CAMPUS:	P. MYNOR RODOLFO PINTO SOLIS, S.J.
SUBDIRECTORA ACADÉMICA:	MGTR. NIVIA DEL ROSARIO CALDERÓN
SUBDIRECTORA DE INTEGRACIÓN UNIVERSITARIA:	MGTR. MAGALY MARIA SAENZ GUTIERREZ
SUBDIRECTOR ADMINISTRATIVO:	MGTR. ALBERTO AXT RODRÍGUEZ
SUBDIRECTOR DE GESTIÓN GENERAL:	MGTR. CÉSAR RICARDO BARRERA LÓPEZ

Quetzaltenango 6 de noviembre de 2020

Lic. Nelly Betzabé de León Reyes.

Coordinadora Académica

Facultad de ciencias jurídicas y sociales

Universidad Rafael Landívar

Presente.

Respetuosamente me dirijo a usted con el objeto de manifestar que fui designado asesor del trabajo de tesis "EVOLUCIÓN DE LA INVESTIGACIÓN CRIMINAL EN EL ROBO DE INFORMACIÓN PERSONAL (PHISHING), ACOSO PEDERASTA (GROOMING) Y SUPLANTACIÓN DE IDENTIDAD (SPOOFING)", investigación realizada por el estudiante de la Licenciatura en Investigación Criminal y Forense, **Kenet Venancio Armando Chac Cotuc,** quien se identifica con el número de carné: 1678915.

Se realizó el acompañamiento respectivo durante la elaboración de la tesis, por lo que una vez finalizada, considero que la tesis cumple con los objetivos propuestos inicialmente y su elaboración ha estado apegada a la objetividad, responsabilidad, y procedimientos necesarios de rigor en la investigación científica. También se ha garantizado su originalidad a través del estricto cumplimiento de todos los requisitos solicitados en el instructivo para la elaboración de Tesis de Graduación de la Facultad de Ciencias Jurídicas y Sociales de Universidad Rafael Landívar.

En virtud de lo anterior, emito **DICTAMEN FAVORABLE,** a efecto de continuar con los trámites correspondientes dentro de la facultad.

Sin otro particular.

Deferentemente.

Licenciado
Moisés Francisco López García
Investigador Criminal y Forense

Licenciado Moisés Francisco López García
Investigador Criminal y Forense
Colegiado: 3,463
Perito Forense Digita (Redlif, Guatemala)
Experto en Detección de Firmas Falsas y
Huellas Dactilares Post-mortem (ICCD-España)

Universidad Rafael Landívar
Tradición Jesuita en Guatemala

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
No. 072735-2021

Orden de Impresión

De acuerdo a la aprobación de la Evaluación del Trabajo de Graduación en la variante Tesis de Grado del estudiante KENET VENANCIO ARMANDO CHAC COTUC, Carnet 16789-15 en la carrera LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE, del Campus de Quetzaltenango, que consta en el Acta No. 07157-2021 de fecha 16 de marzo de 2021, se autoriza la impresión digital del trabajo titulado:

"EVOLUCIÓN DE LA INVESTIGACIÓN CRIMINAL EN EL ROBO DE INFORMACIÓN PERSONAL (PHISHING), ACOSO PEDERASTA (GROOMING) Y SUPLANTACIÓN DE IDENTIDAD (SPOOFING)"

Previo a conferírsele el título y grado académico de LICENCIADO EN INVESTIGACIÓN CRIMINAL Y FORENSE.

Dado en la ciudad de Guatemala de la Asunción, a los 4 días del mes de mayo del año 2021.

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
SECRETARIO DE FACULTAD
U R L

LIC. CHRISTIAN ROBERTO VILLATORO MARTÍNEZ, SECRETARIO
CIENCIAS JURÍDICAS Y SOCIALES
Universidad Rafael Landívar

ÍNDICE

Pág.

LISTADO DE ABREVIATURAS

ADN	Ácido desoxirribonucleico
DIGECAM	Dirección General de Control de Armas y Municiones
DNS	Sistema de Nombres de Dominio
EE. UU.	Estados Unidos
GUI	Interfaz Gráfica del Usuario
Ibid.	En el mismo lugar
IBM	Corporación Internacional de Negocios.
IEC	Comisión Electrónica Internacional
IP	Protocolo de Internet
ISO	Organización Internacional de Normalización
Loc. Cit.	En el lugar citado
MINGOB	Ministerio de Gobernación
MP	Ministerio Público
Op. Cit.	En la obra citada
Pág.	Página
PGN	Procuraduría General de la Nación
PNC	Policía Nacional Civil
RFC	Petición de Comentarios
TICs	Tecnologías de la información y comunicación

Resumen

La presente tesis de grado denominada “Evolución de la investigación criminal en el robo de información personal (phishing), acoso pederasta (grooming) y suplantación de identidad (spoofing)” es un trabajo de investigación monográfica, realizada en el ámbito espacial de los departamentos de Quetzaltenango y Guatemala, cuyo objeto es exponer información certera que sea útil a las entidades estatales encargadas de la investigación criminal respecto al desarrollo de los ciberdelitos y de cómo estos trascienden y vulneran a toda la población en el ámbito cibernético, así mismo se detalla cada uno de los elementos y modus operandi (modo de operar) que poseen los ciberdelincuentes y de las herramientas legales que actualmente el Estado tiene para el combate de los actos ilícitos en materia de la informática, de la misma manera se aborda lo concerniente al rol del perito informático en la investigación, procesamiento, fijación, documentación, recolección, embalaje y análisis de la evidencia digital, se detalla la naturaleza especial de la evidencia informática como sus clasificaciones, de esa cuenta se expone en el siguiente documento las normas, estándares y protocolos que existen a nivel internacional para el tratamiento de los indicios informáticos esenciales para una investigación criminal; con respecto al Estado de Guatemala se analiza brevemente la iniciativa de ley existente para el combate de la cibercriminalidad.

Introducción

La investigación criminal es definida como un conjunto de saberes o conocimientos integrales que coadyuvan al esclarecimiento de una verdad, relacionada a un hecho delictivo, este concepto se resume en la ciencia de la criminalística, ya que, esta disciplina provee de estrategias y conocimientos que contextualizan el papel que cada individuo ha tenido en el proceso de la comisión de un ilícito, la informática es una ciencia que se encarga de la adquisición, preservación, obtención y presentación de datos procesados electrónicamente, en los diferentes dispositivos tecnológicos, aunado a la investigación criminal esta ciencia aporta técnicas científicas y analíticas especializadas en la infraestructura de elementos tecnológicos que permite identificar, preservar y analizar datos que posteriormente sean válidos en un proceso legal.

Este trabajo de investigación tiene por objetivo general exponer información respecto al desarrollo de los cibercriminales, los antecedentes y avances que se han obtenido en la investigación del cibercrimen, así mismo se han trazado objetivos específicos en la investigación siendo el primero de ellos el definir el delito informático, sus antecedentes, características y clasificación, el segundo objetivo es el referir estándares internacionales para la extracción de indicios digitales, el tercer objetivo es mencionar el perfil del perito informático y su rol dentro de la investigación criminal de los delitos informáticos y el último objetivo es presentar los avances que se han obtenido en Guatemala con respecto a la investigación criminal de los delitos informáticos en comparación con otros países, dichos objetivos pretenden responder a la interrogante ¿Cuál ha sido la evolución de la investigación criminal en los actos de phishing, grooming y spoofing en Guatemala?

El contenido del presente trabajo es materia de informática forense que se ha desarrollado considerando a los sujetos de investigación a los peritos informáticos, investigadores de la fiscalía de delitos informáticos, investigadores de la unidad de delitos informáticos y profesionales en el área de informática, así mismo las unidades de análisis han sido el Ministerio Público, Instituto Nacional de Ciencias Forenses y Policía Nacional Civil.

Los limites que se presentaron en la investigación fue el escaso material existente sobre ciberdelitos a nivel nacional, dicha limitante fue superado buscando contenido bibliográfico y electrónico de otros países, otro de los limites fue las pocas instituciones nacionales que tratan y abordan el tema de ciberdelincuencia debido a que pocos o casi nulos son los casos que se conocen de hechos ilícitos de naturaleza cibernética, esta limitante fue superada con el apoyo de las diferentes unidades de análisis de los entes encargados de la persecución penal. El aporte principal de la investigación consiste en exponer un delito de interés social, dar a conocer así mismo el alcance y daño que los ciberdelitos provocan si no son tratados correctamente, por otro lado también hacer conciencia a la población de la urgencia de aprobación y aplicación de una norma jurídica especifica en contra de los ciberdelitos, ya que, en esta materia Guatemala posee atrasos en comparación de otros países, el instrumento utilizado para la investigación fue entrevistas semiestructuradas.

Para la realización y redacción del presente trabajo de investigación fue necesario la lectura de documentos doctrinarios y legales que tuvieran relación con el tema de informática forense, posteriormente se realizó un análisis de lo estudiado para la realización más adecuada del trabajo, por lo tanto el presente documento se desarrolla en cinco capítulos, siendo el primero de ellos sobre la investigación criminal, en él se aborda la historia de la criminalística, la investigación criminal en Guatemala, la ciencias que apoyan la investigación criminal, lo relacionado a la escena del crimen, la criminalística y sus principios, la fijación de la escena del crimen, el embalaje y la cadena de custodia, el segundo capítulo trata sobre la informática detallando antecedentes de la misma y su definición, la informática forense también es un punto tratado y como cada uno de los elementos que lo componen, como las redes informáticas y redes sociales, el hacking, cracking y la seguridad informática como elementos esenciales de la disciplina informática, el tercer capítulo trata lo relacionado a ciberdelitos, definición, características y clasificación de los ciberdelitos, el delito como elemento principal para el tema de investigación criminal, el recorrido criminal o íter críminis, así como el cibercrimen y los ciberdelitos tipificados en la legislación vigente de Guatemala, se aborda así mismo la iniciativa de ley 5601 que dispone aprobar una ley de prevención y protección contra la

ciberdelincuencia, de la misma cuenta detalla los instrumentos y herramientas necesarias para la persecución de cibercriminales, posteriormente se desarrolla el tema de phishing, grooming y spoofing y los métodos de acción de los cibercriminales al atacar a sus víctimas, el cuarto capítulo considera lo relacionado al manejo de la escena de crimen en los delitos informáticos, como punto esencial de la investigación criminal el procesamiento de dicho lugar de los hechos debe tener una tratamiento especial, iniciando por la naturaleza de los indicios que allí pueden ser documentados y embalados para su posterior análisis y obtención de resultados necesarios para la resolución y esclarecimiento del ilícito suscitado, está también lo referente a la evidencia informática, características de la misma y sus métodos de extracción, se hace mención también de los protocolos internacionales sobre la evidencia informática y los estándares que deben ser rigurosamente cumplidos para la correcta aplicación de los protocolos, dichos estándares son también de carácter internacional debido a que en Guatemala aún no se ha creado un procedimiento meramente propio, el embalaje de la evidencia digital es otro punto que se desarrolla, se expone de la misma manera lo concerniente al perito informático y su desenvolvimiento en la investigación criminal, el análisis forense de la evidencia digital complementado por el informe pericial, en el quinto y último capítulo contiene la presentación de resultados y su respectiva discusión.

CAPÍTULO I
1. INVESTIGACIÓN CRIMINAL

1.1. Historia de la Criminalística

Como todas y cada una de las disciplinas científicas existentes, tuvieron un origen, muchas veces provocado por una necesidad, tal es el origen de la criminalística, desde hace mucho tiempo por no mencionar que desde los inicios la criminalidad ha acompañado a las sociedades en sus diferentes etapas de desarrollo, por tal razón los hechos ilícitos han ido suscitándose de diferentes formas pero siempre, trayendo consigo consecuencias inmediatas o daños, por ese motivo las autoridades encargadas de impartir justicia han ido adoptando medidas para la prevención y tratamiento de este tipo de conductas y así sancionar a los responsables, de allí que da inicio el trabajo de la criminalística como una ciencia o disciplina que en principio es considerado como una ciencia auxiliar del derecho y que a través del tiempo, esta misma ha ido desarrollándose cada vez más, llegando a tal punto de considerarse una ciencia completa.

Ahora bien, de los antecedentes conocidos sobre la Criminalística está la obra realizada por el Doctor Hans Gross denominada como el Manual del Juez, en dicha obra se contenía una serie de métodos de investigación que pretendía proveer a los jueces de herramientas útiles al momento de esclarecer algún hecho delictivo complicado, donde en ocasiones es difícil establecer una explicación clara de lo ocurrido con los métodos comunes de investigación y requería de un conocimiento técnico específico, fue Hans Gross quien denominó por primera vez a ese conjunto de técnicas de investigación como Criminalística. En la obra ya citada se encuentran las siguientes técnicas de investigación:

a) *“Antropometría.*
b) *Argot criminal.*
c) *Contabilidad.*
d) *Criptografía.*
e) Dibujo forense.
f) Documentoscopía.

g) *Explosivos.*
h) *Fotografía.*
i) *Grafología.*
j) *Hechos de tránsito ferroviario.*
k) *Hematología.*
l) *Incendios.*
m) *Medicina legal.*
n) *Química legal.*
o) *Interrogatorio".*[1]

Otro personaje predecesor de la Criminalística es Marcelo Malpighi, *"observaba y estudiaba los relieves dactilares de las yemas de los dedos y palmas de las manos realizando valiosas aportaciones al estudio de las impresiones dactilares"*[2], de este precursor de la criminalística se origina los primeros conocimientos sobre la disciplina de la dactiloscopía, empleado hoy día para la identificación de las personas o sospechosos de la realización de un hecho delictivo, basándose en los patrones dactiloscópicos que cada una de las personas posee y que son particularmente individuales e irrepetibles.

"Doctor Boucher, en 1753 realizó estudios sobre balística, disciplina que a la postre se llamaría Balística Forense"[3]. Posteriormente a las aportaciones del doctor Boucher hubieron también otros personajes como Henry Goddard, quien descubrió al autor de un asesinato, mediante particularidades que encontró en el molde de municiones para un arma de avancarga y que esta marca del molde quedaba resaltada en la munición después de ser moldeada, por la cual el hizo una prueba de moldear una munición a modo de emplearlo como indicio indubitado y lo comparó con la munición hallada en el cuerpo de la víctima y efectivamente ambas municiones tenían las mismas marcas lo que hizo que el dueño del arma y molde confesara el hecho.

[1] Montiel Sosa, Juventino. *"Criminalística 1".* México, editorial Limusa, 2da. Edición. 2007, Pág.25
[2] Criminalística Online, RSA, Precursores de la Criminalística, Argentina, 2019, http://criminalistica.online/precursores-de-la-criminalistica/, fecha de consulta: 3 de julio 2019.
[3] Montiel Sosa, Juventino, *Op. Cit.*, Pág. 20.

La fotografía forense como método de documentación en la criminalística tuvo su origen con *"Allan Pinkerton, detective y espía escocés fundador de la primera agencia de detectives del mundo, que en 1886 utilizó a la fotografía como recurso para el registro e identificación de los delincuentes cuando ingresaban al sistema judicial; usó también la fotografía para dejar constancia de las situaciones exactas en las que fue hallada una escena del crimen, registrando así toda la evidencia"*[4]. A partir de ese antecedente de la fotografía se comenzó a usar como método también para la fijación de la escena de crimen, proveyendo de una mayor ayuda a los entes juzgadores al momento de encontrarse una duda sobre la escena de crimen y de los objetos que allí pudieron ser levantados como indicios al momento del procesamiento, a raíz de la fotografía se dio origen al video forense que hoy por hoy es otro medio audio visual que permite evidenciar los procesos realizados en las escenas de crimen, aparte de ser un medio o recurso empleado como método de investigación al momento de darse un hecho delictivo en alguna calle, lugar, edificio, etc. Donde se cuente con cámaras de vigilancia.

Alfonso Bertillón, "*creó en París el servicio de identificación judicial en 1822, con el cual ensayaba su método antropométrico, este método fue aplicado para personas mayores de 21 años*"[5] con él se registró características óseas, posteriormente este método fue reemplazado por la dactiloscopía. De este mismo personaje se atribuye la creación del retrato hablado, mediante la realización de una tesis sobre características de los individuos y su descripción, hoy día esta técnica empleada para la identificación de delincuentes prófugos y en muchas ocasiones como medio para que la víctima describa a su agresor y de esa manera poner en alerta a la población para que colaboren a su identificación, búsqueda y captura. El profesor italiano Orfila "*creó la Toxicología en 1840, ciencia que auxiliaba a los jueces a esclarecer cierto tipo de delitos, en los cuales predominaba el uso de venenos"*[6]. Más adelante el desarrollo de esta ciencia continúo permitiendo obtener un conocimiento mucho más amplio en el área de los elementos

[4]Modo Museo, Museo del objeto del objeto, Fotografía Forense, México, 2015, disponibilidad y acceso: https://elmodo.mx/el-modo-del-modo/fotografia-forense/, fecha de consulta: 3 de julio2019.
[5] Montiel Sosa, Juventino, *Op. Cit.*, Pág. 22.
[6] *Loc. Cit.*

químicos y los mecanismos de acción que estos mismos empleaban para ser mortales en la mayoría de los casos.

Juan Vucetich *"Inauguró la Oficina de Identificación y utilizó la Antropometría y las huellas digitales de ambas manos y creó así la ficha decadactilar"*[7], dicha ficha supuso un avance más en la identificación de las personas, al ser implementado este sistema en la policía de río de plata, Argentina permitió la identificación de varios delincuentes reincidentes que con los sistemas anteriores no habían sido identificados. De esta manera se observa el origen de algunas de las disciplinas que auxilian a la Criminalística, dando así con las ciencias precursoras el paso al desarrollo técnico científico de las ciencias que hoy día componen la Criminalística, es de notar que el origen de esta disciplina posee bases científicas que permiten fundamentar concretamente los resultados que las investigación proveen, también es importante mencionar que esta área posee un porcentaje considerable de conocimiento empírico ya que los primeros investigadores se guiaron de los conocimientos que habían adquirido a lo largo de su carrera como investigadores o como jueces que es el caso del doctor Hans Gross, quien fue el primer personaje de la historia en nombrar Criminalística al conjunto de materias empleadas para la investigación, es entonces desde el lanzamiento de su manual que permitió que muchos más profesionales de la investigación, jueces y científicos tuvieran un interés notable sobre la disciplina que empezaba a nacer, al mismo tiempo que la obra del doctor era traducida a varios idiomas, varios especialistas más daban observaciones y contribuciones en mejorar esta ciencia que estaba empezando a cambiar y revolucionar el enfoque investigativo jurídico establecido en aquellos tiempos.

1.2 La investigación criminal en Guatemala

El trabajo de investigación criminal conlleva una serie de responsabilidades y división de funciones, persiguiendo el mismo fin que es esclarecer un hecho criminal y determinar responsabilidades de los implicados en su comisión, en Guatemala el tema investigativo es tratado por tres órganos básicamente cada uno con una función determinada, pero al final todos ellos pretenden otorgar un resultado en común el cual es descubrir la verdad,

[7] *Ibid.,* Pág. 23.

ahora bien, los entes intervinientes en el tema de investigación criminal son la Policía Nacional Civil, el Ministerio Público y el Instituto Nacional de ciencias Forenses. El primero de los entes mencionados cumple la función de realizar la investigación de campo, la segunda es el encargado de guiar o dirigir la investigación procurando la objetividad así también es el encargado de ejercer posteriormente la persecución penal del delito y el tercero es el encargado de realizar la investigación forense.

1.2.1 Policía Nacional Civil

La actual Policía Nacional Civil (PNC), es lo que anteriormente se conocía como la Policía Nacional y la Guardia de Hacienda, desde 1,997 durante el mandato del presidente Álvaro Arzú Irigoyen, todo esto en virtud de la firma de los acuerdos de paz que sucedió en 1,996, las dos instituciones antes mencionadas fueron unidas convirtiéndose en lo que hoy es la PNC. Como en cualquier parte del mundo la Policía Nacional Civil de Guatemala en principio posee la función de mantener el orden público y velar por la seguridad de la población, pero a través del tiempo las funciones de la policía se han ido extendiendo al punto de implicarse en temas de prevención evitando a través de acciones y operaciones la comisión de delitos, para eso se recurre al despliegue de elementos policiales en puntos estratégicamente señalados, en horas específicas donde anteriormente se haya suscitado hechos delincuenciales, la función de reacción se lleva a cabo al momento que se tiene conocimiento de la comisión o ejecución de un delito, por lo cual en algunos casos se recurre al uso de la fuerza para evitar que la conducta criminal provoque consecuencias ulteriores.

La función de aprehensión de las personas con orden judicial debidamente emitida, de la misma manera poner a disposición de las autoridades correspondientes a las personas que hayan sido sorprendidas en flagrante delito; el auxilio y protección de las personas y bienes que se encuentren en situación de peligro por cualquier motivo es atribución de la institución policial. El combate de la criminalidad es una función articulada entre varias instituciones del Estado como el Ministerio Público y la Policía Nacional Civil, captando, recibiendo y analizando datos de interés para la seguridad, de la misma manera planifica y estudia técnicas y determina estrategias para disminuir la incidencia criminal; en general

la Policía Nacional Civil es un ente que vigila e inspecciona que cada una de las leyes y disposiciones sean debidamente ejecutadas en razón de las ordenes emitidas por los órganos correspondientes. Ahora bien, la función de investigación criminal también es una atribución de la Policía Nacional Civil, como lo establece el Congreso de la República de Guatemala en su decreto 51-92, Artículo 112 *"La policía, por iniciativa propia, en virtud de una denuncia o por orden del Ministerio Público, deberá: Investigar los hechos punibles perseguibles de oficio",* así también coadyuva en reunir los medios necesarios para que el Ministerio Público pueda realizar o formar acusación posteriormente y llevar el caso a la jurisdicción de un órgano determinado el cual se encargará de observar si la conducta realizada por los sujetos detenidos o aprehendidos ameritan ser sujetos de un debido proceso, y de ser demostrada su responsabilidad a través de los diferentes medios de investigación y prueba serán sancionados con una pena.

1.2.2 Ministerio Público

El Ministerio Público en sus inicios se encontraba integrado a la Procuraduría General de la Nación (PGN) debido al decreto 512 emitido por el Congreso de la República, en el año 1993 Guatemala modernizó el sistema penal con el fin de combatir de manera más efectiva la criminalidad en el país, por lo cual en las reformas de dicho año se estableció la división de las tareas de persecución penal, investigación y juzgamiento logrando con esos cambios la eliminación de arbitrariedades, abuso de poder que estaba sucedió con el anterior sistema penal; de la cuenta de cada una de las reformas establecidas en el año mencionado el Ministerio Público se constituyó en una institución autónoma y se separa de la PGN y de la misma forma se definió en dos áreas principales de función que es la dirección de la investigación y la calidad de acusador en la persecución de delitos en ejercicio de la acción penal, de dichos cambios es como se conoce actualmente al Ministerio Público, como una institución encargada de la persecución de cada uno de los delitos.

Congreso de la República de Guatemala, Constitución Política de la República de Guatemala, artículo 251 *"El Ministerio público es una institución auxiliar de la administración pública y de los tribunales con funciones autónomas, cuyos fines principales son velar por el estricto cumplimiento de las leyes del país. Su organización y*

funcionamiento se regirá por su ley orgánica. El jefe del Ministerio Público será el fiscal general de la República y le corresponde el ejercicio de la acción penal pública."

Además, el Congreso de la República de Guatemala, en el decreto 51-92, Artículo 107 *"El ejercicio de la acción penal corresponde al Ministerio Público como órgano auxiliar de la administración de justicia conforme las disposiciones de este código. Tendrá a su cargo el procedimiento preparatorio y de la dirección de la Policía Nacional Civil en su función investigativa dentro del proceso penal"*, Congreso de la República de Guatemala, decreto 40-94, Artículo 1 *"el Ministerio Público es una institución con funciones autónomas promueve la persecución penal y dirige la investigación de los delitos de acción pública; además velar por estricto cumplimiento de las leyes del país",* de estas estipulaciones legales se desprende la función esencial del Ministerio Público (MP), que es la dirección de la investigación de los delitos.

Es de mencionar que hoy día la función de este organismo en el área de investigación no solo se limita a la dirección de la investigación sino también a través de sus diferentes secciones coadyuva en la investigación de los delitos, teniendo así un apoyo más en la determinación de la existencia positiva o negativa del delito y la definición de los responsables. Como la normativa indica la Policía Nacional Civil es el encargado de proveer al Ministerio Público de los recursos o bases necesarias para la realización de una acusación formal y fundamentada que proceda a la resolución de someter a un proceso penal a los posibles responsables y con eso cumplir con la otra función del MP que es la persecución penal de acuerdo con lo establecido por el Congreso de la República de Guatemala, decreto 51-94, con 24, atiende a la clasificación siguiente:

a) *"Acción pública.*
b) *Acción pública dependiente de instancia particular o que requiera autorización estatal.*
c) *Acción privada".*

De esta cuenta el Ministerio Público hace cumplimento a sus funciones como un órgano encargado de ejercer la persecución penal de los delitos.

1.2.3 Instituto Nacional de Ciencias Forenses

"El Instituto Nacional de Ciencias Forenses de Guatemala -INACIF- es creado con el Decreto 32-2006 del Congreso de la República de Guatemala del ocho de septiembre de dos mil seis, como resultado de la necesidad de contar con medios de prueba válidos y fehacientes en los procesos judiciales"[8]. Esta institución como tal, coadyuva al sistema de justicia de Guatemala a realizar una investigación que cumpla con la objetividad, transparencia y profesionalismo, procurando en todo momento permanecer en el marco del derecho.

La característica principal del INACIF en el área de investigación criminal es la de realizar la investigación científica, es decir la investigación forense a través de la utilización de técnicas científicas de cada una de las ciencias aplicables al caso que se presente, la institución cuenta con varias sección y laboratorios donde los indicios recolectados en la escena de crimen son procesados y posteriormente a través de dictámenes periciales se hace efectivo el resultado del análisis de los mismos con datos específicos de los hallazgos relevantes realizados en cada uno de los objetos analizados, dicho dictamen provee a la entidad del Ministerio Público un medio concreto más, para que realice posteriormente una acusación o persecución penal efectiva del delito y los responsables, es así entonces como la institución cumple con su función en colaborar con los órganos de justicia e investigación del país.

El INACIF desde su origen ha ido cada vez más expandiendo sus secciones de análisis técnico científico llegando a tener al momento lo siguientes: "*Patología forense, odontología forense, psiquiatría y psicología forense, antropología forense, medicina legal clínica, histopatología forense, documentoscopía forense, balística forense, toxicología forense, lofoscopía forense, serología forense, identificación de vehículos, fisicoquímica forense, sustancias controladas, genética forense, trayectoria de disparo forense, acústica forense, informática forense"*[9]. Es importante indicar que INACIF por

[8], Instituto Nacional de Ciencias Forenses, Historia, Guatemala, s.f., https://www.inacif.gob.gt/index.php/inacif/historia#, fecha de consulta: 4 de julio 2019.

[9] INACIF, Instituto Nacional de Ciencias Forenses, servicios, Guatemala, S/a, https://www.inacif.gob.gt/index.php/therapies, fecha de consulta: 5 de julio 2019.

determinación jurídica emitida por el Congreso de la República de Guatemala, decreto 32-2006 artículo 5 *"El INACIF no podrá actuar de oficio y realizará los peritajes técnico-científicos conforme la presente Ley."*, con esta estipulación normativa se determina que la institución realizará pericias únicamente en los casos que solicite el MP a través de sus fiscales o por requerimiento de un juez.

1.3 Ciencias que apoyan la investigación criminal

La investigación criminal o Criminalística es una disciplina integral por lo cual actúa y cumple sus fines con el apoyo de distintas ciencias con el cual pretende comprobar o analizar distintos hechos u objetos que estén en cuestión. Es difícil determinar un grupo específico de ciencias que colaboran con la investigación criminal ya que las ciencias existentes pueden llegar en algún determinado momento a contribuir con la investigación criminal aportando conocimientos específicos del área que se requiera; a continuación, se verán algunas disciplinas que colaboran en la investigación criminal.

