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

"ANÁLISIS DEL USO DE LAS REDES SOCIALES COMO HERRAMIENTA EN LA INVESTIGACIÓN CRIMINAL Y FORENSE EN GUATEMALA EN LOS DELITOS DE PLAGIO O SECUESTRO."

TESIS DE GRADO

ANTONINI ARON RIVAS LÓPEZ
CARNET 22105-14

HUEHUETENANGO, MAYO DE 2022
CAMPUS "SAN ROQUE GONZÁLEZ DE SANTA CRUZ, S. J." DE HUEHUETENANGO

UNIVERSIDAD RAFAEL LANDÍVAR

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE

"ANÁLISIS DEL USO DE LAS REDES SOCIALES COMO HERRAMIENTA EN LA INVESTIGACIÓN CRIMINAL Y FORENSE EN GUATEMALA EN LOS DELITOS DE PLAGIO O SECUESTRO."

TESIS DE GRADO

TRABAJO PRESENTADO AL CONSEJO DE LA FACULTAD DE

CIENCIAS JURÍDICAS Y SOCIALES

POR

ANTONINI ARON RIVAS LÓPEZ

PREVIO A CONFERÍRSELE

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

HUEHUETENANGO, MAYO DE 2022

CAMPUS "SAN ROQUE GONZÁLEZ DE SANTA CRUZ, S. J." DE HUEHUETENANGO

AUTORIDADES DE LA UNIVERSIDAD RAFAEL LANDÍVAR

RECTOR:	P. MIQUEL CORTÉS BOFILL, S. J.
VICERRECTORA ACADÉMICA:	DRA. MARTHA ROMELIA PÉREZ CONTRERAS DE CHEN
VICERRECTOR DE INVESTIGACIÓN Y PROYECCIÓN:	ING. JOSÉ JUVENTINO GÁLVEZ RUANO
VICERRECTOR DE INTEGRACIÓN UNIVERSITARIA:	P. JOSE ANTONIO RUBIO AGUILAR, S. J.
VICERRECTORA ADMINISTRATIVA:	MGTR. SILVANA GUISELA ZIMERI VELÁSQUEZ DE CELADA
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. HUGO DANIEL ALVARADO RODAS

TERNA QUE PRACTICÓ LA EVALUACIÓN

LIC. OSCAR FERNANDO HERNÁNDEZ MARTÍNEZ

HUGO DANIEL ALVARADO RODAS
LICENCIADO EN INVESTIGACIÓN CRIMINAL Y FORENSE

Huehuetenango, 13 de noviembre de 2,021

Señores:

Consejo de la Facultad de Ciencias Jurídicas y Sociales

Universidad Rafael Landívar

Guatemala, C.A.

Conforme nombramiento otorgado por el Consejo de Facultad, para ser asesor de la tesis titulada **"ANÁLISIS DEL USO DE LAS REDES SOCIALES COMO HERRAMIENTA EN LA INVESTIGACIÓN CRIMINAL Y FORENSE EN GUATEMALA EN LOS DELITOS DE PLAGIO Y SECUESTRO"**, del estudiante: **ANTONINI ARON RIVAS LÓPEZ**, quien se identifica con carné universitario número: 22105-14, de la Facultad de Ciencias Jurídicas y Sociales, rindo informe:

1. Se procedió a revisar íntegramente el documento presentado por el estudiante Rivas López, del análisis del mismo, se hicieron una serie de recomendaciones, entre las que cabe mencionar las modificaciones de la organización capitular, la forma de presentación, el contenido, las conclusiones, recomendaciones, forma del citado de información, capítulo final, a fin que dicho documento cumpla con los requerimientos establecidos por la facultad.
2. El estudiante ha realizado las correcciones indicadas y de las misma se derivaron nuevos elementos que hacen de dicha investigación un estudio completo, actual y valioso académica y profesionalmente en materia de investigación criminal y forense, y lo convierte en un valioso material de consulta para estudiantes, profesionales e investigaciones futuras.

HUGO DANIEL ALVARADO RODAS
LICENCIADO EN INVESTIGACIÓN CRIMINAL Y FORENSE

Cumplidos los requisitos, tanto de forma como de contenido del trabajo de grado, en mi calidad de asesor otorgo: **DICTAMEN FAVORABLE**, para que el estudiante pueda continuar con la revisión final de tesis y demás trámites para su respectiva graduación.

Sin otro particular,

Lic. Hugo Daniel Alvarado Rodas

Licenciado en investigación criminal y forense

Colegiado No. 3290.

Lic. Oscar Fernando Hernández Martínez
Abogado y Notario
1ª. calle 0-107, zona 1, Huehuetenango
Teléfono 77641867

Huehuetenango, 5 de mayo de 2,022

Miembros del Consejo
Facultad de Ciencias Jurídicas y Sociales
Universidad Rafael Landívar

Respetable órgano colegiado:

Informo que, oportunamente se me nombró Revisor del trabajo de investigación del estudiante ANTONINI ARON RIVAS LÓPEZ carné 2210514, titulado: "Análisis del uso de las Redes Sociales como herramienta en la Investigación Criminal y Forense en Guatemala de los delitos de Plagio o Secuestro"

Asimismo, hago de su conocimiento que, al haber efectuado el estudio y análisis correspondiente, he determinado que la presente investigación de tipo monográfica-descriptiva, es un aporte a las Ciencias Criminalísticas. A través de una amplia y minuciosa revisión documental relacionada a la problemática vinculada con el incremento de hechos delictivos relacionados al plagio o secuestro en el departamento de Huehuetenango; fue posible establecer que plataformas y programas de redes sociales han encontrado un espacio propicio para servir de instrumento en la ejecución de actos criminales como lo es el plagio o secuestro. Los métodos deductivos, analítico y sintético fueron utilizados para dar valoración a los elementos que componen cada uno de los capítulos y establecer conclusiones y recomendaciones; el histórico que permitió contextualizar temporalmente las instituciones en el área criminal, así como procedimientos de investigación criminal pertinentes y analizados en el presente estudio. La técnica utilizada fue la indirecta de bibliografía y la directa de encuesta. Las conclusiones, recomendaciones guardan coherencia; así mismo la redacción del documento es clara y fluida.

La investigación del bachiller ANTONINI ARON RIVAS LÓPEZ carné 2210514 cumple con los requisitos de forma requeridos por el Instructivo para la elaboración de tesis de graduación de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Rafael Landívar y los aspectos sustantivos o de fondo de toda investigación científica, por tanto, emito DICTAMEN FAVORABLE.

Atentamente,

Licenciado
Fernando Hernández Martínez
Abogado y Notario

Oscar Fernando Hernández Martínez
Colegiado 11,652

Universidad Rafael Landívar
Tradición Jesuita en Guatemala

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
No. 073015-2022

Orden de Impresión

De acuerdo a la aprobación de la Evaluación del Trabajo de Graduación en la variante Tesis de Grado del estudiante ANTONINI ARON RIVAS LÓPEZ, Carnet 22105-14 en la carrera LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE, del Campus de Huehuetenango, que consta en el Acta No. 07235-2022 de fecha 5 de mayo de 2022, se autoriza la impresión digital del trabajo titulado:

"ANÁLISIS DEL USO DE LAS REDES SOCIALES COMO HERRAMIENTA EN LA INVESTIGACIÓN CRIMINAL Y FORENSE EN GUATEMALA EN LOS DELITOS DE PLAGIO O SECUESTRO."

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 13 días del mes de mayo del año 2022.

Facultad de Ciencias Jurídicas y Sociales

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

DEDICATORIA

A DIOS

Por permitirme cumplir un sueño y sobre todo agradezco a él ya quien es de donde emana la sabiduría y la inteligencia. Proverbios 2:6-7: Porque Jehová da la sabiduría, y de su boca viene el conocimiento y la inteligencia. Él provee de sana sabiduría a los rectos; Es escudo a los que caminan rectamente.RV60.

A MI PADRE

Gregorio Rivas Martínez

Por todo el apoyo incondicional que me brindó en cada una de las etapas de mi vida, especialmente en este proceso de aprendizaje, aunque ya no esté conmigo, pero me enseñó a luchar por mis sueños y metas trazadas. Gracias padre, lo amo mucho.

A MI MADRE

Berta Leticia López López

Por ser la mejor madre del mundo y por el apoyo incondicional que me ha brindado en cada una de las etapas de mi vida, especialmente en este proceso de aprendizaje que ha sido un pilar fundamental en esta meta trazada. Muchas gracias madre, la amo.

A MI ESPOSA

Karen Jannina Hernández Gómez

Por el apoyo incondicional que me ha brindado en esta etapa de aprendizaje y por ser la persona que lucha juntamente conmigo en mis metas y sueños trazados. La amo mucho, mi querida esposa.

A MIS HIJOS

Antony Adrian Rivas Hernández

Liam Yurem Aarón Rivas Hernández

Por ser la parte más importante de mi vida y ser el motor que me generó energía para culminar este proceso de aprendizaje en mi vida. Los amo hijos.

RESPONSABILIDAD: El autor es la única persona responsable del contenido y de los resultados obtenidos en la presente investigación.

ÍNDICE

Contenido Página

RESUMEN EJECUTIVO

El objetivo de esta investigación es identificar y determinar el uso de las redes sociales como herramienta en la investigación criminal y forense en Guatemala en los delitos de plagio y secuestro, debido a que la delincuencia ha encontrado en las redes sociales un nicho para operar, especialmente en lo vinculado con este delito.

La investigación obedece a la problemática vinculada con el delito de plagio y secuestro que se ha venido incrementando en los últimos años en el municipio de Huehuetenango, departamento de Huehuetenango, donde se han utilizado las redes sociales para perfilar a las víctimas y llegar a la comisión del delito. Esto ha conducido a plantear esta investigación, en la modalidad de monografía, para analizar el aporte de la informática forense para esclarecer este tipo de delitos y coadyuvar para la individualización del delincuente y lograr la sentencia de los mismos.

Se utilizó la técnica de análisis bibliográfico y la encuesta estructurada a miembros de la Unidad de Antisecuestros y miembros de la Sección contra Delitos Informáticos de la Subdirección General de Investigación Criminal, ambas unidades pertenecen a la Policía Nacional Civil -PNC-. Los resultados indican que, en la actualidad, con el fenómeno de las redes sociales han surgido nuevos delitos, tales como grooming, sexting, sextortion, cyberbullyng, phishing y otros. No obstante, también los viejos delitos han encontrado en las mismas un espacio propicio para llegar a sus víctimas, tales como el plagio o secuestro, entre otros, donde éstas son muy importantes para perfilar a las víctimas.

INTRODUCCIÓN

Actualmente el creciente uso de las redes sociales está jugando un papel importante en las investigaciones de delitos, en virtud de la facilidad con que cualquier usuario puede subir prácticamente cualquier cosa en videos o fotografías. Internet ofrece nuevas oportunidades delictivas en connivencia con la proliferación de las nuevas tecnologías, tales como smartphones, tabletas, ordenadores, entre otros.

En este sentido, la utilización de los actuales avances tecnológicos en las tareas de investigación criminal y forense, es esencial para la persecución y resolución de algunos delitos, como el caso del plagio y secuestro, especialmente en aquellos casos en que las Tecnologías de la Información y la Comunicación (TIC) desempeñan un papel muy importante. En este orden de ideas, su utilización constituye el presente y el futuro de la investigación criminal y forense en el país.

La universalización de las redes sociales obliga a estudiarlas y analizar su participación en el desarrollo de conductas delictivas. Por ello, surgió esta pregunta de investigación: ¿Cuál es la importancia de las redes sociales como herramienta en la investigación criminal y forense en Guatemala en los delitos de plagio y secuestro? Como objetivos específicos, se planteó la necesidad de identificar las nuevas tendencias delictivas que han encontrado un espacio propicio en las redes sociales para llegar a sus víctimas, describir el uso de las redes sociales como herramienta en la investigación criminal y forense, analizar el uso de las redes sociales en el delito de plagio o secuestro

y, describir los procedimientos para la investigación del delito de plagio o secuestro a través de las redes sociales.

Por ello, mediante la modalidad de monografía, se partió de la identificación de las nuevas tendencias delictivas que han encontrado un espacio propicio en las redes sociales para llegar a sus víctimas. Luego, se realizó una descripción del uso de las redes sociales como herramienta en la investigación criminal y forense. Posteriormente, se realizó un análisis del uso de las redes sociales en el delito de plagio o secuestro. A continuación, se realiza una descripción de los procedimientos para la investigación del delito de plagio o secuestro a través de las redes sociales. Finalmente, se presenta el análisis y discusión de los resultados obtenidos mediante el trabajo de campo.

La investigación se realizó en el municipio y departamento de Huehuetenango, incluye información de aportada por los miembros de la Unidad de Antisecuestros y miembros de la Sección contra Delitos Informáticos de la Subdirección General de Investigación Criminal, ambas unidades pertenecen a la Policía Nacional Civil -PNC-, de la ciudad de Guatemala. Para la recopilación de la información, se utilizó el cuestionario.

Como límites de la investigación, el Ministerio Público no cuenta con una Fiscalía Especial Contra Delitos Informáticos. Además, son pocos los profesionales idóneos especializados en temas vinculados con el cibercrimen. Por otra parte, no existen carreras judiciales especializadas en el cibercrimen.

El propósito de la presente investigación es identificar las necesidades de la investigación criminalística y así coadyuvar en la investigación y resolución de hechos criminales vinculados con las redes sociales. La investigación ofrece procedimientos investigativos en el ámbito de la informática forense que pueden ser de utilidad en la investigación de este tipo de delitos, especialmente con el delito de plagio o secuestro. Para el efecto, se utilizó el método deductivo, el analítico-sintético y el comparativo-causal.

CAPÍTULO I

LAS REDES SOCIALES

1.1 La comunicación humana

Desde sus orígenes el ser humano ha necesitado relacionarse con otros seres de su especie. Esto se ha posibilitado por la comunicación, como herramienta esencial para que los individuos se relacionen y adapten al entorno en el que se desenvuelven cotidianamente. Por medio de ésta se realizan diversas actividades económicas, informativas, publicitarias, entre otras; especialmente, aquellas que son esenciales, como las relaciones familiares y de amistades.

La comunicación hace referencia a un acto por medio del cual un individuo entabla un contacto con otro u otros, para transmitir información en un tiempo específico. El contenido de lo que se transmite es variado, pueden ser pensamientos, sentimientos, datos, entre otros; es decir, cualquier cosa susceptible de ser transmitida.[1]

Apunta más a un hecho sociocultural que a un proceso mecánico, puesto que constituye una actividad inherente a la naturaleza humana. La comunicación implica la interacción y la puesta en común de mensajes orientados a generar influencia en los individuos, organizaciones y sistemas sociales.[2] Pero no se reduce a un proceso social,

[1] Guardia de Viggiano, Nisla V. Lenguaje y comunicación, San José, Costa Rica, CECC/SICA, 2009, p.15.
[2] Gómez, José & Fedor, Simón. La Comunicación, *Revista Salus*, vol. 20, núm. 3, septiembre-diciembre, 2016, Venezuela. Universidad de Carabobo, p. 5-6.

sino que reviste de un carácter fundamental, en virtud del efecto que produce en la sociedad y la cultura, posibilitando la misma evolución.

1.1.1 La comunicación en los inicios de la humanidad

Desde la etapa primitiva, el ser humano se ha enfocado en la creación de diversas formas y medios de comunicación. Quemó la parte interna de un tronco de un árbol, cubrió el orificio con pieles de animales y, con ello, creó el tambor, con el cual emitía sonidos codificados a largas distancias, los cuales eran interpretados por los miembros de su comunidad. También se utilizaron cuernos de ciertos animales para transmitir sonidos codificados, señales de humo, las palomas mensajeras, sonidos que imitaban el canto de los pájaros, mensajeros, entre otros, los cuales ponen en evidencia la necesidad del ser humano de encontrar soluciones satisfactorias para el problema comunicativo.[3]

Lo anterior, pone en evidencia dos situaciones. La primera, es la importancia que la comunicación humana ha tenido desde el inicio de la historia humana. La segunda, está vinculada con las diversas formas o métodos, resultado de la creatividad humana, para facilitar el proceso comunicativo. La misma necesidad, exige al ser humano la búsqueda de mejores técnicas o recursos que favorezcan una comunicación más rápida y eficiente.

[3] Lifeder.com, Montano, Joaquín, Medios de comunicación antiguos y sus características, España, 2021. Disponibilidad: https://www.lifeder.com/medios-de-comunicacion-antiguos-y-sus-caracteristicas/, consultado el 18/08/2021.

El lenguaje apareció hace unos 40,000 años y se convirtió en método de comunicación interpersonal por excelencia. Luego se inventó la escritura, hace unos 5,000 años, lo cual significó otro avance muy importante en el ámbito de la comunicación. No obstante, los primeros medios de comunicación aparecieron antes del lenguaje y la escritura; después de ello, surgieron otros medios, los cuales se han ido sofisticando con el transcurso del tiempo.[4] En la figura siguiente, se presentan algunas formas de comunicación, utilizadas en la antigüedad.

Figura No. 1

Medios de comunicación antiguos

Fuente: Montano, Joaquín.[5]

[4] Yang, Y., Saladrigas Medina, H., & Torres, Ponjuán. El proceso de la comunicación en la gestión del conocimiento. Un análisis teórico de su comportamiento a partir de dos modelos típicos, *Revista Universidad y Sociedad*, Vol. 8, No. 2, Cuba, Universidad de Cienfuegos, 2016, p. 165-173.

[5] Lifeder.com, *óp. cit.*

1.1.2 La comunicación en la actualidad

Los seres humanos son sociales por naturaleza; por tal razón, ninguna persona puede estar sola e incomunicada. La comunicación cumple una función fundamental en la sociedad, y así ha sido siempre. Esto explica el esfuerzo humano por crear medios que le permitan una comunicación efectiva[6]. En este sentido, los diversos medios o técnicas, en determinado momento, resultan insuficientes, lo que conduce a buscar medios más aptos.

A lo largo de la historia, los estilos de vida de los grupos sociales van cambiando, esto exige medios de comunicación idóneos que permitan desenvolverse adecuadamente en nuevos contextos.[7] En este sentido, la sociedad actual, se caracteriza por vivir inmersa en una serie de actividades que absorben un alto porcentaje del tiempo diario de cada persona.

Esto genera una reducción del tiempo de convivencia familiar y social, pero dicho problema se compensa con los medios de comunicación masiva y sus diversas herramientas, al alcance de la mayoría de los individuos. Los medios de comunicación masiva permiten a las grandes masas estar en contacto con la información más relevante para cada persona. Estos medios son bastos y variados, con características similares y con amplias diferencias; no obstante, son fundamentales para la sociedad.

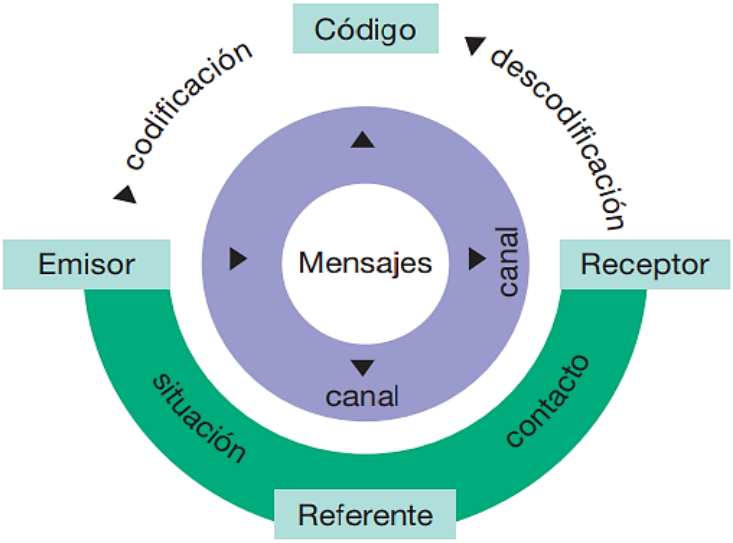
[6] Martin Serrano, Manuel. Evolución e historia en el desarrollo de la comunicación humana. Extraído de Teoría de la comunicación. La comunicación, la vida y la sociedad. Madrid: McGraw-Hill Interamericana de España, 2007, p.1.
[7] Ibíd.