1.3.1 Dactiloscopía

En las escenas de crimen se suelen encontrar huellas dactilares que los delincuentes o personas que han intervenido en el hecho criminal por lo regular manipulan objetos en donde por ende dejan impresiones dactilares que posteriormente, al investigador criminal le pueden servir como medio de identificación e individualización de cada uno de los sujetos implicados en el hecho ilícito, este tipo de indicios pueden ser revelados en la escena de crimen pero hay casos donde en los objetos que donde se presuma existan huellas dactilares deben ser trasladados a un laboratorio para su revelado especial y mediante elementos químicos más complejos que requieran de un conocimientos especial para su aplicación.

1.3.2 Fotografía forense

Es empleada como medio para documentar y fijar la escena de crimen a la vez que para detallar cada uno de los hallazgos realizados en el lugar mediante la tomar de imágenes panorámicas, a mediana distancia y a detalle en caso de cada uno de los objetos que puedan ser difícilmente distinguibles a una larga distancia o que sean de un tamaño poco

visible así mismo para observar característica que puedan ser relevantes para el caso que se cuestiona, otra utilidad que tiene la fotografía en la escena de crimen es también el de documentar mediante video todos los procedimientos que se realizan en el lugar de los hechos.

1.3.3 Balística forense

Para escena de crimen y casos donde haya existido el uso de armas de fuego o se encuentre algún arma de fuego involucrado es necesario proceder a un análisis balístico, para determinar funcionalidad, probabilidad de haber sido percutada el arma, en otros casos para hacer cotejo de proyectiles y observar si coindicen con el anima del cañón y determinar si el proyectil fue disparado del arma analizada o embalada, así también para el análisis de casquillos más específicamente en el área del fulminante y encontrar en la huella balística del arma en cuestión si coincide con la huella que se tiene en el casquillo recolectado en la escena de crimen (indicio dubitado).

1.3.4 Medicina forense

"También llamada medicina legal. Es el aprovechamiento de los conocimientos médicos, clínicos y biológicos en asuntos de interés legal"[10] Esta disciplina es recurrida frecuentemente en hechos violentos o hechos contra la vida a través del análisis médico forense se establecen resultados como causa de muerte, tiempo de muerte, etc. Ahora bien, en estudios clínicos se determina heridas, lesiones, situaciones donde los sujetos de análisis son personas vivas y que pueden haber sido víctimas de alguna agresión. De esta manera la ciencia de la medicina aporta en la investigación y determinación de ciertos hechos útiles para suponer un caso criminal.

1.3.5 Antropología forense

Ciencia que apoya en la investigación con datos sobre sexo, talla, edad y grupos étnico de las personas en situaciones donde los hallazgos que se realicen sean de restos óseos y que sea difícil de determinar la identidad del sujeto, por otro lado, esta ciencia provee

[10] López Rodríguez, Raúl Estuardo. *"Introducción a la criminalística y ciencias forenses"*. Guatemala, 2019, Pág. 127.

de utilidades como la reconstrucción facial de los restos hallados y con eso dar paso a una mayor oportunidad de identificación de la persona.

1.3.6 Documentoscopía

Se manifiesta cuando se realiza el estudio de algún documento del que se tenga necesidad de establecer la autenticidad del documento el tipo de tinta utilizada y desde luego el tiempo que lleva elaborado el documento.

1.3.7 Grafotecnia

Como un derivado del análisis de documentos la grafotecnia provee de la facultad de análisis de firmas, manuscritos para determinar la autoría o autenticidad del escrito y atribuirla a una persona de esa cuenta individualizarla y crear vinculo en los casos que proceda.

1.3.8 Genética

"Esta ciencia forense tiene por objeto la determinación de la identidad de las personas por medio de la comparación o cotejo de perfiles genéticos".[11]El estudio del material biológico que realiza esta disciplina puede ser a través de muestras de saliva, sangre, pelos, semen, elementos que puedan contener ácido desoxirribonucleico (ADN).

1.3.9 Toxicología

Interviene en los casos donde se presuman o se encuentren involucrados elementos químicos tóxicos o venenosos, evalúa aspectos como origen de los elementos tóxicos, capacidad de provocar daños letales, forma de operar o reacciones consecuentes de su uso o exposición a él, por lo cual en la investigación criminal es de utilidad para establecer la presencia de elementos tóxicos en la realización del hecho.

1.3.10 Informática

"Es la disciplina que se refiere al estudio y análisis de los datos digitales de un sistema de dispositivos, u ordenador a efecto de establecer circunstancias dentro de una

[11] *Ibid.*, Pág. 218.

investigación criminal"[12]*.* Esta ciencia auxiliar de la investigación criminal es de características complejas debido a que pretende establecer hechos que existen y fueron cometidos a través de un medio electrónico, además que no son físicamente palpables; hoy en dia su utilidad trasciende en cada uno de los dispositivos electrónicos de uso recurrente como teléfonos móviles, computadoras, tabletas electrónicas, memorias flash, etc. Elementos que contienen información sobre hechos delictivos cometidos en el ambiente informático.

1.4 Escena de crimen

"El lugar donde los hechos sujetos a investigación fueron cometidos, los rastros y restos en víctimas, victimarios, personas presenciales (testigos, cómplices, encubridores, coautores, o cualquier otra persona) de los hechos u omisiones, incluyendo los accesos, zonas aledañas, así como las vías de escape del recorrido que los protagonistas del crimen hayan realizado para su comisión, desenvolvimiento, consumación y ocultamiento"[13]*.* La escena de crimen es el espacio o lugar donde los hechos se ejecutaron, por lo cual su consideración y cada uno de los detalles que lo componen son relevantes porque en ellos pueden realizarse hallazgos de lo ocurrido y la manera en que cada uno de los interventores en el hecho actuó. Las huellas del delito no solo se encuentran en los objetos de la escena de crimen pueden estar también en vestimentas, calzado e incluso en la misma persona que participó en el hecho, por lo cual el procesamiento minucioso del lugar de los hechos coadyuvará a un mejor resultado investigativo.

[12] *Ibid.*, Pág. 231.
[13] Rossotto Herman, Beatriz. *"Manual de criminología y criminalística"*, Guatemala, 13ra. Edición, 2016, Pág. 187.

1.4.1 Clases de escenas de crimen por el lugar

1.4.1.1 Escena de crimen abierta

Esta escena de crimen es la que se observa en áreas abierta o extensas como en la vía pública, campos, parques, carretera, etc. Lugares que sean de una gran dimensión o extensión, donde no haya ningún objeto que limite o determine específicamente el área.

1.4.1.2 Escena de crimen cerrada

Este tipo de escena es la que se da en espacios cerrados o delimitados por paredes o algún otro objeto que reduzca el área, estas son las que se observan en casas, oficinas, habitaciones, etc.

1.4.1.3 Escena de crimen mixta

Se puede dar este tipo de escena de crimen cuando el hecho que se ejecutó abarca dos ambientes que permite ser abierta y cerrada, como lo que sucedería en un caso donde el hecho se dio fuera de un inmueble, pero hubo un desplazamiento hacia dentro del inmueble y concluyó dentro de una habitación por lo cual la escena seria de ambiente abierto empezando desde la calle y concluido en una habitación donde la escena se torna cerrada por la delimitación del área por las paredes.

1.4.2 Clases de escenas de crimen por sus características

1.4.2.1 Escena del crimen primaria

Se determina así al lugar donde el hecho inició o donde el delito empezó, puede ser el punto de contacto entre el victimario y víctima, en este lugar es donde sucede la mayor parte del echo y que más información proporcionará de lo ocurrido y desde luego para intenciones de investigación en esta área es donde más indicios o huellas del delito se encontrarán y podrán ser documentados para iniciar la investigación y análisis.

1.4.2.2 Escena de crimen intermedia

“Es aquella que se ubica entre la escena primaria y la secundaria la que sirve de enlace de un lugar a otro cuando se continua con un hecho delictivo que tiene más de dos escenas normalmente es la escena de traslado. Por ejemplo, vehículos utilizados para

transportar a la víctima de un lugar a otro"[14]*.* Este tipo de escena de crimen es la que crea conexión del punto inicial del delito al punto secundario ya que allí se transfieren objetos o indicios de la presencia en otro lugar previamente y por supuesto esta misma escena será establecida con la observación de la secundaria por el principio de intercambio.

1.4.2.3 Escena del crimen secundaria

"Es aquella posterior a la escena primaria que puede ser donde se concluye el hecho delictivo, o la ruta de escape o lugar donde se deja finalmente a la víctima"[15]*.* En la comisión de un delito puede darse varias escenas secundarias debido a que este tipo de escena incluye cualquier lugar donde pueda hallarse algún vestigio de la actividad delictiva diferente a la escena primaria, en esta escena es donde la interacción, victimario y victima continua, pero en menor medida de la primaria, sin embargo, el rastro de haberse suscitado un evento en el lugar es evidente.

1.4.2.4 Escena de crimen terciaria

Este tipo de escena se manifiesta cuando después de consumado el hecho se da un desplazamiento dinámico o movimiento que haga presumir que el hecho inició en un punto A continúo en un punto B y se ejecutó en un punto C, pero aun así lo hechores con el objeto de confundir o despistar a las autoridades o complicar aún más el hallazgo desplazan elementos del echo a un punto D, que es donde se lleva a cabo el descubrimiento por las autoridades e inicia la investigación histórica del hecho mediante cada uno de los indicios embalados y que posterior a su análisis correspondiente, guía hacia los lugares previos donde se realizó el proceso delictivo.

1.5 Criminalística

1.5.1 Definición

"Es la disciplina que aplica fundamentalmente los conocimientos, métodos y técnicas de investigación, de las ciencias naturales en el examen del material sensible significativo relacionado con un presunto hecho delictuoso con el fin de determinar en auxilio de los

[14] López Rodríguez, Raúl Estuardo. *Op. Cit.,* Pág. 82.
[15] *Loc. Cit.*

órganos encargados de administrar justicia, su existencia o bien reconstruirlo o bien señalar y precisar la intervención de uno o varios sujetos en el mismo".[16] La criminalística es una ciencia de conocimiento integral, muchas de las ciencias existentes coadyuvan con ella para el esclarecimiento e interpretación de los hechos criminales que de otro modo no podrían ser explicados; por tal razón la criminalística es la una disciplina dedicada especialmente al tratamiento del crimen, todas y cada una de las ciencias que colaboran con la criminalística tiene por fin proveer de medios e información concreta para la argumentación de inculpar a un sospechoso de la realización del hecho, siempre en bases comprobables y lógicas que en este caso son las pruebas.

La criminalística se divide en dos grupos básicos que son la técnica y científica, la primera es la *"Actividad específica del perito técnico en criminalística y del perito en balística. Conjunto de conocimientos empleados para descubrir, identificar, examinar, recoger, y embalar todos los elementos materiales, es decir toda la evidencia física"*[17], la criminalística técnica se manifiesta precisamente al momento del procesamiento de la escena del crimen, donde los técnicos en recolección de evidencia seleccionan, eligen o acuerdan algún método específico para la identificación, recolección y embalaje de los elementos descubiertos en la escena de crimen que pudieren ser susceptibles de análisis posteriormente. La criminalística científica *"conocida como ciencias forenses. A diferencia de la anterior, sus estudios deben ser universitarios y de posgrado en la materia para la cual se pretende llevar a cabo dicha actividad criminalística".*[18], la criminalística científica se ejecuta precisamente por un profesional o experto en la materia del que se trate, con el fin de analizar, procesar e interpretar cada uno de los indicios recolectados en la escena de crimen y que pudieran proveer de información para la investigación del caso que se trata y así vincular a los sospechosos de la realización del hecho.

1.5.2 Criminalística de campo

[16] Arburola Valverde, Allan. *"Criminalística parte general".* México, Pág. 13.
[17] López Abrego, José Antonio, *"Criminalística actual, ley, ciencia y arte",* España, Ediciones Euroméxico, S.A. de C.V., 2012, Pág. 13.
[18] *Ibid.,* Pág. 60.

Esta disciplina es aplicable a todos los delitos o hechos de índole criminal por lo que *"Criminalística de Campo se entiende la investigación que se lleva a cabo en el propio lugar de los hechos".*[19] Otra denominación que recibe este tipo de criminalística es el escenario del crimen, esta es la principal fuente de donde se obtendrá la información de lo ocurrido a través de la recolección de indicios, fotografías del lugar que podría servir para una reconstrucción de hechos, revelado y levantamiento de huellas dactilares, etc. medios que pueden ser analizados posteriormente y obtener una posible vinculación de una o más personas al lugar de los hechos.

1.5.3 Criminalística de laboratorio

"Es la que se realiza en los laboratorios de Criminalística donde se encuentran los instrumentos usados para el examen de los indicios, ya sea, en ocasiones, con fines de identificación o cuantificación"[20]*,* este trabajo científico sigue el método general de las ciencias que es el método inductivo, iniciando con la observación, formulación de una hipótesis y posteriormente la experimentación. La labor en los laboratorios que realiza un perito o especialista de alguna disciplina en particular es analizar, procesar y producir un informe detallado de la posibilidad de vincular el indicio a un sospechoso u orientar la investigación del caso a un punto en específico, un ejemplo claro de la criminalística de laboratorio, es cuando en una escena de crimen se hayan indicios balísticos, estos son embalados y remitidos al Instituto Nacional de Ciencias Forenses (INACIF), donde un perito en balística los analiza y redacta un informe del indicio y su posible vinculación con un arma de fuego la cual puede poseer registro en el banco de datos de la Dirección General de Control de Armas y Municiones (DIGECAM) y de esa cuenta vincular al propietario del arma como el sospecho del hecho.

1.6 Principios de la criminalística

Los principios son un conjunto de reglas o estipulaciones establecidas el cual deben ser cumplidas o consideradas porque tienen como propósito ser una guía para lograr los objetivos trazados, ahora bien en la criminalística existen una serie de principios del cual

[19]Jiménez, Francisco. *"Manual de Criminalística de campo Policía Nacional".* Colombia, 2004, Pág. 9.
[20] Moreno, R. "Introducción a la criminalística". México, editorial Porrúa Hermanos, 2000, Pág. 7.

se fundamenta y guía al momento de ser aplicada, estos mismos proveen de ciertas descripciones que hacen entender aspectos importantes para la investigación; de los principios generales de la criminalística se encuentra el principio de uso, de producción, de intercambio, de correspondencia, de reconstrucción de hechos, de probabilidad, de certeza y de rareza.

1.6.1 Principio de uso

En cada uno de los hechos delictivos que se ejecutan *"siempre se utilizan agentes mecánicos, químicos, físicos y biológicos"*[21]. Este principio se refiere a todo aquel medio o agente empleado para llevar a cabo el acto, por ejemplo, en la escena de crimen de un asesinato se hallan casquillos, eso hace suponer que el agente usado para el hecho es un agente mecánico, ya que es un arma de fuego accionado por el asesino.

1.6.2 Principio de producción

En cualquier hecho delictivo que se ejecute independientemente del agente que se emplee sea mecánico, químico, físico o biológico, siempre se producirá indicios o rastros de lo ocurrido, dichos elementos pueden ser posteriormente analizados y procesados para ayudar en la reconstrucción de hechos o descubrir la verdad histórica de lo ejecutado en el lugar. Haciendo alusión al uso de un arma de fuego en un hecho delictivo este producirá casquillos a causa de los disparos realizados, estos inmediatamente servirán de indicios del hecho y proporcionarán información para la investigación.

1.6.3 Principio de intercambio

"Llamada también principio de Locard este es el principio fundamental de la criminalística que consiste en la triangulación, o intercambio de indicios o vestigios del delito, entre la víctima, el victimario y el lugar de los hechos entre sí"[22]. Todas y cada una de las personas diariamente tienen intercambios con cada uno de los ambientes donde se desenvuelven, en los hechos delictivos sucede lo mismo desde el momento que el victimario tiene contacto con la victima inicia una serie de trasferencias de indicios por ejemplo en un

[21] López Abrego, José Antonio (Comp), *"Criminalística actual, ley, ciencia y arte",* España, 2012, Ediciones Euroméxico, S.A. de C.V., Pág. 62.
[22] López Rodríguez, Raúl Estuardo. *Op. Cit.,* Pág. 17.

forcejeo la victima puede usar las uñas llevándose rastros de piel de su agresor, así mismo el agresor lleva fibras, cabellos y demás elementos que la víctima le trasfiere.

1.6.4 Principio de correspondencia

También denominado principio de identidad, "este *principio exige el uso de la lógica entre la evidencia que se logra recabar y el probable responsable"*[23]. Si en una escena de crimen se realiza el hallazgo de un fluido biológico y posteriormente es remitido a un análisis de laboratorio y este no coincide con la víctima, pero si con el sospechoso detenido, esto hace entender la vinculación y posible responsabilidad del sujeto en ejecutar el delito.

1.6.5 Principio de reconstrucción de los hechos

Este principio surge como resultado de todas y cada una de las diligencias realizadas y con la información aportada por los elementos hallados en la escena del crimen y el resultado del análisis de cada uno de dichos hallazgos, la correspondencia de los mismos, da paso a que sea corroborado lo acontecido entonces es realizada la reconstrucción de hechos, este proceso no es más que recrear lo que se presumen ocurrió y la manera en que ocurrió muchas veces apoyadas más fehacientemente por testimonios de la víctima o testigos presenciales del hecho, para así acercar lo más posible al esclarecimiento de la verdad.

1.6.6 Principio de probabilidad

Este principio es consecuencia de la reconstrucción de hechos, con él se razona algunas cuestiones anteriormente incomprendidas del caso, es decir que con los resultados obtenidos de la reconstrucción se da una razón lógica de cómo pudo haber sido usado u ocurrido determinado suceso de allí la probabilidad de saber cómo y quienes participaron en el hecho.

1.6.7 Principio de certeza

[23] López Abrego, José Antonio (Comp), *Op. Cit.,* Pág. 63.

"De conformidad con la calidad de las evidencias, es posible el establecimiento de certezas y decidir con amplias posibilidades"[24]. Gracias al apoyo de cada una de las ciencias forenses la identificación cualitativa, cuantitativa y comparativa de los agentes empleados en un hecho delictivo de concluye con la existencia de certeza y procedencia de cada uno de los objetos hallados en la escena de crimen.

1.6.8 Principio de rareza

"Llamado también principio de infrecuencia de Jones; está basado en el análisis de un elemento que resulte poco frecuente o raro en el contexto del lugar y su relación con los otros elementos o su relación con la víctima"[25]; el hallazgo de un elemento extraño debe mantener la motivación de su explicación y no de descarte como vinculante al hecho, porque puede suceder que a través de este medio puede descubrirse información de la dinámica del hecho ocurrido y sus interventores.

1.7 Fijación de la escena del crimen

Este procedimiento debe ser considerado desde el inicio de la investigación es decir desde antes de ingresar a la escena de crimen debe procurarse fijar la escena mediante fotografías a distintas distancias y ángulos con el fin de detallar la forma, ubicación y distribución de cada uno de los elementos en el lugar y desde luego hacer constancia y registro de todo mediante la redacción de acta por el fiscal a cargo de la investigación.

Tomado en consideración lo anteriormente señalado se procede a establecer el siguiente paso de fijación y documentación de la escena de manera más detallada, no sin antes haberse realizado la labor de búsqueda y señalización de cada uno de los indicios en el lugar para así determinar el orden en que cada uno será fijado y posteriormente embalado para su traslado y análisis respectivo. Los métodos de búsqueda establecidos para la escena de crimen son: método espiral, método de zona, método de franjas o líneas, métodos de rejas o cuadrícula, métodos de punto a punto; cada uno de estos son determinados atendiendo al tipo, forma, ubicación de la escena de crimen al mismo tiempo que cada uno posee distinta efectividad dependiendo del caso y hecho que se

[24] *Ibid., Pág. 64.*
[25] López Rodríguez, Raúl Estuardo. *Op. Cit.,* Pág. 19.

trate. Atendiendo a la fijación de los indicios en la escena de crimen se considera la Planimetría *"esta técnica complementada con la fotografía y video es muy importante para la fijación e ilustración del lugar de los hechos y la ubicación de indicios, pues constituye una herramienta dentro del proceso que permite establecer la ubicación en el espacio del lugar de los hechos y da una visión grafica de donde ha ocurrido el crimen"*[26], la planimetría es una técnica de documentación mediante un plano del lugar donde se sospecha ocurrió un hecho criminal, se realiza sobre una hoja de papel señalando cada uno de los objetos en el lugar a una escala determinada y desde una perspectiva que es denominada vista de pájaro que permite se dibuje el terreno desde una proyección horizontal.

1.8 Embalaje

"Es el procedimiento por medio del cual se coloca convenientemente y de forma segura dentro de sobres, bolsas, cajas, empaques, tubos de ensayo, hisopos, u otros envoltorios o materiales para resguardar los indicios que se han recolectado en una escena de crimen para su traslado y custodia"[27]*;* es de mencionar que el proceso de embalaje lleva en algunos casos un cuidado especial debido a que puede tratarse de indicios húmedos los cuales deben ser secados a temperatura ambiente y manipulado lo menos posible para no ser alterados, destruidos o contaminados, así mismo debe considerarse que todos y cada uno de los indicios por más numeroso que sean deben ser embalados individualmente a modo de ser preservados lo más puro posible, ya que serán objeto de análisis y estudio en los laboratorios correspondientes y en los casos de procedencia.

[26] *Ibid., Pág. 95.*
[27] *Ibid., Pág. 101.*

1.9 Cadena de custodia

"Es el procedimiento de control que se aplica al indicio desde su localización, y su debida conservación hasta que haya de ser valorado como prueba por parte del juzgador y tiene como fin evitar alteraciones, daños, sustitución, contaminación, destrucción o cualquier acción que varíe su estado original, para garantizar que es el mismo que se encontró en el lugar de los hechos y el que se presenta en el debate"[28], este procedimiento se manifiesta concretamente en un documento que contiene la descripción del indicio, la firma e identificación de cada una de las personas que han tenido bajo su custodia el indicio y los procesos que ha realizado con el mismo, este registro cronológico inicia desde el embalador que es la primera persona que tiene contacto con el indicio en la escena de crimen al momento de su levantado y traslado continua con todos los demás sujetos que en determinado momento lleguen a tener contacto con el elemento.

[28] *Ibid., Pág. 103.*

CAPÍTULO II
2. INFORMÁTICA

2.1 Antecedentes históricos

Hoy en día es difícil pensar en un mundo sin computadoras debido que las mismas a través de los años han ido tomando un espacio o lugar esencial en la vida cotidiana de cada una de las personas, con todas y cada una de sus comodidades que tiene para ofrecer a los usuarios desde almacenar y procesar datos hasta producir resultados con la instalación o ejecución de un simple programa, sin embargo, durante mucho tiempo las personas vivieron sin ninguna de las comodidades y ventajas que provee un ordenador moderno en cuanto a registro de información, cálculo o cuantificación de datos, se presume que una primer herramienta de conteo serían los dedos de la mano posteriormente podría haber sido el uso de piedritas que son mucho más abundantes que los dedos de las manos y los pies, es difícil establecer un dato exacto o concreto del origen de la informática, pero lo cierto es que la informática y las computadoras están íntimamente relacionadas debido a que procesan información; la necesidad de cuantificar y llevar un control ordenado de cada uno de los miembros de un grupo, a la misma vez de requerir saber la cantidad de animales que se posee y las provisiones que se tiene para la alimentación, se podría deducir como los inicios de la informática, el conteo y control mediante tablillas de arcilla, nudos en cordones y trocitos de madera como los primeros medios de registro de información.

A través del tiempo se conoce el ábaco, considerado como la primera herramienta para ayuda del cálculo *"un original mecanismo de cálculo manual, formado por cuentas alineadas en ranuras o cordones fijados a un armazón que permite sumar con gran facilidad. Además, cualquier instrumento que puede sumar también puede multiplicar, pues la multiplicación solo es una edición repetida"*[29] , existen algunos otros datos que mencionan que el ábaco fue utilizado en china siempre con el fin de calcular, dicha herramienta de cálculo resultó ser en el trascurso de la historia el primer instrumento

[29] ISA, Universidad de Oviedo, *"Introducción a los computadores"*. España, 2019, http://www.isa.uniovi.es/~alonsog/Microcontrolador/T1%20Introduccion%20a%20los%20computadores.pdf, fecha de consulta: 7 de marzo 2021.

mecánico para tal fin, posteriormente existieron matemáticos y muchos más personajes históricos que fueron contribuyendo en el desarrollo del manejo de la información y el cálculo. El siguiente salto en la historia sobre la computación fue por *"Hollerith, ante la necesidad de mecanizar el censo de los Estados Unidos de 1890, diseñó una máquina que leía tarjetas perforadas similares a las diseñadas por Jacquard y Babbage (Jacquard fue un tejedor francés que usó las tarjetas perforadas para controlar sus telares). En 1896 fundó la Tabulating Machine Company para hacer y vender su invento,"*[30] un tiempo después esta compañía se fusiona con otras dando origen a un gigante y revolucionario personaje de la informática, la conocida mundialmente, International Bussiness Machines Corporation (IBM), esta compañía tenía la orientación específica de la construcción y reparación de máquinas de negocios, destinados al cálculo o manejo de cuentas.

La aparición de las primeras computadoras tal y como se conocen hoy fue a partir de *"1937 y 1944 Howard H. Aiken construyó una máquina calculadora automática que combinaba la tecnología de esa época con las tarjetas perforadas de Hollerith. Las operaciones internas eran controladas automáticamente mediante relés. En muchos aspectos esta máquina, conocida como la MARK 1, fue la realización del sueño de Babbage. Era una computadora electromecánica"*[31], dicha máquina construida fue descontinuada poco tiempo después de su creación, al mismo tiempo que se dio paso al uso de tubos al vacío que aportaría un mejor desempeño y avance en el desarrollo tecnológico de los ordenadores. Es de mencionar que MARK 1 pesaba aproximadamente cinco toneladas.

En pleno desarrollo de la segunda guerra mundial se llevó a cabo otro gran avance en el desarrollo de la informática protagonizado por EE. UU., *"donde el esfuerzo bélico llevó a la construcción del ENIAC (Electronic Numerical Integrator And Computer), una impresionante máquina electrónica diseñada para calcular trayectorias balísticas y en torno a la cual se establecieron las bases de lo que hoy en día entendemos por un*

[30] *Loc. Cit.*
[31] *Loc. Cit.*

ordenador"[32], durante el desarrollo de esta nueva tecnología se integró los circuitos con el objeto de mejorar el desempeño de los tubos al vacío, pero aun así el desempeño se veía reducido a la capacidad máxima del quipo construido. Poco tiempo después de acabada la segunda guerra mundial se alcanzó otro gran logro y fue el desarrollo del primer lenguaje de programación conocido como FORTRAN (Formula Traslator), fue posible con el apoyo de algunos empleados de IBM.

"Jhon Von Neumann, en 1946 el matemático húngaro-estadounidense enuncio el concepto de programa almacenado"[33], la pretensión de Neumann era que los ordenadores creados y en uso hasta ese momento y que eran operados manualmente conectando y desconectando cables cada vez que se quería cambiar de programa o de operación en el ordenador, fueran automáticos y que quedaran programadas para tal función y así evitar estar manipulando los cables frecuentemente, con la idea presentada por este personaje históricos se dio el primer paso de la programación de los ordenadores conocidos actualmente, por tal razón hay personas que denominan a este tipo de programación automática de funciones de los ordenadores como arquitecturas Von Neumann.