1.1.3 Los elementos de la comunicación

Para que exista comunicación, se necesita de varios elementos, tales como emisor, receptor, código y mensaje. Se le denomina emisor, al que emite o envía el mensaje; el receptor es quien lo recibe; el código, es el conjunto se señales o signos utilizados para transmitir el mensaje; y el mensaje, es lo que se pretende transmitir. No obstante, también se necesita de los grupos sociales, los cuales son "la forma de integración social más concreta y universal, esto presupone un proceso relacional colectivo de un conjunto de personas en interacción, relativamente duradera, con cierta conciencia común y cohesión en la acción, con un mayor o menor grado de interdependencia y de integración normativa".[8]

Figura 2

Los elementos de la comunicación



Fuente: Guardia de Viggiano.[9]

[8] Uña Juárez, Octavio & Hernández Sánchez, Alfredo. L*a sociología*, Madrid, España, Esic, 2004, p.34.
[9] Guardia de Viggiano, *óp. cit*., p.39.

El sistema de comunicación específicamente humano, lo constituye el lenguaje. Por tal razón, el ser humano, desde que nace, entra en contacto con la generación que le precede, de la cual adquiere un conjunto de signos, con fines estrictamente educativos, denominados “lengua materna”, con la función de garantizar la interrelación e interacción de los individuos en un grupo social.

1.2 Las redes sociales

Las redes sociales han modificado la forma de comunicación de los seres humanos, puesto que, a partir de las mismas, hay un antes y un después en el ámbito comunicativo, a partir de la generación 2.0 y la inmersión en lo que globalmente se conoce como el “Social Media”.[10] Dentro de las diversas generaciones, es la Generación Z (jóvenes de 16-24 años) los que más utilizan las redes sociales. En segundo lugar están los Millennials (individuos de 25-40 años).

Sin embargo, la comunicación siempre ha sido algo inherente a la humanidad desde sus inicios, primero por medio de señales o signos, luego con la invención del lenguaje y las variadas formas de comunicación descubiertas. Es evidente que la comunicación nunca ha faltado a lo largo de la historia humana y esto constituye el fundamento de la nueva era de las telecomunicaciones.

Con las redes sociales, la comunicación ha alcanzado un nivel muy alto, dado que se ha superado el hecho de enviar un mensaje a un receptor; se ha difuminado la frontera

[10] Bienpensado.com, Gómez, David, Social Media no traduce redes sociales, Bogotá, Colombia, 2012. Disponibilidad: https://bienpensado.com/que-es-social-media-y-su-diferencia-con-las-redes-sociales/ Consultado el 19/08/2021.

entre lo público y lo privado, puesto que un mensaje perteneciente a la esfera de lo privado, es expuesto ante miles de personas. De acuerdo a Cea Jiménez, las redes sociales:

> Son formas de interacción social, definida como un intercambio dinámico entre personas, grupos e instituciones. Un sistema abierto y en construcción permanente que involucra a conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos. La intervención en red es un intento reflexivo y organizador de esas interacciones e intercambios, donde el sujeto se funda a sí mismo diferenciándose de otros.[11]

Las redes sociales han alcanzado popularidad en virtud de ciertas particularidades, tales como dar fama a un individuo anónimo, integración al discriminado, igualdad al diferente, entre otras. Además, afianzan nuevos vínculos y posibilitan que la fuerza del grupo produzca cambios que no podrían implementarse de otra manera. El problema es que también pueden ser utilizadas por los delincuentes, utilizando técnicas de ingeniería social.

De acuerdo a un estudio que realizó la empresa de seguridad informática “Shopos”, con respecto al peligro de robo de identidad en Facebook, concluye que los usuarios de esta red social facilitan el robo de su información personal.[12] La falta de procesos claros

[11] Cea Jiménez, A. D. *Los delitos en las redes sociales: aproximación a su estudio y clasificación*, Madrid, España, CPC, 2012, p.19.

[12] Sophos, Los ataques perpetrados contra las redes sociales crecen un 70%, España, 2021. Disponibilidad: https://www.sophos.com/es-es/press-office/press-releases/2010/02/security-report-2010.aspx, Consultado el 20/08/2021.

y el desconocimiento por parte del usuario sobre la normativa legal existente en función de la penalización de este tipo de prácticas delictivas, generan dificultades para la identificación de los autores materiales e intelectuales de tales hechos.

1.3 Las redes sociales en línea

Como se ya se ha comentado en esta investigación, los elementos que configuran la comunicación humana han sufrido cambios a lo largo de la historia. Sin embargo, Internet, ha implicado una revolución en este ámbito. En su momento, se pensó que la televisión implicaba un giro de 180º en la comunicación; sin embargo, fue Internet el que revolucionó al mundo, modificando todas las formas de comunicación existentes, las cuales han tenido que adaptarse a la red, pero tales cambios han alcanzado a todos los medios de comunicación en general.

Figura 3

Las redes sociales

Fuente: Unitypromotores.com[13]

[13] Unitypromotores.com Unitypromotores. Consejos de seguridad en Redes Sociales, Guatemala, 2020. Disponibilidad: https://www.unitypromotores.com/consejos-seguridad-redes-sociales/ Consultado el 19/08/2021.

No obstante, las redes sociales online (RSO,) son distintas a las redes sociales tradicionales; por lo tanto, es necesario determinar sus particularidades, por medio de las definiciones ofrecidas por los especialistas en la materia. En este sentido, las RSO se definen como “espacios virtuales organizados para desarrollar proyectos, poner en pie servicios que de otra manera no existirían, tomar decisiones en tiempos complejos y proyectarse hacia el mercado global usando toda la potencia de la virtualidad”.[14]

Como se puede apreciar, estos autores sitúan a las RSO como un espacio virtual, poniendo en evidencia que solo se puede acceder a éste por medio de la red, lo que implica que la información debe presentarse en un formato de lectura en línea. Es importante acotar que utiliza la expresión “espacios virtuales” en plural, por lo que se trata de más de uno, requiriendo del aporte de varios individuos, para lograr lo que describen: organizar comunidades, realizar proyectos y fomentar el mercado; los cuales requieren un intercambio social.

Las RSO han logrado popularizarse cuando han llegado a ser “menos redes” y “menos sociales”. “Menos redes”, porque se incluyen en este rubro a sitios como Youtube, que no están enfocados en la comunicación entre los usuarios, y “menos sociales” porque el componente social es secundario frente a otros objetivos[15]. Youtube se enfoca específicamente en subir y visualizar videos.

[14] Carneiro, Roberto; Toscano, Juan Carlos & Díaz, Tamara. *Los desafíos de las TIC para el cambio educativo*, Madrid, España, Fundación Santillana, 2021, p.13.

[15] Román, Ricardo, ricardoroman.cl Las redes sociales online llegan, poco a poco, al móvil, Chile, 2007. Disponibilidad: http://www.ricardoroman.cl/2007/09/08/las-redes-sociales-online-llegan-poco-a-poco-al-movil/ Consultado el 19/08/2021.

En esta definición es importante la expresión “menos sociales”, dado que clarifica que estas redes no se utilizan con el único objetivo de comunicar, sino que la finalidad es cada vez más variada. La expresión “menos redes”, hace referencia a la necesidad de establecer unas características determinadas para evitar el caos.

De acuerdo con Boyd & Ellison[16], una RSO puede definirse como un servicio que permite a cada individuo, las siguientes posibilidades:

- Crear un perfil público o semipúblico dentro de un sistema específico y delimitado.
- Generar un listado de usuarios con los que se comparte una conexión.
- Ver, recorrer la lista de las conexiones, comunicarse con algún miembro de dicha lista y observar las demás listas existentes en el sistema.

Dichas autoras describen la historia de las redes sociales, iniciando con la aparición del SixDegrees.com en el año 1997, el primer sitio con el reconocimiento de red social, hasta la creación de Facebook en el año 2006. De igual manera, presentan algunas referencias de investigaciones vinculadas con la privacidad, la seguridad y las amenazas potenciales para los jóvenes, entre otras.

Las redes sociales constituyen una estructura social que puede ser representada a través de uno o varios grafos, donde los nodos simbolizan a individuos y las aristas, las relaciones existentes entre ellos. Estas últimas pueden ser variadas, tales como

[16] Boyd, D. M., & Ellison, N. B, Sitios de redes sociales: Definición, historia y erudición. Diario de la computadora, Mediated Communication, Vol. 13, No. 1, Michigan, Estados Unidos, 2007, p.11.

intercambios financieros, amistad, relaciones sentimentales o sexuales, rutas aéreas., entre otras.

También es el medio en el que interactúan diversos individuos que se interesan en otro tipo de recursos, como juegos en línea, chats, foros, apoyo en actividades específicas y otros. Además, estos sitios brindan la posibilidad de dar seguimiento a sus relaciones interpersonales y generar nuevas[17]. Las redes sociales constituyen la versión moderna de los sociogramas, donde aparecía un conjunto de puntos que simbolizaban a los individuos, los cuales estaban unidos por líneas, para indicar las relaciones existentes entre ellos.

Una red social puede tener un carácter y un motivo aglutinador diverso, desde la amistad al intercambio de ideas, aficiones, negocios, matrimonio, sexo, entre otros. La denominada Web 2.0, brinda la posibilidad de crear redes sociales para unir a individuos en grandes cantidades, independientemente de la ubicación geográfica.

Un aspecto que destacar en las redes sociales es el denominado “efectos de red”,[18] el cual se refiere al valor de una red con relación al crecimiento de los usuarios, dado que cada nuevo usuario añade valor a la misma, por el solo hecho de unirse a la comunidad de usuarios. A medida que se incrementa la cantidad de miembros, también aumenta el valor para un miembro al pertenecer a ella.

[17] Deitel, P. & Deitel. *Ajax, Rich Internet Aplications y Desarrollo Web para programadores.* Madrid, España, Ediciones Anaya Multimedia, 2008, p.133.
[18] Flores Cueto, Juan José; Morán Corzo, Jorge Joseph & Rodríguez Vila, Juan José. Las redes sociales, Lima, Perú, Unidad de Virtualización Académica de la Universidad de San Martín de Porres, s.f., p.3.

Las redes exitosas cuentan con una arquitectura de participación que determina las preferencias de los usuarios para compartir contenido, en forma automatizada, de manera que éstos contribuyan al valor de la red. Esto se debe a que un buen porcentaje de los usuarios se enfocan en compartir, ni en modificar sus preferencias. Por lo tanto, si las empresas no activan esto de manera automática, habrá una cantidad muy reducida de usuarios que se tome el tiempo para ese tipo de actividades[19]. En este sentido, es relevante contar con una opción para desactivar o eliminar los contenidos previamente compartidos.

Por lo tanto, las RSO están integradas por un conjunto de individuos, quienes pueden conocerse o no en la vida real, que coinciden en buscar la interacción y el intercambio digital a través de un espacio virtual, en el cual también pueden tener acceso a un conjunto de recursos y servicios. Desde esta perspectiva, no es necesario que estén ubicados en las mismas categorías espacio-temporales.

1.3.1 Características

Las redes sociales tienen diversas funciones, las cuales pueden ser de tipo social, laboral o de ocio. El único elemento imprescindible es contar con acceso a Internet; a partir de ello, se ha desarrollado una nueva concepción de los espacios públicos.[20] En este sentido, se han transformado en un punto de encuentro para millones de usuarios procedentes de todo el mundo.

[19] Hütt Herrera, Harold. Las redes sociales: una nueva herramienta de difusión. *Reflexiones*, Vol. 91, No. 2, San José, Costa Rica, 2012, pp. 121-128.
[20] Ibíd.

a) Conectividad

En virtud de las redes sociales, personas que se encuentran en países lejanos, que hablan otros idiomas y con costumbres muy distintas, pueden mantener un contacto cercano.[21] Se crean así vínculos entre individuos, que pueden conocerse o no, y entre grupos de personas que comparten intereses comunes. Finalmente, la conectividad no se reduce a un grupo específico, sino que queda abierta a todo individuo que quiera convertirse en miembro o seguir a cualquier persona que así lo decida.

b) Interacción

La interacción o *engagement* constituye la característica esencial de las redes sociales.[22] Una publicación permite a los usuarios expresarse y establecer diálogos. Así, las empresas pueden conocer la opinión de la audiencia y contactar directamente con su público objetivo para mejorar las relaciones.

c) Personalización

Cada red social cuenta con una configuración propia, la cual se puede ajustar de acuerdo a las preferencias de cada persona.[23] Así, un perfil puede ser totalmente público,

[21] Hütt Herrera, Harold. Las redes sociales: una nueva herramienta de difusión. *Reflexiones*, Vol. 91, No. 2, San José, Costa Rica, 2012, pp. 121-128.

[22] Barrio Fernández, Ángela & Ruiz Fernández, Isabel. Los adolescentes y el uso de las redes sociales. En *International Journal of Developmental and Educational Psychology*, Vol. 1, No.3, España, 2014, p.571-576.

[23] Correduría Inteligente. Mpmsoftware.com Redes Sociales : definición y características, España, 2019. Disponibilidad: https://www.mpmsoftware.com/es/blog/redes-sociales-definicion-y-caracteristicas/#:~:text=Personalizaci%C3%B3n,un%20grado%20elevado%20de%20privacidad. Consultado el 20/08/2021.

hasta tener un grado elevado de privacidad. Estas opciones son configurables desde las mismas redes sociales. El usuario elige quién puede ver determinada información o material multimedia publicado.

d) Tiempo real

Las redes sociales son un tipo de mensajería instantánea, que permiten la entrega de mensajes a tiempo real.[24] De este modo, es posible mantener una interacción continua entre las personas que tengan activadas esas notificaciones concretas y que estén vinculadas a un perfil en particular, en el listado de contactos o de amigos, con quienes se puede intercambiar texto y contenido multimedia mediante mensajería.

e) Viralidad

Este es un término que ha ganado popularidad recientemente, y hace referencia a una característica de las redes sociales, que consiste en que los contenidos se propagan a gran velocidad a través de éstas.[25] Es algo muy apreciado por las empresas, dado que una publicación se exhibe exponencialmente. Sin embargo, a nivel individual constituye un arma de doble filo, debido a que, una publicación o contenido íntimo o una información muy personal, pueda llegar a mucha gente en poco tiempo. Ahora, bien, cuando se tiene la intención explícita de difundir algo con rapidez, especialmente cuando se trata de una oferta de negocios, esta característica se convierte en ventaja.

[24] Rd Station, rdstation.com Redes sociales, España 2020. Disponibilidad: https://www.rdstation.com/es/redes-sociales/ Consultado: 20/08/2021.

[25] Segarra-Saavedra, J. e Hidalgo-Marí , T. (2018): Viralidad e interacción. Análisis del engagement de los diez anuncios más vistos en YouTube en España en 2016, Icono 14, volumen 16 (1), pp. 47-71.

Figura 4.

Redes sociales más utilizadas en el mundo en el año 2021

Fuente: Thesocialmediafamily.com[26]

1.3.2 Usuarios

La magnitud alcanzada por las redes sociales ha generado interés, tanto en académicos como en profesionales del marketing. Se han realizado diversos estudios para identificar quiénes y cómo son los usuarios, para poder trazar un perfil de los mismos. Algunas investigaciones han encontrado diferencias socio-demográficas y de género. En MySpace, se descubrió que las mujeres tenían una mayor inclinación que los hombres a revelar información personal, mientras que, en Facebook, los hombres son más propensos a publicar contenidos obscenos, sin preocuparse por las consecuencias

[26] Thesocialmediafamily.com Conoce las redes sociales más utilizadas (2021). España. Disponibilidad: https://thesocialmediafamily.com/redes-sociales-mas-utilizadas/ Consultado el 29/08/2021.

futuras.[27] Las mujeres, en cambio, tienen la tendencia a compartir fotos y contenidos tiernos o románticos.

En los últimos años han surgido diversas redes sociales especializadas, lo cual permite que los individuos sean usuarios de varias redes, simultáneamente.[28] Los usuarios actuales, no se enfocan en una única red social; en este sentido, tienen características sociodemográficas, psicográficas y de conducta. Hay cuatro tipos y son los siguientes:[29]

- Introvertidos: Se trata de un grupo pasivo, puesto que, usan las redes sociales solo para enviar mensajes privados a su red de amigos.
- Nóveles: Son usuarios ocasionales y, aunque en la mayoría de las ocasiones utilizan las redes sociales para comunicarse con sus amigos, de forma esporádica, también comparten contenidos.
- Versátiles: Son los que realizan todo tipo de actividades en las redes sociales; sin embargo, cada una de ellas, con un distinto nivel de intensidad.
- Experto-comunicadores: Son aquellos realizan una gran variedad de actividades en las redes sociales y con mucha frecuencia e intensidad.

[27] Ibíd.
[28] Hütt Herrera, Harold. Las redes sociales: una nueva herramienta de difusión Reflexiones, vol. 91, núm. 2, 2012, pp. 121-128 Universidad de Costa Rica San José, Costa Rica.
[29] Azuela Fllores, José Ignacio; Baltazar Romero, Isabel; Jiménez Almaguer, Karla Paola; Ochoa Hernández, Magda Lizet; Jiménez Torres, Nadia Huitzilin Tipología de usuarios de redes sociales en México: ¿creadores o espectadores? Investigación y Ciencia, vol. 23, núm. 65, mayo-agosto, 2015, pp. 59-72 Universidad Autónoma de Aguascalientes Aguascalientes, México.
.

La clasificación anterior se realizó en función de lo que los usuarios de las redes sociales comparten con otros miembros de las mismas. Sin embargo, es importante tener en cuenta que, estos usuarios no permanecen fijos en cada categoría, sino que evolucionan constantemente. Se entiende que, un usuario inicial, solo utiliza las funciones mínimas, pero conforme va adquiriendo experiencia, explota otros recursos de las redes.

Otra clasificación de los usuarios de las redes sociales, tiene cuatro grupos y es la siguiente:[30]

- Principiantes: Son aquellos cuyo uso y frecuencia en las redes sociales es esporádica y baja.
- Usuarios habituales: Son los que utilizan las redes sociales con regularidad.
- Usuarios destacados: Son aquellos que utilizan las redes sociales con frecuencia y van en aumento, mientras se acercan al usuario experto.
- Expertos: Utilizan constantemente las redes sociales, y no solo comparten contenido, sino que también lo crean.

La clasificación anterior, se realiza con base a la frecuencia con la que los usuarios utilizan las redes sociales, independientemente de lo que compartan en las mismas. Ahora bien, esta variable responde a diversas razones, dentro de las cuales se puede señalar el grado de experiencia, la edad (no todas las generaciones poseen habilidades

[30] Hurtado Guapo, Ma Antonia; Fernández Falero, Ma del Rosario. Reconciliando las tipologías de usuarios de internet. Razón y Palabra, núm. 89, marzo-mayo, 2015 Universidad de los Hemisferios Quito, Ecuador, p.5

para el manejo de las redes sociales virtuales) y la finalidad al usarlas (búsqueda de amistades, negocios, compartir contenido, entre otros.

Finalmente, se encuentra otra tipología en cinco grandes grupos:[31]

- Socializadores alfa: Utilizan las redes sociales durante cortos periodos de tiempo, con la finalidad de conocer gente nueva y entretenerse.
- Buscadores de atención: La característica principal de este grupo es la búsqueda de atención y comentarios de los demás, generalmente por medio de fotos llamativas que publican en las redes sociales.
- Seguidores: Son los que se unen a las redes sociales, con la finalidad de estar informados con respecto a lo que sus compañeros o familiares están haciendo.
- Fieles: Son aquellos que utilizan las redes sociales para fortalecer las relaciones familiares y de amistad, existentes, y no buscan crear nuevas.
- Funcionales: Son los que utilizan las redes sociales con un objetivo específico, como buscar música, películas o alguna información particular de interés.

En esta última clasificación, el fundamento está constituido por la finalidad con las que los usuarios utilizan las redes sociales, las cuales son muy variadas e incluso, pueden confluir diversos objetivos en el mismo usuario. Estos objetivos, son los siguientes: entretenimiento; búsqueda de amistad, amor o sexo; fortalecimiento de relaciones

[31] Azuela Fllores, José Ignacio; Baltazar Romero, Isabel; Jiménez Almaguer, Karla Paola; Ochoa Hernández, Magda Lizet; Jiménez Torres, Nadia Huitzilin Tipología de usuarios de redes sociales en México: ¿creadores o espectadores? Investigación y Ciencia, vol. 23, núm. 65, mayo-agosto, 2015, pp. 59-72 Universidad Autónoma de Aguascalientes, Aguascalientes, México
.

familiares o amistosas; buscar seguidores para un determinado contenido y, finalmente, un objetivo muy particular, como contenido multimedia, noticias, entre otros.

1.3.3 Clasificación de las redes sociales

Las redes sociales se clasifican en dos grandes grupos: redes sociales directas y redes sociales indirectas. Cada uno de estos grupos se subdivide a la vez, de acuerdo a diversos parámetros o características. Las redes sociales directas son aquellas donde existe una colaboración entre los grupos que comparten intereses comunes, quienes interactúan en igualdad de condiciones y tienen el control de la información que comparten, la cual gestionan desde sus propios perfiles.

Las redes sociales directas,[32] se dividen en los siguientes subgrupos:

- Según finalidad: Se tiene en cuenta el objetivo que busca el usuario en una red social-Puede ser el ocio o entretenimiento, interactuar con otros usuarios, uso profesional, entre otros. En este sentido, se pueden señalar todas las redes sociales, dado que cada una tiene una o más finalidades específicas.

- Según modo de funcionamiento: Se tiene en cuenta una serie de procesos de las redes sociales que las orientan hacia actividades concretas, tales como las redes sociales de contenidos, las redes sociales basadas en perfiles tanto personales como profesionales y las redes sociales de microblogging. En este sentido, las redes sociales se clasifican en diversos grupos. Las redes sociales de contenidos

[32] Observatorio Nacional de las Telecomunicaciones y de la SI. Las redes sociales en internet, España, ONSI 2011, p.13.

son: Youtube, Instagram, Tik Tok, entre otras. Las redes sociales con perfiles personales y profesionales, son: LinkedIn, Facebook, Twitter, entre otras. Finalmente, las de microblogging: Twitter, Pownce, Jaiku, y otras.

- Según grado de apertura: Se tiene en cuenta el nivel de acceso o restricción de las mismas, tales como las redes sociales públicas (Facebook, Twitter y LinkedIn), que están disponibles para cualquier usuario y las redes sociales privadas (Yammer, Couple, Edmodo, Notabli), que están disponibles solo para ciertas personas, grupos u organizaciones.

- Según nivel de integración: Se tiene en cuenta el nivel de afinidad, interés e involucramiento en materias o actividades de tipo, preferentemente, profesional. En este tipo, están las redes sociales de integración vertical, utilizadas por un grupo de usuarios con un mismo nivel de formación, interés o disciplina profesional, tales como: Flickr y LinkedIn. ProfesionalTambién están las redes sociales de integración horizontal, cuyo empleo se enfoca en grupos de usuarios con intereses diversos, tales como: Facebook y Twitter.

También están las redes sociales indirectas[33], cuyos usuarios que cuentan con un perfil visible para todos. Existe una persona o grupo que administra, controla o dirige la información o las discusiones en torno a un tema específico. Se subdividen en los siguientes grupos:

[33] Observatorio Nacional de las Telecomunicaciones y de la SI, op cit., p.16.

- Foros: Son servicios que se prestan por medio de Internet, los cuales, generalmente son utilizados por expertos en determinada disciplina o como una herramienta de reunión con carácter informativo. A través de los foros, se realizan intercambios de información, valoraciones y opiniones. Se da un cierto grado de bidireccionalidad, dado que es posible responder a una pregunta formulada o comentar lo expuesto por otro usuario.

- Blogs: Son servicios brindados a través de Internet, los cuales se actualizan constantemente y suelen contener una recopilación cronológica de uno o varios autores. Con frecuencia, se insertan enlaces en las anotaciones y son administrados por el mismo autor que los crea, con el objetivo de plasmar aspectos que son importantes desde su punto de vista particular.

CAPÍTULO II

NUEVAS TENDENCIAS DELICTIVAS EN LAS REDES SOCIALES

2.1 Consideraciones generales

El tremendo aumento de la popularidad de las redes sociales durante los últimos años ha provocado un cambio drástico en la comunicación personal, tanto online como offline. La popularidad de sitios como Facebook, YouTube, Twitter, Instagram, Tik Tok, con millones de usuarios cada uno, ha hecho que la comunicación para las personas no solo sea conveniente, sino también instantánea, lo que permite a los usuarios conectarse y comunicarse de manera inmediata con cualquiera que tenga internet.

No obstante, ante el fenómeno masivo de las redes sociales, es lógico que los delincuentes de cuello blanco y de alta tecnología, adapten sus habilidades al panorama cambiante de Internet o se apoye en ellas. El ejemplo clásico es el del perpetrador que revisa detenidamente los perfiles de los usuarios, buscando posibles víctimas en las proximidades, que no se encuentren en casa. Algunos usuarios suelen publicar en las redes sociales, prácticamente todo lo que hacen y, en algún momento, publican que estarán fuera por la noche o que encuentran de viaje, lo que les da a los delincuentes una oportunidad para perpetrar un robo a la propiedad.

Otro error que suelen cometer algunos usuarios, es publicar su ubicación en tiempo real. De igual manera, el estilo de vida que se publica en las redes sociales, los vehículos que poseen, los lugares a donde viajan, los muebles de la casa, el lugar de

trabajo, entre otras cosas, permite a los delincuentes evaluar el nivel económico de sus posibles víctimas, para planificar un robo o secuestro.

2.2 Nuevas formas de delincuencia vinculadas con las redes sociales

Para bien o para mal, Internet se ha convertido en una parte integral de la vida de la mayoría de los ciudadanos, de todas las edades. Desde un enfoque negativo, la interconectividad ha generado nuevas formas de delincuencia, como el acoso cibernético y el *phishing*, lo que constituye un nuevo desafío para las fuerzas del orden, que deben actualizarse constantemente, para tener la capacidad de investigar este tipo de delitos y dar con los perpetradores.[34]

El anonimato intrínseco de las actividades digitales, contribuye a la ejecución de comportamientos socialmente recriminados como el racismo, la homofobia y otros delitos. Este es un motivo de preocupación, dado el continuo aumento del uso indebido de las redes sociales, por ejemplo, los beneficios del terrorismo posmoderno de la tecnología, en particular la tecnología de las comunicaciones, que permite la planificación, coordinación y ejecución de actos delictivos. Estos actos se cometen sin la presencia de barreras territoriales, políticas y financieras.

Los delincuentes mantienen canales de comunicación a través de las redes sociales en línea y miles de páginas web para sus propios intereses, explotando un área no regulada, de fácil acceso y altamente anónima. La demarcación online a través de las

[34] Capacitarte. capacitarte.org ¿Qué es el ciberdelito? Buenos Aires, Argentina, 2021. Disponibilidad: https://www.capacitarte.org/blog/nota/que-es-el-ciberdelito Consultado: 29/08/2021.

redes sociales se produce de forma similar. El fuerte engagement de los usuarios en las redes sociales ha permitido a los delincuentes una ventaja nunca vista.[35]

Antes de la popularización de la Web, el área de actividad de los delincuentes estaba restringida a barreras geográficas. Ahora, gran parte de la población está rodeada de tecnología, redes sociales y, por lo tanto, de actividades delictivas en línea.

Por otro lado, la creciente sofisticación y la mejora de la integración de las redes sociales también han creado oportunidades incomparables para que los organismos encargados de hacer cumplir la ley, se conecten con la comunidad de formas distintas e innovadoras. El análisis de redes sociales se puede utilizar para investigar o anticipar actividades, perfiles, relaciones y publicaciones delictivas.

Esto permite identificar información relevante sobre las operaciones realizadas por los delincuentes, así como la ubicación y los participantes. La Web puede beneficiar el desarrollo de herramientas y mecanismos de software para apoyar la investigación y la prevención de actos delictivos.

2.3 La esteganografía

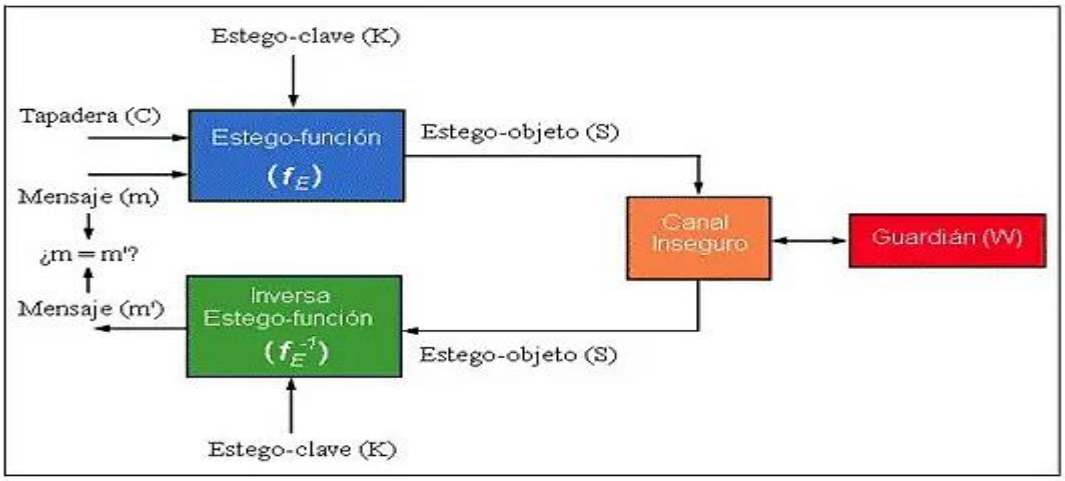
Los delincuentes pueden ocultar su comunicación de diversas formas, como imágenes, videos, cifrado o técnicas de esteganografía, lo que dificulta la lucha contra los delitos en la Web. La esteganografía es una técnica que se utiliza para ocultar

[35] Barreira, R.; Pinheiro, V.; Furtado, V. Un marco para el análisis forense digital basado en el etiquetado de roles semánticos. En Actas de la Conferencia Internacional IEEE 2017 sobre Inteligencia e Informática de Seguridad: Seguridad y Big Data, ISI 2017, Beijing, China, 22–24 Julio 2017; pp. 66–71.

información en algún otro elemento o recurso. No es una estrategia moderna, vinculada con la informática, puesto que surgió cuando el ser humano vio la necesidad de que cierta información confidencial no fuera interceptada por los enemigos. Se trataba de técnicas rudimentarias, las cuales han ido evolucionando, hasta llegar a la informática actual.[36] En la ilustración siguiente, se pueden apreciar los elementos de la esteganografía.

Figura 6

La esteganografía



Fuente: Pérez Beristain (2020).[37]

La esteganografía utiliza dos elementos: el mensaje y el camuflaje. El primero, hace referencia a la información confidencial que se pretende ocultar. El camuflaje o tapadera, por su parte, es el elemento que disfraza al mensaje, para que éste pase desapercibido. En algunos casos, se requiere de un tercer elemento, que es la clave para descifrar el mensaje.[38]

[36] Pérez Beristain, M. A. Esteganografía de la información en nuestra vida. En *Logos* No. 2, Vol. 7, No. 14, México, D. F., 2020, p. 7.
[37] *loc. cit.*
[38] *loc. cit.*

Los delincuentes utilizan las redes sociales en línea para diversas actividades, incluida la comunicación, la planificación y la ejecución de actos delictivos. Para ello, emplean publicaciones cifradas utilizando expresiones en clave, que están restringidas a grupos específicos.

También se practican delitos como la pedofilia con el apoyo de las redes sociales. Los pedófilos utilizan las redes sociales para atraer a sus víctimas. La alienación se produce inicialmente de forma discreta, apuntando al aislamiento de la víctima. Con la víctima aislada, los depredadores sexuales cambian su enfoque y utilizan textos directos con contenido sexual o comunicación por video. Este proceso tiene como objetivo último, permitir un encuentro presencial.[39]

2.4 Riesgos de compartir información en redes sociales

La mayoría de las personas que utilizan las redes sociales, suelen compartir fotografías y videos de viajes de trabajo y vacacionales, en centros formativos, hoteles, restaurantes, lugares de descanso, entre otros. Esto facilita el rastreo, cuando alguien pretende cometer un ilícito.

Es imposible no compartir información en redes sociales; sin embargo, es importante tener en cuenta que es posible tener un mayor control, así como compartir datos con un mayor nivel de seguridad.[40] Para ello, se debe recurrir a la configuración de

[39] Lima Malvido, María de la Luz. Delitos Electrónicos. Academia Mexicana de Ciencias Penales, Editorial Pomia, México, 2018, p.98.
[40] Semymas, semymas.com Riesgos de compartir información personal en redes sociales, España, 2018. Disponibilidad: https://semymas.com/riesgos-informacion-personal/ Consultado: 20/08/2021.

privacidad, dado que no es conveniente que un perfil esté abierto a todo público, a excepción de que esté vinculado con cuestiones de negocios o profesionales. Por otra parte, cuando se trata de información sensible, debe ser compartida con un grupo reducido de personas, que incluya a familiares y amigos únicamente.

Activar la función de geolocalización, tampoco es recomendable, dado que permite ubicar inmediatamente a una persona y constituye una ventaja para los delincuentes. Además, es importante que los niños sepan de los riesgos que supone compartir información personal o hacerse amigos de extraños en redes sociales.

2.5 Delitos informáticos

Los delitos informáticos, cibernéticos o electrónicos, han recibido diversas definiciones. Téllez, los define como las "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".[41] Siguiendo esta línea de reflexión teórica, María Lima, los denomina “delitos electrónicos", y los define como “cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin."[42]

[41] Téllez Valdez, Julio, (1987). Derecho Informático. México, D. F.: Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, 1987, p. 188.

[42] Lima Malvido, María de la Luz. Delitos Electrónicos. Academia Mexicana de Ciencias Penales, Editorial Pomia, México, 2018, p.100.

En estas definiciones destacan tres elementos. El primero está vinculado con lo que se entiende, generalmente, por delito; es decir, una acción u omisión, típica, antijurídica y culpable. En segundo lugar, está la referencia a recursos relacionados con las tecnologías de la información y, finalmente, el resultado, el cual lesiona la integridad, disponibilidad y confidencialidad de los datos[43] (información, audio, video, fotografías, libros, entre otros).

Algunos enfoques doctrinales ponen en evidencia que el delito informático no constituye una forma específica de delito, sino una diversidad de modalidades delictivas asociadas, de alguna manera con las computadoras. Desde esta perspectiva, para Romeo Casabona, la expresión "delito informático", debe utilizarse en forma plural, debido a que se usa para hacer referencia a un conjunto de conductas ilícitas y no una sola de carácter general.[44]

Por lo tanto, hay una serie de delitos que entran en esta categoría, lo que representa una gran dificultad para crear un grupo homogéneo. Desde este enfoque, González Rus, llegó a la conclusión de que resulta imposible realizar una agrupación de todos los delitos relacionados con los computadores, internet y las redes sociales en un concepto de delito único.[45]

[43] González Rus, J. J.: "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", en Revista de la Facultad de Derecho de la Universidad Complutense, 12, 1986, p. 107-164.

[44] Romeo Casabona, Carlos María. Poder informático y seguridad jurídica. Madrid, España: FUNDESCO, 1988, p.23.

[45] González Rus, J. J.: "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", en Revista de la Facultad de Derecho de la Universidad Complutense, 12, 1986, p. 107-164.

Por tal razón, el autor citado hace referencia a la heterogeneidad de estos delitos. No obstante, sin la pretensión de elaborar un catálogo de los mismos, los clasifica en dos grandes grupos: en el primero, están aquellos que constituyen amenazas para la intimidad personal y el ámbito privado en virtud de la enorme cantidad de datos alojados en dispositivos físicos o virtuales; luego, están los delitos patrimoniales, los cuales se ven facilitados por las ventajas que ofrecen estas nuevas tecnologías.

De acuerdo a lo que se propone desde el ámbito doctrinario, se constata la dificultad para realizar una clasificación unificada, puesto que los criterios que los diversos autores proponen son muy diversos, así como los delitos. En algunos casos, la computadora o internet son indispensables para la comisión de un delito. En otros casos, solamente lo facilitan, puesto que ciertos delitos, pueden cometerse sin necesidad de recurrir a una computadora, internet o las redes sociales.

2.5.1 Estructura de la información

María Pinto define el término clasificación como “todo sistema artificial de signos normalizados, que facilitan la representación formalizada del contenido de los documentos para permitir la recuperación, manual o automática, de información”[46].

En esta definición se hace referencia a un sistema de tipo artificial. La diferencia radica en que un sistema artificial está conformado por signos normalizados, para eliminar la ambigüedad, propia de un sistema natural. Por lo tanto, se trata de palabras,

[46] Pinto, María. Manual de clasificación documental. Madrid, España: Síntesis, 1997, p.67.

números o símbolos cuyo significado es unívoco y se utiliza para la descripción de documentos, de manera que se pueda acceder a la información contenida en estos en un momento posterior.

Considerando la organización de la información, se puede hablar de estructura jerárquica o combinatoria. A la primera, también se le denomina estructura arbórea o sistemática, donde los términos son distribuidos en clases o categorías siguiendo un orden lógico, de manera que unos dependen de otros y se establecen con un método deductivo. Mientras que, en la estructura combinada, la cual también se conoce con el nombre de asociativa, los términos son representados en orden alfabético y son asociados y combinados entre sí[47].

Una clasificación está conformada por una serie de elementos, los cuales no tienen carácter obligatorio; sin embargo, forman parte de la mayoría de las clasificaciones existentes. Según Rowley[48], estos elementos son las tablas, la notación y el índice alfabético. A este listado se añaden las tablas auxiliares, propuestas por Gil Urdiciain[49].

De manera que, al integrar ambas propuestas, los elementos que conforman una clasificación quedan de la manera siguiente:[50]

- Tablas principales: en ellas se muestran los términos organizados y las vinculaciones entre ellos.

[47] A. D. Cea Jiménez. *Óp. Cit*., p.51.
[48] Rowley, J. E. La organización del conocimiento: una introducción a la recuperación de la información. Hampshire, Inglaterra: Ashgate, 1992, p. 176.
[49] Gil Urdiciain, Blanca. Manual de lenguajes documentales. Gijón, España: Trea. 2004, p.29.
[50] Rowley, J. E. Op. cit., p. 179.

- Tablas auxiliares: tienen la finalidad de hacer puntualizaciones sobre los términos, especificando características de forma, lugar, tiempo, idioma, entre otros.
- Código o notación: hace referencia a la serie de signos alfabéticos o numéricos que, individualmente o en conjunto, son asignados a los términos de la clasificación.
- Índice: es el listado alfabético de todos los términos incluidos en la clasificación.

En esta investigación, se utilizará una clasificación especializada y jerárquica, puesto que se trabajará con un área determinada del conocimiento (los delitos que pueden darse en las redes sociales online), con fundamento en unas categorías específicas pertenecientes a una estructura. Los autores que abordan esta temática son variados, por lo que no existe dificultad alguna para acceder a la información respectiva. Aunque la información no siempre es coincidente, se pueden apreciar algunos patrones en los distintos autores. Con base a ello, se establecen las fases siguientes:[51]

- Limitar el contexto: como punto de partida, es fundamental conocer el tema que se va a representar, considerando el área del conocimiento al que pertenece y los elementos que lo integran. Esto facilita las búsquedas específicas de términos vinculados con dicho contenido.