Hasta la década de los sesenta la programación de ordenadores fue considerada una tarea eminentemente femenina; entrada la década de los sesenta se muestra un prototipo de la computadora moderna, con un mouse y una interfaz gráfica de usuario que proveía de iconos y símbolos en las pantallas de los ordenadores, el lanzamiento de esta tecnología al público supuso el fin del uso específicos de los ordenadores por científicos, matemáticos, militares y compañías, su manifestación desde entonces empezó a ser mucho más común y accesible.

Iniciado el siglo XXI la evolución de las tecnologías habían avanzado, poco tiempo llevaba acuñado el término informático Wi-Fi, que no es más que la tecnología de conexión sin

---

[32] Molero Prieto, Xavier. *"Un viaje a la historia de la informática".* España, editorial Universitat Politécnica de Valéncia, 2016, Pág. 18.

[33] ISA, Universidad de Oviedo, *"Introducción a los computadores"*. España, 2019, http://www.isa.uniovi.es/~alonsog/Microcontrolador/T1%20Introduccion%20a%20los%20computadores.pdf, fecha de consulta: 7 de marzo 2021.

cables a internet, así mismo la interfaz de cada una de las máquinas de dicha fecha empezaba a tener una interacción mucho más dinámica en referencia a iconos y sin la necesidad de teclear códigos informáticos para activar o desactivar funciones.

2.2 Definición de Informática

"Conjunto de conocimientos que permiten el tratamiento automático de la información y se utiliza para abarcar todo lo relacionado con el manejo de datos mediante equipos de procesamiento automático como las computadoras".[34] Este término no solo describe el funcionamiento o desempeño de las computadoras en el manejo de la información, también abarca la programación, arquitectura de las computadoras, inteligencia y robótica entre muchas más áreas tecnológicas. *"Es un campo de estudio que abarca el diseño, la construcción y la utilización de las computadoras para todo tipo de información".*[35]

De los aspectos básicos sobre la informática resaltan el hardware, software, sistemas operativos, redes, programación, de estos elementos su consideración es relevante toda vez que provean de los conocimientos más generales sobre el funcionamiento de los sistemas informáticos. El procesamiento almacenamiento de la información hoy día ha cobrado una gran importancia debido a que la sociedad en las últimas décadas ha incrementado más su dependencia a las computadoras u ordenadores para distintas funciones como inventario, registro de ingresos y egresos monetarios, cartera de clientes, acreedores, etc. Por lo cual la informática se ha extendido hasta estratos políticos, sociales y económicos.

2.3 Informática forense

"Es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional".[36] Este término es una subdivisión de la informática, ya que consiste en la aplicación de los conocimientos,

[34] Villazán Olivares, Francisco José. *"Manual de informática I"*. México, editorial UMSNH, 2009, Pág. 8.
[35] Díaz Alonso, Arturo. *"Informática I".* México, editorial FCA, 2003, Pág. 16.
[36] López, Oscar y otros. *"Informática forense: Generalidades, aspectos técnicos y herramientas".* Colombia, Universidad de los Andes, Pág. 2.

herramientas, procedimientos y métodos de la informática en la preservación, análisis y presentación de evidencia digital que pueda ser ofrecida, proveída y admitida en un proceso legal, donde sirva como medio de prueba para determinado delito. De la informática forense existe ciertas distinciones de la informática convencional, la primera pretende obtener información sobre un determinado hecho punible, mientras que la informática convencional busca procesar, mantener y organizar información en sus sistemas, para proveer al usuario un acceso fluido y sencillo a los datos; la diferencia radica en que la informática forense emplea métodos criminalísticos para obtención de indicios y/o evidencia digital, todo esto realizado en la escena donde se presuma se cometió el crimen o desde los medios donde se ejecutó la comisión del delito, pudiendo ser estas computadoras, discos duros, memorias USB, router, dispositivo móvil, etc. Por otro lado, para su ejercicio deben velarse determinados parámetros de cuidado y preservación de la evidencia recolectada, porque la naturaleza de esta es de muy alto riesgo de ser perdida o afectada por factores externos como campos magnéticos, corrientes eléctricas, interferencias, etc.

En esta área no solo se requiere de personal especializado en informática sino alguien que también posea conocimientos sobre el cuidado y preservación de la evidencia digital así también sobre su utilidad y presentación en un proceso penal, a este personal calificado se conoce como perito informático.

2.3.1 Importancia de la informática forense

Es claro y cada día más predominante la inclusión de la tecnología en la vida cotidiana, cada año las compañías tecnológicas más grandes del mundo van presentando nuevas y mejoradas creaciones, lo cual supone el avance y/o desarrollo que las sociedades están teniendo, ahora bien, situaciones tan cotidianas como ordenar una comida en un restaurante ha ido digitalizándose, también las diferentes formas de delinquir han ido adaptándose y presentándose en formas diferentes, pero siempre con el mismo fin. En este sentido se ha señalado que las estructuras delictivas aun operan como frecuentemente se ha conocido, es decir, que poseen distribución de funciones y cargos en las diferentes escalas o posiciones en la organización, el desafío mayor de cada uno

de los organismos encargados de impartir justicia es esclarecer hechos no físicos sino digitales, de allí la importancia de la informática forense.

Es relevante considerar que todos los tipos de delitos conocidos hoy en día pueden contenerse en un solo dispositivo electrónico, por ejemplo un teléfono inteligente o smartphone, con la cantidad de aplicaciones y facilidades que día con día ofrece y la conectividad a internet cada vez más fluida, es notable la oscuridad de la ley respecto a lo que se puede generar en el ciberespacio; la principal forma de delincuencia digital además de las estafas en productos son el phishing o suplantación de identidad más concretamente en los datos bancarios, hoy día supone el delito más importante y más rentable para las estructuras criminales anualmente.

La consolidación actual de una policía especializada es de emergencia primaria, de no ser atendido dicho espacio digital, las pérdidas económicas irán cada vez más en ascenso. Ahora bien, la importancia de la informática forense es clara al abarcar el lugar de la impunidad en temas de ciber espacio donde la delincuencia actualmente prolifera a sus anchas. *"La informática forense no es una tarea fácil, implica mucha responsabilidad y conocimiento técnico para realizar adecuadamente los pasos de recolección, cadena de custodia, almacenamiento de la evidencia, entre otros; de lo contrario el análisis y los hallazgos que resulten no van a servir como medio probatorio a las organizaciones que deciden adelantar procesos judiciales contra empleados y terceros, como casos de estudios jurídicos, y no serían de utilidad en las entidades judiciales o policiales que buscan evidencias para poder aplicar la justicia a aquellos que han cometido estos delitos"*[37], la incidencia de la informática forense en la investigación de esta naturaleza de delitos es aportar elementos de convicción en los procesos judiciales que no son físicos sino digitales.

2.3.2 Objetivos de la informática forense

[37] Cruz Quintero, Gloria Esperanza. "Importancia de la informática forense". Colombia, Universidad Piloto, 2012, Pág. 3.

Toda disciplina posee metas y proyecciones de alcance tal es el caso de la informática forense, de manera general busca o pretende cubrir aspectos como la prevención de la comisión de hechos delictivos desde una perspectiva de rastreo y control constante del ciber espacio, las susceptibilidades que puede haber para que suceda un hecho ilícito, de la misma manera coadyuva en el caso de compañías o instituciones que manejan datos sensibles a detectar vulnerabilidades en los sistemas o redes, se considera a la informática como un área dinámica y constantemente cambiante, los intrusos informáticos siempre buscan una nueva y creativa forma de romper los esquemas de seguridad e infiltrarse en el banco de datos objetos muchas veces de robo. Por otro lado, está la orientación sobre ciberseguridad que no es más que una manera estratégica de crear medidas y protocolos de estabilidad ante intento de ataques, por último, se encuentra el principal objeto de la informática forense y es la recopilación de información y evidencia útil para la persecución penal de un hecho punible.

Otros objetivos de informática en sentido jurídico son:

a) *"La compensación de los daños causados por los criminales o intrusos.*
b) *La persecución y procesamiento judicial de los criminales.*
c) *La creación y aplicación de medidas para prevenir casos similares".*[38]

En dichos preceptos se contiene el fin social de reparar el daño y promover la justicia, en cada una de las personas que han quebrantado alguna de las disposiciones legales, además de vulnerar un bien jurídico tutelado de otras personas con la acción criminal perpetrada, esta última resarcida con la sanción penal.

2.3.3 Principios

El establecimiento de principios rectores en cada una de las ciencias forenses es esencial toda vez que se busca determinar y concretar el fin principal que posee la disciplina que se trate, en sentido informático forense dichas determinaciones rectoras son:

2.3.3.1 Identificación

[38] ECURED, Enciclopedia Cubana, Informática forense, Cuba, https://www.ecured.cu/Inform%C3%A1tica_Forense, fecha de consulta: 12 de julio 2019.

"Consiste en el conocimiento y la comprobación del hecho delictivo"[39], por sentido común y para evitar contratiempos innecesarios antes de iniciar cualquier procedimiento judicial es necesario comprobar primeramente si el hecho del que se trata encuadra como delito y amerite la intervención de un investigador o bien autoridades judiciales correspondientes al caso que se pretenda averiguar.

2.3.3.2 Preparación

"La preparación y planificación de las herramientas, las técnicas a utilizar y la obtención de los permisos necesarios para efectuar las acciones pertinentes"[40], esta indicación de la informática forense es con el fin de realizar un procedimiento efectivo en atención al cuidado que debe considerarse sobre la evidencia informática, iniciando por preparar dispositivos de almacenamiento que no contaminen o alteren la evidencia en caso de crear copias, equipos actualizados para evitar contratiempos en el lugar de intervención y desde luego también la preparación de las aplicaciones necesarias para la creación de copias de la evidencia así como el escaneo probable que se necesite del sistema de los equipos en el lugar o la extracción segura de la información en cada uno de los dispositivos sospechosos de haber sido utilizado para perpetrar el ilícito.

2.3.3.3 Planificación estratégica

"Desarrollar una estrategia tendente a maximizar la recolección de pruebas y minimizar el impacto sobre la víctima"[41].

Al momento de trasladarse y hacer presencia cada una de las autoridades correspondientes a la escena del crimen informático, es importante que puedan llegar con un conocimiento preliminar de lo ocurrido para así considerarse las medidas necesarias en caso de existir víctimas en el lugar o para conocer posibles conexiones por cable o inalámbrico en los dispositivos presentes para evitar pérdida de datos relevantes o destrucción de evidencias físicas importantes para el caso que se pretende investigar, por otro lado antes de iniciar cualquier contacto con la evidencia digital es necesario

[39] Rodríguez Más, Francisca y Alfredo, Doménech Rosado, "La informática forense: El rastro digital del crimen", *Derecho y cambio social*, No. 25, ISSN-e 2224-4131, 2011, Pág. 18.
[40] *Loc. Cit.*
[41] *Loc. Cit.*

contar con el asesoramiento de un especialista en informática que pueda determinar puntualmente los procesos a ejecutar tomando en cuenta que no en todos los casos los dispositivos serán personales también los hay de uso corporativo o compartido que desde otra ubicación pudieren eliminar los rastros y así entorpecer la investigación.
De cualquier forma, no siempre se contará con todos los recursos y conocimientos para cada uno de los casos, sin embargo, la decisión final de los procedimientos a ejecutar queda a discreción del encargado de la investigación.

2.3.3.4 Aseguramiento de la escena, tanto física como digital

"En todo escenario de un hecho delictivo, y al igual que se toman las debidas medidas y precauciones para no contaminar la escena de aquellos vestigios que sean susceptibles de ser enviados a los laboratorios para su examen (huellas digitales, ADN, elementos balísticos, etc.), así se deben tomar las debidas precauciones para no contaminar la escena digital, ya sea por medios físicos o electrónicos"[42], todas las escenas de crimen son totalmente únicas e irrepetibles por lo tanto debe siempre tratarse a cada una de ellas como si fuera la primera con todos los cuidados y respetando cada una de las recomendaciones de los manuales de intervención de hechos informáticos o en todo caso los protocolos internacionales.

Una manipulación incorrecta en el lugar del hecho informático puede alterar, modificar o incluso perder información valiosa irrecuperable, por ejemplo se sabe que la electricidad estática daña o altera los dispositivos magnéticos y muchas veces las prendas de vestir dependiendo de su material producen este tipo de energía y al estar en contacto con un elementos magnético o circuito puede provocar la pérdida total de los datos almacenados en el dispositivo, así mismo los golpes o accidentes en el lugar de intervención pueden hacer que otros elementos indiciarios se estropeen como huellas de calzado, manchas hemáticas, pelos, fluidos, etc. Esta instrucción sobre la informática forense está encaminado a crear una coordinación efectiva entre los peritos recolectores de evidencias comunes y los peritos informáticos.

[42] *Ibid.,* Pág. 19.

2.3.3.5 Recogida de pruebas

"Registrar la escena del delito, recoger y empaquetar adecuadamente las evidencias digitales, garantizando su integridad, y prestando atención a la cadena de custodia"[43], esto último que indica el principio informático es debido a las muy variadas situaciones o entornos que pueden ser una amenaza para la evidencia informática. Es importante que el registro de cada uno de los dispositivos y su posterior empaquetado sea por la misma persona esto para mantener en todo lo posible el mismo cuidado con todos los elementos hallados en el lugar y que necesiten ser trasladados al laboratorio para su análisis, en algunos casos hay dispositivos que deben ser analizados en el lugar por el riesgo que supone apagarlos o desconectarlos de la red al que se encuentran vinculados, pero fuera de dichas excepciones es recomendado realizar el análisis en un laboratorio esto primeramente para contar con la comodidad y tranquilidad del perito al realizar su trabajo, al mismo tiempo que en el laboratorio se cuenta con todas las herramientas adecuadas y necesarias para cada uno de los dispositivos, sin embargo es importante que en el lugar de la intervención se pueda realizar una copia o clonado de la evidencia digital y la misma lleve una firma digital con el fin de que no sea alterado en su transporte hasta el laboratorio.

2.3.3.6 Examen

Para este procedimiento se debe contar con los conocimientos técnicos adecuados. *"No se ha de olvidar el cumplimiento exacto de la cadena de custodia, y se debe estar en posesión de la autorización necesaria para proceder al examen y análisis de las evidencias"*[44]*.* Anteriormente se hacía mención de que el trabajo de registro y empaquetado fuese por una misma persona, en este apartado también seria en el mejor de los casos lo adecuado es decir que la misma persona o perito que se encargó del registro y empaquetado de los dispositivos sea el mismo que realice su examen debido a que solo el conoce los dispositivos recogidos, sus características físicas y técnicas de cada uno, así como su estructura, formato, etc.

[43] *Ibid.,* Pág. 20.
[44] *Loc. Cit.*

2.3.3.7 Análisis e interpretación

"Analizar metódicamente las pruebas. Interpretar los datos que se obtengan e interrelacionarlos adecuadamente para tratar de explicar los hechos y su distribución temporal"[45], esta instrucción es concretamente para los peritos informáticos debido a que son ellos los encargados de realizar el proceso de análisis, interpretación y obtención de resultados de cada uno de los dispositivos tecnológicos involucrados en un hecho criminal de carácter informático, también supone la etapa más laboriosa del proceso investigativo porque en muchos de los casos la cantidad de información a analizar e interpretar en enorme por lo que conlleva un esfuerzo mayor el obtener un resultado de inmediato.

2.3.3.8 Documentación

"El objetivo final de un análisis forense, es plasmar por escrito de una forma exacta, comprensible, clara y completa, los pasos realizados en el análisis, los hallazgos, su interpretación y la conclusión que de ellos se derivan"[46]*.* Este apartado también es encaminado a los peritos informáticos por razones claras de que ellos son los encargados de redactar y presentar el informe conclusivo del análisis forense de la evidencia informática y de esa cuenta convencer a las autoridades judiciales de admitir o rechazar la información al caso del que se esté investigando. Es importante tener claro el carácter forense que tiene el análisis informático, por lo que en toda la redacción del informe debe ser en un lenguaje sencillo y comprensible para el o los destinatarios finales que en su mayoría no posee conocimientos sobre informática pueda interpretar la información y sirva de apoyo en la toma de decisiones sobre el caso investigado y los sujetos que se encuentren vinculados al mismo.

2.3.4 Utilidad de la informática forense

Esta clara y concretamente establecida que la delincuencia digital provoca un severo impacto y variadas consecuencias ulteriores de gravedad a cada una de las víctimas, ya que el alcance de cada uno de ellos es amplio llegando a impactar sectores educativos,

[45] *Loc. Cit.*
[46] *Ibid.,* Pág. 21.

sociales y por demás el sector económico. La utilización de los conocimientos técnicos en informática abarca tres elementos básicos sobre los conocimientos de dicha área y son la búsqueda, adaptación y aplicación, esto a raíz del trabajo de la ingeniería inversa. La ingeniería inversa *"se refiere a dar la vuelta al proceso de elaboración de un producto. En este caso que nos ocupa, se viene a referir a un software compilado del cual se carece de cualquier tipo de código fuente, esquema de diseño, pseudocódigo, o cualquier tipo de información referente al funcionamiento interno del software"*[47], la utilidad concreta de la informática en el sentido forense es razonada por la ingeniería inversa, que busca a través de proceso analíticos el medio por el cual se realizó el hecho punible y de esa concepción parte la reconstrucción de hecho y adquisición de prueba contundentes que orienta la investigación a realizar.

2.4 Redes

"Es un conjunto de al menos dos computadoras y otros dispositivos enlazados entre sí con el objetivo de intercambiar datos, archivos y otros recursos".[48] En las redes los equipos no necesariamente deben estar cerca el uno del otro, puede haber redes donde sus elementos o equipos que lo integran están repartidos por todo el mundo llegando a ser muchas veces miles o millones, como sucede con internet, que posee servidores esparcidos por distintas partes del mundo que dan alojamiento a la información y así mismo el usuario puede acceder a ello en cualquier momento y desde cualquier lugar donde pueda o tenga acceso a internet. Existen distintos tipos de redes dependiendo de la utilidad que se le quiera dar, algunas son de uso o área personales, otros de uso corporativos, otros de uso nacional o de cobertura amplia, etc. Cada uno de ellos dependiendo de su objetivo, alcance de área o cobertura.

2.4.1 Clasificación de redes

Cada una de las redes cumplen y se adecuan a cada necesidad de los usuarios, por tal razón existe una clasificación de ellos y son *"según su área de cobertura, según su*

[47] Garrote García, Rubén. *"Ingeniería inversa teoría y aplicación".* España, editorial Ra-Ma, 2017, Pág. 16.
[48] Fernández Montoto, Carmen, Montes de Oca Richardson, Martha. *"Computación: herramientas informáticas".* Cuba, editorial Félix Varela, 2005, Pág.45.

privacidad, según su relación funcional, según su topología".[49] Esta clasificación existe en concordancia a la funcionalidad de cada una de las redes en los distintos medios donde sean empleados, sin dejar ajeno el objeto y necesidad que poseen los usuarios.

2.4.1.1 Según área de cobertura

Son todas aquellas redes que tiene un alcance o señal con un área determinada entre ellos y los más conocidos se pueden mencionar el PAN (red de área personal) que tiene un alcance de pocos metros y por otro lado está la red WAN (red de área amplia), que abarca hasta miles de kilómetros.

2.4.1.2 Según su privacidad

Se refiere específicamente a la accesibilidad o disponibilidad de ingreso que llegue a tener la red por ejemplo en redes privadas las que ocupan en ámbitos de oficina permite enviar documentos entre ordenadores sin embargo está limitado únicamente a las maquinas autorizadas o usuarios, por otro lado, está el internet que es una conexión publica al cual todas las personas alrededor del mundo pueden acceder libremente.

2.4.1.3 Según su relación funcional

Se denomina así a la red que en la que todos los usuarios están conectados a un servidor central en donde se aloja todos y cada uno de los recursos que se disponen así mismo las aplicaciones con que se cuentan.

2.4.1.4 Según su topología

Es la distribución física con que se conecta una red a todos los usuarios, en pocas palabras se refiere a la forma que va a tener la red en sus conexiones pueden ser en forma de estrella, anillo o malla, esto va siendo determinado en sentido de la ubicación que cada uno de los usuarios tendrá o tiene.

[49] Xunta de Galicia Conselleria de educación, Universidade e formación profesional, Xunta de Galicia, Redes y seguridad, España, S/a, https://www.edu.xunta.gal/centros/iesvalleinclan/aulavirtual2/pluginfile.php/14217/mod_resource/content/1/Tema %20redes%20y%20seguridad.pdf, fecha de consulta 18 de febrero de 2019.

2.4.2 Tipos de redes

Las redes en su tipo existen variedad, cada una poseen distintos alcances y por supuesto puede ser por medio de cableado o conexión inalámbrica, así también dependiendo del uso que se le pretenda dar, estas son:

a) *"Redes de área personal.*
b) *Redes de área local.*
c) *Redes de área Metropolitana.*
d) *Redes de área extensa.*
e) *Internet.*
f) *Intranet.*
g) *Extranet.*
h) *Cliente servidor.*
i) *Redes entre iguales.*
j) *Malla, estrella, árbol, bus, anillo".*[50]

2.4.3 Riesgos en la red

Desde el ingreso al navegador el usuario o internauta ya se encuentra expuesto a variados y numerosos riesgos debido a que el internet hoy día ha abierto una puerta al mundo del que todos pueden ver e ingresar sin mayor dificultad, los riesgos en la red aumentan aún más cuando el usuario ingresa contraseñas, datos personales, números de teléfono, números de tarjeta de crédito o débito, etc. Información que puede ser usado por algún cibercriminal para vaciar cuentas de banco, robar identidad en redes sociales y realizar comprar a nombre de otra persona, etc. Existen numerosas formas de operar de los ciberdelincuentes, pero algunas de ellas resaltan muchas veces por la problemática que representa a los usuarios desprevenidos del ciberespacio y estos son:

2.4.3.1 Los virus

Son programas de códigos que se instalan o cargan en el equipo de una persona sin su consentimiento y muchas veces ni siquiera se sabe de su existencia en el sistema debido a que son programas que se ocultan. *"Algunos virus son simplemente molestos, pero la*

[50] *Loc. Cit.*

mayoría de los virus son destructivos y están diseñados para infectar y tomar el control de sistemas vulnerables".[51]

2.4.3.2 Troyanos

"Un troyano es un tipo de virus que simula ser algo útil, de ayuda o divertido pero que, de hecho, provoca daños o el robo de datos".[52] Comúnmente este tipo de archivo malicioso se propaga a través de descargas de aplicaciones, juegos, videos incluso por medio de correos electrónicos, estos mismo se esconden y cuando el dispositivo u ordenador no posee protección adecuada abre en el sistema un acceso remoto del cual se puede obtener desde el historial de navegación hasta las pulsaciones del teclado lo que da al cibercriminal facilidad de acceder y robar información de la víctima o propietario del dispositivo infectado.

2.4.3.3 Botnet

"Una botnet, o, mejor dicho, una red de bots (también conocida como ejército zombi) es una red constituida por un gran número de equipos informáticos que han sido "secuestrados" por malware, de forma que quedan a disposición de un hacker".[53]

Para que un dispositivo o equipo de informática pase a formar parte de una red de bots necesita estar infectado por algún tipo de software malicioso o programa descargado junto con otro e instalado sin autorización, ahora bien, un equipo secuestrado servirá para enviar spam o publicidad basura, propagar virus o realizar ataques sin el conocimiento del propietario real del equipo.

2.4.3.4 Ransomware

"El ransomware es un programa de software malicioso que infecta la computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del

[51] Avast, Avast Software S.R.O., Ciberdelito, Estados Unidos, 2015, pág. 1, disponibilidad y acceso: https://www.avast.com/es-es/c-cybercrime, fecha de consulta 21 de febrero 2019.
[52] *Loc. Cit.*
[53] Avast, Avast Software S.R.O, Botnet, España, 2016, disponibilidad y acceso: https://www.avast.com/es-es/c-botnet, fecha de consulta: 21 de febrero 2019.

sistema".[54] Este es un modo muy frecuente de ataque malicioso de los cibercriminales con ello obtienen dinero, porque bloquean la pantalla o todo el sistema de un equipo hasta que se realice el pago exigido, en ocasiones no bloquea todo sino el criminal detrás de todo bloquea archivos específicos o importantes para tener un modo de presión aun mayor a la víctima y realice el pago y así se le otorgue la contraseña para desbloquear el archivo y acceder a su uso.

2.4.3.5 Keylogger

"Este tipo de malware monitoriza de manera encubierta cada tecla pulsada en el teclado de un dispositivo".[55] Este programa malicioso busca recopilar la información de los usuarios como clave de cuentas, pin de tarjetas, contraseñas, direcciones de correo, nombre de usuarios o alguna información sensible tecleada desde el quipo donde se encuentre instalado el keylogger, existen dos tipos de este malware y son software y hardware, este último es poco frecuente porque requiere que se manipule directamente el teclado físico lo cual se complica si el delincuente o espía no tiene acceso al dispositivo, el tipo software es el más usado debido a que puede instalarse remotamente a través de descargas sin que el usuario se dé cuenta y más si el equipo no cuenta con la seguridad adecuada se encuentra aún más expuesto a este tipo de riesgos.

2.5 Redes sociales

"Son formas de interacción social definidas como un intercambio dinámico entre personas, grupos e instituciones en contextos de complejidad. Consisten en un sistema abierto y en construcción permanente que involucran a conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos".[56] Red social o comunidad virtual es un servicio o espacio que se brinda a través de un sitio web, en el que los usuarios pueden crear un perfil con su información personal y así ser identificado por otros usuarios, las redes sociales poseen la característica de

---

[54] Kaspersky, AO Kaspersky Lab, ransomware, Estados Unidos, 2018, disponibilidad y acceso: https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware, fecha de consulta: 23 de febrero 2019.
[55] *Loc. Cit.*
[56] Martos Carrión, Esther. *"Análisis sobre las nuevas formas de comunicación a través de las comunidades virtuales o redes sociales".* España, Universidad politécnica de Valencia, 2010, Pág. 2.

ser un ambiente virtual donde se comparte ideas, fotografías, intereses, comunicación con familiares y personas alrededor de todo el mundo.

2.5.1 Riesgos en las redes sociales

Es inminente el riesgo al que todos los internautas se exponen al momento de ingresar a cualquier página web y más cuando no se tiene la seguridad adecuada en el equipo, pero existen algunos riesgos no precisamente de carácter informático sino de criminalidad común, es decir personas mal intencionadas asechando desde las redes sociales, aún más cuando el número de usuarios menores de edad va en incremento día a día, de allí el riesgo de ser víctima de acoso cibernético y otras formas de peligro en las redes. "*La mayoría de las veces son los mismos usuarios quienes autoinfligen su imagen, colocando en Internet información dañina o potencialmente peligrosa para ellos mismos, debido muchas veces a la ingenuidad o imprudencia, que sin medir los alcances que los actos puedan tener vean afectada su vida".*[57]

Uno de los riesgos presentes en las redes sociales precisamente en caso de menores de edad es el Grooming, *"término para describir la manera en que algunas personas se acercan a niños y jóvenes a través de plataformas sociales en internet y/o por medio de las TIC (Tecnologías de la comunicación e información), ganar su confianza creando lazos emocionales y poder abusar sexualmente de ellos posteriormente".*[58] Este tipo de criminalidad en las redes sociales busca obtener un beneficio de carácter sexual precisamente pidiendo imágenes o videos al menor (victima), también persigue alcanzar a tener un contacto real con la víctima y quizás abusar del mismo.