- Buscar descriptores: hace referencia a aquellos conceptos más significativos, que faciliten la organización de la información a representar.

[51] A. D. Cea Jiménez. Óp. Cit., p.55.

- Normalizar nombres: si un concepto se describe con términos diferentes, se debe elegir cuáles serán utilizadas como descriptores y cuáles no.

- Definir descriptores: para que los términos se puedan organizar de forma lógica, es necesario que cada uno de ellos sea descrito para su correcta comprensión.

- Establecer categorías: las categorías hacen referencia a las diversas características por las que es posible organizar un mismo tema.

- Organizar los descriptores: se refiere a la organización lógica y justificada de los descriptores, considerando la categoría más idónea para su descripción.

2.5.2 Analizando clasificaciones ya existentes

Previo a la tarea de elaborar cualquier clasificación, es esencial la revisión de los trabajos existentes en la materia. En la temática de esta investigación, existen clasificaciones realizadas por organismos oficiales, tales como la Organización de las Naciones Unidas (ONU), el Consejo de Europa, además, algunos juristas especializados han realizado aportes en este sentido. El Consejo de Europa, por medio de su Convenio de Ciberdelincuencia[52], establece la siguiente clasificación:

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos: acceso ilícito a sistemas informáticos, interceptación ilícita de

[52] Consejo de Europa, coe.int Convenio de Ciberdelincuencia. Estrasburgo, Francia, 2021. Disponibilidad: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm Consultado el 30/09/2021.

datos informáticos, interferencia en el funcionamiento de un sistema informático, abuso de dispositivos que faciliten la comisión de los anteriores delitos.

Delitos informáticos: falsificación informática mediante la introducción, alteración, borrada o supresión de datos informáticos, fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

Delitos relacionados con el contenido: producción, oferta, difusión, transmisión, adquisición o tenencia, en sistemas o soportes informáticos, de contenidos de pornografía infantil.

Delitos relacionados con infracciones de la propiedad intelectual y derechos afines: En esta clasificación destaca la falta de normalización en sus categorías. En una primera aproximación, da la sensación de que se realizó en función del objeto al que se ataca (la confidencialidad, la integridad, la disponibilidad de datos y sistemas informáticos y la propiedad intelectual); sin embargo, existe una categoría que contempla los delitos vinculados con el contenido y otra para delitos informáticos en general. Aunque figura la inclusión de un apartado específico, el de “delitos informáticos”, no tiene relación con sus términos relacionados y solo abarca la pornografía infantil.

En los verbos que hacen referencia a las diversas acciones vinculadas con material ilícito, se ha prescindido de aquellas relacionadas con la difusión de fotografías de terceras personas sin su consentimiento. Por otra parte, llama la atención que un apartado tenga el título de “delitos informáticos”, cuando esa es precisamente la materia que se está clasificando. Sin embargo, se rescata el hecho de que presenta una idea

general que puede tomarse como fundamento para realizar otras clasificaciones más precisas.

Luego está la clasificación ofrecida por la ONU, en el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos[53], donde los delitos informáticos están estructurados de la manera siguiente:

- Fraudes cometidos mediante manipulación de computadoras: manipulación de los datos de entrada, la manipulación de programas, manipulación de los datos de salida, fraude efectuado por manipulación informática.

- Falsificaciones informáticas: como objeto y como instrumento: Daños o modificaciones de programas o datos computarizados: sabotaje informático, virus, gusanos, bomba lógica o cronológica, acceso no autorizado a sistemas, servicios, piratas informáticos o hackers, reproducción no autorizada de programas informáticos de protección legal.

Esta clasificación solamente considera los delitos de fraude, falsificación y daño, dejando fuera otros vinculados con sistemas informáticos. No se comprende bien el delito de fraude, dado que no están especificadas sus atribuciones. También se hace referencia a las acciones no contempladas en ninguna de las tres anteriores, pero no indica ningún tipo específico de actividad.

[53] Organización de las Naciones Unidas. Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos. Revista Internacional de Política Criminal, 1994, p. 43-44.

Esto dificulta la aplicación a casos particulares. Y, en virtud de otras falencias, tal clasificación no se considera ideal para englobar los diversos delitos informáticos en general[54]. En la ilustración siguiente, se presenta gráficamente una clasificación de los delitos informáticos.

Figura 7.

Clasificación de delitos informáticos

Fuente: slidesahere.net

2.6. Ciberdelitos

Con la expansión global de Internet, se ha comprobado que ésta facilita la comisión de delitos. Es importante destacar que no han aparecido nuevos delitos o conductas

[54] A. D. Cea Jiménez. Óp. Cit., p.57.

antisociales; no obstante, las ya conocidas prácticas delictivas, encontraron un nuevo medio para facilitar su comisión. La ventaja es que, un delito cometido a través de internet o las redes sociales, también facilita su persecución y enjuiciamiento.

De acuerdo con Gustavo Sain, desde la perspectiva criminológica, existen dos aproximaciones a este nuevo fenómeno criminal.[55] La primera, es que los delitos informáticos son delitos tradicionales o convencionales que han encontrado en los dispositivos informáticos, internet y las redes sociales, una manera de llegar a nuevas posibles víctimas que, de otro modo, no sería posible llegar.

La segunda aproximación, es que las tecnologías de la información y comunicación constituyen herramientas novedosas para la comisión de delitos que no existían previo a la aparición de tales tecnologías. Dichos delitos no pueden cometerse sin la mediación de un dispositivo tecnológico, internet o las redes sociales. Resulta que ambos puntos de vista son verídicos, puesto que, algunos delitos adquieren nuevas formas mediante la tecnología, así como también surgen nuevos delitos supeditados a la misma.

La expansión de las redes de transmisión de datos, especialmente Internet, ha contribuido a generar nuevos conceptos en el denominado derecho penal informático. Desde esta perspectiva, un sector doctrinario ha comenzado a dejar en desuso el término

[55] Sain, Gustavo. Delito y nuevas tecnologías: Fraude, narcotráfico y lavado de dinero por internet, Buenos Aires, Argentina, Editores del Puerto, 2012, p.69.

delito informático y lo han sustituido por ciberdelito o cibercrimen. En este contexto, el término “cibercrimen”, hace referencia al:

> conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual.[56]

De acuerdo con esta definición, ha surgido un nuevo conjunto de delitos que no están asociados de manera directa con los sistemas o dispositivos informáticos, sino con el uso de redes de transmisión de datos. En este sentido, dichos sistemas o dispositivos, ocupan un lugar secundario. Fue precisamente, la proliferación de Internet, la que generó que nuevos delitos o los delitos tradicionales se aprovecharan de esta tecnología para su comisión.

Por lo tanto, se puede hacer referencia a dos grandes grupos de delitos con respecto a las tecnologías de la comunicación y la información. En primer lugar, están aquellos que requieren un nivel avanzado de conocimientos de informática y programación y consiste, generalmente en el desarrollo de programas maliciosos para hackear dispositivos o redes, casi siempre con fines económicos. El segundo grupo está conformado por los delitos que utilizan el proceso de comunicación para engañar a los

[56] Fernández Teruelo, J. G. La sanción penal de la distribución de pornografía infantil a través de Internet, *Boletín de la Facultad de Derecho de la UNED*, 20, España, 2002, p.251.

usuarios, con una finalidad económica, sacarle dinero o lo que se conoce como suplantación de identidad, para obtener sus datos personales.

Las diversas conductas antijurídicas o delitos informáticos, son susceptibles de clasificación, a partir del bien jurídico protegido. Desde la opinión de Aboso & Zapata[57] esta perspectiva, se pueden señalar los grupos siguientes:

a) Los delitos cometidos por medio de las redes sociales, tales como atentados a la intimidad, el honor y la integridad moral, en sus diversas modalidades.

b) El delito de “stalking”, el cual se refiere a una conducta intencionada y maliciosa de persecución, acecho o acoso contra un individuo en particular, el cual puede realizarse a través de distintos medios, pero internet no constituye la excepción.

c) Los delitos sexuales contra los menores de edad (*online grooming*), ataques realizados a través de medios tecnológicos o el fomento y uso de drogas.

d) La ciberpornografía infantil, en la que se utilizan sitios web donde para traficar material pornográfico de menores de edad.

e) El “ciberodio”, que incluye la xenofobia, el racismo, el odio y la discriminación.

[57] Aboso, Gustavo E. & Zapata, María F. Cibercriminalidad y derecho penal. Montevideo, Uruguay, Ed. Euros Editores, 2006, p. 47.

f) Los delitos contra la propiedad intelectual, que consisten en aprovecharse del trabajo de otros, difundiendo obras sin el consentimiento del autor o la piratería que hace referencia a realizar copias de material multimedia, con fines económicos.

g) "*Phishing*" y "*pharming*", los cuales se dan en el ámbito financiero. Consiste en que un individuo se hace pasar por trabajador de una entidad bancaria y solicita al cibernavegante datos de tarjetas de crédito o claves bancarias. Esto se hace generalmente por medio de un correo electrónico con un enlace que conduce a un sitio web falso, que simula ser auténtico. Si logran su cometido, mediante la clave de acceso a las cuentas, realizan retiros o transferencias de las mismas.

h) Ofertas falsas de trabajo: Como su nombre lo indica, se trata de enviar ofertas de trabajo falsas, con la finalidad de utilizar a estos individuos para blanqueo y envío de dinero robado a otros países.

i) Scamming: Se denomina así al delito que se comete mediante correos electrónicos fraudulentos, con la finalidad de estar económicamente a gente incauta. Generalmente, ofrecen préstamos, donaciones, sorteos, promociones, becas, entre otros. Mediante esta estrategia convencen a un individuo para que les proporcione información personal. Este delito tiene diversas manifestaciones, tales como la oportunidad de cobrar una importante suma de dinero en otro país, una persona amiga en el extranjero o el propio país lo refirió para un sorteo o viaje

en un crucero, solicitud de ayuda para una aparente causa noble, ofrecimiento de préstamos a un interés muy bajo y con mínimos requisitos, entre otros.

j) Las estafas y fraudes, que dañan el patrimonio de terceras personas.

k) El robo y secuestro, los cuales no se realizan directamente desde internet, pero esta tecnología ayuda a identificar a las posibles víctimas, por medio de la información que se comparte en redes sociales.

Sin embargo, para que estas conductas repudiables, sean consideradas delitos, es necesario que puedan encuadrarse en un tipo penal específico. Esto, en virtud del principio de legalidad que señala que no existe delito ni pena, sin una ley previa a la comisión del hecho.

En este orden de ideas, Flores Salgado[58], indica que existen ciertos elementos del tipo penal, los cuales deben tenerse en cuenta para considerar a un delito como delito electrónico o ciberdelito, es decir, un delito vinculado con internet o las redes sociales. El autor señala los siguientes:

a) El bien jurídico que se tutela a través de la sanción de los delitos informáticos es la pureza técnica vinculada con la informática, así como el resguardo y protección de los medios implicados en la computación electrónica.

[58] Flores Salgado, Lucerito. Derecho Informático, México, D. F., Editorial Patria, 2009, p.82.

b) El elemento objetivo es todo hecho o acción que se realiza con la intención de dañar o desviar el uso correcto del computador o dispositivo, con una finalidad explícita de perjudicar a un individuo o empresa, para obtener un beneficio económico o moral, para sí mismo u otra persona, sin la autorización respectiva.

c) El elemento subjetivo, por su parte, lo constituye la culpa o dolo con que actúa el sujeto activo del cibercrimen o delito informático.

d) En lo que respecta al sujeto activo de tales delitos, las investigaciones realizadas demuestran que, generalmente se trata de individuos que poseen un determinado nivel de inteligencia, conocimientos y educación, que supera a la mayoría. Básicamente, son los mismos programadores, analistas de sistemas y todos aquellos que conocen la estructura y vulnerabilidades de dichos sistemas.

e) EI sujeto pasivo en los delitos informáticos está constituido por las entidades bancarias, puesto que son las víctimas, debido a que son las que más utilizan transferencias electrónicas de fondos y movilizan grandes sumas de dinero a través de operaciones electrónicas. De igual manera, sujeto pasivo de este delito, es todo aquel individuo que es víctima de cualquier daño, a través de un sistema que utiliza tecnologías de la información.

Por lo tanto, no se puede hablar de delito informático, si este no se encuentra tipificado en una ley ordinaria. En este sentido, destaca la importancia de la tipificación legal de este tipo de delitos y preguntarse si la legislación existente se puede aplicar a las diversas conductas realizadas a través de la informática. De no ser así, surge la

necesidad de crear nuevos tipos penales que permitan el establecimiento de mecanismos de control que limiten y garanticen la utilización correcta de las tecnologías de la información y la comunicación. Por otra parte, hay delitos que no corresponden precisamente a la clasificación de delitos informáticos, pero que se ven favorecidos por la tecnología y redes sociales, como el caso del delito de plagio o secuestro, el cual ha tomado nuevas modalidades, a partir de la informática.

CAPÍTULO III

EL DELITO DE PLAGIO O SECUESTRO

3.1 Consideraciones generales

El secuestro se considera uno de los negocios ilícitos que ha experimentado una rápida expansión a nivel mundial. Para el crimen organizado y terroristas, constituye una manera rápida de agenciarse de capital. Prospera en aquellos países caracterizados por la corrupción y el deterioro social y económico. En zonas conflictivas, puede convertirse en un verdadero flagelo.[59]

Cuando se incrementa el secuestro, disminuye la confianza pública y la credibilidad en las autoridades de Gobierno, tanto a nivel interno como externo. Las repercusiones negativas, no son solamente de tipo social o económico, sino también para la seguridad, hasta el extremo de que llega a convertirse en un círculo vicioso. El Gobierno tiene el mandato constitucional de garantizar la seguridad, la paz y el orden para todos los ciudadanos. Esto implica proteger a las personas, prevenir la delincuencia y castigar a quienes atentan contra el bienestar individual y colectivo.

En el caso específico del secuestro, para enfrentarlo se requiere de una política nacional clara, leyes adecuadas, una justicia pronta y firme, mecanismos de coordinación

[59] Oficina de las Naciones Unidas contra la Droga y el Delito. Manual de lucha contra el secuestro. Viena, Austria, ONU, 2006, p.iii.

nacionales e internacionales y sistemas para facilitar la cooperación internacional, entre otros.[60]

Con respecto a la política pública, es necesario tener en cuenta las medidas de tipo preventivo, recursos y procedimientos adecuados, aplicación de la ley, coordinación interinstitucional, asistencia y apoyo a la familia de la persona secuestrada, unidades especializadas de los cuerpos de policía, entre otros. En el ámbito legislativo, el secuestro o su equivalente, debe aparecer como un delito penal específico en el sistema jurídico.

La legislación debe incluir lo vinculado con la privación de la libertad, la restricción de la libertad personal, el rapto y similares. La doctrina ha identificado cuatro elementos a tener en cuenta en este ámbito[61] y son los siguientes:

- Capturar, transportar o probar de la libertad, de manera ilegal a un individuo y sin su consentimiento.
- Utilizar la violencia, amenazas de violencia y engaño para cometer el delito.
- Mantener a la víctima en un lugar aislado y/o desconocido, en condiciones indignas.
- Tener como finalidad un beneficio económico, político o de otro tipo.

El secuestro es un delito grave; por tal razón, se castiga con una pena de prisión importante. Las distintas penalidades que se aplican, en diversos países, van desde los

[60] Pax Christi. La industria del secuestro en Colombia ¿Un negocio que nos concierne? Utrecht, Holanda, Pax Christi Holanda, 2016, 120-121.
[61] Toc López, Sandra Dominga. Estudio sobre el delito de secuestro en la sociedad guatemalteca (Tesis de pregrado), Guatemala, Universidad de San Carlos de Guatemala, 2007, p.19.

cinco hasta los setenta años de prisión, incluso, cadena perpetua. En la pena de prisión, se contemplan factores atenuantes y agravantes. Los factores agravantes, son los siguientes:[62]

- Los secuestradores obtuvieron el rescate, lo solicitaron a los familiares de la víctima o fueron capturados en el momento en el que se disponían a recibir el rescate.
- Los secuestradores utilizaron armas e hicieron uso de la fuerza y amenazas.
- Se infligieron lesiones a la víctima, se le amenazó de muerte o se provocó la muerte de esta.
- La víctima fue sometida a maltratos, torturas y crueldad.
- Se provocó daño psicológico a la víctima.
- El delito fue cometido por una organización delictiva o hubo una conspiración criminal.
- Los secuestradores fingieron ser autoridades del Gobierno.
- El delito fue cometido por personas que ofrecían servicios privados de seguridad, aseguradoras o alguno de sus trabajadores.
- El autor intelectual del delito es un funcionario público.
- El cautiverio en el que se mantuvo a la víctima fue extenso.
- Hubo varias víctimas de secuestro y mantenidas en cautiverio.
- La víctima fue agredida o explotada sexualmente.

[62] Centro de Documentación, Información y Análisis. Delito de secuestro: (Segunda Parte). Estudio de Derecho Comparado Interno (32 códigos penales locales) y a Nivel Internacional (8 países) y Opiniones Especializadas. México, D. F. Cámara de Diputados, LX Legislatura, 2008, p.3.

- La víctima fue obligada a contraer matrimonio.
- La víctima fue secuestrada para obligarla a formar parte de un grupo delictivo.
- La víctima era un menor de edad, un adulto mayor o una persona con capacidades diferentes (física o mentalmente).
- La víctima fue conducida al extranjero.
- La víctima era un funcionario gubernamental, público o representante diplomático.
- La víctima era un testigo en un caso judicial.
- La víctima fue secuestrada debido a su nacionalidad, raza, etnia, ideología política, credo religioso o falta de fe religiosa.

Los factores agravantes expuestos anteriormente, contribuyen a incrementar la pena de prisión. Sin embargo, también existen factores atenuantes, los cuales ayudan a mitigar el castigo.[63] Aunque esto es discutido, tales factores pueden ayudar a reducir la pena de prisión y son los siguientes:

- Liberar a la víctima antes de que se produjera una lesión.
- Proteger a la víctima de los demás secuestradores, para que no fuera lesionada físicamente o abusada sexualmente.
- Distanciarse de la acción de los demás secuestradores.
- Arrepentimiento post factum, que consiste en liberar espontáneamente a la víctima, dentro de los tres días siguientes a la privación de la libertad, sin conseguir ninguno de los objetivos previstos con dicho delito.

[63] Conti, N. J. Secuestro coactivo. Buenos Aires, Argentina, Asociación Pensamiento Penal, 2008, p.22.

- Uno de los secuestradores colabora activamente para liberar a la víctima o víctimas de secuestro.

El juez es el responsable de analizar tales factores, tanto los agravantes como los atenuantes, para dictar la sentencia. Los primeros, son contemplados en la legislación de la mayoría de los países. Los atenuantes, solo se consideran en algunos países, debido a que el delito ya está consumado. Por tal razón, dichos factores son discutibles.

3.2 El delito de plagio o secuestro

En cualquier definición, es importante considerar el principio etimológico. En este sentido, Landinez Olaya, afirma lo siguiente: “Etimológicamente hablando, la palabra secuestro tiene su origen en el vocablo latino secuestrare, que significa "apoderarse de una persona para exigir rescate, o encerrar a una persona ilegalmente. Antiguamente, también se le denominó plagio”[64].

El contenido del secuestro como figura delictiva, ha experimentado cambios generados por la evolución social. Este delito, consiste en poner a la persona en una condición determinada que impide la libertad de locomoción en su totalidad o parcialmente, de acuerdo a las limitaciones impuestas por el sujeto activo. En este orden de ideas, Toc López, señala que, este delito:

> Constituye una violación a los derechos humanos, que atenta contra la libertad, integridad y tranquilidad de las familias víctimas del delito.

[64] Landinez Olaya. A. Tratamiento del secuestro en los medios escritos el tiempo y el nuevo siglo, 2001. Disponibilidad: http// intellectum.unisaba.edu.co:8080/jspui/bitstream/108186317/1/126696.Pdf Consultado: 10/09/2021.

Igualmente, es una violación a los derechos. Por lo tanto, el secuestro no solo afecta a la víctima sino a la familia en general; ya que éstos son sometidos a lo que los psicólogos, que trabajan el duelo, conocen como el proceso de la "muerte suspendida", que es la angustia que caracteriza al secuestro, y que se suma a lo que los juristas llaman la pérdida de libertad[65].

El derecho a la libertad está regulado en el artículo 4º. de la Constitución Política de la República de Guatemala, que establece lo siguiente:

> Artículo 4º. En Guatemala todos los seres humanos son libres e iguales en dignidad y derechos. ... Ninguna persona puede ser sometida a servidumbre ni a otra condición que menoscabe su dignidad. Los seres humanos deben guardar conducta fraternal entre sí.

En este sentido, el secuestro atenta contra el derecho a la libertad que posee toda persona, el cual está garantizado por la Constitución Política de la República de Guatemala, así como los tratados internacionales en materia de derechos humanos, de los cuales el Estado guatemalteco es signatario.

Por tal razón, el Código Penal guatemalteco, Decreto 17-73 reformado por el Decreto 81-96 del Congreso de la República de Guatemala, establece lo siguiente:

> ARTÍCULO 201.- Plagio o Secuestro. (Reformado por los Decretos 38-94, 14-95 y por Artículo 1 del Decreto 81-96 del Congreso de la República). A

[65] Toc López, S. Estudio sobre del delito de secuestro, 2007. Disponibilidad: http: //biblioteca.usac.edu.gt/tesis/04/04_6808.pdf Consultado: 10/09/2021.

los autores materiales o intelectuales del delito de plagio o secuestro de una o más personas con el propósito de lograr rescate, canje de personas o la toma de cualquier decisión contraria a la voluntad del secuestrado o con cualquier otro propósito similar o igual, se les aplicará la pena de muerte y cuando ésta no pueda ser impuesta, se aplicará prisión de veinticinco a cincuenta años. En este caso no se apreciará ninguna circunstancia atenuante.

Los cómplices o encubridores serán sancionados con pena de veinte a cuarenta años de prisión.

A quienes sean condenados a prisión por el delito de plagio o secuestro, no podrá concedérseles rebaja de pena por ninguna causa.

(Párrafo adicionado por Artículo 24 del Decreto 17-2009 del Congreso de la República).

Igualmente incurrirá en la comisión de este delito quien amenazare de manera inminente o privare de su libertad a otra persona en contra de su voluntad independientemente del tiempo que dure dicha privación o la privare de sus derechos de locomoción con riesgo para la vida o bienes del mismo, con peligro de causar daño físico, psíquico o material, en cualquier forma y medios, será sancionado con prisión de veinte (20) a cuarenta (40) años y multa de cincuenta mil (Q.50,000.00) a cien mil Quetzales (Q 100,000.00).

(Párrafo adicionado por Artículo 24 del Decreto 17-2009 del Congreso de la República). Este delito se considera consumado, cuando la persona sea privada de su libertad individual o se ponga en riesgo o en peligro inminente

la misma o se encuentre sometida a la voluntad del o los sujetos que la han aprehendido, capturado o sometido ilegal o ilegítimamente, por cualquier medio o forma y en ningún caso se apreciará ninguna circunstancia atenuante.[66]

3.3 Antecedentes históricos del delito de secuestro

En la antigüedad, el secuestro estaba vinculado con las guerras, puesto que consistía en una forma normal de sometimiento o comercio de personas. En virtud de la superioridad de un ejército sobre otro, el vencedor se atribuía el derecho a apropiarse del territorio conquistado y también de las personas derrotadas. Las guerras eran constantes, debido a que, en sociedades arcaicas, esta era la única manera de resolver las diferencias entre los pueblos o de imponerse sobre los demás.[67]

Por lo tanto, las personas caídas en cautiverio iban en aumento, lo que produjo que se comenzara a comercializarlas, dando origen a la esclavitud. Los fenicios, por ejemplo, secuestraban a doncellas y mancebos griegos, por quienes exigían un rescate o los comercializaban en ciudades que se caracterizaban por este tipo de negocios.

Después de Cristo, en el siglo XVIII, en Inglaterra, aparecieron algunas bandas de secuestradores, denominados *press-gangs*, los cuales operaban para el ejército y la marina, obligando y reclutando a los hombres para integrarse a las filas del ejército

[66] Decreto Numero 17-73 del Congreso de la República, Código Penal, título IV, De los Delitos contra la Libertad y la Seguridad de la Persona, Capítulo I De los Delitos contra la Libertad Individual.
[67] Jiménez Ornelas, R. A. El secuestro, uno de los males sociales del mexicano. México, D. F., Departamento de Investigaciones Jurídicas de la UNAM; 2010, p.17.

británico. En el pasado reciente, también este delito ha sido cometido por terroristas, quienes lo utilizan como medio de presión para que sus peticiones sean escuchadas.

En la actualidad, el secuestro, en la mayoría de los casos, busca beneficios de tipo económico; sin embargo, el delito como tal, no es moderno. Han cambiado los métodos y fines, pero en el fondo, mantiene lo básico: privar de manera ilegal del derecho a la libertad a un individuo, mediante amenazas.

3.4 Elementos constitutivos y estructura del delito de secuestro

De acuerdo con el tratadista Muñoz Conde, "en la composición de los tipos penales entran una serie de elementos de distinta procedencia y significación. Es imposible delimitar todas las peculiaridades que presentan los distintos tipos delictivos, lo que se puede hacer es precisar aquellos elementos que están siempre de manera constante en la composición del todos los tipos; los cuales son: sujeto activo, acción y bien jurídico"[68].

En la parte objetiva del tipo (positivo) habrá como mínimo los siguientes elementos: un sujeto activo, una acción y un bien jurídico. Estos van a estar siempre presentes en la composición de los tipos. Ahora bien, en el caso del delito de secuestro, deben darse los siguientes elementos[69]:

[68] Muñoz Conde, F. Teoría General del Delito. Valencia, España, Tirant lo Blanch, 1991, p.53.
[69] Monge Orejel, Brenda Leticia. El delito de secuestro sancionado con la pena de muerte pone en mayor riesgo la vida de las víctimas (Tesis de pregrado), Guatemala, Universidad de San Carlos de Guatemala, 2006, p.6.

a) Que exista materialmente una detención de la persona: debe existir una persona a quien se le ha puesto en tal condición material que no puede hacer ejercicio de su libertad de locomoción.
b) Que la detención sea arbitraria o ilegal: realizada bajo violencia física o moral y que el agente no cuente con la autoridad ni el derecho para hacerlo.
c) Que dicha detención sea intencional: es decir, que exista la intención de privar de la libertad a la persona.
d) Que los fines sean obtener otros beneficios: el motivo de la detención no es el de privar de la libertad a una persona, sino un medio para cobrar un rescate por la víctima, causar daño a familiares o ejercer presión sobre una autoridad para que realice o deje de realizar determinada actividad.

3.5 Naturaleza y causas del delito de secuestro

El delito de secuestro obedece a causas de diversa índole, entre las que se pueden señalar las sociales, económicas, psicológicas, políticas, culturales e incluso, religiosas. Sin embargo, prevalecen las de tipo económico, puesto que el dinero constituye la principal motivación en la mayoría de los crímenes.[70]

Por tal razón, este delito, el narcotráfico y el sicariato, son los que más destacan, en virtud de las ganancias que pueden generar los delincuentes. El secuestro para obtener rescate, también conocido como secuestro económico o secuestro con fines de

[70] Arrona-Palacios, Arturo; Banda-Cruz, Daniel Alberto; Guevara-López, Carlos Alejandro; Villarreal-Sotelo, Karla El secuestro en Tamaulipas y sus repercusiones. CienciaUAT, vol. 6, núm. 2, octubre-diciembre, 2011, pp. 70-74 Universidad Autónoma de Tamaulipas, Ciudad Victoria, México.

lucro, es un delito realizado principalmente por organizaciones criminales y no por delincuentes individuales, dado que requiere de una planificación cuidadosa de las diversas etapas del proceso.

En este sentido, se puede apreciar que el delito de secuestro, a excepción del secuestro exprés, no es algo improvisado, sino debidamente planificado. En la ilustración siguiente, se presenta de manera gráfica el esquema de un secuestro.

Con respecto a la naturaleza de este delito, es necesario analizar lo que la legislación guatemalteca dice sobre el mismo. En este orden de ideas, ocupa un lugar esencial el artículo 201 del Código Penal guatemalteco, Decreto 17-73 reformado por el Decreto 81-96 del Congreso de la República de Guatemala, el cual establece que “el plagio o secuestro consiste en el propósito de lograr rescate, canje de personas o la toma de cualquier decisión contraria a la voluntad del secuestrado o con cualquier otro propósito similar o igual…”.

Es evidente que los objetivos de los perpetradores, independientemente de cuáles sean estos, deben estar en conflicto con los de la víctima; por ello, se le priva de la libertad, para presionarla a que acceda a las peticiones de los perpetradores.

Sin embargo, el esquema de un secuestro suele seguir los mismos pasos. Hay un autor intelectual o partícipe, quien induce a cometer el delito o participa en él; un captor o captores, que se encargan de ubicar, seguir y capturar a la víctima; un cuidador, que se encarga de alimentar a la víctima y evitar que escape; un negociador, que se encarga de intentar reducir la cantidad que se exige como rescate; un lugar de encuentro, para

pagar el rescate y devolver a la víctima a los familiares; un cobrador, que se encarga de recibir el rescate; la liberación de la víctima; los medios de comunicación, que informan del delito cuando éste se comete o después de ello y, por supuesto, una víctima del delito.

Figura 8

Esquema de un secuestro

Fuente: Meluk, E.[71]

3.6 Tipos de secuestro

3.6.1 Secuestro de información privilegiada

Este tipo de secuestro se está volviendo más frecuente e implica secuestrar información a organizaciones más que a individuos, puesto que el impacto es mayor,

[71] Meluk, E. El secuestro, una muerte suspendida. Su impacto psicológico. Bogotá, D.C.: Uniandes, 1988, p.23.

dado que afecta a una mayor cantidad de personas. Este tipo de secuestro consiste en hacer que una institución no tenga acceso legítimo a sus bases de datos; el secuestrador solicita un monto económico para reestablecer el acceso.[72]

Pero, como sucede con todo secuestro, el desenlace del mismo no siempre es favorable para el afectado, puede que el atacante pueda desaparecer cuando recibe el pago, puesto que nada le obliga a cumplir con lo ofrecido. Para un secuestro de información, los delincuentes requieren de la complicidad de trabajadores, personal de seguridad o de limpieza de la empresa, a quienes sobornan o amenazan, para tener acceso al equipo de cómputo y extraer la información privilegiada.

3.6.2 Secuestro exprés

Es aquel que no requiere de una buena planificación como el secuestro habitual, generalmente es realizado por individuos y no por una banda crimina organizada. Este tipo de delincuentes busca algo rápido, sin complicaciones y sin hacer daño a la víctima, excepto en su economía.[73] Este tipo de secuestro tiene una duración mínima (generalmente menos de un día), en ese periodo, tratan de extraer el máximo de efectivo en retiros de cajeros automáticos o realizando compras, las cuales efectúa la víctima con sus tarjetas de crédito y, finalmente, el rescate que puedan pagar los familiares.

[72] ASOBANCARIA, Secuestro de información o "Ramsonware": una amenaza para todos, Cartagena, Colombia, Asobancaria, 2017, p.2-3.

[73] Parababire, Carmen. Perspectiva sociológica del secuestro express como una nueva modalidad de delito caso estudio: municipio Naguanagua Estado Carabobo año 2012 y el primer periodo del 2013 (Tesis de pregrado). Carabobo, Venezuela, Universidad de Carabobo, 2013, p.30.

Los delincuentes, generalmente buscan un lugar donde no exista vigilancia de la policía y no existan cámaras en los negocios o en las calles. Luego esperan una víctima que reúna ciertas características que indiquen que posee un trabajo o negocio que le permita disponer de una cantidad aceptable de dinero, en efectivo o en tarjetas de crédito o débito, a quien secuestran para realizar retiros de dinero o compras con tarjeta. Luego de realizar su cometido, la dejan en libertad, casi siempre en un lugar desolado.

3.6.3 Secuestro con rehenes

Es cuando una o más personas son secuestradas para obligar a otra a cometer un crimen, que puede ser cualquier cosa, desde robo, extracción de un rescate, hasta asesinato, en beneficio de los secuestradores.[74] También puede tratarse de un robo con rehenes, o por ejemplo, secuestran a los familiares de un empleado bancario, para obligarlo a abrir las cajas fuertes.

3.6.4 Secuestro terrorista

Es un tipo de secuestro motivado por razones financieras y políticas, se realiza en países con condiciones políticamente inestables donde existe injerencia extranjera, la cual es rechazada por ciertos grupos extremistas.[75] En este sentido, las víctimas son personas extranjeras y de nacionalidades perfiladas. No obstante, aunque las demandas

[74] Unidad Editorial Internet, S. L., elmundo.es Un 'secuestro tigre' en Irlanda se salda con un botín de siete millones de euros, España, 2009. Recuperado de: https://www.elmundo.es/elmundo/2009/02/27/internacional/1235752696.html Consultado el 02/09/21.
[75] Neira Brunetti, Bernardo. El delito de secuestro y el secuestro terrorista, Santiago, chile, Universidad Andrés Bello, 1997, p.11.

iniciales son políticas, pueden pasar a beneficios financieros a medida que las negociaciones avanzan.

3.6.5 Piratería por rescate

Son incidentes se producen en zonas marítimas en las que no existe el derecho de soberanía del Estado. Este tipo de secuestro hace referencia a la captura física de la carga de un buque como la exigencia de un rescate a cambio del buque, la tripulación y la carga; representa un desafío multijurisdiccional cuyas cifras crecientes, en relación tanto con la frecuencia de los ataques como con el pago medio de rescates, plantean graves amenazas para el sistema financiero, de seguros y de envío.[76]

3.6.6 Secuestro virtual

Es cuando la víctima no sabe que ha sido secuestrada, porque se le lleva con engaño a un lugar donde no puede comunicarse o ser contactado, al mismo tiempo que un familiar recibe llamadas de alguien que afirma haber secuestrado a su ser querido y exigen un rescate para liberar al rehén.[77]

[76] Ibáñez Gómez, Fernando & Esteban, Miguel Ángel. Análisis de los ataques piratas somalíes en el Océano Índico (2005- 2011): evolución y modus operandi, Zaragoza, España, Universidad de Zaragoza, 2013, p.10-35.
[77] Ministerio Público Fiscal. El Ministerio Público Fiscal de la nación recomienda algunas precauciones para evitar ser víctima de los denominados “secuestros virtuales”, Buenos, Aires, Argentina, Procuraduría General de la Nación, 2014, p.1.

3.6.7 Secuestro con fines de explotación sexual

Es aquel en el que no se solicita rescate, porque involucra a mujeres y niños que serán vendidos en el extranjero, con la finalidad de ser explotados sexualmente. Puede incluir abusos deshonestos o matrimonio.[78] El *modus operandi*[79] puede ser diverso. En algunos casos, los delincuentes observan a alguien que les interesa y le siguen la pista, o bien, a través de las redes sociales buscan perfiles de usuarios que reúnen las características buscadas, se hacen amigos de las posibles víctimas y, luego de ganarse la confianza de éstos, programan un encuentro personal, para efectuar el secuestro.

3.6.8 Autosecuestro

Es cuando la propia víctima simula estar secuestrada y puede hacerlo solo o con la colaboración de amistades, compañeros o la pareja, con el objetivo de obtener un beneficio material.[80] Por lo tanto, se trata de un secuestro planificado por la propia víctima, con el fin de obtener un beneficio económico.

3.6.9 Secuestro extorsivo

Es un tipo de secuestro que implica el hecho de que se exija un beneficio ilegal a cambio de liberar a la víctima; por tal razón, hace referencia a arrebatar, sustraer, retener

[78] Oficina de las Naciones Unidas Contra la Droga y el Delito. Manual sobre la investigación Del delito de trata de personas. Guía de autoaprendizaje, San José, Costa Rica, UNODC, 2010, p.15.
[79] Expresión latina que significa 'modo de obrar' y se usa para referirse a la manera especial de actuar o trabajar para alcanzar el fin propuesto.
[80] Observatorio Nacional Ciudadano. Análisis integral del secuestro en México. Cómo entender esta problemática, México, D. F., 2014, p.17

u ocultar a un individuo con el objetivo de exigir cualquier beneficio a cambio de su libertad.[81]

Por lo que se puede apreciar, el secuestro constituye un fenómeno diverso, dado que, en función del tipo de delito, puede estar vinculado con delincuentes organizados, infractores menores e incluso oportunistas. En algunos casos, puede incluir a terroristas o grupos de insurgentes. La motivación puede ser un beneficio económico, el rencor o la desesperación. El secuestro de víctimas puede ser general (como el caso de los secuestros express) o específico (políticos, gente adinerada, migrantes).

Figura 9

Algunos tipos de secuestro

Fuente: Molina, B. et. al.[82]

[81] Góngora Pimentel, G. Evolución del poder Judicial y las decisiones del Poder Judicial de la Federación en la materia, México, D. F., Porrúa, 2003, p.51-52.

[82] Molina, B., Agudelo, M., De los Ríos, A., Builes, M., Ospina, A., Arroyave, R. et al. El secuestro: su repercusión en las creencias y en la estructura de relaciones en un grupo de familias antioqueñas. Revista Colombiana de Psiquiatría, 32(1), 27-50, 2003.

3.7 Problemática en el delito de secuestro

En todo delito se hace referencia a la participación y esta se da cuando varios sujetos activos intervienen en la comisión del acto o del conjunto de actos que configuran la infracción penal que amerita una sanción con base a la ley. Con respecto a la autoría y participación, el sujeto es el individuo a quien se le puede imputar un hecho como suyo. Es autor, en sentido estricto, aquel que realiza un acto sin la intervención de otra persona. Los partícipes están supeditados al principio de accesoriedad de la participación respecto del hecho realizado por el autor real. En este sentido, aunque el Código Penal establezca que el inductor es autor, para que se hable de inducción, debe existir un hecho antijurídico por parte del autor real, porque la inducción por sí sola, no es delito[83].

Por tal razón, el mismo Código Penal guatemalteco, en el artículo 17, indica que la inducción, la instigación, la conspiración, la proposición o la provocación a cometer un delito no son punibles en sí mismas, a excepción de aquellos casos que la ley señale expresamente. En este orden de ideas, la inducción a cometer un homicidio o un secuestro, no se puede sancionar, si el inducido no realiza ninguna acción dirigida a cometer el delito. Ahora bien, las excepciones son válidas, cuando exista un tipo penal que describa tales acciones.

En el caso específico del delito de secuestro, hay tentativa cuando el *iter criminis* no se completa, dándose únicamente tres primeras etapas. En este sentido, el artículo 14 del Código Penal, establece que “hay tentativa, cuando con el fin de cometer un delito,

[83] Cauhapé-Cazaux, Eduardo. Apuntes de derecho penal guatemalteco. La teoría del delito. Guatemala, Fundación Myrna Mack, 2003, p.127.

se comienza su ejecución por actos exteriores, idóneos y no se consuma por causas independientes de la voluntad del agente".

La tentativa es punible cuando la decisión del agente en cometer el delito se exterioriza, mediante la realización de actos dirigidos a tal fin, pero el delito no es consumado por diversas circunstancias que no dependen de su voluntad. En este caso, queda al criterio del juzgador la clasificación del delito o la tentativa en su caso, considerando los elementos concretos en el mismo.