2.6 Hacking

Consiste en *"Recurrir a la manipulación de la conducta normal de un equipo y de los sistemas que tiene conectado".*[59] El hacker como se le denomina a la persona que realizar estas operaciones, es en principio un programador experto en manipular o modificar

[57] Góchez, Rafael Francisco. *"Los riesgos en las redes sociales virtuales".* 2009, Pág. 14.
[58] SVET, Secretaría contra la Violencia Sexual, Explotación y Trata de personas, Cuidado con el Grooming, Guatemala, S/a, disponibilidad y acceso: http://www.svet.gob.gt/campana/cuidado-con-el-grooming, fecha de consulta 26 de febrero de 2019.
[59] Avast, S/a, Avast Software S.R.O., Ciberdelito, Estados Unidos, 2015, disponibilidad y acceso: https://www.avast.com/es-es/c-cybercrime, fecha de consulta 10 de febrero de 2019.

sistemas o redes informáticas, este individuo por lo general posee acceso directo a la información de un sistema o red, pero por distintas razones este mismo manipula con herramientas de programación como virus, troyanos, rootkits y denegación de servicio de algún servidor conectado a la red la información para beneficios maliciosos. La diferencia entre un cracking y un hacking consiste en que el primero no posee acceso a los servidores o datos que pretende atacar por lo cual emplea herramientas totalmente distintas para lograr su objetivo rompiendo todos los filtros y medidas de seguridad de alguna red, ahora bien, el segundo si posee acceso directo a los datos o red al que ataca por lo cual solo emplea herramienta de manipulación de la información y no requiere de medios más sofisticados para romper la seguridad.

2.7 Cracking

"El término "cracking" hace referencia a la práctica que consiste en atacar sistemas informáticos y software con intención maliciosa".[60] Estos casos se dan cuando alguien con conocimientos específicos de programación, logra obtener las claves o contraseñas de usuarios de alguna red y con ello inicia una operación de interceptación de datos que circulan por ella.

2.8 Seguridad de red

"Conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propia y negarlo a terceros".[61] La ciberseguridad es una *"Rama de la seguridad de la información que trata de proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida".*[62] Hoy día uno de los activos más valiosos de cualquier empresa, profesional y personas en general es la información que posee, sea esta de cuentas de banco, información personal, clientes, etc. Esta misma en las manos equivocadas puede significar no solo problemas sino hasta la ruina para alguien que posea información sensible o clasificada con los que trabaja o simplemente desee tener en almacenamiento.

---

[60] *Loc. Cit.*
[61] *"Ciberfensa-ciberseguridad riesgos y amenzas".* Argentina, editorial Cari, 2013, Pág. 2.
[62] Escrivá Gascó, Gema y otros. *"Seguridad informática".* Editorial Macmillan, 2013, Pág. 7.

La ciberseguridad se compone de varias medidas y procedimientos que permiten proteger la información que se tenga, observando las características de integridad de la información que quiere decir que no se altere o cambie el contenido del archivo, la confidencialidad esto indica que solo las personas autorizadas se les dé acceso a la información para observarla, modificarla o extraerla, también existe la disponibilidad que quiere decir que se pueda tener facilidad de acceso a la información en el momento deseado y sin dificultades, atrasos o impedimentos. Sin embargo, la seguridad informática se divide en sentido de lo que se pretende proteger o asegurar.

2.8.1 Tipos de seguridad

2.8.1.1 Seguridad física

También denominado seguridad hardware, *"se asocia a la protección física del sistema ante amenazas como inundaciones, incendios, robos, etc"*[63] Se entiende como hardware a toda la parte física de un ordenador CPU, teclado, el monitor, etc. Entonces la seguridad física se encarga del cuidado de todos y cada uno de los elementos físicos de un sistema informático, esto desde el lugar donde cada uno de ellos se alojen sea esta una casa, edificio, cuarto, etc. Con frecuencia la seguridad física está destinada a evitar que cualquier agente externo pueda vulnerar el sistema, por ejemplo un incendio que pueda destruir todos los servidores o equipos, para lo cual se instala un sistema contra incendios en el lugar donde se alojen los equipos informáticos, algunas medidas de seguridad física son el uso de tarjetas para acceder a los cuartos donde están instalados los servidores, cámaras de vigilancia que permita ver quien ingresa a las instalaciones donde estén los equipos y recientemente se ha empezado a emplear el analizado de retina con el fin de identificar a todos los sujetos que pretendan ingresar al centro de alojamiento de todos los equipos computacionales.

2.8.1.2 Seguridad lógica

Se conoce también como seguridad software y *son "mecanismos que protegen la parte lógica de un sistema informático (datos, aplicaciones y sistemas operativos). Uno de los*

[63] *Loc. Cit.*

medios más utilizados es la criptografía".[64] Cualquier medida que se tome antes de acceder a un banco de datos o programa se considera seguridad lógica, debido a que tiene por fin identificar a los usuarios del sistema informático y si los mismos cuentan con autorización de acceder a los datos y de esa manera autenticar las credenciales del usuario mediante algún programa de seguridad instalado en el sistema, esta medida de seguridad afecta en concreto a todos los datos que se almacenan en los servidores o discos de almacenamiento, una formar de seguridad lógica común es el ingreso de nombre de usuario y contraseña en algún sistema como por ejemplo al momento de iniciar sesión en una computadora.

2.8.2 Medidas para la ciberseguridad

La ciberseguridad concepto en expansión y desarrollo en muchos estratos como social, familiar, educativo, científico, corporativo, económico, etc. Es un tema seriamente tratado por muchos motivos, ya que su incidencia en cada sección o área que se trate puede evitar graves desastres. Para abordar el tema de ciberseguridad es importante conocer que dicha actividad consiste básicamente en defender un sistema de computadoras o servidores del cual se abastece o depende el funcionamiento de muchos organismos, por tal motivo su aplicación ahora mismo es a numerosos elementos así también procura no solo proteger, sino evitar desastres y de suceder este establecer medios o métodos de recuperación, también aborda la sección de preparación para cada uno de los usuarios de la red como parte de la estrategia de una ciberseguridad completa. Son muchas las amenazas que cada día están latentes en las redes, pero hay algunas que sobre salen como *"el cibercrimen, que incluye actores individuales o grupos que dirigen ataques a sistemas para obtener ganancias financieras; la ciberguerra, que a menudo involucra recopilación de información con motivaciones políticas; y el ciberterrorismo, cuyo propósito es comprometer los sistemas electrónicos y causar pánico o temor".*[65]

---

[64] *Loc. Cit.*

[65] Kaspersky, AO Kaspersky Lab, Ciberseguridad, Estados Unidos, 2018, disponibilidad y acceso: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security, fecha de consulta 15 de julio de 2019.

Los medios o malware utilizados en los ciberataques tiene una razón y fin por el cual son elegidos para determinadas tareas por ejemplo un spyware, este elemento malicioso pretende infectar un ordenador o computadora con el fin de recopilar información que posteriormente puede ser medio de lucro para el creador del malware, vendiendo la información adquirida que en ocasiones puede ser de característica sensible o confidencial de una empresa en concreto donde se contenga descripciones de proyectos secretos o en desarrollo del cual la competencia pueda tomar ventaja; phishing otro elementos malicioso que pretende robar información pero en su mayoría de información personal como correo electrónico, contraseñas, nombre de usuarios, números de tarjeta, etc. Su expansión es muy frecuente a través de correos electrónicos con aparentemente origen legítimo.

Ante las amenazas que en las redes existen la ciberseguridad no es un problema únicamente de empresas, sino un tema que afecta a toda la población por tal motivo algunas medidas básicas para adoptar puede ser:

2.8.2.1 Confirmar la identidad de todo aquel que solicite información

"Un consejo especialmente útil para recepcionistas, empleados de 'call center' o soporte técnico, personal de recursos humanos y otros profesionales cuyo trabajo, de una u otra forma, requiera proporcionar datos en determinadas ocasiones. Los atacantes se aprovechan en muchas ocasiones de la ingenuidad o la buena fe de estos trabajadores para recabar información de la manera más sencilla y obvia: pidiéndola".[66] El modo más frecuente por el cual estos eventos suceden es aparentando la identidad de un cliente o miembro de la compañía, para ello es relevante establecer medios de registro y corroboración en el sistema de la empresa para así determinar la identidad inmediatamente al primer contacto con un desconocido.

2.8.2.2 Una buena contraseña

[66]Panda, Panda security, Diez consejos de ciberseguridad que toda empresa debería dar a sus empleados, España, 2016, disponibilidad y acceso: https://www.pandasecurity.com/spain/mediacenter/empresas/consejos-ciberseguridad-empleados/, fecha de consulta 15 de julio de 2019.

“Si con las claves que utilizamos para nuestras cuentas personales hay que tener ciertas precauciones presentes, con las que dan acceso a información corporativa todavía más”.[67] Lo más frecuente en las personas al momento de definir una contraseña es el uso de contraseñas con el nombre de su mascota, fecha de nacimiento, número de teléfono, nombre de la pareja o el propio, equipo de futbol favorito, etc. En principio son medidas básicas para evitar el olvido de este, pero para fines de seguridad es primordial la composición de una contraseña con diferentes combinaciones entre letras mayúsculas, minúsculas, números, símbolos. La observación que se da frecuentemente en situaciones cotidianas es escribir la contraseña en papeles o notas visibles al público y fácilmente robado.

2.8.2.3 La vulnerabilidad del disco duro

Es claro que día a día se maneja información de todo tipo, la sensibilidad de estos también es variada, en un sentido común todos esos datos son almacenados en el disco duro de la computadora cuando lo mejor es *“pedir a los empleados que almacenen los archivos en los servidores de la compañía – si los hubiera – o en algún servicio en la nube”*[68]*,* esto último es lo más recomendado ya que las empresas que brindan este tipo de servicios de alojamiento en la nube poseen más y mejores medios de seguridad ante ciberataques. Por otro lado, si la única opción de almacenamiento es en el disco duro del ordenador es mejor realizar copias de seguridad ante cualquier pérdida o inconveniente.

2.8.2.4 La copia de seguridad no es útil si se extravía a la vez.

“Si los trabajadores utilizan un portátil y realizan copias de seguridad en un pendrive, es fundamental que no los guarden ni transporten en el mismo sitio”.[69] Un ejemplo claro de este caso imprudencial es hacer una copia de toda la información en una memoria USB, luego esta misma trasportarla en una mochila junto con la computadora portátil y por cualquier razón esta resulte perdida, robada, olvidad, etc. Cualquiera que sea la situación, al final la información fue perdida y la copia de seguridad también.

---

[67] *Loc. Cit.*
[68] *Loc. Cit.*
[69] *Loc. Cit.*

2.8.2.5 No usar cualquier memoria USB

Es una situación muy frecuente que cuando se encuentra una memoria tirada en el suelo la primera acción a realizar sea conectar la memoria a una computadora y ver cuál es su contenido; *"una memoria USB puede ser peligrosa porque nunca se sabe lo que puede contener; puede ser malware capaz de causar graves daños a la red de tu empresa o a tu dispositivo físico".*[70]

2.8.2.6 Correo electrónico

Uno de las herramientas comúnmente utilizado por los ciber-atacantes sigue siendo el correo electrónico por lo que a través de él se puede obtener muchos beneficios en cuanto a información se trata, es frecuente el uso de un mismo correo electrónico para todas las actividades que se realizan en internet, así como las contraseñas, resulta práctico emplear la misma para todas las cuentas, dicha situación significa un alto riesgo tanto para la persona individual como para las empresas si el correo empleado, resulte ser de uso corporativo, lo que expondría no solo a la persona sino a la propia empresa de ser objetivo de un ciberataque.

2.8.2.7 No instalar programas de fuentes desconocidas

Es muy normal para el usuario común instalar programas o aplicaciones a los ordenadores descargados de cualquier página de internet o mediante un link proporcionado por una fuente externa y que redireccione a un alojamiento en la nube, por lo tanto, debe ser *"habitual que las empresas restrinjan la capacidad de sus trabajadores para instalar nuevos programas en sus ordenadores mediante los permisos del sistema operativo"*[71]*,* ya que al momento de ejecutar el instalador puede activar algún elemento malicioso en el sistema que posteriormente robe información y lo trasmita a un ciberdelincuente.

2.8.2.8 Cuidado con las redes sociales

---

[70] Kaspersky, AO Kaspersky Lab, Ciberseguridad, España, 2018, disponibilidad y acceso: https://www.kaspersky.es/blog/cybersecurity-tips-for-work/14744/, fecha de consulta 15 de julio de 2019.
[71] *Loc. Cit.*

Las redes sociales son por decir la principal fuente de comunicación de hoy día, ya sea por su accesibilidad, sencillez, comodidad, etc. Pero de ser los más y frecuentemente usados no existe duda, por tal razón el manejo de ellas debe ser cuidadoso y responsable porque desde allí puede brindarse gran información delicada y que puede exponer a cualquier persona a ser víctima de algún ciberataque e incluso de delincuencia común, algunas medidas básicas para tomar en consideración pueden ser evitar publicar fotografías con geolocalización, seleccionar quienes pueden ver la información del perfil, no hablar o establecer comunicación con extraños además de evitar facilitar información como lugar de residencia, ocupación, edad, centro de estudios, etc.

2.8.2.9 Un buen antivirus

Una decisión fundamental antes de conectar a internet cualquier dispositivo móvil como también un ordenador, esta medida es importante en situaciones domésticas aún más cuando los usuarios o los dispositivos también sean para uso corporativo, ya que los datos tanto de la organización como del usuario estarán allí vinculados. *"Una solución de seguridad para empresas protege los equipos y los datos de la organización en multitud de circunstancias, incluso cuando los empleados cometen un error o alguna imprudencia".*[72]

[72] Panda security. *Op. Cit., Consejo de ciberseguridad.*

CAPITULO III

3. LOS CIBERDELITOS

3.1 Definición

Este también recibe el nombre de delitos informáticos, consiste en todas aquellas actividades con fines delictivos desarrolladas a través de medios tecnológicos como las computadoras, internet, dispositivos móviles, etc. *"El ciberdelito puede hacer uso de diferentes métodos y herramientas, como el phishing, los virus, spyware, ransomware o la ingeniería social, normalmente con el objetivo de robar información personal o de realizar actividades fraudulentas"*[73]. Los ciberdelitos tienen numerosas formas de manifestarse, así como diferentes fines sin embargo de manera generalizada se señala dos categorías los recurrentes y los puntuales, el primero hace referencia a situaciones como la distribución de pornografía infantil, el ciberacoso, ciberterrorismo, por otro lado, el segundo indica aquellas acciones de instalación de virus que pretendan robar información puntualmente a una organización.

3.2 Ciberdelincuencia

Término acuñado para hacer referencia a los delincuentes o criminales que operan con objetivos ilícitos a través del ciberespacio, utilizando medios electrónicos y herramientas digitales para la comisión de dichos actos.

3.3 Características de los ciberdelitos

Los ciberdelitos como cualquier otro delito poseen elementos que lo distinguen de los demás entre ellos están: "*Que son conductas criminógenas de cuello blanco dado que solo algunos poseen los conocimiento para cometerlos, son acciones ocupacionales, son acciones de oportunidad, provocan seria pérdidas económicas, ofrecen facilidad de tiempo y espacio, son sumamente sofisticados y relativamente frecuentes en el ámbito militar, presenta grandes dificultades para su comprobación, son imprudencias y no necesariamente intencional, ofrece facilidad de comisión por menores de edad, prolíferas*

[73] Avast, S/a, Avast Software S.R.O., Ciberdelito, Estados Unidos, 2015, disponibilidad y acceso: https://www.avast.com/es-es/c-cybercrime, fecha de consulta 10 de febrero de 2019.

cada vez más, muchos aún son impunes".[74] Hay varios delitos informáticos que aún no son perseguidos penalmente, en muchos países aun no cuentan con una tipificación legal vigente sobre esta naturaleza de hechos delictivos, por lo cual a pesar de que estas acciones ilícitas provocan y dañan muchos de los bienes jurídicos tutelados, no pueden ser procesados o los casos conocidos no prosperan y quedan en la impunidad, por lo cual coadyuva al crecimiento e intromisión cada día más de este tipo de criminalidad en la comunidad digital.

3.4 Clasificación de los ciberdelitos

Los ciberdelitos por su naturaleza dinámica es imposible determinar una clasificación en concreto de sus tipos, sin embargo, el Doctor Santiago Acurio Del Pino, ha hecho una clasificación de ellos, los cuales son: *"Los fraudes, el sabotaje informático, el espionaje informático y el robo o hurto de software, robo de servicios, acceso no autorizado a servicios informáticos".*[75] De dicha clasificación existe una subdivisión más específica de las modalidades en que estos ciberdelitos se manifiestan y los objetos sobre el cual recae su efecto al momento de ser ejecutados, algunos de ellos pueden ser sobre bancos, cuentas bancarias, sistemas de control interno en empresas privadas, tarjetas de crédito y débito, robo de identidad comercial, etc. Todos ellos provocando una afección a distintos bienes o recursos.

3.5 El delito

"Acción u omisión voluntaria, típica, antijuridica y culpable"[76]*. "Delito es aquello que la ley describe como tal, toda conducta que el legislador sanciona con una pena".*[77] *"Infracción de la ley del Estado, promulgada para proteger la seguridad de los ciudadanos, y que resulta de un acto externo del hombre, positivo o negativo, moralmente imputable y socialmente dañoso"*[78]*.* El delito es una conducta que quebranta y transgrede a una

[74] Téllez Valdés, Julio. *"Delitos cibernéticos".* México, editorial UNAM, 2008, Pág. 113.
[75] Acurio Del Pino, Santiago. *"Delitos informáticos".* Ecuador, Pág. 22.
[76] Girón Palles, José Gustavo. *"Teoría del delito".* Guatemala, editorial Instituto de la Defensa Pública Penal, 2da. Edición. 2013, Pág. 3,
[77] González Cauhapé, Eduardo. *"Apuntes de derecho penal guatemalteco".* Guatemala, 2003, pág. 27.
[78] Castro Cuenca, Carlos Guillermo. *"Manual de teoría del delito"*. Colombia, editorial Universidad del Rosario, 2017, página 53.

norma legal, las normas legales contienen todas aquellas libertades, derechos, obligaciones y límites que cada una de las personas poseen, ahora bien, en caso de que una sujeto no cumpla alguna de ellas, por ejemplo, darle muerte a un individuo es una acción sancionada con prisión según el código penal guatemalteco, por lo cual toda persona que le diere muerte a otra será sancionada con una pena, que pretende castigar la conducta desviada ante la sociedad.

3.6 Íter críminis

"Consiste en una serie de etapas que van desde la idea criminal y la selección de los medios, hasta la ejecución y el agotamiento, el cual tiene dos fases una interna y otra externa".[79] Es importante considerar que por sí sola una idea no puede ser sancionada o perseguida penalmente, sin embargo, si esta es exteriorizada y causa un daño o se convierte en una acción en concreto, puede ser sancionada toda vez que produce una consecuencia visible, vulnera derechos y quebranta normas legales. Cada fase que atraviesa el delito representa diferencias relevantes y por supuesto el quebrantamiento de un cierto orden establecido de tipo ético-social, todas las fases que el íter críminis atraviesa son en su mayoría en un solo sujeto que puede calificarse como el autor del hecho; por otro lado cuando la legislación describe o tipifica determinado delito lo hace en sentido consumado, es decir que los hechos son sancionadas desde el punto de vista jurídico cuando ya se haya producido una consecuencia visible. Otra observación importante en el íter críminis es que solo se supone o se cumple con él, cuando se trata de delitos dolosos, porque se sobreentiende y determina la existencia de premeditación para la comisión del hecho ilícito.

3.6.1 Etapa interna del delito

Esta etapa se comprende desde la concepción de la idea de ejecutar determinado hecho, todo sucede en la mente del sujeto activo, desde esta etapa la voluntad de la persona para realizar determinada conducta criminal ya es manifiesta, en pocas palabras de esta etapa se origina el dolo, porque la idea ya se tiene, se delibera en la mente del sujeto el

[79] Girón Palles, José Gustavo. *"Teoría del delito".* Guatemala, editorial Defensa Pública Penal, 2013, Pág. 115.

motivo para realizar el hecho y por último se determina o se toma la decisión en base a la deliberación anteriormente resuelta, la determinación de los medios para la comisión del hecho es el siguiente paso que el sujeto activo realiza.

3.6.2 Etapa externa del delito

Esta etapa se da con la manifestación objetiva de la idea delictiva y con el empleo de los medios necesarios y seleccionados para alcanzar el fin; una persona ya puede ser sancionada penalmente desde esta etapa, sin embargo, la sanción o penalización del acto no necesariamente debe ser en el momento que se perciba una consecuencia física o se haya consumado el hecho en tu totalidad, sino puede darse el caso de una tentativa lo cual interrumpiría la consumación del acto criminal en su totalidad, sin embargo, la manifestación de la intención es evidentemente de origen criminal.

3.7 Cibercrimen

Un crimen describe la acción que una determinada persona ejecuta con fines ilícitos o quebrantando una norma legal estipulada, concretamente todo acto cometido por un sujeto que este en contra de las leyes es un crimen. Para el ámbito informático la denominación de las acciones ilícitas es cibercrimen, que corresponde a cualquier conducta contra la ley en materia informática, la persona que quebrante alguna legislación, dañando a su vez el derecho y bien jurídico tutelado de otra es considerado criminal. Ahora bien, es de resaltar que entre crimen y delito se determina una leve diferencia en cuanto al impacto que el hecho mismo posee, es decir que delito es atribuido a hechos con menos impacto o gravedad, el crimen es considerado en casos de alto nivel en cuanto a gravedad. Por tal motivo las acciones delictivas en el ciberespacio son consideradas crimen por cuestiones de impacto que genera en las víctimas, así como lo "*señala la última asamblea general de la Organización Internacional de Policial Criminal (Interpol) donde se dio a conocer que son casi 170 millones de ciberdelitos los que se cometen por año en todo el mundo y que provocan un impacto económico que supera los 445,000 millones de dólares"*[80], que por sí mismo la cantidad es alarmante, por tal

[80] Télam, Telenoticiosa América, Ciberdelitos: ¿Cómo pueden afectarnos?, Argentina, 2017, disponibilidad y acceso: http://www.telam.com.ar/notas/201711/223623-ciberdelitos.html, fecha de consulta 16 de julio de 2019.

motivo y la expansión cada vez más, de este tipo de hechos criminales el cibercrimen es considerado una situación de alto impacto.

3.7.1 Cibercriminal

Denominación otorgada para aquel sujeto que realiza conducta susceptible de delito a través de medios tecnológicos. Un cibercriminal es un individuo que aprovechando las vulnerabilidades de un sistema ejecuta actos característicamente criminales o quebrantando la ley, entre ellos se menciona el robo de información, ciberterrorismo, robo de identidad, falsificación de información digitalizada, etc. Es relevante señalar que entre hacker y cibercriminal existe una diferencia clara y es que el primero pretende mejorar las medidas de seguridad que una red tiene o también encontrar vulnerabilidades y de allí partir y adoptar estrategia y métodos de seguridad a esta actividad se le conoce como hacking ético, por el contrario, el cibercriminal o cracker otra forma de denominación de este tipo de criminales, ellos buscan vulnerabilidades no con el fin de garantizar o mejorar la privacidad, seguridad de los usuarios de una red sino para realizar ciberataques y así obtener beneficios propios o de terceros mediante el resultado del ataque.

3.7.2 Perfil del cibercriminal

Para hacer referencia a los delincuentes informáticos es esencial priorizar los aspectos que componen el perfil de estos en sentido del conocimiento que poseen, los recursos con que cuentan, autoridad o acceso que ostentan, los motivos que los impulsa a realizar los ilícitos en los medios informáticos. Las personas que cometen delitos informáticos tienen una característica particular que los diferencia de la delincuencia común y es que poseen *"habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos"*[81], la consideración de la posición, conocimiento, recursos que la ciberdelincuentes poseen es clave al momento de realizar cierto hechos donde de otro modo no podría ser ejecutado, tomando en cuenta que la motivación no

[81] Acurio Del Pino, Santiago*. Op. Cit.,* Pág.15.

puede ser únicamente económica sino político, terrorista, etc. Se ha conocido que los intrusos o ciber atacantes son atribuidos en una gran cantidad de veces a los mismos empleados de las compañías es decir son agentes interiores y las cifras de atacantes externos es relativamente inferior.

A modo de análisis, la causa de este tipo de criminalidad no se puede determinar por algunos interesantes aspectos a la motivación de la comisión del delito, ya que en este tipo de criminalidad no se puede suponer una carencia de recursos económicos, poca inteligencia, clase social o falta de educación, porque los sujetos autores de este tipo de criminalidad cibernética, son por lo general pertenecientes a un nivel socioeconómico alto, es entonces donde el establecimiento de dicha conducta ilícita es impulsada por otros factores como la reputación o el honor del cibercriminal en el ciberespacio o comunidad internauta.

3.8 Los delitos informáticos en la legislación guatemalteca

Los delitos informáticos no son un caso omiso en Guatemala, aun siendo un país con desarrollo tecnológico atrasado, las acciones criminales en las tecnologías existentes ya son evidentes, la vulnerabilidad del país en torno al tema de criminalidad cibernética es total, debido a la escasa regulación que se posee sobre este asunto. Guatemala ya posee una estrategia de seguridad sobre asuntos digitales pero aún carece de una sólida fundamentación debido a que la legislación vigente en torno a delitos informáticos es únicamente lo contenido en los artículos 274 “A” hasta el artículo 274 “H” del código penal decreto 17-73 del Congreso de la República de Guatemala, en dichos artículos se contienen presupuestos sobre destrucción de registros informáticos, alteración de programas, reproducción de instrucciones o programas de computación, registros prohibidos, manipulación de información, uso de información, programas destructivos y alteración maliciosa de número de origen, dichos presupuestos son casi inefectivos en el combate de la criminalidad digital, al mismo tiempo que la diversidad de ciberdelitos es basta que no puede ser cubierta y sancionada en su totalidad; las modalidades más frecuentes de ciberdelitos en el país *“son las estafas y los ransomware o secuestro de la información, en donde la encriptan para que la víctima pague por recuperarla. Otra*

modalidad frecuente de ataque es la clonación o suplantación, mediante la cual hackers toman la información de un sitio y la hacen aparecer en otro, ya sea distorsionada o alterada, para confundir a los usuarios".[82]

La carencia de cobertura jurídica específica sobre la modalidad delictual cibernética es un caso de abordaje en las políticas de seguridad, por el gran impacto que tiene en las diversas esferas sociales, sobre todo en la económica y estatal en sus diversos organismos que lo integran, ya que varios de los informes emitidos por entidades internaciones que han realizado estudios sobre ciberseguridad asumen que del cien por ciento de ataques maliciosos que se realizan a través de internet un porcentaje importante como del setenta por ciento, son dirigidos hacia entidades de gobierno y bancos, en Centro América sobre todo y de manera generalizada ocupa el lugar con mayor vulneración ante ciberataques debido que la mayoría países son considerados aún, espacios vírgenes y sin protección ante la criminalidad digital, por tal motivo la proliferación de esta criminalidad va en aumento silenciosamente, ya que muchos de los países carecen de organismos específicos sobre la vigilancia o control del ciber espacio y en el caso de Guatemala la ausencia de una regulación legal especifica en delitos informáticos.

Las políticas de privacidad y protección de datos es uno de los temas relativamente importantes abordar mediante planes de seguridad nacional en Guatemala, esto haciendo alusión a lo establecido en el artículo segundo de la Constitución Política de la República de Guatemala donde el Estado otorga la garantía y es obligado a brindar a cada uno de los habitantes la seguridad, por lo tanto la legislación en torno a temas cibernéticos debe ser considerada como un espacio más de cobertura del Estado en cumplimiento a la estipulación legal mencionada; el ministerio de gobernación (MINGOB) a través del viceministerio de tecnología ha señalado que el país *"cuenta con bases sólidas para alcanzar los objetivos en la lucha contra este delito, y que nuestro país cuenta con una estrategia nacional de seguridad cibernética, además de un centro contra*

[82] Prensa Libre, Muñoz Palala Geldi, No hay ley contra los ciberataques, Guatemala, 2016, disponibilidad y acceso: https://www.prensalibre.com/guatemala/comunitario/no-hay-ley-contra-los-ciberataques/, fecha de consulta 22 de agosto de 2019.

incidentes informáticos"[83]*,* la importancia de detallar un fundamento legal sobre esta modalidad de delitos con observación del convenio de Budapest es preeminente, porque de esa manera se obtendrá una legislación de calidad internacional o con menos vacíos legales aprovechables por la delincuencia cibernética.