3.8 Concurrencia del delito de secuestro

Existe es necesario recurrir a más de un delito para tipificar la conducta realizada por un autor, se está ante un concurso de delitos; es decir, si el autor ejecutó varios hechos y cada uno de ellos es delito. Ahora bien, si varios delitos se cometen con un mismo hecho, hay un concurso ideal de delitos.[84] En este orden de ideas, antes de analizar los distintos concursos, se debe determinar cuándo concurre un hecho o cuando son varios. El concepto de unidad de hecho es eminentemente valorativo. Al respecto, la doctrina ha elaborado criterios específicos.

Lo primero a considerar es el criterio jurídico. En este sentido, la tipificidad es la característica esencial que delimita cuando se está ante un hecho.[85] Una conducta se convierte en un hecho, cuando se encuentra tipificada, por ejemplo, un apoderamiento

[84] Toc López, op. Cit. p.46-47.
[85] Calderón Martínez, A. T. Teoría del delito y juicio oral, 23ª. Ed. México, D. F., Departamento de Investigaciones Jurídicas de la UNAM, 2012, p.14.

de algo que pertenece a otro individuo, utilizando la violencia, es un hecho de robo, de acuerdo al Artículo 251 del Código Penal guatemalteco, y varios bajo otros tipos.

Para la determinación de un tipo, de manera que se pueda hacer referencia a un hecho, se requiere de una sola acción y un solo resultado material, aunque con ello se hayan vulnerado diversos resultados típicos.[86] Por ejemplo, al asesinar a un agente de la Policía Nacional Civil, se trata de una sola acción y un solo resultado; no obstante, se han cometido dos delitos.

Se hace referencia a un concurso de delitos, cuando el mismo hecho, constituye un o más delitos tipificados en una ley, tal como lo establece el Código Penal guatemalteco, en el artículo 70. Esto obedece a que no se puede valorar de la misma manera aquellos supuestos en lo que un hecho produce varios delitos y los que solo producen un delito.

3.9 Secuestro y redes sociales

En las redes sociales se observa con frecuencia como muchas personas publican fotografías de sus vehículos, propiedades, empresas, actividades, los nombres de sus mejores amigos, de la pareja y de sus padres. Incluso, comparten datos específicos vinculados con centros educativos, universidades, clubs, gimnasio, número telefónico y hasta su dirección personal.[87] Esto debido a que los teléfonos actuales, cuentan con la

[86] *Ibíd.*

[87] Pineda, Billy Alexander. Estado situacional de la educación secundaria ante el uso de redes sociales digitales, Guatemala, Universidad de San Carlos de Guatemala, Dirección General de Investigación, 2020, p.15.

tecnología para tener acceso permanente a las redes sociales y compartir material multimedia de manera automática, así como ubicaciones y otro tipo de información, que permite ubicar con facilidad a un individuo.

Toda esta información es de mucha utilidad para los secuestradores, puesto que se valen de ella para seleccionar a sus posibles víctimas y llegar con facilidad a ellas. Por ejemplo, publicar que se está estrenando vehículo o que se acaba de adquirir la versión más reciente del IPhone, puede ser muy peligroso.

Hay personas muy interesadas en examinar todos los movimientos de otros individuos, dónde estudian y trabajan, las rutas utilizadas, los horarios, el salario aproximado de acuerdo al puesto de trabajo, tipo de vehículo, lugares visitados, estilo de vida, objetos personales, tipo de vivienda, entre otras cosas. Todo ello, hace que una persona se convierta en presa fácil de los delincuentes.

La manera de operar de los delincuentes que se dedican al secuestro, es por medio de cuentas falsas en las redes sociales con datos inexistentes, con fotos que no son suyas y que roban de otros perfiles.[88] Se hacen pasar por adolescentes, jóvenes, mujeres o empresarios, de acuerdo a las características de la posible víctima. Envían invitaciones, conversan con los adolescentes, obtienen la información que necesitan, incluso planifican encuentros personales y luego los secuestran. La identificación de estas cuentas y sus propietarios, es difícil de realizar, puesto que, generalmente, son creadas en cafés internet, lo que dificulta su rastreo.

[88] *Ibíd.*

Sin embargo, esta no es la única modalidad de secuestro a través de las redes sociales. También existe el secuestro virtual y el secuestro de datos y perfiles. El secuestro virtual, consiste en falsificar un secuestro. Para ello, se necesita el número telefónico de la víctima, contar con Skype u otra plataforma de números telefónicos virtuales y conocer los horarios y actividades de la misma.[89]

Por ejemplo, cuando un adolescente se encuentra en horario de clases en un centro educativo, los delincuentes saben que no puede atender llamadas telefónicas, entonces crean un número virtual (el mismo de la víctima), para hacer creer que tienen en sus manos dicho teléfono y a la víctima, por supuesto, y piden una determinada suma de dinero, la cual no es muy grande, para que pueda ser reunida y transferida de inmediato. Se trata de una suplantación de identidad; por ello, al final, se descubre que la supuesta víctima nunca estuvo secuestrada.

Se trata de un tipo de estafa muy difícil de eliminar, en virtud del lugar de origen, el cual, en la mayoría de los casos, coincide con el de un centro penitenciario. Los delincuentes encarcelados, suelen sobornar a los guardias para adquirir y utilizar teléfonos celulares. Y como cuentan con el tiempo suficiente para navegar en las redes sociales en búsqueda de posibles víctimas, con facilidad encuentran perfiles que se adaptan a sus requerimientos.

[89] Muñoz Arango, C. E. El delito del secuestro. Anuario de Derecho N° 48, Págs. 178 -186, 2019, p.183.

Ahí es cuando los estafadores o piratas informáticos envían mensajes para que parezca que provienen de alguien que la víctima conoce, pidiéndoles que renuncien a la información o que realicen una acción, como ingresar una contraseña.

La suplantación de identidad, no es un problema de tecnología, sino de psicología humana.[90] Los delincuentes saben que la mayoría de las personas están demasiado ocupadas, como para ponerse a revisar la autenticidad de cada mensaje que se recibe; por tal razón, cualquiera puede ser víctima de este tipo de fraude. Muchas víctimas de este delito, no lo denuncian ni lo comentan con otras personas, porque se avergüenzan de haber sido estafadas; por otra parte, es muy difícil que las autoridades puedan dar con los culpables.

Además del secuestro virtual, existe el secuestro digital y la ciberextorsión.[91] Esto sucede, porque en una computadora se almacenan datos y archivos muy importantes, de los cuales, muchas veces no se cuenta con copia en otros dospositivos o medios. Toda esta información, puede estar en peligro ante un secuestro digital, una modalidad de extorsión que consiste en instalar un programa no deseado en la computadora, el cual puede llegar a través de un mensaje electrónico o un programa instalado desde un sitio no seguro.

Cuando dicho programa se instala automáticamente en la computadora, restringe el acceso a los archivos, los cuales solo pueden ser recuperados mediante una

[90] Mintic, enticconfio.gov.co Ciberextorsión por medio de secuestros de perfiles digitales. Colombia, 2020. Disponibilidad: https://www.enticconfio.gov.co/poder-digital/ciberextorsion-mediante-secuestro-de-perfiles-digitales Consultado: 18/09/2021.
[91] Ibíd.

contraseña que solamente conoce el criminal. A cambio de dicha contraseña, se pide un rescate de tipo económico; de no hacerlo, los archivos son destruidos.

Esta modalidad criminal, denominada *ransomware* “secuestro de datos”, no afecta únicamente a los archivos, puesto que actualmente también existe el secuestro de perfiles digitales, dado que hay varias maneras para robar las contraseñas de acceso y el usuario pierde el control de sus cuentas y correos.[92]

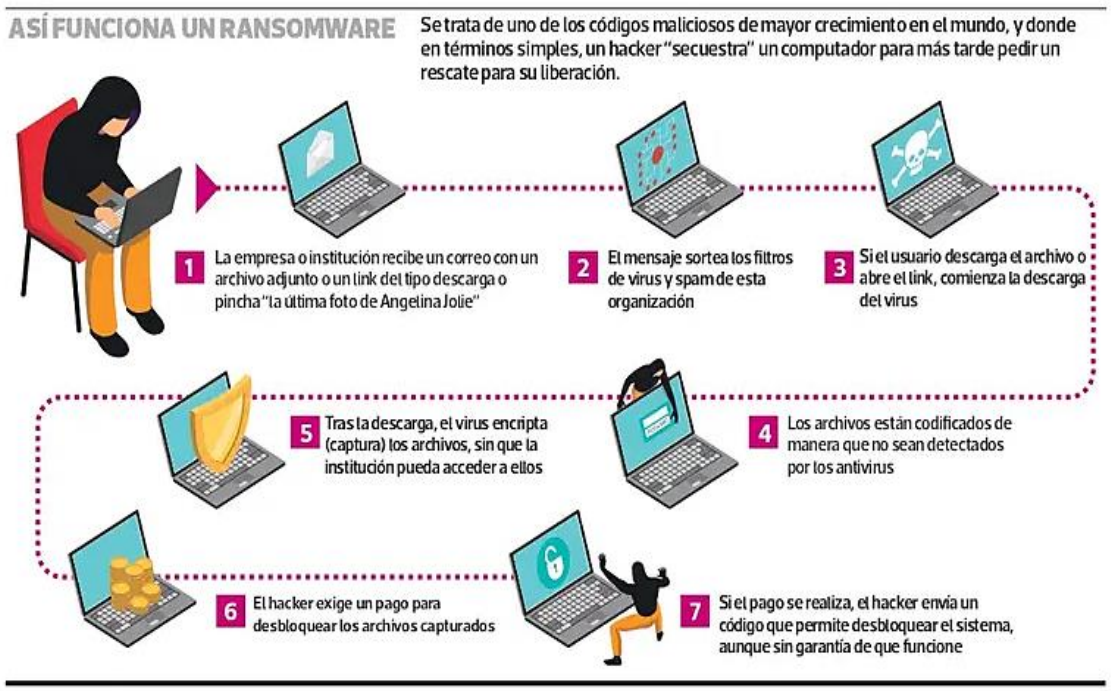
En este sentido, la extorsión se enfoca en devolver el control de la cuenta o perfil al usuario, a cambio de una suma monetaria, con la amenaza de publicar contenido privado que se encuentre en la cuenta. Esto también afecta los perfiles en redes sociales que cuentan con miles de seguidores, puesto que las empresas propietarias de tales sitios, pagan determinada cantidad de dinero a los usuarios que tienen más seguidores. Los delincuentes conocen el valor de tales perfiles, por ello, se convierten en blanco de sus ataques.

Ante un caso de secuestro digital, el usuario solo tiene dos opciones: pagar el rescate o contratar a un experto en informática, para recuperar la cuenta. En cualquiera de los dos casos, se requiere de un desembolso de dinero. En la ilustración siguiente, se presenta de una manera gráfica el funcionamiento del secuestro de datos.

[92] Redacción Tecnósfera, eltiempo.com Ramsomware: aumenta el delito de secuestro de datos, Colombia, 2021. Disponibilidad: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ransomware-riesgos-del-secuestro-de-datos-y-consejos-para-evitarlo-609194 Consultado: 20/10/2021.

Figura 10

Proceso del ransonmware o secuestro de datos



Fuente: Amescua (2010).[93]

La dinámica de los ataques es básicamente la misma y se da en tres pasos: el aterrizaje, la extracción y el secuestro. El punto de partida es el acceso a los sistemas de una empresa específica, por medio de un correo electrónico que engaña a un trabajador, un archivo multimedia (fotografía de una actriz o modelo) que contiene un programa malicioso, un dispositivo de almacenamiento sin protección, un servidor vulnerable, entre otros.[94]

[93] Lazcano, Patricio & Montes, Carlos. Latercera.com Así funciona un ransomware, el virus que tiene en jaque a Banco Estado y es la principal ciberamenaza en Chile, Chile, 2020. Disponibilidad: https://www.latercera.com/que-pasa/noticia/asi-funciona-un-ransomware-el-virus-que-tiene-en-jaque-a-bancoestado-y-es-la-principal-ciberamenza-en-chile/7C5WJ2LOVZFDNAGV636LJ4WQYQ/ Consultado: 12/10/2021.

[94] Tarlogic Security Experts. Tarlogic.com Ransomware o cómo quedarse sin empresa en unas horas, España, 2021. Recuperado de: https://www.tarlogic.com/es/blog/ataque-ransomware-en-horas/ Consultado el 12/10/2021.

Una vez dentro, inicia la extracción, tanto como sea posible, para comprometer su continuidad. Desde ese servidor, los delincuentes se apoderan de toda la información de la empresa y la encriptan. A partir de ello, solicitan el rescate, en función de los datos secuestrados y la importancia de la empresa. Amenazan con no devolver la información o hacerla pública, por lo que constituye una doble extorsión.

Para tener una idea más clara de la magnitud del problema, durante el primer semestre del año 2020, Guatemala recibió 25 millones de intentos de ciberataques de "fuerza bruta", o intentos repetidos y sistemáticos de descubrir una credencial a través de diversos nombres de usuario y contraseñas.[95]

3.10 Rastros en redes sociales de un delito de secuestro

Las víctimas de un delito de secuestro donde los delincuentes se apoyan en las redes sociales, generalmente son contactadas por medio de un perfil falso, tal como sucedió en un hecho registrado en el municipio de Gualán, departamento de Zacapa, en el año 2018.[96] En este caso, la interacción con la víctima por medio de mensajes, queda guardada en el historial de mensajería.

Para que pueda materializarse el delito, los delincuentes necesitan estar en contacto con la víctima durante un tiempo indefinido, hasta que obtengan toda la

[95] MRInternacional S.A. newsinamerica.com Guatemala sufrió más de 25 millones de intentos de ciberataques en la primera mitad del año, 2020. Recuperado de: https://newsinamerica.com/pdcc/tecnologia/2020/guatemala-sufrio-mas-de-25-millones-de-ciberataques-en-la-primera-mitad-del-ano/ Consultado el 12/10/2021.

[96] Morales, Mario, prensalibre.com Usaron perfil falso de Facebook para secuestrar a joven; PNC los captura Guatemala, 2018. Disponibilidad: https://www.prensalibre.com/ciudades/zacapa/usaron-perfil-falso-de-facebook-para-secuestrar-a-joven-pnc-los-captura/ Consultado: 27/10/2021.

información que necesitan. Esto implica una serie de conversaciones y de intercambio de fotos, videos u otro tipo de material, hasta que finalmente concertan un encuentro personal, o bien la víctima informa inocentemente en dónde se encontrará en determinada fecha y horario.

Entonces, para la investigación del delito, se debe revisar el historial de conversaciones entre la víctima y los delincuentes, luego investigar la cuenta o perfil utilizado por éstos, la dirección IP y todo aquello que contribuya a identificarlos. A este conjunto de estudios e investigaciones que se realizan con la finalidad de obtener una prueba o evidencia electrónica que pueda ser aplicada para el esclarecimiento de un delito, se denomina peritaje informático.

CAPÍTULO IV

INVESTIGACIÓN Y PERITAJE INFORMÁTICO

4.1 Definición de peritaje informático

El desarrollo de la tecnología, cuestiones sociales y de tipo legal han permitido un avance en el ámbito de la investigación en la informática forense; sin embargo, estos mismos elementos terminan afectando, en virtud de que este aumento en el uso de recursos tecnológicos va de la mano con el crecimiento de los delitos vinculados con estos medios digitales. Por lo tanto, los métodos de investigación delictiva deben actualizarse constantemente, para responder de una manera eficaz a los riesgos que presentan los avances tecnológicos en el ámbito de la criminalidad.

En este orden de ideas, el peritaje informático hace referencia a los estudios e investigaciones que se realizan con la finalidad de obtener una prueba o evidencia electrónica que pueda ser aplicada en un asunto judicial o extrajudicial, de manera que contribuya a establecer la culpabilidad o inocencia de una de las partes[97].

La informática forense es muy importante, en virtud de la ubicuidad de la tecnología en la vida diaria, dado que se utiliza en casi todo; por tal razón, se incrementan los delitos en este ámbito y la informática forense hace lo que le corresponde en el proceso de

[97] Torres, Enrique. Cyta.com.ar Informática forense: el camino de la Evidencia digital, Buenos Aires Argentina, 2020. Recuperado de: http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/informatica_forence.htm Consultado el 13/10/2021.

investigación.[98] Desde la perspectiva de la aplicación de la ley, la mayoría de los casos tienen alguna relación, aunque mínima, con la tecnología informática. Por ejemplo, la evidencia de un delito puede vincularse a un teléfono celular o computadora portátil, enviarse por correo electrónico, publicarse en las redes sociales o ser algo almacenado en la nube o en una cuenta de Dropbox.[99]

Hoy en día, el aumento en el uso de dispositivos móviles, se ha convertido en un desafío para las investigaciones y ha marcado un cambio en la forma en que se recopilan las pruebas. Con la informática, se está dando el paso a la domótica, es decir, la automatización de procesos y tareas domésticas. Por ejemplo, los asistentes digitales Echo, Siri y Portal, junto con los refrigeradores, microhondas y focos conectados a la web y otros electrodomésticos, se encuentran cada vez en más hogares con conectividad a Internet, bocinas y micrófonos. Se trata de una era en la que todo debe ser examinado.[100]

Hay una serie de herramientas de informática forense, de uso común para todo informático forense por ser básicas en su trabajo: clonadoras de datos, bloqueadoras de escritura, creación de imágenes forenses, cálculo de firmas hash, análisis de memoria volátil, suites de herramientas forenses, herramientas de firma electrónica, entre otros.

[98] Cruz Quintero, Gloria Esperanza. Importancia de la informática forense, Bogotá, Colombia, Universidad Piloto de Colombia, 2016, p.1.
[99] Es un espacio virtual, para almacenar archivos en la nube.
[100] Bryson, Joanna. Bbvaopenmind.com La última década y el futuro del impacto de la IA en la sociedad, España, Grupo BBVA, 2022. Recuperado de: https://www.bbvaopenmind.com/articulos/la-ultima-decada-y-el-futuro-del-impacto-de-la-ia-en-la-sociedad/ Consultado el 16/02/2022.

4.1.1 Análisis forense informático

La ciencia forense en el ámbito informático es un área relativamente nueva; por tal razón, existen diversas denominaciones para hacer referencia a esta actividad. Las más utilizadas, son las siguientes: análisis forense informático, informática forense, análisis forense digital, *computer forensics, digital forensics*, cómputo forense, entre otras[101].

De la misma manera que existen varias denominaciones para hacer referencia a la actividad forense en el ámbito informático, también existe una serie de definiciones que describen la esencia de esta actividad. De acuerdo con Barrére Cambrún, el análisis forense informático es el "conjunto de principios y métodos científicos que comprende la recolección, preservación, documentación, validación, identificación, análisis, interpretación, y presentación de evidencia digital derivada a partir de fuentes digitales con el propósito de facilitar la reconstrucción de eventos delictivos en un modo legalmente aceptable, y anticipar acciones no autorizadas que puedan perturbar el curso normal de las operaciones"[102].

Es de suma importancia la presentación de pruebas en cualquier ámbito o proceso legal; no obstante, con respecto a la evidencia informática, el reto es aún mayor. Se requieren conocimientos avanzados en la materia y mucho cuidado para el manejo de las pruebas, de manera que sufran alteraciones. Para que un medio pueda ser

[101] Barrére Cambrún, Martín. Análisis Forense Informático. Automatización de Procesamiento de Evidencia Digital. Montevideo, Uruguay, UDR, 2010, p.15.
[102] *loc. cit.*

presentado como prueba del delito, este debe ser competente y relevante, con el fin de demostrar que la culpabilidad o inocencia de un individuo.

4.2 Perito informático forense

Tal como se ha afirmado, la informática forense es la recopilación, examen, preservación y presentación de evidencia digital. Los expertos en informática forense adquieren y examinan posibles pruebas durante una investigación, incluidos los datos que se han eliminado, cifrado o dañado. Se documentan todos los pasos que se toman durante este proceso y se utilizan metodologías específicas para evitar que la evidencia sea alterada, corrompida o destruida. Cualquier caso relacionado con la informática forense, siempre debe tratarse como si fuera a un tribunal, y cualquier documentación y evidencia eventualmente será entregada a un fiscal.[103]

En casos penales, el abogado defensor también puede contratar a su propio experto para revisar las pruebas y determinar si se cometieron errores durante el examen de un dispositivo digital vinculado con algún delito. El experto también documentará las acciones que tomó, que generalmente se incorporarán en un informe final que presentará el abogado. A este experto también se le puede solicitar que testifique en el tribunal, pero esta vez en nombre del abogado defensor.

[103] González, Yolanda. protecciondatos-lopd.com La informática forense en la investigación de delitos, Madrid España, Grupo Atico34, 2020. Recuperado de: https://protecciondatos-lopd.com/empresas/informatica-forense/ Consultado el 13/10/2021.

Mientras actúa como experto de la defensa, el experto forense informático debe permanecer imparcial y cualquier análisis que realice implica examinar, preservar y presentar pruebas, y también podría requerir de la recopilación de pruebas adicionales que se pasaron por alto durante la investigación. Al hacerlo, el experto debe encontrar razones alternativas para explicar la presencia de datos, como identificar si un caballo de Troya, botnet u otro software malicioso estaba presente en el dispositivo.[104]

Los expertos en informática forense también pueden ser de utilidad en litigios civiles. Debido a que la información relacionada con un caso puede almacenarse en computadoras u otros dispositivos, los expertos en informática forense pueden buscar datos como correo electrónico, mensajes de texto, registros de chat, historial del sitio web, archivos de calendario, hojas de cálculo, documentos, imágenes, entre otros. El examen de estos datos puede revelar hechos que revelen una relación adúltera, fraude, malversación, descarga o visita de material ilegal o perturbador (como pornografía), u otras actividades que podrían determinar el resultado de una demanda.

Debido a que los datos adquiridos a través de la informática forense incluyen documentos, hojas de cálculo y otros archivos que contienen información fuera del alcance del conocimiento del experto en informática, se requiere del apoyo de expertos adicionales para explicar lo que se ha encontrado. En tales situaciones, la investigación

[104] Ministerio de Defensa. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio, Madrid, España, Ministerio de Defensa, 2010, p.26-28.

y los litigios penales o civiles subsiguientes, a menudo utilizarán otros expertos que se adapten a las pruebas.[105]

El perito informático forense, se encarga de la cadena de custodia de una evidencia digital, el cual consiste en un procedimiento documentado, que permite confirmar el origen, autenticidad e integridad de los elementos digitales vinculados con un hecho relevante para el proceso judicial, desde que es encontrado e intervenido. En el ámbito de la informática forense, es esencial, si se pretende acudir a tribunales de justicia para dirimir responsabilidades y daños informáticos causados por terceros.

Aquí entra en juego la importancia de la evidencia digital, puesto que esta es la que tiene valor probatorio en los procesos judiciales. Para que sea eficaz, se requiere que se acredite el origen y la existencia de los datos, mediante diversos métodos; se debe garantizar que la obtención de los datos sea lícita; que los datos no hayan sufrido alteración alguna, entre otros.

4.3 Habilidades del perito informático forense

Un perito informático forense, debe poseer diversas habilidades y aptitudes, que le permitirán descubrir las evidencias necesarias que contribuyan a confirmar la culpabilidad o inocencia de alguien ante un delito que se investiga.

[105] Londoño Rojas, Edna Margarita. La interdisciplinariedad de la informática forense en la era digital, Bogotá, Colombia, UNIPILOTO, 2015, p.1-2.

4.3.1 Aptitud técnica

Como su nombre lo indica, los trabajos de informática forense se centran en la tecnología. Por lo tanto, el perito informático forense deberá trabajar en una variedad de tecnologías, desde computadoras hasta dispositivos móviles y sistemas operativos, para identificar y responder a las brechas de seguridad y los ataques a la red.[106]

4.3.2 Atención al detalle

Como investigador, deberá estar orientado a los detalles para poder clasificar cuidadosamente cantidades significativas de datos para descubrir y examinar evidencia digital. La minuciosidad y el buen ojo para los detalles son habilidades esenciales en informática forense.[107]

4.3.3 Comprensión del derecho y la investigación penal

La informática forense está vinculada con la investigación criminal y con la tecnología. Por lo tanto, el perito informático forense, debe tener una sólida comprensión de los diversos delitos, el derecho penal y la investigación criminal, habilidades que se pueden desarrollar a través de un título a nivel superior en informática forense. Además,

[106] Bassini, Andrés Eduardo. derechopenalonline.com El perito informático y la prueba pericial, Argentina, 2013. Disponibilidad: https://derechopenalonline.com/el-perito-informatico-y-la-prueba-pericial/ Consultado: 10/10/2021.

[107] Romero Castro, Martha; Choez Chele, Miguel Angel; Álava Mero, Christian José, et, al. La informática forense desde un enfoque práctico, Manabí, Ecuador, Área de Innovación y Desarrollo, 2020, p.21.

debe conocer las leyes que protegen el ámbito de la intimidad y la privacidad de la información.[108]

4.3.4 Habilidades de comunicación

Como investigador, a menudo se le pedirá que explique sus hallazgos a otras personas dentro de su organización, o incluso a un tribunal como parte de un caso penal. Las habilidades de comunicación, junto con otras habilidades sociales clave, son esenciales en informática forense. El perito deberá poder transmitir información técnica de manera clara y concisa a personas de diferentes niveles de comprensión técnica.[109]

Las habilidades de comunicación son importantes para el perito informático forense, dado que necesita hablar con ejecutivos de empresas e incluso con personas comunes en una sala de audiencias, y describir temas complejos a personas que pueden no tener idea de lo que está hablando.

4.3.5 Comprensión de los fundamentos de la ciberseguridad

Si bien, la ciberseguridad y la informática forense son dos campos separados, están estrechamente relacionados, y tener una base en ciberseguridad puede ayudar al perito a sobresalir en su carrera de informática forense. Para poder resolver eficazmente los delitos digitales, deberá tener un conocimiento sólido de las tácticas que utilizan los

[108] Fintech School, escuelafintech.com Las funciones del perito informático, España, 2019. Disponibilidad: https://escuelafintech.com/que-es-perito-informatico/ Consultado: 11/10/2021.
[109] PJ Group, peritojudicial.com Las 11 habilidades clave de un perito, España, 2020. Disponibilidad: https://peritojudicial.com/11-habilidades-clave-perito/ Consultado: 11/10/2021.

delincuentes para violar los sistemas y cómo trabajan los profesionales de la ciberseguridad para prevenir dichos ataques. La mayoría de los programas de grado en informática forense tienen un componente de ciberseguridad por este motivo.[110]

4.3.6 Habilidades analíticas

Tener una aptitud natural para el pensamiento analítico es imprescindible para todo perito informático forense. Como investigador, deberá analizar pruebas, observar situaciones de cerca, notar patrones y discrepancias, interpretar datos y, en última instancia, resolver delitos, todo lo cual requiere un alto nivel de capacidad analítica.[111]

4.3.7 Deseo de aprender

Como ocurre con cualquier campo técnico, la informática forense cambia constantemente. Cualquiera que trabaje en este ámbito, deberá comprometerse a actualizarse permanentemente con las mejores prácticas y las tendencias emergentes de la industria, y siempre deberá aprender y autoeducarse, tanto dentro como fuera de los horarios laborales.[112]

[110] Ciberseguridad, ciberseguridad.com Perito informático forense y judicial, España, 2019. Disponibilidad: https://ciberseguridad.com/servicios/perito-informatico/ Consultado: 11/10/2021.
[111] García, Luis. Onretrieval.com El Investigador Forense y la pérdida de datos. España, 2021. Disponibilidad: https://onretrieval.com/el-investigador-forense-y-la-perdida-de-datos/ Consultado: 12/10/2021.
[112] Matesanz, Vanesa. Xataka.com ¿Cómo se llega a ser el perito informático que analiza los discos duros de Bárcenas? España, 2016. Disponibilidad: https://www.xataka.com/ordenadores/como-se-llega-a-ser-el-perito-informatico-que-analiza-los-discos-duros-de-barcenas Consultado: 12/10/2021.

4.3.8 Capacidad para trabajar con material desafiante

Se requiere que muchos especialistas en informática forense, en particular aquellos que trabajan en funciones de aplicación de la ley, realicen investigaciones que involucren material ofensivo o perturbador. La capacidad de trabajar con contenido tan desafiante, de forma regular, es importante.[113]

Si bien, algunas de las habilidades enumeradas anteriormente son las que debería tener naturalmente, por ejemplo, una inclinación natural por el pensamiento analítico y la tecnología, otras son las que deberá desarrollar a través de la capacitación o la educación formal. Dependiendo de su experiencia, un título en informática forense es un buen lugar para comenzar: le dará una base sólida en los principios de la investigación forense informática, además de una descripción general del derecho penal, ciberseguridad y habilidades técnicas específicas, como las vinculadas con computadoras y sistemas operativos y redes, entre otras.

Para trabajar en análisis forense informático, es beneficioso tener conocimientos y habilidades en tecnología informática y programación de software, pero también lo es tener una curiosidad natural por resolver acertijos y problemas. El impulso para mantenerse actualizado en tecnología también es importante.

[113] Herranz, Arantza. Xataka.com Soy perito informático y estos son algunos de los casos más surrealistas en los que he trabajado. España, 2020. Disponibilidad: https://www.xataka.com/seguridad/soy-perito-informatico-estos-algunos-casos-surrealistas-que-he-trabajado Consultado: 12/10/2021.

Para ser un investigador forense informático exitoso, se debe estar familiarizado con más de una plataforma informática y todo lo relacionado con este ámbito. Además de las plataformas más antiguas, como DOS y Windows 9x, se debe estar familiarizado con Linux, Macintosh, Windows y las plataformas móviles actuales, como Android.[114] Sin embargo, nadie puede ser un experto en todos los aspectos de la informática. Del mismo modo, no se puede saber todo sobre la tecnología que está investigando. Por tal razón, para complementar sus conocimientos, el perito debe desarrollar y mantener contacto con profesionales de la informática, las redes y la investigación, así como otros profesionales con los que ha trabajado.

4.4 Deberes y roles del perito informático forense

Los deberes y roles de un testigo experto forense informático, a menudo giran en torno a una investigación criminal en la que una computadora o dispositivo móvil, es parte de la actividad ilegal. Sin embargo, estos mismos expertos también pueden investigar un caso de litigio civil, relacionado con la piratería, secuestro, un delito de “cuello blanco”, u otro, donde un experto puede resultar invaluable para probar la actividad detrás de la computadora.[115]

Un experto en informática forense a menudo tiene la capacidad de reconstruir los delitos a partir de la información que queda de las transacciones informáticas. Si la

[114] Indubitado. Indubitado.com Informática forense: resumen. España, 2021. Disponibilidad: https://indubitado.com/2021/informatica-forense-resumen/ Consultado: 12/10/2021.
[115] Perito Legal. Peritolegal.es Perito informático: la solución a tu caso con medios digitales. España, 2020. Disponibilidad: https://peritolegal.es/wp-content/uploads/2020/11/Perito-informatico-.-La-solucion-a-tu-caso-con-medios-digitales.pdf Consultado: 12/10/2021.

persona comete fraude, secuestro, malversación en una empresa, se involucra en pornografía infantil o tiene una conexión con el fraude de seguros u otros delitos, el experto forense puede descubrir tales actividades.

Para ello, deberá analizar la computadora o los dispositivos móviles donde se presuma que se encuentra la información relevante. En muchos casos, se requiere de software, herramientas y otros equipos para acceder a los archivos y datos borrados, que ya no están disponibles para la mayoría de las personas que usan la computadora o dispositivo móvil. Es posible que también necesite verificar la red, cualquier información previamente guardada en la empresa, en la nube o la persona que tuvo acceso a través de la intranet.

4.5 La evidencia digital

El término evidencia se refiere a los medios contribuyen a aceptar o rechazar un hecho.[116] Pueden ser testimonios, objetos, documentos, antecedentes, entre otros, los cuales ayudan a demostrar, aclarar, negar o confirmar los hechos. Toda evidencia debe cumplir con tres requisitos: tener relación directa con el caso (pertinencia), deben ser adecuadas, confiables y suficientes (validez), y deben estar comprendidas dentro de los parámetros físicos, psíquicos, legales y científicos (competencia).

Ahora bien, evidencia digital, son “todos aquellos datos aislados o relacionados entre sí que poseen características esenciales de recuperabilidad, preservación y

[116] Acurio Del Pino, Santiago. Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0, Quito, Ecuador, Instituto Nacional de Tecnología de la Información, 2015, p.3.

demostración de su existencia, frente a un escenario de cibercrimen, ciberdelincuencia o factores que afectaron los principios fundamentales de la seguridad en la información, integridad, disponibilidad y confidencialidad"[117]. Por lo tanto, engloba todo aquello que se produce, transmite y recibe por medio de un dispositivo electrónico o informático y que archiva o reproduce audio, imagen, video y otros datos. En definitiva, se trata de campos magnéticos y pulsos electrónicos, los cuales se recogen y analizan mediante técnicas y herramientas especiales.

En los inicios de la informática forense, en los equipos informáticos se buscaba evidencia digital de tipo constante y persistente; es decir, aquella que se almacena en un disco duro u otros medios y que se guarda al cerrar un archivo o cuando la computadora se apaga. Posteriormente, cuando surgieron las redes de interconexión, los investigadores forenses se encontraron ante el reto de buscar evidencia volátil, alojada temporalmente en la memoria RAM, o en el caché; se trata de evidencias inestables, las cuales se pierden cuando se apaga el computador. Por tal razón, las evidencias volátiles deben ser recuperadas casi de inmediato.[118]

En la actualidad se ha dado un auge de las redes de comunicaciones, por medio de celulares, internet, redes sociales, entornos 2.0, entre otros. Las relaciones interpersonales se canalizan a través de medios electrónicos y telemáticos. Por tal razón, también son más frecuentes los fraudes de todo tipo en este ámbito.

[117] Ortiz, Emanuel. Evidencia Digital: Fundamentos aplicables para el abordaje de la Examinación Forense. Boston, Massachusetts, Estados Unidos, RedCiber, 2019, p.1
[118] López Delgado, Miguel. Análisis forense digital, España, 2007, p.14.

En virtud de esta situación, se impone la necesidad de probar o acreditar la legitimidad de diversas operaciones como transferencias bancarias, declaraciones de impuestos, *e-commerce*, entre otras. De la misma manera, es necesario prevenir y detectar conductas ilícitas, tales como *phishing,* acosos en las redes sociales, amenazas mediante SMS, secuestro, suplantación de identidad en redes sociales, publicación de videos y fotografías íntimas sin consentimiento en medios electrónicos, entre otros. Todos tienen algo en común: el formato digital.[119]

4.6 Funciones adicionales de un experto en informática forense

El experto en informática forense, a menudo necesita armar un caso para determinar quién tiene la culpa en el crimen o en el caso civil y cómo proceder a partir de ahí. En un caso civil, el conocimiento y la comprensión de las computadoras, dispositivos móviles, internet, redes sociales y juegos online, por parte del experto puede proporcionar una mejor comprensión del modus operandi de los de los individuos que delinquen a través de estos medios, o donde estos, facilitaron la identificación y seguimiento de la víctima. En casos de secuestro, las redes sociales son fundamentales en este sentido, tanto para el delincuente, como para el perito.[120]

En el caso de una empresa, el perito debe demostrar la responsabilidad y los daños que ésta o un trabajador de la misma ha ocasionado a la víctima. En el caso de un secuestro, el perito debe demostrar cómo el delincuente utilizó las redes sociales en

[119] López Delgado. Op. cit. p.16.
[120] Acurio Del Pino, Santiago. Op cit. p. 4.

la comisión del delito. Se debe demostrar el hecho, los autores, la fecha y la hora y el lugar donde se produjo la conducta delictiva.[121]

En un caso penal, el experto en informática se convierte en la persona con la que el abogado puede comunicarse sobre el delito. Esto suele suceder para que la fiscalía explique a la sala del tribunal cómo se llevó a cabo el acto ilegal. La mayoría de los jurados y jueces, solo un conocimiento y una comprensión promedio de cómo funcionan las computadoras y dispositivos móviles, y cómo estos pueden utilizarse para la comisión de un delito. Sin embargo, en la mayoría de los casos, no saben cómo rastrear un mensaje, detectar una IP, recuperar archivos eliminados, entre otros.

En estos casos, es fundamental la intervención del perito, puesto que éste explicará cómo sucedieron los hechos, a través de las evidencias encontradas, las cuales sólo él puede descubrir, mediante la aplicación de técnicas y software especial.

4.7 Informática forense versus otras disciplinas relacionadas

Alguien con conocimientos de acceso a computadoras comprometidas, duplicación y recuperación de archivos, verificación de correo electrónico y restauración de sistemas, dispositivos móviles y de almacenamiento, redes e Internet, es un experto en informática. Pero alguien que puede analizar lo anterior en búsqueda de evidencias para dar con el autor intelectual y material de un delito, es un experto en informática forense.

[121] Ortiz Pradillo, Juan Carlos. La investigación del delito en la era digital, Madrid, España, 2014, p.7.

La informática forense implica examinar y analizar científicamente los datos de los medios de almacenamiento informáticos, para que los datos puedan utilizarse como prueba en los tribunales.[122] Por lo general, investigar las computadoras, dispositivos móviles y dispositivos de almacenamiento, incluye recopilar datos informáticos de forma segura, examinar datos sospechosos para determinar detalles como el origen y el contenido, presentando esta información a los tribunales y la aplicación de las leyes a la práctica informática.

En general, la informática forense investiga los datos que se pueden recuperar del disco duro de una computadora u otro medio de almacenamiento, así como la información compartida en redes sociales, correo electrónico o en la nube.[123] Como un arqueólogo que excava un sitio, los investigadores informáticos recuperan información de una computadora, un dispositivo móvil o dispositivos de almacenamiento extraíbles. La información es posible que se encuentre almacenada, pero puede que no sea fácil de acceder a ella o descifrarla.

El análisis forense de la red proporciona información sobre cómo un perpetrador o un atacante obtuvo acceso a una red. Los investigadores forenses de la red utilizan archivos de registro para determinar cuándo los usuarios inician sesión y determinar a

[122] Areitio Bertolín, Javier. Conectronica.com, Seguridad forense, técnicas antiforenses, respuesta a incidentes y gestión de evidencias digitales, España, 2009. Recuperado de: https://www.conectronica.com/tecnologia/seguridad/seguridad-forense-tecnicas-antiforenses-respuesta-a-incidentes-y-gestion-de-evidencias-digitales. Consultado el: 15/10/2021.

[123] López Molina, Keren Hapuc & Vindell Olivas, Juan Carlos. Laboratorio de computación forense para el Departamento de Criminalística de la Policía Nacional de Nicaragua (Tesis de pregrado), Managua, Nicaragua, UNAN, 2011, p.34.

qué URL.[124] accedieron los usuarios, cómo iniciaron sesión en la red, y desde qué lugar.[125] Sin embargo, el análisis forense de redes también intenta determinar qué pistas o archivos nuevos quedaron en la computadora de la víctima o qué cambios fueron realizados.

La informática forense también es diferente de la recuperación de datos, que implica recuperar información de una computadora que se eliminó por error o se perdió durante una subida de tensión o caída del servidor. En la recuperación de datos, se sabe exactamente qué se busca, dado que se cuenta con el nombre del archivo, la extensión del mismo o el contenido. Con esa información, se facilita enormemente la recuperación de un archivo, a través de un software adecuado.[126]

La informática forense, en cambio, es la tarea de recuperar datos que los usuarios han ocultado o eliminado, con el objetivo de garantizar que los datos recuperados sean válidos para que puedan utilizarse como prueba. La prueba puede ser inculpatoria (en casos penales, la expresión es "incriminatoria") o exculpatoria, lo que significa que podría vincular al sospechoso.