3.9 Iniciativa de ley 5601: Ley de prevención y protección contra la ciberdelincuencia

El Estado como ente supremo sobre los habitantes del país otorga derechos, obligaciones y garantías a las personas, de esta última derivan una serie de tareas y deberes que por ley deben ser cumplidas, entre dichas atribuciones se encuentra la seguridad tal y como lo indica el Congreso de la República de Guatemala en la Constitución Política de la República de Guatemala, artículo 2 *"es deber del Estado garantizarle a los habitantes de la república, la vida, la libertad, la justicia, la seguridad, la paz y el desarrollo integral de la persona"*, de esta cuenta es imprescindible conceptualizar la seguridad en todos sus entornos, sin excepción del ciberespacio. La justicia y el desarrollo integral de cada una de las personas, la garantía de confianza del usuario al emplear cada una de los servicios de internet, el derecho a la privacidad es otorgada a cada uno conforme a las diferentes determinaciones legales básicas para todas las personas, ante dichos antecedentes el Estado de Guatemala se encuentra obligado a darle cumplimiento pleno a cada uno de los derechos y garantías mediante la creación de instrumentos jurídicos, que promuevan la justicia, equidad y bien común, velando la protección ante amenazas o violaciones del Estado de derecho.

En la proposición de ley contra delitos informáticos, se introducen figuras penales que buscan establecer y encuadrar las conductas que vulneran diferentes bienes jurídicos tutelados a través de hechos ejecutados en el ciberespacio, las normas penales son herramientas para que los órganos competentes de administración de justicia sancionen y hagan valer cada una de las leyes, además otorga al Estado mismo, la vía de cooperación internacional en materia de persecución y sanción de los delitos de origen

[83] Portal electrónico del Diario de Centro América, López Yuri, Mesa técnica analiza proyecto de ley contra ciberdelincuencia, Guatemala, 2019, disponibilidad y acceso: https://dca.gob.gt/noticias-guatemala-diario-centro-america/mesa-tecnica-analiza-proyecto-de-ley-contra-la-ciberdelincuencia/, fecha de consulta 27 de agosto de 2019.

informático. La iniciativa 5601 establece figuras delictivas nuevas para el derecho penal existente, así mismo facilita la adecuación de las normas vigentes a hechos ilícitos de carácter electrónico-digital, en consideración del derecho se establece también reglas procesales específicas para la persecución penal de los injustos informáticos; en este ámbito se determina la inclusión de las pruebas digitales y electrónicas, de la misma manera la creación de un órgano encargado de la vigilancia del ciberespacio será posible con la aplicación de la normativa, así como se señaló anteriormente el mantenimiento de un Estado de derecho e inviolabilidad de los bienes jurídicos tutelados como los datos personales, intimidad informática, indemnidad sexual de las niñas, niños y adolescentes, integridad y disponibilidad de la información, bienes activos y pasivos de las personas físicas y jurídicas.

La aplicación de las normas penales son de carácter extensivo a fin de adecuar la figura de persona jurídica o física posiblemente vinculada a la comisión de diferentes hechos ilícitos o deshonestos a través de los espacios cibernéticos como también la conexión de personas nacionales y extranjeras; la iniciativa de ley de prevención y protección contra la ciberdelincuencia encuadra elementos tales como la responsabilidad de las personas jurídicas y sus representantes, así mismo define la atribución de la investigación al Ministerio Público con la asistencia de la Policía Nacional Civil y el Institución Nacional de Ciencias Forenses, la conformación de una equipo de respuesta ante incidentes informáticos se figura también dentro de la norma en cuestión, este último fungiría la tarea de interceptación de información y comunicación de posibles criminales, la protección de datos y sistemas será su atribución, evitando la falsificación informática y la apropiación indebida de identidad.

Engloba así mismo la figura sobre ciberdelitos contra las personas y los menores de edad, estableciendo figuras delictuales especificas relacionados con el abuso infantil, acoso por medios electrónicos o ciberacoso, engaño pederasta, propiedad intelectual y las formas o medios para la reparación civil del daño ocasionado, de la misma forma la incorporación de las penas como la consecuencia jurídica de la falta al presupuesto penal tipificado en dicha ley penal especial; el punto focal o principal sobre el tema informático en Guatemala radica en la seguridad sobre los datos personales en internet y no solo a nivel particular

sino también corporativo, la iniciativa en cuestión pretende crear dentro de la organización estatal un grupo denominado CSIRT-GT que no es más que un centro de seguridad interinstitucional de respuesta técnica ante incidentes informáticos, como normativa nueva para el derecho penal nacional, se ha comprendido también las reglas procesales del cual se regirán las medidas cautelares, procesales y procedimentales de los delitos que tengas la naturaleza cibernética. La incorporación de una organización especifica en temas de control internauta a través del CSIRT-GT hará la función de alerta permanente con la facilidad de reacción en hechos susceptibles de delito ocurridos en cualquier momento, dentro de cada una de las instituciones conceptualizadas se indica la cooperación en materia de extradición y la posible creación de un tribunal especial para el procesamiento de casos informáticos.

3.10 El phishing

El término phishing en su traducción original del inglés significa pescar, ya que el modus operandi de este tipo delincuencia es realizar ataques o envíos masivos de material engañoso esperando que las víctimas distraídas o con desconocimiento sobre esta modalidad de delincuente caiga en la trampa de los phishers denominación común hecha a los delincuentes o personas que realizan estas prácticas deshonestas a través de diferentes medios electrónico-digital, con el fin de sustraer información privada. *"El phishing es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias".*[84]

Cuando el phishing se da, los mensajes que aparecen simulan tener origen legítimo de las páginas por ejemplo un banco, agencia de viaje, empresa, etc. Sin embargo, lo que busca es solamente dirigir a la víctima a una página falsa donde introduzca datos como nombre de usuario, contraseña, número de tarjeta, información personal, etc. Todo tipo de información que posteriormente pueda ser utilizado por el cibercriminal. La ingeniera de este tipo de ataques es de códigos maliciosos que aprovechan las fallas o vulnerabilidades en los sistemas de seguridad y precaución de los usuarios, hay situaciones donde la forma de ataque no es directa y en esa modalidad de ataque es

[84] Avast, *Op. Cit.*, phishing.

donde los banners o publicidad falsa redirecciona al usuario a otra página donde se proporcione la información confidencial y de allí hacer caer a la víctima en el engaño.

En el país son muchos los crímenes de naturaleza informática, de los que se pueden mencionar la sustracción ilícita de información, datos bancarios, contraseñas, distribución de material pornográfico a través de internet, etc. De estos muchos no pueden ser investigados debido a la carencia de una legislación que los tipifique como delitos, aun considerando que muchos de los bienes jurídicos tutelados indicados en la constitución son vulnerados con la ejecución de este tipo de hechos criminales a través de las plataformas digitales.

3.10.1. Clasificación del phishing

3.10.1.1 Phishing clonado

Este tipo de engaño cibernético es generalmente conocido como phishing tradicional ya que este es el método de operación más clásica de los cibercriminales que pretenden robar información, suplantando o clonando páginas web legitimas donde la víctima es engañada para que facilite sus datos confidenciales; la forma más común en que este tipo de engaño se manifiesta es a través de mensajes al correo electrónico de las víctimas y estas solicitan directamente datos como contraseñas, numero de cuentas bancarias o números de tarjetas, etc. La denominación de clonado es porque este tipo de phishing mediante sus envíos masivos de emails busca interpretar el origen de una entidad real como un banco, universidad, empresa, etc. Pero al final resulta ser un total engaño realizado por un deshonesto programador o informático.

3.10.1.2 Phishing basado en páginas web o malware

Esta modalidad de engaño cibernético o ataque se da de manera indirecta al usuario, porque suele manifestarse mediante banner o anuncios llamativos, como el típico anuncio de ser el usuario número un millón y que se ha ganado un premio, el cual invita a hacer clic en el anuncio para cobrar el premio y este redirecciona a otra página web aparentando ser legítimo, al estar en la página web solicita nombre, numero de documento de identificación, número de tarjeta o número de teléfono, etc. Información

básica que al final suele ser usado para fines ilegítimos o ilegales, esta modalidad de engaño también se manifiesta en correos electrónicos con el mismo objetivo enviar links con intenciones maliciosas que al acceder a ellos dirige al usuario a una página extraña pero lo que no sabe es que al mismo tiempo se realiza la descarga de un programa malicioso el cual pretende sustraer la información del usuario en el dispositivo que este en uso sea este computador, teléfono celular, Tablet, etc. Y enviárselo al cibercriminal detrás de la operación.

3.10.1.3 Pharming

"El pharming, una combinación de los términos "phishing" y "farming", es un tipo de cibercrimen muy semejante al phishing, en el que el tráfico de un sitio web es manipulado para permitir el robo de información confidencial"[85] Este tipo de ataque informático consiste en alterar los archivos host de un servidor es decir que altera la conexión de los computadores que solicitan conexión con un servidor especifico al momento de ingresar la dirección de una página web, esta operación lleva al usuario a otra maquina distinta a la original o autentica y desde allí aparenta ser la página legitima sin embargo es una copia autentica de la original con ciertas alteraciones que pretenden obtener la información del usuario.

Esta clase de operación suele ser considerados de alta peligrosidad ya que puede hacer victima a una maquina con todas las seguridades posibles, existen dos formas en que este ciberdelito se manifiesta *"en la primera, los hackers utilizan diferentes métodos para instalar virus u otro malware en el equipo del usuario. A continuación, este virus redirige su equipo del sitio que desea visitar (como su banco o un sitio de comercio electrónico) para llevarlo a otro que, aunque es en apariencia exactamente igual, resulta ser falso. La segunda forma de pharming es la que hace este tipo de ciberdelito especialmente*

[85] Kaspersky, AO Kaspersky Lab, Ques es el pharming y como evitarlo, España, disponibilidad y acceso: https://latam.kaspersky.com/resource-center/definitions/pharming, fecha de consulta 7 de septiembre de 2019.

peligroso. Consiste en que un ciberdelincuente infecta todo el servidor DNS, de forma que todos los usuarios que intentan acceder a él son redirigidos al sitio web falso"[86]*.*

3.10.1.4 Smishing

"Smishing es una palabra compuesta por "SMS" (servicios de mensajes cortos, más conocidos como mensajes de texto) y "phishing". Cuando los cibercriminales hacen "phishing", envían correos electrónicos fraudulentos que intentan engañar al destinatario para que abra un archivo adjunto cargado de malware o haga clic en un enlace malicioso. El smishing simplemente utiliza mensajes de texto en lugar de correo electrónico"[87]

Este tipo de fraude fue uno de los métodos más usados hace varios años atrás, por motivos que la mayoría de la población del mundo aun no poseían acceso a internet y los teléfonos inteligentes con aplicaciones de redes sociales no eran lo que hoy se conoce; hoy dia esta técnica de robo de información ha tenido un cierto cambio porque ya no opera mediante mensajes de texto directo a los teléfonos, sino que a migrado a las redes sociales como WhatsApp, Messenger, etc. Donde se envían mensajes indicando que la aplicación que el usuario esté usando sufrirá cambios, se borrará cuentas de no ser atendido el mensaje o en ocasiones solicita a los usuarios acceder y confirmar su identidad en un link que regularmente acompaña al mensaje y desde allí solicita el número de teléfono, correo electrónico, nombre completo, contraseñas, etc. Con el fin de robar la información del usuario, como ejemplo de estos casos, son los mensajes que suelen hacerse viral en WhatsApp indicando que el servicio empezará a ser de paga a partir de cierta fecha y de no ser atendido el mensaje con la confirmación o descarga de cierto "actualización" la cuenta será anulada, es entonces como se identifica la actual y más reciente modalidad operativa del smishing. La manera mejor manera de protegerse ante este tipo de acción criminal es ignorar los mensajes que se reciban, o verificar mediante otras fuentes oficiales la veracidad del aviso que se reciba.

3.10.1.5 Vishing

[86] Avast, Avast Software S.R.O., Pharming, Estados Unidos, 2015, disponibilidad y acceso: https://www.avast.com/es-es/c-pharming, fecha de consulta 9 de septiembre de 2019.
[87] Kaspersky*. Op. Cit.*, Smishing.

"El término deriva de la unión de dos palabras: 'voice' y 'phishing' y se refiere al tipo de amenaza que combina una llamada telefónica fraudulenta con información previamente obtenida desde internet"[88], este método de robo de datos personales sucede cuando el ciberdelincuente ya ha obtenido información de la víctima por el cual pretende convencer al individuo para que facilite contraseña o números de cuenta el cual podrían ser usado para acceder a cuentas bancarias online y desde allí realizar trasferencias y vaciar la cuenta de la víctima. El modo de persuadir del delincuente mediante esta técnica es indicando al usuario que se ha detectado anomalías en su cuenta bancaria por el cual se requiere la verificación de datos personales como número de cuenta, nombre completo, número de tarjeta y contraseña en fin los datos personales del individuo.

La confianza de muchos de los usuarios en los bancos no suelen dudar de este tipo de llamadas, omitiendo la atención a la capacidad que pueden llegar a poseer los estafadores o ciberdelincuentes de acceder a medios electrónicos o voz digitalizada que hace llamadas desde cualquier parte del mundo y busca engañar a las personas; las consecuencias de este tipo de cibercriminales son realmente graves de no ser consideradas con el debido cuidado ya que puede hacer que una persona pierda los ahorros bancarios de toda una vida.

3.10.2 Consecuencias del phishing

Como se ha indicado en cada una de las modalidades del phishing el principal fin de todos es el robo de información personal de los usuarios de internet; las consecuencias de un ataque de phishing presentan una de las pérdidas más altas y costosas en varios sentidos no precisamente económico. Años atrás se había señalado la existencia de dos tipologías generales del phishing orientadas a un nicho internauta puntual y específico que son los consumidores y las empresas, el primero de ellos se da por medio de ataques individuales, es decir a ciertas personas, específicamente a los que poseen un perfil económico relevante o personalidad electrónica constante que provea del ambiente esencial para que el phisher realice actividades ilícitas como los mencionados anteriormente, últimamente el phishing ha ido mutando un nuevo uso y es para el lavado

[88] BBVA, Castillo Claudia, phishing, vishing, mishing, ¿que son y como protegerse de estas amenazas?, España, 2018, disponibilidad y acceso: https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/, fecha de consulta 9 de septiembre de 2019.

de dinero a través de cuentas o identidades electrónicas robadas, está claro que muchas de las personas al ser empleadas sus cuentas para operaciones sospechosas son sujetas a procesos penales o problemas judiciales donde enfrentan cargos que realmente desconocen el origen, ya que en su mayoría no saben que su información privada había sido empleado para cometer ilícitos; más recientemente los delincuentes se han dado cuenta que hay más que ganar con un ataque a una empresa o corporación que con un ataque individual, aprovechando el anonimato que internet provee, los ciber delincuentes ven una oportunidad amplia de conseguir más beneficios por lo cual la tendencia de ataque se ha ido inclinando en una cifra más alta a empresas y organizaciones comerciales que emplean bancos de datos digitales el cual son susceptibles de ser sustraídos y posteriormente empleadas para distintas operaciones que solo producen regalías al ciberdelincuente.

De las consecuencias que produce el ataque de phishing a nivel empresarial, es el costo de la violación, es decir el riesgo en que se pone todos los datos e información de la empresa al momento del ataque desemboca una serie de gastos para recuperar la seguridad y desde luego garantizar que en una futuro no vuelva a suceder otro ataque, esto mismo incurre en la compra de un nuevo y mejorado equipamiento además de la contratación de un personal especializado en ciberseguridad, el daño reputación es otra consecuencia que implica para las empresas el ataque de phishing, tomando como ejemplo los bancos, instituciones donde las personas confían sus activos financieros que de darse a conocer un ataque podría provocar una alarma que por demás esta indicar traería consigo la perdida de una gran cantidad de clientes y la reputación dañada de la institución con la desconfianza y una percepción negativa de la marca en un futuro, la pérdida de propiedad intelectual es una consecuencia también, porque cuando se realiza el ataque muchos de los proyectos que las empresas estén desarrollando se ven comprometidos a ser sustraídos por otras personas o empresas en una competencias desleal y que podría concluir en la patente de productos con un valor fácilmente descrito en millones y posiblemente la perdida de años de investigación y desarrollo; los costos directos que un ataque de robo de información provocan son realmente importantes además de las penalizaciones que muchas empresas reciben por parte de los entes

reguladores de internet por no proveer a sus usuarios la seguridad adecuada en resguardo de los datos sensibles que determinada compañía podría manejar de sus clientes por eso mismo *"las empresas estadounidenses gastan alrededor de $ 12.6 millones en el ataque de cibercrimen promedio. Suplantación de identidad y la ingeniería social representan el 13% del costo anual del delito cibernético para las empresas"*[89], por eso la toma de una serie de pasos contundentes para ciberseguridad es relevante para toda empresa que se desarrolle en ámbito digital actual.

3.10.3 Phishing en Guatemala

Se han registrado acontecimientos cibercriminales en Guatemala, precisamente en instituciones financieras nacionales, pero han sido mantenidos en reserva por varios motivos, dichas instituciones son reconocidas y frecuentemente recurridas por las personas, por tal motivo el informe de dichos casos ha sido por medios no oficiales y posteriormente confirmadas por los gerentes y representantes de las instituciones financieras.

En el año dos mil once miles de usuarios habían estado recibiendo en los últimos días y semanas correos electrónicos donde solicitaba la confirmación de datos de identidad y contraseñas de la banca en línea, algunos lograron ser engañados y al realizar llamadas a las instituciones financieras inmediatamente se bloquearon las cuentas de dichos usuarios para evitar consecuencias más graves, algunos clientes fueron vaciadas sus cuentas en su totalidad, posteriormente los gerentes del Banco Banrural y Banco Industrial se pronunciaron indicando que se habían tomado medidas de seguridad para que dichos eventos no sucedieran nuevamente y se acordó en conjunto con todos los demás bancos la formulación de estrategias y filtros anti phishing, aun consideradas dichas acciones para evitar ataques futuros los ejecutivos de las instituciones mencionadas indicaron *"uno de los problemas es que no está tipificado el fraude cibernético en la legislación nacional y que no se cuenta con la tecnología para dar con los estafadores. Según De León, a pesar de que en el Congreso aún se discute una iniciativa de ley sobre el tema de delito cibernético, el Código Penal en su Artículo 274*

[89] Vade Secure, Gendren Andrien, Impacto corporativo del phishing, 2015, disponibilidad y acceso: https://www.vadesecure.com/en/the-corporate-impact-of-phishing/, fecha de consulta 2 de octubre de 2019.

reconoce violaciones a los Registros Prohibidos, Manipulación de Información y uso indebido de la misma, las cuales contemplan penas de 6 meses a 5 años de prisión, así como multas monetarias"[90]*,* dichas estipulación legal fue en algunos casos el medio para la resolución y reparación el daño ocasionado a los clientes de los bancos atacados, a dichos actos las instituciones bancarias fueron los que respondieron para la reposición de los fondos sustraídos.

Así mismo en el año dos mil siete la página web del Congreso de la República de Guatemala, había sufrido un ataque del cual se realizó la respectiva denuncia ante el MP como ente encargado de realiza la persecución penal del ilícito, pero este hecho quedó en investigación y no se logró establecer el origen del ataque; en el año dos mil ocho un usuario del banco Uno, indicó mediante haber recibido un correo electrónico donde se le solicitaba información sobre datos de cuenta bancaria y datos generales de identificación, pero el navegador de la computadora no dejaba al mismo abrir el link y realizar dicha confirmación por lo cual se le notifico por parte del banco que dicha confirmación no había sido enviada por la institución, de esa forma se evidencio el ataque phishing.

Del caso phishing más reciente fue en el año dos mil quince donde a uno de los periódicos más importantes del país denominados Prensa Libre, se le clonó la información en sus publicaciones mediante el uso de un dominio similar al empleado por la institución pero fue detectado por la variación en su dirección web de www.prensalibre.com y la pagina clonada como www.prensallibre.com, se realizó la investigación correspondiente obteniendo como responsable a Héctor Mauricio Rodríguez y con los *"datos de la investigación, hecha por expertos en informática, Rodríguez reside en San Salvador, en la colonia Manzano, calle Villanova, pasaje 1"*[91]*,* seguidamente se determinó por los investigadores que el hecho era perteneciente a phishing y se procedió al informe correspondiente al MP.

[90] Summa, Usuarios de banca en línea de Guatemala sufren intentos de phishing, Costa Rica, 2011, disponibilidad y acceso: https://revistasumma.com/13674/, fecha de consulta 2 de octubre de 2019.
[91] Prensa Libre, Redacción, Identificado autor de falsificación de sitio de Prensa Libre, Guatemala, 2015, disponibilidad y acceso: https://www.prensalibre.com/guatemala/justicia/identificado-autor-de-falsificacion-de-sitio/, fecha de consulta 2 de octubre de 2019.

3.11 Grooming

El tema de internet aún no se le ha otorgado la responsabilidad y alcances que puede llegar a tener, especialmente por todos los atractivos modernos como las redes sociales, que dan a los más jóvenes una ventana al mundo, el hecho de conocer nuevas personas o "hacer nuevas amistades" es un gancho poderoso para los menores; desde el momento que se realiza un registro en internet o red social es casi imposible borrar o hacer desaparecer los datos, porque de cualquier forma quedan registros en alguna parte aunque el usuario borre el contenido original siempre existirá una copia, de todo eso, el riesgo mayor se presenta a los usuarios más desprevenidos, inexpertos y distraídos en sentido de lo que publican en las redes y estos son los niños, adolescentes y jóvenes.

La advertencia y concientización es especialmente relevante al momento de iniciar el uso de alguna red social de manera puntual en los niños y adolescentes ya que suelen ser más despreocupados y curiosos al momento de establecer una amistad con algún desconocido; en las redes sociales existen máscaras que ocultan la identidad de todos y de allí es donde se origina el fenómeno llamado grooming, *"término para describir la manera en que algunas personas se acercan a niños y jóvenes a través de plataformas sociales en internet y/o por medio de las TIC (Tecnologías de la comunicación e información), para ganar su confianza creando lazos emocionales y poder abusar sexualmente de ellos posteriormente".*[92], está por demás indicar que el sujeto activo de este ilícito se hace pasar por alguien que no es, aunque en la descripción de perfil de la red social indique o aparente tener la misma edad o que van al mismo colegio y vivan en el mismo sector que la víctima. El groomer denominación que se otorga al sujeto que realiza este tipo de actos ilícitos a través de las redes sociales; el anonimato de internet es el detalle más riesgoso para todos los usuarios porque no puede individualizarse fácilmente a cada uno de los usuarios; la creación de confianza en el menor y que este al poco tiempo le empiece a facilitar fotografías, datos de ubicación o residencia, centro de estudios, información general sobre su familia, lugar de labores de sus padres y horarios principalmente cuando no estén estos últimos son el primer paso a realizar del

[92] SVET, Secretaría contra la Violencia Sexual, Explotación y Trata de personas, Cuidado con el Grooming, Guatemala, disponibilidad y acceso: http://www.svet.gob.gt/campana/cuidado-con-el-grooming, fecha de consulta 26 de febrero de 2019.

groomer, con el fin de obtener lo que desea, ahora bien, este fenómeno es clasificado como un tipo de acoso pederasta ya que las personas que realizan este tipo de actos suelen solicitar al menor fotografías al desnudo o videos, lo que posteriormente es utilizado por el groomer de menara personal o comercializándolo a través de internet, posteriormente se chantajea al menor para que envíe al groomer más material lo que incurre en otro hecho ilícito que es la pornografía infantil.

El engaño o acoso pederasta conlleva un proceso de semanas y en algunos casos hasta meses de convencimiento en lo que el menor es engañado, como se ha mencionado el fin principal muchas veces es obtener videos o fotografías, pero también puede suceder que el agresor o groomer busque tener un contacto real con el menor y así abusar de él lo que incurre en otro tipo de hecho criminal como la violación y en casos extremos el homicidio para que la víctima no acuse al agresor ante las autoridades y de esa manera evitar dejar rastro de su identidad. De esta modalidad de ciberdelincuencia en los últimos años distintos gobiernos han analizado su alcance debido a que según informes de distintas instituciones de ciberseguridad indican que puede ser mucho más grave de lo que aparenta ya que se ha venido sospechando la vinculación de delincuencia organizada en este tipo de operaciones a través de internet y que buscan reclutar o captar jóvenes con fines de trata, es por eso que la atención a este fenómeno no debe ser secundaria debido a la gran vulnerabilidad que se tiene en la población juvenil cada dia. Los esfuerzos en Guatemala por tratar de darle seguimiento a este tipo de hechos criminales se ha venido dando con el apoyo de la Organización de las Naciones Unidas (ONU), *"Guatemala es sede de una iniciativa a nivel regional organizada por la ONU para visibilizar los ciberdelitos contra niños"*[93] dicho esfuerzo desde el año dos mil dieciséis se ha tratado de promover como un medio para la protección y el cumplimiento de la garantía de la seguridad otorgada al Estado como una tarea hacia toda la población.

3.11.1 Modalidades

El grooming posee principalmente dos tipos de manifestación y son:

[93] SOY 502, Lainfiesta Javier, phishing, spoofing, extortion: los ciberdelitos comunes en Guatemala, 2016, disponibilidad y acceso: https://www.soy502.com/articulo/phishing-spoofing-extortion-ciberdelitos-comunes-guatemala-68696, fecha de consulta 11 de septiembre de 2019.

3.11.1.1 Típico

Esta modalidad de grooming es el más común debido a que sigue las características antes descritas, que son crear confianza en el menor contactando por un cierto tiempo hasta lograr que las víctimas bajen la guardia y faciliten videos o fotografías que posteriormente el groomer utiliza para chantajear al menor y que este le continúe enviando más material de este tipo.

De esta clasificación de grooming se deriva una serie de pasos que el groomer realiza hasta alcanzar su objetivo y son:

1. Enganche, sucede cuando el groomer inicia con preguntas sobre localización y edad de la víctima con esa información irá adaptando jerga o lenguaje y gustos para generar coincidencias aparentes con la víctima.
2. Fidelización, en esta fase el acosador hará que la víctima empiece a tener ganas de seguir contactándose con él y que se convierta en su confidente a quien le cuente sobre situaciones familiares, sentimentales, etc.
3. Seducción, para este momento el acosador con todos los datos que obtuvo en la fase anterior hará manipular a la víctima e iniciará a incluir el tema sexual en las conversaciones envidando fotografías de otros menores con tal de solicitar un intercambio.
4. Acoso, llegado a este nivel el groomer ya posee información y material para hostigar al menor y hacer lo que él le indique.
5. El chantaje, es el último escalón del grooming en esta etapa el acosador iniciará con amenazas al menor de publicar o compartir sus fotografías y de esa manera hacer que el mismo le siga facilitando más material.

3.11.1.2 Indirecto o agresivo

Este tipo de acoso pederasta obtiene su denominación porque el groomer actúa de una manera persuasiva con la víctima; es importante indicar que en este tipo de acoso el groomer ya ha obtenido material comprometedor de la víctima previamente y este mismo es lo que emplear para hostigar a su víctima mediante la amenaza de difundir el material o enviárselo a sus familiares lo cual claramente intimida al menor, este tipo de casos

suele suceder por descuido de la víctima al publicar y compartir fotografías o videos muchas veces subidas de tono a su pareja sentimental o amigos, el cual por algún motivo el groomer llega acceder o adquirir y lo aprovecha como carnada para que la víctima haga lo que el groomer le indique. Es esencial reconocer que este ciberdelito en general únicamente se manifiesta o sucede mediante el acoso de un adulto hacia un menor.

3.11.2. Tipos de acosadores

3.11.2.1 Groomer pederasta digital

"El interés por conocer a su víctima en persona suele ser nulo, a pesar de ello pueden provocar un gran daño psicológico. Generalmente oculta su verdadera identidad, posee material de abuso sexual infantil de sus víctimas, ya sea para uso personal o con fines económicos, pueden financiar, comercializar, publicar o distribuir material de extrema dureza. Su comportamiento se vuelve una obsesión compulsiva. La conversación se sexualiza rápidamente, no pierden tiempo y el pedido de imágenes como de envíos se realiza de manera veloz y repentina"[94]. Este tipo de groomer generalmente presenta una actitud agresiva hacia sus víctimas como una forma de persuadir y tratar de conseguir lo que desea, por otro lado, el groomer pederasta digital actúa únicamente online, es decir solamente por internet y lo hace en organización con otros groomers, por lo general planean sus ataques o acoso en "manada" por medio de grupos de WhatsApp con el fin de presionar a la víctima y que esta facilite fotografías y videos distintos, tomando en cuenta que el fin que tiene la "manada" es tratar de conseguir la mayor cantidad de material de su víctima. Este tipo de acosador también es denominado como acosador directo.

3.11.2.2 Groomer pederasta

"Puede usar su verdadera identidad, sus comunicaciones y diálogos no suelen ser agresivos, de carácter manipulatorio. Conocer al menor en persona es el objetivo para satisfacer sus necesidades"[95]. Este tipo de acosador suele manifestarse en muchos de

[94] NORTE, ONG Grooming Argentina, peligro en las redes: detectan 4 formas de groomers, 2019, disponibilidad y acceso: http://www.diarionorte.com/article/182065/peligro-en-las-redes-detectan-4-formas-de-groomers, fecha de consulta 18 de septiembre de 2019.
[95] *Loc. Cit.*

los casos de grooming y se encuentra al asecho en redes sociales, esperando que alguno de todos los menores que tiene en la mira como víctimas potenciales sea engañada con el previo establecimiento de confianza y la manera pasiva en que trata de convencer a sus víctimas para que le faciliten videos y fotografías de contenido sexual, ahora bien, esta modalidad de acoso encuadra en la conducta de pedofilia ya que el fin principal del groomer es tener contacto físico y real con el menor y suele seleccionar a sus víctimas de manera cuidadosa para que posean un ubicación cercana a la de él y en algunas ocasiones la víctima puede ser un familiar.

3.11.2.3 Groomer cazador

"No es un Groomer tradicional, son delincuentes organizados que mueven miles de millones de dólares, su objetivo principal es la trata de personas y para ello utilizan las redes sociales como método de captación. Hoy en día estas redes criminales actúan de un modo más sutil y disimulado, intentando no dejar rastros o huellas. No actúan solos, existe más de una persona involucrada que puede ser hombre o mujer para colocar como anzuelo a otro niño"[96]. La presencia de delincuencia organizada en este tipo de hechos ilícitos contra menores agrava aún más el acoso debido a que ya no solo se trata de la interacción del menor con un desconocido sino de un peligro inminente a la integridad y vida del niño porque el fin principal de este grupo es la trata, que por demás esta indicar que este delito implica la retención y obligación de la víctima a realizar ciertas actividades contra su voluntad y posteriormente su traslado a un destino desconocido que puede llegar a traspasar fronteras.

3.11.2.4 Groomer depredador

"Es el más violento dentro del tipo. Pueden llegar al homicidio, el grooming es el delito iniciador para culminar con su fase homicida. Pueden develar su verdadera identidad o, por el contrario, falsear la misma. Entablan contacto con varias posibles víctimas, esto le da una imagen de poder ya que el menor entiende que, si puede hacer con varios lo mismo que con él, se encuentra acorralado, atrapado y con pocas chances de escapar

[96] *Loc. Cit.*

de las garras de su victimario"[97]*.* Las conductas de cada uno de los tipos de criminalidad establecen el grado de peligrosidad que este mismo puede llegar a representar para la sociedad, es decir, entre más extrema o anormal es la manifestación del delincuente, más inmediato debe ser su tratamiento para evitar consecuencias graves en el peor de los casos evitar más víctimas; para el groomer depredador la importancia de borrar o evitar dejar evidencia de sus hechos es preeminente, además que no acepta que su víctima le niegue una petición, por lo cual emplea amenazas como la de muerte no solo al propio menor sino amenazas en contra de la familia de la víctima y esto mismo hace que la víctima ceda a las pretensiones del acosador.

3.11.3 Consecuencias del grooming

Todas y cada una de las personas atraviesan dificultades después de haber sido víctima de un delito, independientemente del hecho que se haya suscitado, está siempre deja una huella latente temporal en algunos casos y en otro permanente que nunca alcanza a ser superado; es relevante analizar la victimización que tiene los menores al momento de ser acosados, atendiendo a la naturaleza del ciberdelito grooming, se encuentra que la victimización puede ser permanente o constante porque tanto el groomer como el menor tiene contacto constante a través de las redes sociales lo cual no limita el lugar y la hora en que el acosador hostigue al menor. Considerando la constancia en la victimización del menor se deriva el análisis concreto de las consecuencias visibles del menor acosado lo que no solo es psicológica sino también física. *"Las principales consecuencias para el menor que ha sufrido grooming son: desconfianza hacia otros, alteración del autoconcepto y dificultades para establecer relaciones futuras de pareja y para establecer un apego seguro. Lo más preocupante y la diferencia principal entre el acoso cara a cara y el acoso ejercido a través de internet, es que en este último está descrito un mayor riesgo de que la víctima sufra depresión grave y suicidio"*[98]*.*

Además de lo descrito como las secuelas del grooming se ha determinado también que las víctimas desarrollan un cambio de personalidad debido al trauma que adquieren por

---

[97] *Loc. Cit.*

[98] SEMA, Red.es. *"Guía clínica sobre el ciberacoso para profesionales de la salud".* España, Gobierno de España, 2015, Pág. 21.

el acosador lo que lleva al menor a llevar una vida fuera de lo común o normal que posee un niño o adolescente, hay casos también donde el menor después de haber sido acosado empeora su rendimiento escolar y desarrollan cuadros de déficit de atención, hiperactividad como también en el entorno social suelen ser discriminados por el entorno donde se desarrolla sea esto escuela, colonia o lugar de residencia e inclusive algunos familiares, una de las secuelas observadas es los perjuicios psicóticos que causan daños irreparables ya que llevan a sexualizar las relaciones afectivas posteriores o se dan bloqueos emocionales, donde el sujeto no es capaz de manifestar sus emociones de manera concreta; el descenso de la autoestima o desconfianza en la victima suele ser una consecuencia casi inmediata que en algunos casos conlleva al desarrollo de un cuadro de bipolaridad, aislamiento, alteraciones de sueño y alimentación.

3.11.4 Grooming en Guatemala

Está claro que los ciberdelitos son latentes en todas las partes del mundo pero en el caso de Guatemala el reporte de dichos hechos electrónicos-digitales aun es un tema inconcluso y con una gran cantidad de cifra negra de los casos que no son reportados, existen informes que declaran que de los hechos cibernéticos en Guatemala el noventa por ciento no es denunciado, por diferentes factores, entre ellos la vergüenza o el sentimiento de culpa de las víctimas de grooming y por otro lado el miedo a alguna represalia. Por ejemplo, un caso sobre el grooming expuesto por un medio de comunicación escrito, fue en el año dos mil dieciséis donde un joven de veintidós años denominado como José Luis, usando un perfil falso en una red social fingía ser mujer para solicitar fotografías a varios menores de edad, la mayoría eran varones, dicho sujeto o acosador por un tiempo determinado estableció el clima de confianza característica descrita anteriormente sobre el tema de groomer, previo a solicitar o ejecutar su plan con la victima seleccionada; José Luis, solicitaba fotografías de sus víctimas de manera particular, ya que pedía poses y colores de ropa interior puntuales a lo que los menores atendían y le enviaban, pero todo eso no le fue suficiente por lo que procedió a citar a las víctimas a una determinada zona cerca de su residencia pero lejana de la población con un acceso complicado para el que no conozca el área, cuando estaba en el lugar empleado un arma de fuego y amenazas sometió a sus víctimas y los violó al mismo

tiempo que graba todo los hechos que posteriormente empleo para extorsionar a los menores y que estos mismos le continuaran enviando más material con las características que el acertadamente les había instruido.

Al momento de la captura del acosador se le conocía tres ataques, pero se sospechaba que habría más casos de los cuales no habían sido reportados; *"José Luis y sus víctimas llegarán a la etapa intermedia del proceso judicial en los próximos días, dos años después de los ataques"*[99], de dicha cuenta es esencial resaltar la condición psicológica en que se encontraría el acosador debido a sus tendencias extremadamente agresiva de trato a sus víctimas y el modus operandi que empleo en la cooptación de los menores.

3.12 Spoofing

"Es una técnica que permite que un atacante adopte la identidad de un host confiable (modificando su dirección IP por la dirección de este) y obtenga de este modo accesos no autorizados a otros sistemas".[100] Este tipo de ataque se da con la suplantación de identidad o falseo del origen de un usuario u ordenador conectado a la red, el funcionamiento de las redes es por medio de usuarios y cada usuario posee un número designado conocido como IP al cual es siempre reconocido por el mismo, ahora bien, cuando el atacante suplanta la identidad toma ese número por el cual se identifica un equipo y el sistema lo reconoce como otro equipo que realmente no es.

3.12.2. Clasificación

3.12.1.1 IP spoofing

Este tipo de ciberataque *"consiste en ocultar el origen del ataque, suplantando o falseando la dirección IP"*[101], comúnmente es realizado mediante ordenadores debido las especificaciones técnicas y físicas que poseen y permite el acceso a distintas funciones

[99] El Periódico, Lopéz José David, Daniel Villatoro, El crimen que destruye la inocencia, Guatemala, 2018, disponibilidad y acceso: https://elperiodico.com.gt/domingo/2018/03/18/el-crimen-que-destruye-la-inocencia/, fecha de consulta 2 de octubre de 2019.
[100] Panda, Panda Security, IP spoofing, España, 2018, disponibilidad y acceso: https://www.pandasecurity.com/spain/support/card?id=31442, fecha de consulta 13 de febrero de 2019.
[101] Gallardo, Erik de Luis. *"La seguridad para los menores en internet".* España, editorial UOC, 2017, Pág. 25.

informáticas y digitales desde donde es realizado el ataque; la IP es una matrícula que se le es asignada o en ocasiones escogida para identificar a cada usuario de una red, se presenta en dos modalidades que es la estática y dinámica la primera atiende a que esta nunca va a cambiar y el usuario tendrá siempre esa matricula de identificación, la segunda consiste en que cada vez que el usuario u ordenador se conecte a la red tendrá un código diferente a la que tuvo la última vez que se conectó. Atendiendo directamente al IP spoofing, este consiste en el cambio de la IP de un ordenador o maquina autorizada para acceder a una red determinada, el ataque es mediante paquetes de información que pretenden engañar a la seguridad de la red y acceder a ella de manera ilícita, con el fin de interrumpir el funcionamiento normal del servidor o el tráfico de la red, por otro lado también se puede emplear dicha técnica para enviar a la red información maliciosa o códigos maliciosos que sustraigan o hagan llegar información sensible al remitente del ataque esto mediante el empleo de un dispositivo no autorizado; la suplantación de identidad en una red no es ejecutada únicamente cuando el usuario se encuentra fuera de línea, también puede llevarse a cabo en el mismo momento que el usuario de una red está conectado y con sesión activa, el atacante duplica la IP del dispositivo autorizado y con eso puede realizar transferencias bancarias o compras en línea de productos que el usuario autentico no ha autorizado ni realizado.

3.12.1.2 ARP spoofing

Esta es una técnica de hackeo muy utilizada en redes de área local por sus siglas en ingles LAN, debido a que este tipo de redes poseen un protocolo de seguridad basados en la verificación física del usuario de la red es decir emplea la dirección MAC de cada dispositivo para verificar su autenticidad y con eso autorizar al dispositivo para que continúe navegando en la red así como enviar y recibir información; la dirección MAC (Media Access Control), es un código único que identifica la tarjeta de la red de cada dispositivo conectado en la red local de forma inequívoca, la dirección MAC, son concebidas por los fabricantes de hardware y son únicas a nivel global.

"El proceso de ARP spoofing consiste en manipular la tabla ARP de las dos máquinas a las que se desea suplantar"[102], dicho proceso es realizado con el objetivo de interferir en la comunicación de las dos máquinas conectadas a la red loca, a manera de ejemplo el atacante primeramente establece la conexión y la dirección MAC del dispositivo proveedor de internet y posteriormente establece otra conexión con la máquina de la víctima empleando enlaces con la ayuda de las tablas ARP de la maquina proveedora, de allí es como se completa el esquema conocido como Man in the Middle (MITM) que significa hombre en medio, la denominación de este esquema es debido a que al realizar los enlaces el atacante interfiere en la comunicación de la víctima hacia el proveedor es decir que el esquema normal consta de dos dispositivos por ilustrarlo de mejor forma existe un emisor (usuario) y un receptor (Gateway o enlace) que permite que el usuario pueda acceder a internet, el esquema es entonces de dos elementos pero con el ataque de ARP spoofing se une un tercer elemento intermediario entre el usuario y el enlace de allí que el atacante realiza sus operaciones ilícitas porque con el enlace realizado correctamente el atacante puede espiar toda la información que circula en la red y puede modificarla antes que llegue a su destino o simplemente evitar que llegue y denegar el servicio o conexión a los demás usuarios de la red atacada. Este tipo de ataques se manifiesta *"dado que todas las máquinas de una misma red local comparten el mismo medio y que, por lo tanto, son capaces de ver el tráfico originado en la red, las tarjetas ethernet incorporan un filtro que ignora todo el tráfico que no está destinado a ellas mismas. Esto se consigue ignorando aquellos paquetes cuya dirección MAC no coincidan con la suya"*[103].

3.12.1.3 DNS spoofing

"El DNS (Domain Name System) o sistema de nombres de dominio es un sistema que hace legibles para los usuarios las direcciones IP. Para ello, asocia direcciones numéricas con direcciones alfanuméricas, como por ejemplo 173.194.34.16 con www.google.com"[104]. Este sistema de dirección facilita a los internautas ubicar y consultar

[102] *Loc. Cit.*
[103] *Loc. Cit.*
[104] Carceller Cheza, Román y otros. *Servicio en Red*. España, editorial Macmillan Iberia, S.A., 2013, Pág. 33.

las páginas web que deseen; cada página web se encuentra hospedad en un servidor y se identifica por una IP, pero recordar la dirección IP de cada sitio web resultaría un trabajo demasiado duro y de allí la función del DNS, que establece la identificación, traducción y conexión de cada usuario que teclea un dominio a un servidor e indicar a donde debe ir a recogerse la página web que se desea consultar.

Teniendo en cuenta la función del DNS, los ataques de *"DNS spoofing, provocan un direccionamiento erróneo en los equipos afectados, debido a una traducción equivocada de los nombres de dominio a direcciones IP, lo que facilita la redirección de los usuarios afectados hacia páginas web falsas"*[105], está claro que el DNS permiten la resolución de nombres en direcciones IP. De esta forma no es necesario para el usuario recordar las direcciones IP, sin embargo, el ciber atacante aprovecha dicha dependencia que existe con los servidores de nombres de dominio para la ubicación de una página web determinada, de allí que se realiza la alteración de las direcciones IP de los servidores DNS de la víctima para que al momento de teclear un nombre de dominio la victima sea apuntada a un servidor malicioso de esta manera se daría por hecho un ataque de DNS spoofing; para llevar a cabo un ataque de esta naturaleza se puede realizar de distintas maneras por ejemplo montando sitios falsos que sean réplica de alguna autentica y que al momento que la víctima ingrese el nombre de dominio este sea redireccionado al sitio web espejo de donde el atacante podrá realizar la obtención de los datos del usuario como contraseñas, número de tarjetas de crédito o débito, numero de cuentas bancarias, claves de acceso, etc.

3.12.2 Modalidades

Anteriormente se había mencionado el ataque DNS spoofing en modalidad de sitio espejo o réplicas de sitios web, así mismo se pueden realizar la explotación de otros métodos o modalidades como los exploits que se utilizan al momento de visitar las páginas web ejecutando el applet Java esto ocurre cuando se supone el usuario visita una página web de confianza, otra forma de realizar el DNS spoofing y con mucho la más frecuentemente empleada por los atacantes es mediante el aprovechamiento de una mala configuración

[105] Gallardo, Erik de Luis. *Op. Cit.*, Pág. 26.

del router, esto en el caso de usuarios hogareños, el recurso aprovechado por el atacante en este caso es la habilitación de la opción de gestión del router remotamente, es decir, que el dispositivo emplea una IP pública el cual cualquier atacante puede identificar y usar, con esta mala configuración en conjunción con el hecho de que muchas personas dejan las contraseñas por defecto de los dispositivos permite aún más al atacante ingresar a la configuración del mismo y desde allí operar y ejecutar el ataque.

3.12.3 Consecuencias del spoofing

Es claro que cualquier actividad criminal del cual se llegue a ser víctima trae consigo resultados desfavorables esto impactando de una u otra manera al individuo afectado, en el caso de ataques spoofing o suplantación de identidad los daños provocados pueden ser pérdida económica, ya que mucho de los atacantes sustraen cantidades económicas en cuentas bancarias, o realizar compras y estas ser cargadas a la cuenta de la víctima sin que se entere, también puede suceder la denegación del usuario a sus servicios digitales como banca virtual, gestor de algún sistema, aplicaciones de uso recurrente el cual el atacante modifica la contraseña y evitar que el dueño autentico acceda al mismo, por otro lado también está el robo de datos sensibles de alguna sistema local al cual varias computadoras o dispositivos estén asociados, puede ser empleado también para el espionaje a nivel comercial en el caso de empresas automotrices que se encuentren desarrollando algún proyecto confidencial el cual un competidor quiera acceder de manera ilícita y hacerse con el mismo para eventualmente favorecer la competitividad en el mercado, en casos más particulares de los datos obtenidos del ataque pueden realizarse ciberbullying o ciberacoso debido a que el atacante puede haber sustraído información sensible que exponga a la víctima como fotografías, videos, etc. Que comprometa a la víctima en su pudor o cargo que desempeñe en el caso que el atacado sea una persona conocida, por otro lado, puede suceder que el atacante suplante la identidad a nivel social de la víctima es decir que de la información obtenida del ataque el delincuente cree perfiles falsos en plataformas sociales, correo electrónico con el fin de crear una imagen negativa de la víctima.

3.12.4 Spoofing en Guatemala

Está claro que cada día los procesos y haceres cotidianos se han ido adaptando al entorno digital mediante la incorporación de los teléfonos inteligentes con acceso a internet permanente, que acerca aún más al ciber delincuente a víctimas potenciales que navegan descuidadamente en internet. En Guatemala actualmente no se tiene registro de ataques informáticos de spoofing concretamente, debido a que los ciberataques que se han ido registrando con los años viene acompañado por una o más técnicas más como el phishing y sus variantes, de allí que se llevan a cabo la captura de los datos sensibles de las víctimas para posteriormente ser empleados para la suplantación de la identidad de las mismas al cual se le ha robado los datos personales como nombres de usuarios, contraseñas, accesos a redes privadas, cuentas bancarias, etc.

Es importante indicar así mismo que de los ciberataques contabilizados existe una cifra grande denominada cifra negra, que corresponde a todos aquellos usuarios que no realizan ningún reporte o denuncia de haber sido victimizados por este tipo de delincuencia, pudiendo también interferir el desconocimiento de las personas sobre este tipo de delincuencia como también la carecía de una sección especializada que trate este tipo de casos, por otro lado, está presente la debilidad de carencia de una legislación sobre ciberdelitos.

3.13 Métodos de acción de los cibercriminales

La naturaleza de los criminales es dinámica, debido a que cada uno de los grupos actúa y opera de una distinta manera, aun cuando cometen los mismos ilícitos por lo cual es una tarea muy difícil establecer un solo método de acción criminal, pero en el ámbito cibernético las acciones criminales están asimiladas debido a una serie de pasos que generalmente los ciber atacantes deben realizar para llevar a cabo su cometido. Hay que tener en cuenta que los ataques cibernéticos cada día se van renovando y explorando nuevas vías para llevar a cabo los objetivos maliciosos de los hackers; los métodos más básicos para le ejecución de un ciberataque son Spyware, que no es más que un software malicioso que espía la actividad del usuario de una red y enviar la información a su creador o hacker, phishing, es otro de los métodos más comunes empleados para la captación de los datos personales de la víctima, adware, es un tipo de software empleado regularmente para mostrar publicidad mediante ventanas emergentes pero también ha

sido empleado para espiar la actividad de información personal del usuario, así mismo realiza seguimientos de los sitios web que visita el usuario, ransomware, es empleado para bloquear el acceso a los dispositivos, troyano, es un tipo se virus informático que muchas veces tiene la apariencia de ser algo útil pero sirve para el robo de datos de los usuarios de un dispositivo suele propagarse mediante correos electrónicos que viene como agregados y se instalan muchas veces sin la autorización del usuarios del dispositivo infectado.

CAPÍTULO IV

4. MANEJO DE LA ESCENA DE CRIMEN EN LOS DELITOS INFORMÁTICOS

4.1 Evidencia informática

Cuando se ejecuta un ciberataque a través de medios informáticos, muchas veces la información directa o indirectamente que se relaciona con el hecho ilícito queda almacenada en forma digital dentro de cada uno de los sistemas informáticos, este conjunto de datos se convierte en evidencia de la infracción cometida y eso es denominado evidencia informática.

4.1.1 Clasificación de la evidencia informática

Atendiendo a como debe ser ubicada y distinguida la evidencia informática se establece una clasificación en razón a los elementos materiales que pueden contener la evidencia al que se le denomina evidencia electrónica y en cuanto a la información que se encuentra en los elementos materiales se denomina evidencia digital.

4.1.1.1 Evidencia digital

"La evidencia digital es todo registro informático almacenado en un dispositivo informático o que se transmite a través de una red informática y que pudiera tener valor probatorio para una investigación"[106] Se considera evidencia digital a cualquier información que ha sido extraída de un sistema tecnológico como computadoras, redes, internet, etc. Y esta es almacenada en una unidad de almacenamiento flash como memorias USB para su posterior análisis con herramientas técnicas especiales.

4.1.1.2 Evidencia electrónica

Todos los elementos materiales de un hecho ilícito de carácter informático es evidencia electrónica es decir el hardware, de allí la evidencia digital que es toda la información contenida en el hardware.

---

[106] Nessi, Alan Martín.*" Manual de evidencia digital"*. Perú, Ministerio de justicia y derechos humanos, 2017, Pág. 15.

4.2 Características de la evidencia informática

4.2.1 Volátil

"Si no es preservada adecuadamente puede cambiar o variar con facilidad de forma poco previsible"[107], por la naturaleza que posee la evidencia informática y que muchos de ellos son contenidos en dispositivos de almacenamiento temporal como memoria RAM, al no considerarse las medidas adecuadas pueden ser alterados o completamente perdidas en el peor de los casos, pudiéndose producir con el hecho de desconectar la fuente de suministro del equipo electrónico o apagándolo, de esta manera podría perderse datos sobre procesos ejecutados en el equipo como las conexiones de red, archivos abiertos, etc.

4.2.2 Duplicable

"Puede ser duplicada de manera exacta y copiada tal y como si fuese el original"[108]. Esta característica de la evidencia informática provee de una ventaja al momento de su análisis debido a que permite realizar varias formas de análisis con resultados más fieles y apegados a la verdad histórica de los hechos en el caso de un ilícito ejecutado a través de un equipo informático.

4.2.3 Alterable y modificable

"Con las herramientas adecuadas es relativamente fácil alterar, destruir o modificar"[109]. Atendiendo al origen y delicadeza de le evidencia informática los datos que de ella se puedan obtener son precisos y puntuales, sin embargo, de no tomarse en cuenta las medidas necesarias los resultados podrían ser totalmente alterados incluso de manera remota, por lo cual es importante que la persona que se encargue de su obtención, extracción, conservación y transporte debe ser calificada en la materia informática con el fin de realizarse con los medios y cuidados adecuados.

4.2.4 Eliminable

---

[107] *Ibid.*, Pág. 17.
[108] *Loc. Cit.*
[109] *Loc. Cit.*

"Con las herramientas adecuadas puede ser eliminada por completo"[110]. Esta característica es aplicable en algunos casos mayormente en el manejo de información volátil de un sistema informático que con los conocimientos específicos y herramientas pueden ser eliminados los rastros o indicios informáticos de la ejecución de una determinada operación.

4.3 Métodos de extracción

Al momento de realizar el proceso de extracción de los datos en un dispositivo tecnológico existe un número notable de herramientas y procedimientos que deben ser tomados en cuenta atendiendo a la naturaleza de la evidencia informática, de allí es que se detallan los pasos generales para la extracción de la información necesaria para los casos que procede una investigación criminal, primeramente debe resguardarse el lugar del hallazgo con el fin de que ningún objeto o máquina pueda ser manipulada y así alterar los elementos del lugar, posteriormente debe observarse los elementos del lugar de los hechos como *"anotaciones de claves de usuario o de correos que pudieran encontrarse en soportes distintos a los electrónicos"*[111], estos podrían ser papeles, comprobantes de pago, facturas donde pudiere haberse escrito alguna clave de acceso o nombres de usuario de alguna plataforma digital, así mismo en el lugar debe considerarse *"huellas digitales no visualizadas"*[112] que puedan ser procesadas y posteriormente cotejadas con los posibles sospechosos del hecho, de la misma forma la consideración de objetos asociados al lugar y los sospechosos debe observarse la existencia de gorras, pelos, huellas de calzado etc. Por otro lado, debe tomarse en extremo cuidado de *"no tropezar, jalar o cortar cables de conexión de equipos, periféricos o conexiones de entrada o salida de datos"*[113] debido a que puede interrumpirse algún proceso en desarrollo como salas de chat, audios o trasmisiones que incriminen el hecho cometido.

---

[110] *Loc. Cit.*
[111] Orrego Pinzón, Jhon Leonardo y Jonathan Vargas Roa. "*Manual para manejo de la evidencia digital*", Colombia, Universidad Autónoma de Colombia, 2017, Pág. 40.
[112] *Loc. Cit.*
[113] *Loc. Cit.*

El aseguramiento en todo sentido del lugar debe ser realizado de la manera más inmediatamente posible *"debido a que existen muchos equipos que si son apagados de manera incorrecta pueden dañarse"*[114] ya que un procedimiento inadecuado haría irrecuperable la información contenida en los dispositivos. Realizado todos los pasos anteriores debe documentarse el lugar mediante informes escritos y fotografías indicando el *"estado y posición de los equipos, así como de sus puertos (conectores de cables, lectores de CD, lectores de disquete y cualquier otro punto de contacto del equipo con el exterior)"*[115], después de los procesos preliminares a la extracción de la evidencia digital en caso de encontrar los equipos tecnológicos apagados *"no encenderlo por ningún motivo y por el contrario, si están encendidos, no apagarlos por ningún motivo"*[116], el procedimiento debe ser completado con la toma de fotografías detalladas de la imagen de la pantalla, con la documentación del lugar y los equipos debe darse paso a la intervención de un experto en informática forense.

La actividad principal del experto en informática es la extracción segura y original de los datos en las unidades de disco y a través del volcado de memoria RAM de los dispositivos presentes en la escena procesada, esto con el objeto de evitar la pérdida de la información volátil o la modificación de datos contenidos en los diferentes equipos electrónicos. La copia de los discos duros de las computadoras es mediante herramientas de software debido a que en los últimos años la capacidad de almacenamiento de los discos duros ha ido creciendo exponencialmente lo cual dificulta aún más la toma de imágenes de discos manualmente; se requiere que la herramienta seleccionada para la copia de los discos realicen la duplicación del *"flujo de bits o una imagen de disco original, que la herramienta no modifique el disco original, la herramienta sea capaz de verificar la integridad de un archivo de imagen de disco, la herramienta deberá registrar los errores de entrada y salida"*[117], con dichos requerimientos cumplidos se dice que la extracción de la información en la creación de una copia de bit a bit a través de una imagen forense de

[114] *Loc. Cit.*
[115] *Ibid.* Pág. 41.
[116] *Ibid.* Pág. 42.
[117] *Ibid.* Pág. 47.

los equipos ha sido segura y se procede al embalaje de los elementos que serán transportados para su posterior análisis en el laboratorio forense.

4.4. Protocolos internacionales sobre evidencia informática

Los protocolos que a continuación se mencionan son los reconocidos a nivel internacional por el grupo de trabajo de ingeniera de internet por sus siglas en inglés IETF, es el organismo principal de estándares de internet que se desarrollan a través de procesos abiertos en una comunidad internacional en la red.

4.4.1 RFC 3227 Directrices para la recopilación de las evidencias y su almacenamiento

Describe los métodos de extracción de la información en los diferentes dispositivos estén estos apagados o encendidos, así mismo recoge directrices para la recolección y almacenamiento de las evidencias digitales, atendiendo puntualmente a la delicada naturaleza que dichos elementos poseen, es de mencionar también que dicho documento proporciona los modelos y cada uno de los procedimientos que deben ser tomados en cuenta por el perito informático al momento de realizar el procesamiento de la información recolectada en los dispositivos electrónicos. Los fundamentos de la evidencia informática son un tema que es desarrollado en el mismo, debido que es una disciplina que debe ser ejecutada con todas las diligencias necesarias; se toma en cuenta puntos esenciales para cada dispositivo como el orden de la volatilidad de la información almacenada, las acciones que pueden realizarse y las que estrictamente deben ser evitadas con el propósito de realizar un procesamiento efectivo, la observación de la privacidad es también un apartado desarrollado ya que en muchos casos puede resultar la exposición de información innecesaria para la investigación y que comprometa aún más al agraviado por un ciberataque; un punto valorativo del RFC 3227 es la indicación de las herramientas necesarias para el perito informático al momento de la realizar el análisis respectivo de las evidencias digitales.

4.4.2. RFC 4810 Preservación de la información a largo plazo

Para cualquier investigación o trabajo forense la preservación de los elementos del delito es de alto interés debido a que estos pueden revelar la memoria histórica del hecho ejecutado, para el caso informático la instrucción RFC 4810 menciona los pasos adecuados para la preservación de la información recolectada, porque este último es uno de los puntos clave para el éxito del informe pericial en un proceso investigativo judicial. La autenticidad y validez de los datos son los elementos primarios para una evidencia por lo cual este documento refiere a los peritos informáticos como se debe verificar una firma digital después de haber pasado mucho tiempo desde su generación en un sistema digital.

4.4.3 RFC 4998 Sintaxis del registro de evidencia

Describe el formato de datos para un archivo de evidencia, el registro de la evidencia que sirva para certificar la autenticidad y origen del archivo, de la misma manera la verificación de la integridad del archivo, para que este pueda ser procesado y presentado como prueba fidedigna de un hecho que se encuentre en investigación. El objeto de esta instrucción es el aseguramiento de las firmas digitales donde se haya producido determinado archivo y de esta manera encontrar coincidencia e identidad.

El documento RFC 4898 debe su origen a la seguridad en la red y la validez de la información en cada uno de los documentos firmados digitalmente y que son almacenados durante un largo tiempo; se sabe que la seguridad en los documentos a largo plazo es ineficaz debido a que los algoritmos se debilitan y se vuelven inválidos es por eso que debe de probarse que un archivo ya existía antes de un ciber ataque y no fue generado hasta el momento del hecho de esa manera la agilización y análisis de la información perteneciente al caso que se indaga se distingue y clasifica como evidencia y prueba del hecho. El protocolo RFC 6283 es el documento que complementario de la sintaxis del registro de evidencia en dicho documento se describen las reglas del proceso que debe ser seguido para la creación de evidencias íntegras y así evitar que pueda ser rechazado en proceso judicial, los procedimientos para la verificación de autenticidad de

los datos y las reglas de procesamiento para crear evidencia son caracteres abordados en la RFC 6283.

4.5. Estándares internacionales sobre escena de crimen digital

La organización internacional de normalización por sus siglas en inglés ISO, es una agrupación internacional no gubernamental con su oficina central en Ginebra, Suiza a través de sus miembros, reúne a expertos con amplia experiencia en diferentes disciplinas con el fin de desarrollar normas internacionales voluntarias que puedan regir diferentes procesos que brinden soluciones a varios de los desafíos globales, en este caso sobre la informática forense.

4.5.1 ISO/IEC 27037: 2012 Indicaciones para la identificación, recolección, adquisición y preservación de la evidencia digital

Este estándar proporciona instrucciones relacionadas con la identificación, recolección, adquisición y preservación de evidencias digitales que puedan poseer valor probatorio en una investigación criminal; dicho documento instruye en materia de manejo de la evidencia digital desde el momento de su hallazgo, su procesamiento, análisis y redacción de informe respectivo al peritaje practicado en cada una de las evidencias recolectas del hecho que se cuestiona, de la misma manera incluye directrices de conservación de la evidencia digital y la cada de custodia respectiva de cada archivo extraído de los dispositivos electrónicos. Puede ser complementado este estándar con la RFC 3227 que hace mención sobre el manejo y recolección de la evidencia informática y su almacenamiento en digital.

4.5.2 ISO/IEC 27042: 2015 Tecnología de la información. Técnicas de seguridad. Directrices para el análisis y la interpretación de la evidencia digital

Es una norma que sirve para el análisis e interpretación de las evidencias digitales, así mismo instruye en como poder ejecutar de manera correcta y segura el análisis de la información facilitando los modelos de análisis que pueden ser utilizados por el perito informático para el caso que se refiera.

Dicho estándar refiere también los puntos que debe incluir un informe pericial, siempre y cuando el perito informático no posea instrucciones previas de cómo realizar el informe por parte de un organismo legal, como un juez, policía, etc. Esto con el fin de coadyuvar en la entrega de un informe integro, confiable, eficaz, útil y que pueda ser interpretado fácilmente por otros organismos en dado caso que la investigación sea llevada a cabo con la colaboración de órganos internacionales o extranjeros para el esclarecimiento de un hecho; menciona también la formación y mantenimiento de las habilidades que el perito informático debe poseer con el fin de estar al paso de los avances informáticos y los posible nuevos métodos de acción en ciber espacio.

4.6 Embalaje de evidencia digital

En la investigación criminalística el proceso de embalaje toma importancia relevante debido a que esto evita que los elementos o evidencia pierda su valor probatorio del hecho que se investiga, aunado a dicho proceso se encuentra la cadena de custodia que es un procedimiento que tiene por fin el control del indicio recolectado en la escena de crimen y que posteriormente es valorado como evidencia del hecho criminal suscitado.

Para el caso de la evidencia digital el procedimiento de embalaje común no es el más adecuado debido a la naturaleza de la evidencia, por tal motivo se han establecido pasos específicos para el resguardo de dichos elementos como lo son la determinación de los datos relevantes para la investigación, atender la volatilidad de la evidencia, eliminar la interferencia del exterior para no perder la información almacenadas en los dispositivos electrónicos, ya que muchos dispositivos operan con memorias magnéticas, para tal caso se recomienda el uso de bolsas Faraday diseñadas especialmente para la recolección y transporte de dispositivos móviles e inalámbricos, el material de estas bolsas brinda una protección alrededor de los dispositivos bloqueando toda señal de radio, wifi o celular y por último documentar bien cada una de las evidencias con su debida descripción, así mismo todos los elementos embalados deben ser transportados en cajas con capacidad de contener cada uno de los aparatos informáticos con el fin de evitar pérdidas, daños o confusiones con cada una de las evidencias.

4.6.1 Medidas de seguridad para la evidencia digital

Siendo un especialista en informática forense quién extraerá la evidencia digital de los dispositivos electrónicos implicados en la comisión de un hecho ilícito el procedimiento debe ser complementado por los siguientes procedimientos:

a) *"Esterilidad de los medios informáticos de trabajo.*
b) *"Verificación de las copias de los medios informáticos.*
c) *"Documentación de los procedimientos, herramientas, y resultados sobre los medios informáticos analizados".*
d) *"Mantenimiento de cadena de custodia de las evidencias digitales".*
e) *"Informe y presentación del análisis de los medios informáticos".*
f) *"Administración del caso realizado".*
g) *"Auditoría de los procedimientos realizados en la investigación"*[118]

4.7 El perito informático

4.7.1 Definición

"Perito es la persona que posee determinados conocimientos técnicos, y por tanto, especializados. El perito es experto en determinada materia, que coincide normalmente con un campo de actividad profesional, ya sea en cuestiones estrictamente científicas, artísticas o prácticas"[119]*.* Para los casos donde se hayan involucrado dispositivos tecnológicos el experto que participa en la investigación es el perito informático, que se encarga de realizar todos los procedimientos de extracción, análisis y emisión del dictamen pericial que es el procedimiento conclusivo del perito informático. El perito informático surge en razón de que la mayoría de los funcionarios judiciales no poseen formación especializada en tecnologías, por lo que no pueden tener la certeza total de validar una evidencia o prueba tecnológica, los peritos informáticos son profesionales que se encargan de dar soporte a la hora de presentar medios electrónico-digitales como evidencia de algún hecho ilícito, la disciplina que desempeña el perito informático nace con el fin de ofrecer fundamentos científico y técnico en los casos judiciales que requiera el análisis de pruebas informáticas, la intervención del perito es en aquellos casos en los

[118] *Loc. Cit.*
[119] Antón, Francisco. *"Policía científica I"*, España, editorial Universidad de Valencia, 1990, Pág. 401.

que se sospecha o se tiene la certeza de que se ha producido el uso inadecuado o ilícito de un medio tecnológico por ejemplo espionaje, delitos contra la propiedad intelectual, accesos ilegales a documentos o ficheros, interceptaciones de comunicaciones, difusión de datos personales, daños a equipos informáticos, etc.

4.7.2 Rol del perito informático en la investigación criminal

La participación principal del perito informático en la investigación criminal consiste en recibir todos los elementos informáticos recolectados en la escena de crimen, posterior a su recepción realiza un cuidadoso control de que ninguno de los elementos informáticos haya sido alterado, cambiado o destruido, dichos procesos de control son necesarios para garantizar la fidelidad de cada uno de los indicios informáticos. El perito informático en la investigación forense colabora en la parte analítica de indicios e interpretación de datos de donde obtendrá resultados que puedan ser aclarados y trasmitidos a cada uno de los interesados en la investigación a través de una dictamen o informe técnico sobre cada uno de los elementos analizados. Es importante mencionar que el perito informático debe actuar en el proceso de investigación de manera neutral, objetiva y profesional, buscando proveer resultados reales con el fin de coadyuvar en la investigación al esclarecimientos de la verdad, la parte más relevante en la investigación forense del perito informático es la de brindar su opinión profesional de los objetos analizados y que este pueda ser plasmado en un documento escrito e integrado a un proceso judicial de manera sencilla y entendible para cualquiera de los intervinientes en el caso investigado.

4.7.3 Perfil del perito informático

Un perito informático es un profesional con conocimientos, habilidades y experiencia en el manejo de la tecnología y sus diferentes funciones en cada uno de los dispositivos como computadoras, teléfonos inteligentes, dispositivos de almacenamiento o memorias, tableta y por supuesto internet; el perito deber ser capaz de extraer las evidencias electrónicas y digitales necesarias para el caso que se esté tratando, el perito informático no solo debe llenar las cualidades técnicas y prácticas de la ciencia informática, también debe poseer los conocimientos judiciales necesarios para su participación en la investigación de un delito. Es de mencionar que actualmente no se posee una carrera

específica para ser certificado como perito informático sin embargo existen varias posibilidades de especializarse en dicha disciplina.

4.8 Análisis forense de la evidencia digital

Se refiere al *"conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y prestación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial. Por evidencia digital se entiende al conjunto de datos en formato binario, esto comprende los ficheros, su contenido y referencias a éstos (metadatos) que se encuentren en los soportes físicos o lógicos del sistema atacado"*[120]*.* El análisis de la evidencia para el caso informático se divide en dos ramas generales que son el hardware y software en el primero se analiza físicamente cada uno de los elementos tecnológicos hallados en escenario criminal como el estado general de los dispositivos y sus componentes, el segundo caso es el análisis lógico de los elementos indiciarios en el sistema informático del dispositivo hallado, es decir la interpretación de los datos almacenados en las memorias del dispositivo electrónico que pueda proveer de información útil para investigación forense, algunas herramientas de software de acceso libre en la web son Tequila SO entre sus funciones está la de análisis de archivos jpg, png, volcado de memoria RAM y fuerza bruta para descifrar contraseñas, FTK imager programa que crea imagen de disco de almacenamiento, maltego que ayuda a encontrar información sobre personas y empresas en internet, ChromePass una herramienta básica de Windows que permite visualizar los usuarios y contraseñas almacenadas a los largo de los años en Google Chrome, recuva herramienta que permite recuperar fotos, música, documentos, videos y archivos borrados en un dispositivo de almacenamiento, Autopsy herramienta que permite realizar auditorías forenses, OS forensic herramienta que permite realizar un análisis profundo del equipo electrónico con el fin de obtener alguna pista que guie hacia los datos que se debe extraer del dispositivo y observar minuciosamente para obtener algún indicio del hecho en investigación .

El análisis forense de la evidencia digital conlleva una serie de pasos que son la identificación de los hechos, la recopilación de las evidencias, la preservación de los

[120] Lopez Delgado, Miguel. *"Análisis forense digital",* 2007, Pág. 5.

elementos obtenidos, el análisis de la evidencia adquirida y la presentación de los resultados. El proceso que conlleva el análisis de la evidencia digital es con el propósito de repasar lo que el cibercriminal ha realizado en un sistema atacado luego de haberse suscitado un evento malicioso cibernético, dicho análisis pretende identificar a través de que medio o medios se realizó el ataque, la ubicación geográfica posible de la operación, el día que todos los eventos sucedieron y por supuesto tratar de identificar al posible responsable del hecho criminal investigado.

Los recursos que se obtendrán podrán ser posteriormente valorados como pruebas del ciberdelito y que claramente confirmarían o descartarían la existencia de la acción criminal, la fase de análisis de la evidencia supone la etapa más laboriosa del perito informático debido a que este empleará todos y cada uno de sus conocimientos como su experiencia sobre el tema informático para reconstruir cada uno de los sucesos ocurridos procurando no alterar el estado original de cada una de las evidencias, como también establecer en concreto el patrón que siguió el cibercriminal al ejecutar la operación maliciosa.

4.9 El informe pericial

Se define el informe pericial como *"el documento confeccionado por una o varias personas acerca de los hechos, circunstancias o condiciones personales inherentes al hecho punible, conocidos dentro del proceso, para lo que es necesario poseer determinados conocimientos científicos, artísticos o prácticos"*[121]. Las pericias más que la confirmación de un hecho controvertido busca brindar una explicación técnica sobre los elementos y eventos sucedidos, así mismo busca también coincidencias con otros medios de prueba que hayan sido analizados; de tal cuenta la actividad pericial se considera un proceso analítico y deductivo que se desarrolla completamente cuando esta es valorada como prueba en proceso penal.

Existe tres tipos de informes los cuales son el informe técnico, ejecutivo y mixto, el primero de ellos contiene el resultado de una investigación realizada sobre un hecho concreto que permite la exposición de lo sucedido a través de la visión del perito

[121] Loc. Cit.

informático, en él se explica los detalles desde una postura objetiva e independiente, así mismo, es un texto principalmente expositivo, su contenido no es de carácter conclusivo sin embargo señala lo que ha acontecido mas no emite ninguna argumentación, este informe es proveído con frecuencia a los estudiados en la materia informática. El informe ejecutivo es un documento corto donde se pretende resaltar los datos más relevantes del caso investigado aborda los detalles más relevantes pero sin profundizar en detalles más específicos sobre los resultados obtenidos; el informe mixto posee las características de los dos informes ya descritos sin embargo este posee la característica principal que puede ser redactada con el fin de ser presentado ante un tribunal como también ante el público en general, debido a que su contenido es de carácter detallado, simple, explicativo, conclusivo y con un lenguaje accesible a todos los destinatarios.

CAPÍTULO V
5. PRESENTACIÓN Y DISCUSIÓN DE RESULTADOS

El presente trabajo de investigación está enfocado en exponer información respecto al desarrollo de los cibercriminales, los antecedentes y avances que se han obtenido en la investigación del cibercrimen en Guatemala, tal como lo indica el objetivo general de la investigación, de esta cuenta se realizó una entrevista la cual contiene diez preguntas, teniendo en cuenta como sujetos de la investigación a profesionales del área de informática del Instituto Nacional de Ciencias Forenses, Policía Nacional Civil, Ministerio Público y expertos que laboren en el área informática.

Al inicio de la investigación se planteaba que el Estado garantiza a través de la Constitución Política de la República de Guatemala la libertad, justicia, seguridad, paz y desarrollo de cada uno de los habitantes del país, de allí es que se traza el tema sobre ciberseguridad, debido a que son pocos e insuficientes los esfuerzos que algunas instituciones nacionales realizan para el tratamiento y sanción de esta modalidad delictiva. Según el modelo de entrevista dirigida a los sujetos de investigación se obtuvieron los siguientes resultados:

- **¿Según su experiencia cuál es el estado actual de la seguridad informática en el país?**

En la primera pregunta se requiere que los sujetos de investigación establezcan cual es el estado actual de la seguridad informática en el país, a lo que varios de ellos señalan como crítico y precario a la vez, debido a una falta de cultura sobre ciberseguridad en la población, así mismo existe una falta de interés en inversión sobre ciberseguridad en los sectores empresariales privados que son el principal foco de ataques informáticos, por otro lado se indica también la falta de un presupuesto estatal en temas de ciberseguridad nacional, puntualmente en los datos financieros y otros sectores potenciales para el correcto funcionamientos y desarrollo del país.

Discusión

De la respuesta recibida por parte de cada uno de los sujetos de investigación antes mencionados se determinó que el estado actual de la ciberseguridad en el país es crítico, atribuido a varios factores que juntos concluyen en la debilidad que el país posee en cuanto a ciberdelitos se trata, a lo largo del trabajo se ha venido desarrollando y mencionando varios de los factores indicados por los sujetos de investigación como los principales vulnerantes ante la ciberdelincuencia, los cual son congruentes con la situación que actualmente enfrenta el país en cuanto a ciberseguridad se refiere, por lo que es importante abordar el tema de la adaptabilidad y facilidad que poseen los ciberdelincuentes hoy por hoy para realizar sus ataques y obtener resultados positivos para sus intereses, debido a que en el país aún hay una cifra muy baja de personas con cultura de ciberseguridad y muchos de los trabajadores que operan desde un ordenador creen estar protegidos ante todas las amenazas con la simple instalación de un antivirus, sin tomar en cuenta las diversas y casi infinitas maneras en que un ciber ataque puede realizarse, de esa cuenta se puede entender que las respuestas recibidas por parte de los sujetos entrevistados son congruentes con la descripción desarrollada sobre la ciberdelincuencia.

- **¿Cómo incide la ciberdelincuencia a nivel nacional?**

La segunda pregunta de la entrevista los sujetos de investigación responden en base a la incidencia de la ciberdelincuencia a nivel nacional, lo señalan como un tema que no debe ser tratado como un fenómeno local sino global, debido a varios motivos, iniciando porque los ciberataques que se dan, no son de origen nacional sino internacional, mencionando a Pakistán, India como algunos países desde donde se originan los ciberataques, se menciona también que países como Guatemala que se encuentra en vías de desarrollo muchas veces sirven de laboratorio, es decir de área de práctica para los cibercriminales que se inician en el hackeo y vulneración de sistemas de seguridad informáticos, por otro lado también se indica por parte de los sujetos de investigación que la incidencia de la criminalidad cibernética no es clara ni precisa debido a los casi nulos centros de asesoramientos y atención que hay a nivel nacional en temas de cibercriminalidad, por lo que en gran parte de los afectados por este tipo de criminalidad pasan a formar parte de la cifra flotante de impunidad en el país.

Discusión

Guatemala no es el único país donde peligra la seguridad de las personas en la red, este tema es de carácter global tal como lo describen los sujetos de investigación, ya que se ha dado a conocer a través de los diversos medios de comunicación la manera en que estos criminales operan y causan graves daños en distintos sectores de la sociedad, dicha referencia encaja con la información expuesta en el presente trabajo sobre la naturaleza del ciberdelito y ciberdelincuencia; es casi generalizado la idea de que en el país afecta principalmente este fenómeno delictivo a nivel financiero como se puede visualizar en las campañas que las entidades financieras promueven para que sus clientes no puedan ser victimizados, la creciente tendencia del uso de los TICs en menores y de la mano la penetración del internet residencial en la población aumenta potencialmente la exposición ante la cibercriminalidad; por otro lado el hecho de que la ciberdelincuencia no sea de origen local impide aún más la realización de una investigación efectiva en tanto el Estado no procure la atención debida en temas de ciberdelitos la cifra de impunidad en los ciberataques seguirá aumentado.

- **¿Cuál es la limitante para la investigación criminal en delitos informáticos?**

La tercera pregunta de la entrevista consiste en que los sujetos de investigación determinen cuales son las limitantes para la investigación criminal en los delitos informáticos a lo que casi en su totalidad respondieron con la ausencia de una legislación vigente y específica sobre ciberdelitos como también alguna regulación jurídica sobre la protección plena de los datos personales y la ausencia de convenios o recursos de mediación para obtener datos de servidores de alojamientos fuera del país que permita la obtención de la información necesaria para la determinación posible del origen del ataque, el modo de operación y el o los responsables del hecho, por otro lado también existe la falta de una política interinstitucional que permita articular esfuerzos de cada una de las dependencias estatales encargadas de la investigación criminal para el correcto procedimiento de los casos informáticos forenses, también se hace mención de la falta de profesionales en el área de informática forense, así mismo se indica por los sujetos de investigación que aún hay algunos funcionarios judiciales que no han entendido

completamente el valor probatorio que la evidencia informática provee por lo que en algunos casos es descartado esta área para la resolución de los casos.

Discusión

La investigación forense de hechos relacionados con el ciberespacio en Guatemala aun es poco frecuente debido a muchas limitantes iniciando con que las operaciones o ataques de naturaleza cibernética se realiza desde puntos que no pueden ser localizados, debido a que los autores se encargan de emplear técnicas que ocultan la ubicación del dispositivo desde donde se realiza el ataque lo cual complica la labor de definir un sospechoso en concreto, a nivel nacional existen algunas regulaciones jurídicas que obligan o facilitan que ciertas empresas brinden información respecto algún hecho investigado, sin embargo, las leyes locales no tiene alcance internacional por lo que limita la eficacia y desarrollo de una investigación relacionada al área informática debido que los servidores de alojamiento de las páginas web o plataforma digital donde se haya realizado un hecho criminal se encuentran fuera de las fronteras de Guatemala lo que hace que las empresas propietarias de dichos servidores no estén obligadas a facilitar información o datos respecto a un incidente donde sus servidores estén o hayan sido utilizados para la ejecución de un ataque malicioso cibernético.

En lo relacionado a las limitantes de la investigación de ciberdelitos existe a nivel local un detalle muy importante que las autoridades encargadas de su gestión han hecho a un lado y le han quitado importancia y es la creación de una legislación específica sobre ciberdelitos, lo que vulnera aún más la efectividad y reacción que puedan tener las entidades encargadas de la persecución penal de los hechos ilícitos, también se indica por parte de los sujetos de investigación que muchos de los funcionarios encargados de la impartición de justicia actualmente le quitan valor probatorio a las evidencias electrónicas y digitales perdiendo así la oportunidad de poseer un sistema de justicia mucho más cercana a la verdad histórica de los hechos ocurridos, existe también una escasez considerable de profesionales dedicadas al área de informática forense, esto por la inconciencia que muchos sectores de la sociedad guatemalteca aún tiene sobre la ciberdelincuencia.

De los expuesto es importante hacer hincapié en que el planteamiento del problema del presente trabajo de investigación se había considerado como uno de los puntos relevantes sobre los avances en la investigación criminal en Guatemala con relación al phishing, grooming y spoofing la falta de una tipificación jurídica de los mismos, que provea a los entes encargados de impartir justicia de una herramienta, para la persecución, investigación y sanción de los responsables de dichos hechos, por lo tanto con lo definido por los sujetos de investigación se puede confirmar que la falta de la legislación específica en temas de ciberdelitos hace que muchos de los mismos queden sin ser investigados y que los afectados estén totalmente expuesto y abandonados por el sistema judicial del país al menos en los casos de phishing, grooming y spoofing.

La carencia de una tecnificación o capacitación específica a muchos de los investigadores actuales, hace que se cometan muchos errores en relación al procesamiento, obtención, extracción, almacenamiento, análisis y presentación de resultados de evidencia digital, la falta de coordinación y cooperación interinstitucional para la investigación Informática es otro elemento que los sujetos de investigación señalan como esencial para el desarrollo de una estrategia efectiva en el procesamiento de hechos criminales informáticos, de esta cuenta se puede indicar que por causa de todo lo mencionado en cuanto a limitantes en la investigación criminal de hechos informáticos existe una brecha donde se da el crecimiento y operación de delincuencia transnacional que son responsables de otros delitos comunes como la trata de personas, el tráfico y comercio ilícito de armas de fuego, por citar unos ejemplos.

- **¿Cuáles son los ciberdelitos que se cometen con más frecuencia en el territorio nacional?**

Como cuarta pregunta de la entrevista es en relación a cuales son los ciberdelitos que se cometen con más frecuencia en el territorio nacional, los sujetos de investigación pertenecientes a la policía nacional civil indican que de los ciberdelitos que con más frecuencia se investigan es lo relacionado a la pornografía infantil, posesión y distribución de material con contenido de violencia sexual hacia menores y la captación de menores de edad en las redes sociales con fines de trata de personas, por otro lado algunos

sujetos de investigación pertenecientes al ministerio público manifiestan que de los casos conocidos sobre ciberdelitos es en relación a la clonación de tarjetas de crédito o robo de datos de tarjetas de crédito, fraudes y robo de credenciales de acceso, sin embargo se menciona también que se ha sabido de otras modalidades cibernéticas delictivas pero que en ocasiones no proceden contra ellas debido a que son casos que no trascienden debido a la falta de un instrumento jurídico que los respalde y de paso a su persecución penal.

Discusión

Está claro que a nivel global y en Guatemala los ciberdelitos están presentes, pero para el interés de este trabajo y con al apoyo de los sujetos abordados para la investigación se define que a nivel local los ciberdelitos con más frecuencia son la clonación de tarjetas de crédito, el robo de identidad principalmente en redes sociales, robo de credenciales, muchos de estos se resume en phishing y spoofing para el caso de empresas, así también está presente la pornografía infantil o material con contenido de abuso sexual a menores que si se encuentra tipificado por la ley nacional vigente, el sexting, el ciberacoso, la captación de menores para trata de personas, secuestro o chantaje, muchos de estos casos se resume en grooming, debido a que en gran parte de las situaciones los menores victimizados en estos ciberdelitos suelen ser abordados por acosadores o pederastas desde las plataformas web donde ocultan su identidad y persuaden a los menores de enviar o compartir videos o imágenes que vulneren el pudor de las víctimas.

- **¿Qué protocolos o métodos utiliza la institución para los hechos informáticos?**

Como quinto punto de la entrevista se cuestiona en relación a los protocolos o métodos utilizados en hechos informáticos por las distintas instituciones a las que pertenecen los sujetos de investigación a lo que se menciona la norma ISO/IEC 17025, para los procesos de laboratorio forense, tomando buenas prácticas, algunas guías a nivel internacional para la adquisición, preservación, obtención, presentación y almacenamiento de la evidencia digital como el RFC 3227, NIST 800-86, NIST 800-101,

así mismo se indica por parte de los sujetos el empleo de procedimientos internos que no se especifican en concreto cuales son, pero que se asegura están basadas en normas y protocolos internacionales.

- **¿Qué recursos se posee actualmente para la investigación forense del cibercrimen?**

En la sexta pregunta de la entrevista los sujetos deben responder con respecto a los recursos que se posee actualmente para la investigación forense del cibercrimen, en los que responden y mencionan equipos y programas forenses, estaciones FRED, equipo forense de extracción de datos de dispositivos móviles, programas para el manejo y restauración de evidencia digital, programas para el análisis de información de dispositivos móviles, herramientas nativas de redes sociales, insumos para el embalaje de la evidencia informática, unidades institucionales de información, investigación y operación de la delincuencia, unidades de inteligencia y tecnología, dispositivo universal de extracción de información forense.

Discusión

Los esfuerzos que se realizan actualmente para el tratamiento del cibercrimen hacen que las herramientas para la investigación que son descritas por los sujetos de investigación en el sexto cuestionamiento de la entrevista, sean en ocasiones insuficientes o inefectivas, por el diferendo operativo que existe entre las instituciones en cuanto a investigación de casos informáticos se trata como fue observado en las respuestas brindadas por los sujetos de investigación en la quinta interrogante, debido a la falta de una estandarización general sobre el procesamiento, documentación, fijación, embalaje, transporte, análisis y almacenamiento de la evidencia informática lo cual abre aún más el margen de error que desfavorezcan totalmente a la investigación y distorsionen resultados debido a que hoy por hoy existen protocolos y estándares que fueron abordados en un apartado del presente trabajo el cual todas las instituciones encargadas de la investigación criminal deberían estar sujetas, sin embargo en Guatemala hasta el momento no se encuentra estandarizado el procesamiento de incidentes cibernéticos al

menos en las unidades de análisis abordados en el presente trabajo que son la policía nacional civil, ministerio público y el instituto nacional de ciencias forenses.

- **¿Qué conoce del ciberdelito phishing, grooming y spoofing?**

La séptima pregunta solicitar a los sujetos de investigación que definan lo que saben sobre el phishing, grooming y spoofing, a lo que la mayoría responde como phishing al robo de datos personales, correos, contraseñas, cuentas bancarias, tarjetas de crédito, en general es definida por los sujetos de investigación como una estafa a los usuarios desprevenidos de los dispositivos tecnológicos, además que indican que regularmente estos eventos se dan en plataformas bancarias y redes sociales, con relación al grooming, algunos lo detallan como lo referente a un acoso desde una perspectiva sexual aunque por otro lado se indica por parte de profesionales en el área informática como un ciberdelito de acoso a menores de edad principalmente en redes sociales, donde el acosador entra en contacto con la víctima utilizando distintas formas de persuasión y cierto nivel de carisma al mantener conversaciones con los menores, hasta que logran entablar un nivel de confianza donde inicia a solicitar fotografías y videos principalmente y si todo marcha bien para el acosador, en ocasiones tratan de pactar un encuentro personal con la víctima, este tipo de acosadores son en general pederastas disfrazados; el spoofing es conocido por los sujetos de investigación como el proceso de engaño, mediante el uso de técnicas de suplantación de identidad en ocasiones con fines malicioso y a veces con fines investigativos ya que no solamente es usado para el secuestro de información, sino también para la obtención de información en un caso de investigación donde exista una red compartida de datos y donde varias computadoras estén conectadas a un mismo host interfiriendo en el tráfico de la red.

Discusión

De los antecedentes desarrollados en el presente documento sobre el phishing, grooming y spoofing son concluyentes con la descripción dada por los sujetos de investigación en relación a que el phishing es una técnica informática que busca hacer caer por medios engañosos a las victimas con el fin de facilitar información personal sensible o confidencial como pueden ser contraseñas, correos electrónicos, nombres de usuario,

claves de acceso, cuentas bancarias y credenciales de redes sociales, por otro lado el grooming en primera instancia es señalada como un hecho de carácter sexual sin embargo es importante resaltar que el grooming concluye muchas veces en la obtención de material con contenido sexual de menores, pero inicia con el acoso de una persona mayor hacia un menor, empleando diferentes métodos para hacerle bajar la guardia a la víctima y crear un ambiente de confianza para luego solicitar distintos favores a los menores que posteriormente se define con exigencias y amenazas hacia la victima por parte del acosador o groomer, el spoofing es descrito como un proceso de engaño para el secuestro de información según los sujetos de investigación sin embargo el carácter principal del spoofing es el de la suplantación de identidad mediante diferentes y muy variadas técnicas informáticas que buscan falsificar los datos en un sistema de comunicación, es de relevancia mencionar que de la respuesta brindada a la séptima interrogante se refiere al uso del spoofing para la obtención de información en un sistema de redes que comparte un mismo centro de datos del cual puede ser analizado para la extracción de información importante para una investigación.

- **¿Quiénes tienen un mayor riesgo de ser víctimas de un ciberdelito?**

La octava interrogante es sobre quienes tienen un mayor riesgo de ser víctimas de phishing, grooming y spoofing, los sujetos de investigación enlistan a un grupo mayormente vulnerable a estos ciberdelitos y son las personas confiadas, menores de edad, pequeñas y medianas empresas que no invierten en un sistema de ciberseguridad, personas que ingresan a páginas web sin ningún tipo de control o filtro de seguridad, personas que realizan descargas desde fuentes no oficiales, personas consideradas como adultos mayores y algunas otras personas que simplemente desconocen esta modalidad delictiva, considerando a la sociedad guatemalteca con una gran población sin instrucción académica y desconocimiento total en temas de tecnología.

Discusión

Los individuos con mayor vulnerabilidad en ciberdelitos identificados por los sujetos de investigación en la octava interrogante son los menores de edad, adultos mayores que desconocen sobre ciberseguridad y ciberdelincuencia, personas confiadas o

desprevenidas al navegar en el ciberespacio, empresas que manejen base de datos de clientes, sin un adecuado sistema de ciberseguridad, de esta cuenta se puede complementar que nadie es absolutamente seguro en la red debido a las muy variadas y distintas formas de operación de los cibercriminales que ha sido abordado en la presente investigación en los distintos apartados sobre ciberdelitos y los peligros existentes en la red.

- **¿Cuáles son las recomendaciones para evitar ser víctima del phishing, grooming y spoofing?**

La novena pregunta solicita a los entrevistados mencionar algunas recomendaciones para evitar ser víctimas de phishing, grooming y spoofing al cual respondieron con las siguientes evitar ingresar a cualquier link o enlace que llegue al correo electrónico, establecer un control parental para los menores de edad, no brindar teléfonos con acceso a internet a niños menores de doce años, evitar que los menores de edad tengan redes sociales y si las tienen estar en constante monitoreo por parte de los padres, no acceder a links cortos, no descargar programas de páginas dudosas, no ingresas credenciales (usuarios o contraseña) en cualquier página sin antes verificar que sea la página oficial, revisar los certificados de seguridad de cada página con la que se interactúa principalmente si en ella se realizan compras, transacciones bancarias, para los cuentahabientes en caso de tener dudas o sospechar de un mensaje recibido en el teléfono celular, correo electrónico o redes sociales acudir de inmediato a su banco y resolver su situación.

Discusión

Existen varias recomendaciones sobre los cuidados en el ciberespacio, para evitar ser victimizado por algún ataque malicioso dichas recomendaciones son la verificación de autenticidad de las páginas desde donde se realizan consultas, compras o descargas, así mismo el monitoreo de los menores en el uso del internet para no ser captados por algún malintencionado cibernauta, implementar medidas rigurosas de seguridad personal desde la instalación de un antivirus y otros filtros de seguridad para disminuir aún más la probabilidad de un ciberataque que pueda causar daños lamentables; en el apartado

sobre medidas para la ciberseguridad y seguridad en la red se mencionan algunos elementos que desde luego deben y tienen que ser tomados en cuenta para evitar en la medida posible una red personal o empresarial sea vulnerada y por ende concluya en daños costosos.

- **¿Qué avances o atrasos considera que ha tenido Guatemala en sus diferentes dependencias para combatir el cibercrimen?**

La décima pregunta solicita a los sujetos de investigación mencionar los avances o atrasos que consideren que ha tenido Guatemala en sus diferentes dependencias para combatir el cibercrimen, las respuestas fueron que actualmente se cuenta con unidades de tecnología e información en varias de las dependencias estatales, existe un instituto nacional de ciencias forenses donde hay una sección de informática forense, ya existen algunas entidades privadas dedicadas a la investigación de informática forense, en la policía nacional civil se cuenta con una sección de delitos informáticos así mismo en el ministerio público; en los atrasos se indica la falta de una política nacional encaminada a la colaboración interinstitucional para la investigación criminal de ciberdelitos, no existe una política nacional de ciberseguridad, no hay un presupuesto para el desarrollo y seguridad de las tecnologías, hace falta un comité nacional que inspecciones las operaciones cibernéticas, de la misma manera se requiere de la especialización o capacitación de los funcionarios públicos en temas de informática forense para la estandarización operativa de cada uno de ellos en la escena de crimen informática, procesamiento, recolección, embalaje, transporte y análisis de la evidencia Informática y sobre todo Guatemala no cuenta con un ordenamiento jurídico que regule todos aquellos ilícitos relacionados a los delitos informáticos.

Discusión

Se ha mencionado por parte de los sujetos de investigación varios avances y atrasos que Guatemala tiene en el tema de la investigación forense en incidentes informáticos, sin embargo, ninguno de los elementos disponibles para la investigación de ciberdelitos es efectivo sin una legislación específica en el tema informático, en el código penal guatemalteco hace referencia sobre algunos ciberdelitos, mismas que no responden a la

necesidad actual, debido a la innegable variación de las tecnologías de la información, se cuenta con una iniciativa de ley la cual fue dado a conocer al honorable congreso de la república de Guatemala y que fue brevemente abordado en el presente trabajo, pero ha quedado estancada, hasta el momento solo se tiene regulación sobre el comercio electrónico contenida en el decreto 47-2008 ley para el reconocimiento de las comunicaciones y firmas electrónicas, con base a la existencia de esta ley se hace aún más necesario emitir una ley especial para prevenir y sancionar los delitos de naturaleza informática que pudieran afectar el objeto material de la normativa del comercio electrónico y todos aquellos actos ilícitos de naturaleza informática.

Esta investigación realizada con el apoyo de varios profesionales y expertos en el área de informática tenía por objetivo general, exponer información respecto al desarrollo de los cibercriminales, los antecedentes y avances que han obtenido en la investigación del cibercrimen, lo que se ha alcanzado en los diferentes capítulos del presente trabajo. Para este proyecto de investigación se tenían objetivos específicos siendo el primero de ellos, definir el delito informático, sus antecedentes, características y clasificación, este mismo fue alcanzado y abordado en los capítulos dos y tres, donde se define los relacionado a ciberdelitos, las características principales que estos poseen, las diferentes maneras en que pueden ser realizados, como segundo objetivo específico se tenía el referir estándares internacionales para la extracción de indicios digitales, dicho tema se abordó en el cuarto capítulo en el apartado sobre características de la evidencia informática, métodos de extracción y protocolos internaciones sobre evidencia informática acompañado de sus entandares internacionales para la escena de crimen digital el cual algunos de los indicados por organizaciones internacionales sobre cibercrimen son utilizados en Guatemala como el RFC 3227, NIST 800-86, NIST 800-101 y otros protocolos referidos a nivel; como tercer objetivo específico se tenía trazado, mencionar el perfil del perito informático y su rol dentro de las investigación criminal de los delitos informáticos, este mismo fue tratado en el cuarto capítulo de la tesis en el apartado sobre el perito informático donde se detalla las calidades y cualidades que debe poseer el perito informático al desempeñarse en la investigación forense; como cuarto y último objetivo específico se tenía señalado presentar los avances que han obtenido en Guatemala con

respecto a la investigación criminal de los delitos informáticos en comparación con otros países, este fue abordado en distintos apartados de los capitulo tercero y cuarto donde se desarrollan temas sobre las herramientas y disposiciones legales que Guatemala ha adoptado y tiene en proceso de adopción para el tratamiento, persecución y sanción de ciberdelitos, es importante indicar que a través del desarrollo del trabajo de investigación cada uno de los objetivos fueron alcanzados, mediante la recopilación de información documental y con el aporte proveído de los sujetos de investigación que se ha mencionado a lo largo de esta sección de presentación y discusión de resultados.

Con el trabajo de investigación que se ha realizado en la presente tesis se permite responder a la pregunta de investigación que se trazó al inicio del proyecto siendo ella ¿Cuál ha sido la evolución de la investigación criminal del phishing, grooming y spoofing en Guatemala?, la respuesta es que la evolución en la investigación de dichos ciberdelitos aun es poca debido a cada una de las carencias que se ha mencionado a lo largo del presente capítulo de resultados y con los análisis realizados los instrumentos disponibles actualmente para el phishing, grooming y spoofing, son inefectivos para su investigación, iniciando principalmente con que ahora mismo en Guatemala dichos temas aun no son delitos por la carencia de una legislación que los tipifique como tal y a su lado la falta de un plan vigente sobre ciberseguridad a nivel nacional que involucre directrices y objetivos interinstitucional sobre ciberseguridad y cibercrimen.

CONCLUSIONES

- Los delitos informáticos son todos aquellos actos que permiten la comisión de agravios, daños y perjuicios en contra de las personas, grupos, organizaciones y entidades, ejecutados por lo general por el ciberespacio y con el uso de computadoras con el fin de destruir, dañar o secuestrar información altamente importante, que pueden llegar a causar inestabilidad e interrumpir el funcionamiento correcto de sectores como salud, economía, seguridad y todas las dependencias estatales debido a que la mayor parte de estos ataques van dirigidos a la infraestructura.

- Para la investigación y adecuado procedimiento de los incidentes informáticos se deben seguir una serie de guías y pautas que permitan por un lado recolectar, preservar y analizar la evidencia informática adecuadamente, y por otro presentar resultados eficaces, la aplicación de estándares y protocolos internacionales en la investigación forense logra el alcance de una adecuada identificación de líneas de investigación, enlace de los indicios al hecho ocurrido y reducción de riesgos en cuanto a la pérdida, daño, destrucción de la evidencia informática que posteriormente se traduce en el resultado satisfactorio de una investigación.

- El perito informático es aquel profesional cuyo objetivo y función en una investigación es la de emitir dictámenes o informes periciales interpretando y analizando la evidencia informática de donde se extrae información que coadyuve a la reconstrucción de los hechos en un incidente informático, así mismo asiste en el conocimiento técnico sobre los sistemas de información tecnológicos en un proceso legal donde los funcionarios judiciales carecen de dicho entendimiento.

- Guatemala actualmente no cuenta con una estrategia nacional para el desarrollo y educación sobre ciberseguridad, por lo que solo se tiene una capacidad limitada de investigar y sancionar los incidentes delictivos de naturaleza cibernética, hasta que no se cuente con una legislación integral vigente sobre delincuencia informática el sistema judicial nacional seguirá teniendo dificultades para el proceso eficaz de dichos casos, dichas limitantes seguirán aumentando y

vulnerando a la sociedad guatemalteca como también a las instituciones estatales que son el principal objetivo de ciberataques.

RECOMENDACIONES

- Es necesario la integración de esfuerzos a través de metodologías operativas basadas en la transparencia, seguridad y desarrollo continuo desde la sociedad civil, académicos, instituciones estatales y organismos internacionales que coadyuven en la mitigación, reacción, prevención y tratamiento de eventos cibernéticos atendiendo a un plan resiliente que fortalezca en el menor tiempo posible los servicios o sistemas vulnerados en la infraestructura nacional.

- Al ministerio público, policía nacional civil y el instituto nacional de ciencias forenses crear un manual interinstitucional que permita la articulación y coordinación de esfuerzos en el procesamiento, fijación, recolección, embalaje, transporte, análisis de la evidencia informática específicamente, basada en normas y protocolos internaciones que permita la reducción en el margen de riesgos sobre le evidencia informática.

- Al instituto nacional de ciencias forenses es importante descentralizar y crear unidades departamentales de laboratorio de informática forense para poder agilizar mucho mejor la atención y reacción ante los peritajes informáticos forenses requeridos por las identidades encargadas de la investigación criminal.

- Al consejo nacional de seguridad como máxima autoridad del sistema nacional de seguridad es importante que promuevan en conjunto con el órgano legislador la creación y aprobación de una ley específica en ciberdelitos y protección de los sistemas informáticos apegado al convenio de Budapest como referencia para la verificación interna de dicha legislación, acompañado del desarrollo de una política de divulgación y educación nacional en ciberseguridad para ampliar los alcances y disminuir riesgos desde la población civil hasta los funcionarios públicos de cada una de las dependencias del Estado así mismo se requiere de un comité multidisciplinario para la evaluación de riesgos y detección de amenazas en los sistemas informáticos del país, donde se persiga el monitoreo permanente del acceso a dichos sistemas y los usuarios.

REFERENCIAS

Bibliográficas

1. Acurio Del Pino, Santiago. *"Delitos informáticos".* Ecuador, Pág. 22.
2. Antón Barbera, Francisco. *"Policía científica I"*, España, editorial Universidad de Valencia, 1990.
3. Arburola Valverde, Allan. *"Criminalística parte general".* México, Pág. 44.
4. Carceller Cheza, Román y otros. *Servicio en Red*. España, editorial Macmillan Iberia, S.A., 2013.
5. Castro Cuenca, Carlos Guillermo. *"Manual de teoría del delito"*. Colombia, editorial Universidad del Rosario, 2017.
6. Colmenares Mendoza, Alberto Yesid. Diego, Cruz Guzmán. *"Importancia de la informática forense".* México, editorial Centro universitario México AC, 2013.
7. Cruz Quintero, Gloria Esperanza. "Importancia de la informática forense". Colombia, Pág.17.
8. Díaz Alonso, Arturo. *"Informática I".* México, editorial FCA, 2003.
9. Escrivá Gascó, Gema y otros. *"Seguridad informática".* Editorial Macmillan, 2013.
10. Fernández Montoto, Carmen, Montes de Oca Richardson, Martha. *"Computación: herramientas informáticas".* Cuba, editorial Félix Varela, 2005.
11. Gallardo, Erik de Luis. *"La seguridad para los menores en internet".* España, editorial UOC, 2017.
12. Garrote García, Rubén. *"Ingeniería inversa teoría y aplicación".* España, editorial Ra-Ma, 2017.
13. Girón Palles, José Gustavo. *"Teoría del delito".* Guatemala, editorial Instituto de la Defensa Pública Penal, 2013, Pág. 3, 2da. Edición.
14. Góchez, Rafael Francisco. *"Los riesgos en las redes sociales virtuales",* 2009.
15. González Cauhapé, Eduardo. *"Apuntes de derecho penal guatemalteco".* Guatemala, 2003.
16. González, Leandro. *"Responsabilidad legal en redes sociales de internet".* Argentina, 2010.
17. Jiménez, Francisco. *"Manual de Criminalística de campo Policía Nacional".* Colombia, 2004.
18. López Abrego, José Antonio (Comp), *"Criminalística actual, ley, ciencia y arte",* España, 2012, Ediciones Euroméxico, S.A. de C.V.
19. López Delgado, Miguel. *"Análisis forense digital",* 2007.
20. López Rodríguez, Raúl Estuardo. *"Introducción a la criminalística y ciencias forenses"*. Guatemala, 2019.
21. López, Oscar y otros. *"Informática forense".* Colombia, Miramar, Pág.23.
22. Molero Prieto, Xavier. *"Un viaje a la historia de la informática".* España, editorial Universitat Politécnica de Valéncia, 2016.

23. Montiel Sosa, Juventino. *“Criminalística 1”.* México, editorial Limusa, 2007, 2da. Edición.
24. Moreno, R. *“Introducción a la criminalística”.* México, editorial Porrúa Hermanos, 2000.
25. Nessi, Alan Martín.*” Manual de evidencia digital”*. Perú, Ministerio de justicia y derechos humanos, 2017.
26. Orrego Pinzón, Jhon Leonardo y Jonathan Vargas Roa. “*Manual para manejo de la evidencia digital”*, Colombia, Universidad Autónoma de Colombia, 2017.
27. Rossotto Herman, Beatriz. *“Manual de criminología y criminalística”*, Guatemala, 2016, Pág. 187, 13 edición.
28. Rodríguez Más, Francisca y Alfredo, Doménech Rosado, “La informática forense: El rastro digital del crimen”, *Derecho y cambio social*, No. 25, ISSN-e 2224-4131, 2011, Pág. 18.
29. *“Ciberfensa-ciberseguridad riesgos y amenzas”.* Argentina, editorial Cari, 2013.
30. SEMA, Red.es. *“Guía clínica sobre el ciberacoso para profesionales de la salud”.* España, Gobierno de España, 2015.
31. Téllez Valdés, Julio. *“Delitos cibernéticos”.* México, editorial UNAM, 2008.
32. Universidad de Málaga. *“Introducción a los computadores”*. España, editorial E.T.S.I., 2004.
33. Villazán Olivares, Francisco José. *“Manual de informática I”*. México, editorial UMSNH, 2009.

Electrónicas

34. Avast, Avast Software S.R.O., Ciberdelito, Estados Unidos, 2015, https://www.avast.com/es-es/c-cybercrime, fecha de consulta 21 de febrero de 2019.
35. BBVA, Castillo Claudia, phishing, vishing, mishing, ¿que son y como protegerse de estas amenazas?, España, 2018, https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/, fecha de consulta 9 de septiembre de 2019.
36. Criminalística Online, RSA, Precursores de la Criminalística, Argentina, 2019, http://criminalistica.online/precursores-de-la-criminalistica/, fecha de consulta 3 de julio de 2019.
37. ECURED, Enciclopedia Cubana, Informática forense, Cuba, https://www.ecured.cu/Inform%C3%A1tica_Forense, fecha de consulta 12 de julio de 2019.
38. El Periódico, Lopéz José David, Daniel Villatoro, El crimen que destruye la inocencia, Guatemala, 2018, https://elperiodico.com.gt/domingo/2018/03/18/el-crimen-que-destruye-la-inocencia/, fecha de consulta 2 de octubre de 2019.

39. INACIF, Instituto Nacional de Ciencias Forenses, Historia, Guatemala, https://www.inacif.gob.gt/index.php/inacif/historia#, fecha de consulta 4 de julio de 2019.
40. ISA, Universidad de Oviedo, *"Introducción a los computadores"*. España, 2019, http://www.isa.uniovi.es/~alonsog/Microcontrolador/T1%20Introduccion%20a%20los%20computadores.pdf, fecha de consulta: 7 de marzo 2021.
41. Kaspersky, AO Kaspersky Lab, Ciberseguridad, España, https://www.kaspersky.es/blog/cybersecurity-tips-for-work/14744/, fecha de consulta 15 de julio de 19.
42. Kaspersky, AO Kaspersky Lab, ransomware, Estados Unidos, https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware, fecha de consulta 23 de febrero de 19.
43. Modo Museo, Museo del objeto del objeto, Fotografía Forense, México, 2015, https://elmodo.mx/el-modo-del-modo/fotografia-forense/, fecha de consulta 3 de julio de 2019.
44. NORTE, ONG Grooming Argentina, peligro en las redes: detectan 4 formas de groomers, 2019, http://www.diarionorte.com/article/182065/peligro-en-las-redes-detectan-4-formas-de-groomers, fecha de consulta 18 de septiembre de 2019.
45. Panda, Panda security, Diez consejos de ciberseguridad que toda empresa debería dar a sus empleados, España, 2016, https://www.pandasecurity.com/spain/mediacenter/empresas/consejos-ciberseguridad-empleados/, fecha de consulta 15 de julio de 2019.
46. Portal electrónico del Diario de Centro América, López Yuri, Mesa técnica analiza proyecto de ley contra ciberdelincuencia, Guatemala, 2019, https://dca.gob.gt/noticias-guatemala-diario-centro-america/mesa-tecnica-analiza-proyecto-de-ley-contra-la-ciberdelincuencia/, fecha de consulta 27 de agosto de 2019.
47. Prensa Libre, Redacción, Identificado autor de falsificación de sitio de Prensa Libre, Guatemala, 2015, https://www.prensalibre.com/guatemala/justicia/identificado-autor-de-falsificacion-de-sitio/, fecha de consulta 2 de octubre de 2019.
48. Summa, Usuarios de banca en línea de Guatemala sufren intentos de phishing, Costa Rica, 2011, https://revistasumma.com/13674/, fecha de consulta 2 de octubre de 2019.
49. SVET, Secretaría contra la Violencia Sexual, Explotación y Trata de personas, Cuidado con el Grooming, Guatemala, http://www.svet.gob.gt/campana/cuidado-con-el-grooming, fecha de consulta 26 de febrero de 2019.
50. SVET, Secretaría contra la Violencia Sexual, Explotación y Trata de personas, Cuidado con el Grooming, Guatemala, http://www.svet.gob.gt/campana/cuidado-con-el-grooming, fecha de consulta 26 de febrero de 2019.

51. Télam, Telenoticiosa América, Ciberdelitos: ¿Cómo pueden afectarnos?, Argentina, 2017, http://www.telam.com.ar/notas/201711/223623-ciberdelitos.html, fecha de consulta 16 de julio de 2019.
52. Vade Secure, Gendren Andrien, Impacto corporativo del phishing, 2015, https://www.vadesecure.com/en/the-corporate-impact-of-phishing/, fecha de consulta 2 de octubre de 2019.
53. Xunta de Galicia Conselleria de educación, Universidade e formación profesional, Xunta de Galicia, Redes y seguridad, España, S/a, https://www.edu.xunta.gal/centros/iesvalleinclan/aulavirtual2/pluginfile.php/14217/mod_resource/content/1/Tema %20redes%20y%20seguridad.pdf, fecha de consulta 18 de febrero de 2019.

Normativas

54. Constitución Política de la República de Guatemala, Asamblea Nacional Constituyente.
55. Código Penal, Congreso de la República de Guatemala, Decreto 17-73.

ANEXOS

Modelo de instrumento

UNIVERSIDAD RAFAEL LANDIVAR

CAMPUS DE QUETZALTENANGO

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES

LICENCIATURA EN INVESTIGACION CRIMINAL Y FORENSE

PROFESION:

TEMA DE TESIS: EVOLUCIÓN DE LA INVESTIGACIÓN CRIMINAL EN EL ROBO DE INFORMACIÓN PERSONAL (PHISHING), ACOSO PEDERASTA (GROOMING) Y SUPLANTACIÓN DE IDENTIDAD (SPOOFING).

Instrumento

Guía de entrevista para profesionales que laboran en el área de informática.

1. ¿Según su experiencia cuál es el estado actual de la seguridad informática en el país?
2. ¿Cómo incide la ciberdelincuencia a nivel nacional?
3. ¿Cuál es la limitante para la investigación criminal en delitos informáticos?
4. ¿Cuáles son los ciberdelitos que se cometen con más frecuencia en el territorio nacional?
5. ¿Qué protocolos o métodos utiliza la institución para los hechos informáticos?
6. ¿Qué recursos se posee actualmente para la investigación forense del cibercrimen?
7. ¿Qué conoce del ciberdelito phishing, grooming y spoofing?
8. ¿Quiénes tienen un mayor riesgo de ser víctimas de un ciberdelito?
9. ¿Cuáles son las recomendaciones para evitar ser víctima del phishing, grooming y spoofing?
10. ¿Qué avances o atrasos considera que ha tenido Guatemala en sus diferentes dependencias para combatir el cibercrimen?