Los investigadores, a menudo examinan una computadora, dispositivo móvil o dispositivo de almacenamiento extraíble, sin saber si contiene evidencia; deben analizar

[124] *Uniform Resource Locator,* es la dirección única y específica que tiene cada uno de los recursos disponibles de la World Wide Web. Es lo que aparece en el explorador, cuando se navega en internet.
[125] Manage Engine. Manageengine.com Análisis forense de redes con NetFlow Analyzer, 2021. Recuperado de: https://www.manageengine.com/latam/netflow/analisis-forense-de-redes.html Consultado el: 15/10/2021.
[126] Netinbag. netinbag.com ¿Cuál es la diferencia entre informática forense y recuperación de datos?, España, 2020. Disponibilidad: https://www.netinbag.com/es/internet/what-is-the-difference-between-computer-forensics-and-data-recovery.html Consultado: 15/10/2021.

los medios de almacenamiento y si encuentran datos, los vinculan para producir evidencia. Para el efecto, se utilizan varias herramientas de software forense; no obstante, en casos extremos, los investigadores utilizan microscopios electrónicos y equipo sofisticado para recuperar información de máquinas que han sido dañadas o reformateado a propósito.

Cuando se trata del ámbito empresarial, estas suelen prevenir la pérdida de datos mediante el uso de copias de seguridad, fuentes de alimentación ininterrumpida (UPS) y monitoreo externo. De igual manera, se utilizan sistemas avanzados y complejos de encriptación, de difícil acceso para los delincuentes. Sin embargo, en el ámbito individual, la mayoría de las personas no suele preocuparse por la seguridad de sus contraseñas o lo que comparte en redes sociales.[127] Por otra parte, los padres de familia, no siempre monitorean lo que sus hijos hacen en redes sociales, videojuegos, entre otros, donde es fácil ponerse en contacto con desconocidos. Estos medios suelen ser utilizados por los criminales para cometer diversos delitos, como el secuestro, la extorsión y otros.

En el caso del delito de secuestro, los delincuentes crean perfiles falsos en las redes sociales o son usuarios de los juegos online preferidos de los niños y adolescentes, donde también crean perfiles falsos.[128] Se hacen compañeros de juego, luego se ganan la confianza de la posible víctima, incluso pueden tener reuniones en directo con

[127] Owaida, Amer. Welivesecurity.com Contraseñas: 5 errores comunes que deberías evitar, España, 2020. Recuperado de: https://www.welivesecurity.com/la-es/2020/05/07/errores-comunes-crear-contrasenas/ Consultado el: 14/19/2021.

[128] El Fisco. Elfisco.com Revista nº 151. El crimen organizado y las nuevas tecnologías, Argentina, 2020. Recuperado de: http://elfisco.com/articulos/revista-no-151-el-crimen-organizado-y-las-nuevas-tecnologias Consultado el: 15/10/2021.

conversaciones aparentemente reales, pero suelen utilizar moduladores de voz, para aparentar tener la voz de un niño o niña. También utilizan software para generar hologramas y aparentar que se está conversando con un niño o niña real. De esta manera, es posible engañar incluso a un adulto. Para conocer el lugar de residencia de la víctima, basta con solicitar que comparta su ubicación actual o en tiempo real, por medio de un archivo adjunto a través de WhatsApp, por ejemplo.

Posteriormente, proponen un encuentro real, el cual puede darse en un lugar cercano a la vivienda del niño o adolescente, como una tienda de barrio, un parque u otro. En el caso de un niño o niña, pueden sugerir que pidan a sus padres que los lleven a determinado lugar y allí buscarán la forman de entrar en contacto con la víctima y concretar el hecho.

No obstante, en la red quedarán los registros de las conversaciones, videos, fotos y otros, intercambiados entre la víctima y el delincuente. Estos son los rastros que busca el perito informático forense. Incluso, si el delincuente los elimina intencionalmente, para desaparecer toda evidencia en su contra, un experto puede recuperarla.

4.8 Fases del análisis informático forense[129]

"La persona encargada de la obtención de la prueba electrónica es el factor que más influye en el valor probatorio que se le pueda atribuir"[130]. Esta afirmación destaca la

[129] López Delgado, Miguel. Análisis forense digital, España, OAS, 2007, p.10.
[130] Citado por Cano Martínez, Jeimy José. El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas, Bogotá, Colombia, Ediciones UNIANDES, 2010, p.108.

importancia de que la manipulación de la prueba electrónica sea realizada por especialistas en la materia.

La recolección de las evidencias constituye otra tarea del procesamiento de la escena del delito, por medio del cual se extrae de la misma la evidencia encontrada para luego ser analizada en el laboratorio criminalístico. En el caso de la informática forense, hace referencia a la obtención de los datos guardados en dispositivos de almacenamiento o en la nube, que luego serán analizados para el esclarecimiento del delito. Esta actividad se desarrolla siguiendo una metodología secuencial y lógica, garantizando la debida cadena de custodia.

En cuanto al proceso de recolección de la evidencia, considerando los diversos problemas vinculados con la manipulación de las pruebas electrónicas, en el Reino Unido, la *Association of Chief Police Officers* –ACPO- sugiere un procedimiento forense estandarizado conformado por cuatro etapas[131], y son las siguientes:

4.8.1 Etapa de recolección

Esta etapa incluye la búsqueda, reconocimiento, recolección y documentación de la evidencia electrónica. El aspecto más relevante al recolectar evidencia, es preservar la integridad de ésta; especialmente cuando se trata de información almacenada en medios magnéticos, la naturaleza volátil de ésta hace que dicha tarea sea más difícil. Por

[131] Escobar de León, Luis Eduardo, Manejo de la cadena de custodia en la recolección de evidencia digital (Tesis de pregrado), Quetzaltenango, Guatemala, Universidad Rafael Landívar, 2017, p.41.

lo tanto, se requiere de prácticas y cuidados adicionales que no son necesarios en la recolección de evidencia convencional.

La obtención, conservación y tratamiento de la evidencia digital es fundamental para garantizar el éxito de las investigaciones, vinculadas con un delito específico, en el cual se hizo uso de la informática.

4.8.2 Proceso de examen de la evidencia

Esta etapa hace que la evidencia sea visible; además, tiene la función de explicar su origen y alcance. En este proceso, se realizan las siguientes tareas: documentar el contenido y el estado de toda la evidencia y separar la evidencia útil de toda aquella que se puede encontrar en los medios electrónicos.

La evidencia digital, se refiere a documentos informáticos, correos electrónicos, mensajes de texto e instantáneos, transacciones, imágenes, videos, llamadas a través de aplicaciones o redes sociales. También es necesario tener en cuenta que los dispositivos de almacenamiento utilizan respaldos en línea, lo que se conoce como “la nube”. Esto brinda al investigador forense el acceso a dicha información.[132]

Además, la mayoría de dispositivos actuales, almacenan información vinculada con los lugares o ubicaciones en las que se ha encontrado el dispositivo recientemente.

[132] Escobar De León. Op. Ci. p.43.

Se puede tener acceso a las últimas 200 ubicaciones de un dispositivo móvil específico.[133]

Las fotografías que se publican en redes sociales también contienen información relativa a la ubicación. Toda esta evidencia digital es analizada por especialistas certificados, quienes poseen la formación y experiencia para trabajar de manera adecuada esta evidencia sensible.

4.8.3 Fase de análisis

Toda la evidencia útil encontrada, debe ser analizada, con la finalidad de indagar por su valor probatorio y la relevancia de la misma, en función del delito que se investiga. Hay varias herramientas que se pueden utilizar para el análisis de las evidencias digitales. Esta fase consiste en la identificación de las evidencias más pertinentes, de manera que se pueda realizar una reconstrucción del delito. Esta fase tiene varios momentos:[134]

a) Preparación para el análisis: Como su nombre lo indica, consiste en preparar todo lo que se va a requerir para el análisis de las evidencias.
b) Reconstrucción del ataque: Consiste en crear una línea de tiempo con toda la evidencia recolectada.

[133] Ciberseguridad. Ciberseguridad.com Evidencia digital, 2021. Disponibilidad: https://ciberseguridad.com/servicios/analisis-forense/evidencia-digital/#Funcionamiento Consultado: 27/10/2021.
[134] Informática Forense. https://duartecarito.wixsite.com Fases en la informática forense. Colombia, 2015. Disponibilidad: https://duartecarito.wixsite.com/eportafolioforense/single-post/2015/05/18/fases-en-la-informatica-forense Consultado: 27/10/2021.

c) Determinación del ataque: Consiste en establecer el punto en el que el atacante ingresó al sistema, o las páginas, sitios web, redes sociales o cuentas de correo utilizadas para el efecto.
d) Identificación del atacante: Para ello se requiere identificar la dirección IP, cuentas de correo, perfiles en redes sociales e identificar al propietario o usuario de las mismas.
e) Perfil del atacante: Hay diversos tipos de atacantes, tales como hackers, profesionales de informática o delincuentes comunes que utilizan internet o redes sociales para ubicar a posibles víctimas.
f) Evaluación del impacto causado en el sistema: Cada ataque impactará de manera distinta a un sistema o a una persona. En el caso de un sistema, quizá solo se ingrese al mismo, pero no se modifique nada, o se apoderen de ciertos archivos y lo peor, un secuestro de datos. Con respecto a las personas, quizá solo se había mantenido diálogos y compartir ciertos archivos, pero en el peor de los casos, la persona podría ser secuestrada.

4.8.4 El reporte o declaración

El reporte o informe pericial, consiste en una descripción detallada del proceso de examen, la información que obtenida por medio de dicho proceso y el análisis del perito sobre dichos aspectos.[135] Incluso, deben conservarse las notas tomadas por el examinador, debido a que, el investigador en determinado momento puede verse exigido

[135] Couso García, Fernando. El informe pericial criminológico como herramienta de protección de los derechos fundamentales de víctimas y victimarios (Tesis de pregrado). Bilbao, España, Universidad del País Vasco, 2020, p.54.

a testificar con respecto a la validez del procedimiento utilizado para el análisis de la evidencia digital.

En el proceso de recolección de pruebas, es fundamental obtener una copia fidedigna de los datos encontrados en los medios electrónicos que son objeto de investigación. En este sentido, el perito debe proceder con cautela, especialmente con respecto al hardware y software elegido, de manera que no se comprometa la información original.[136]

Por otra parte, es importante destacar que cada legislación impone criterios específicos para la manipulación de pruebas electrónicas,[137] aparte de que deben seguirse las reglas de las pruebas tradicionales con relación a la observancia de la cadena de custodia, los parámetros de legalidad de la prueba y otros; de lo contrario, podría ponerse en duda la admisibilidad de las mismas en un estrado judicial.

Por lo tanto, es necesario enfatizar que, para la tarea de manipular pruebas electrónicas, se exige un nivel de conocimiento y destreza superior al requerido para las pruebas tradicionales, debido a que la admisibilidad de las mismas puede ser cuestionada por razones específicas de tipo técnico.

[136] Maldonado Escobar, Carlos Alejandro. Herramientas forenses de análisis digital para la obtención de información aplicado a ordenadores y dispositivos móviles (Tesis de pregrado), Quetzaltenango, Guatemala, Universidad Rafael Landívar, 2020, p.7

[137] Ramírez Estrella, Alex Guillermo, La prueba electrónica: los medios electrónicos como recurso para la práctica de la prueba (Tesis de postgrado), Guayaquil, Ecuador, Universidad de Santiago de Guayaquil, 2016, p.15.

4.8.5 Análisis e investigación de la evidencia digital

Una vez que se cuenta con toda la evidencia digital, se separan los archivos prioritarios en virtud del caso específico y el criterio del perito.[138] Estos procesos de clasificación y análisis pueden ser iterativos (repetir varias veces un proceso hasta alcanzar el resultado deseado), con el propósito de obtener una mayor cantidad de evidencia pertinente. El proceso concluye cuando el perito considera que cuenta con la evidencia suficiente para resolver el caso o ya no existen datos para analizar.

Acto seguido, se genera el listado de los archivos comprometidos en el caso, los cuales forman parte de la evidencia del caso. También se debe obtener la línea del tiempo de la evidencia a partir de las características de los archivos, lo que posibilita una correlación y enriquecimiento de la evidencia. Los sistemas operativos, generalmente manejan tres clasificaciones de tiempo: fecha de modificación, fecha de acceso y fecha de creación.

La fecha de modificación hace referencia a la última vez que un archivo específico fue modificado. La fecha de acceso se refiere a la última vez en que alguien accedió al mismo. La fecha de creación corresponde a la fecha en la que el archivo fue generado por primera vez. En algunos casos, por diversas razones, puede resultar imposible la tarea del análisis temporal, por lo que debe consignarse en el informe final. Finalmente, a partir de los diversos hallazgos, se realiza el informe final, con una descripción detallada de los descubrimientos relevantes para el caso.

[138] MINTIC. Seguridad y privacidad de la información, Bogotá, Colombia, 2016, p.26.

CAPÍTULO V

PROCEDIMIENTOS DE LA INVESTIGACIÓN EN LA INFORMÁTICA FORENSE

5.1 La recolección de evidencias digitales

Tal como ya se indicó, la evidencia digital hace referencia a una serie de datos en formato digital, tales como archivos de texto, fotografías, videos, audios, guardados en dispositivos de almacenamiento (discos duros, tarjetas, memorias USB, memorias internas), perfiles o cuentas de internet y en la nube. Por lo tanto, se trata de información registrada en medios informáticos.[139]

Cuando se trata de información vinculada con un delito, suele ocultada, cifrada o eliminada. Se puede modificar, dañar o destruir de manera sencilla e incluso a distancia. Para recuperar dicha información, se requiere de herramientas específicas. Puede tratarse de recuperar información eliminada, encriptada o de una cuenta y su respectiva contraseña.

5.2 El navegador web

Internet ha cambiado el estilo de vida de las personas, en todos los ámbitos, tales como los sociales, educativos, sanitarios e incluso gubernamentales. Y con ello, surgen nuevos problemas, como los delitos cibernéticos, para los cuales lo básico es contar con

[139] Lemontech blog blog.lemontech.com Evidencias digitales: significado, objetivo y tratamiento, Perú, 2021. Disponibilidad: https://blog.lemontech.com/evidencias-digitales/ Consultado: 08/11/2021.

un navegador de Internet, es decir, un programa que permite ver el contenido de un sitio o página web.

La facilidad de acceso es también una amenaza, puesto que se puede ingresar a los servidores web de empresas privadas y públicas y robar o secuestrar información, o simplemente, el fraude desde perfiles falsos en redes sociales. El navegador web está diseñado para almacenar cualquier información, como el localizador URL, abreviatura en inglés de *Uniform Resource Locator*, por lo que guarda términos de búsqueda, direcciones de sitios y páginas web, contraseñas, fechas, horarios y otros datos del usuario al navegar por internet.[140]

Sin embargo, para seguridad del usuario, para que la información no se almacene en el sistema informático, el navegador web también permite el "modo de navegación privada" "navegación segura" o "navegación de incógnito",[141] en la cual no se almacena la información, sino que se elimina al cerrar una página web. Estas funciones de seguridad y privacidad del sistema permiten su utilización por parte de los delincuentes, para no dejar rastros de un crimen. También suelen utilizarse otros métodos anti-forenses, como el uso de un navegador web portátil con el modo privado, el cual está diseñado para no dejar un rastro de evidencia digital en la computadora y elimina los registros mientras se navega. Un navegador portátil es un navegador web que se ejecuta sin instalarlo en la computadora, por lo que se almacena en un dispositivo de

[140] GCF Global. edu.gcfglobal.org.es ¿Qué es una URL? España. Disponibilidad: https://edu.gcfglobal.org/es/como-usar-internet/que-es-una-url/1/ Consultado: 03/10/2021.
[141] Latto, Nica. Avast.com Navegación privada: cómo activar o desactivar el modo de incógnito, España, 2021. Disponibilidad: https://www.avast.com/es-es/c-guide-to-private-browsing#gref Consultado: 03/10/2021.

almacenamiento externo, por tal razón, no deja rastros en el dispositivo de navegación. Existen varios, tales como: Google Chrome portable, Mozilla Firefox portable, Private Browsing portable, Maxthon Portable, Opera Portable, Opera GX Portable, K-Meleon portable, Falkon portable, entre otros.[142]

Un registro es una base de datos de información informática que guarda la información vinculada con cada actividad donde se ejecuta software o hardware en una computadora. Entonces se convierte en un desafío para los investigadores al hacer un análisis forense para investigar la actividad en Internet de los sospechosos, en el caso de ciberdelito.

Un navegador web portátil, constituye un desafío para el perito informático forense, puesto que no deja rastros; además, si se utiliza un navegador convencional, el historial puede ser eliminado intencionalmente, para desaparecer todo indicio. En ese caso, el investigador trata de reconstruir el historial de la navegación reciente. Para ello, se procede con el método forense conocido como *Live forensics*. Este método se utiliza para obtener los datos en la memoria de acceso aleatorio (RAM)[143] porque, como se explicó anteriormente, el navegador web utilizado es el de navegación portátil y privada.

Live forensics es un método para obtener los datos contenidos en el RAM volátil, para que el crimen se pueda descubrir a partir del análisis de los datos volátiles. Este

[142] Onieva, David, softzone.es Navegadores. Usa Internet de forma más segura con estos navegadores portables, España, 2021. Disponibilidad: https://www.softzone.es/programas/navegadores/navegadores-internet-portables/ Consultado: 01/11/2021.
[143] Memoria de un equipo informático, que utiliza el procesador para recibir instrucciones y guardar los resultados.

método de investigación tiene ventajas cuando se requiere trabajar con navegadores web en general y, especialmente, los portátiles.

5.3 Navegador web forense

El navegador web es una aplicación de software para la toma, presentación y ejecución de recursos e información alojada en Internet o World Wide Web (WWW).[144] Una fuente de la información se identifica mediante un identificador uniforme de recursos (URI) y pueden ser páginas web, imágenes, videos u otras piezas de contenido.

Un navegador web forense es una actividad forense para encontrar información almacenada en un navegador web. Como evidencia digital, se puede encontrar contenido diverso; como mínimo, se encuentran cachés, historial, cookies, lista de archivos de descarga y sesiones. Los investigadores siempre encuentran algo, por cuidadoso que sea el delincuente.

5.4 Técnicas anti-forenses

Las técnicas anti-forenses son intentos para frustrar la investigación y evitar la detección de eventos, interrumpir la recopilación de información necesaria, gastar tiempo dedicado a la investigación y arrojar dudas sobre los informes.[145] Hay cuatro categorías

[144] Ionos, ionos.es ¿Qué son los navegadores? España, 2020. Disponibilidad: https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/que-es-un-navegador/ Consultado: 08/11/2021.
[145] Welivesecurity. welivesecurity.com/la-es ¿Qué son las técnicas antiforenses? España, 2015. Disponibilidad: https://www.welivesecurity.com/la-es/2015/07/02/tecnicas-anti-forenses/ Consultado: 03/10/2021.

de métodos anti-forenses que son la ocultación de datos, la limpieza de dispositivos, la ofuscación de rastros y los ataques contra el proceso o las herramientas forenses.

- Ocultación de datos: Ocultar datos mediante técnicas de cifrado, esteganografía y otros.

- Limpieza de dispositivos: La limpieza de dispositivos es una técnica que se utiliza para sobrescribir los datos en el disco duro o en un dispositivo de almacenamiento extraíble, para que no se pueda recuperar.

- Ofuscación de rastros: La ofuscación de pistas tiene la intención de engañar a los investigadores al ocultar o eliminar evidencia sobre la fuente y la naturaleza del ataque. Esta técnica se puede utilizar para modificar el registro de limpieza de archivos de registro o modificar las marcas de tiempo de los metadatos.[146]

- Ataques contra procesos o herramientas forenses: Los ataques contra el proceso o las herramientas forenses son métodos anti-forenses poco comunes, puesto que se requiere trabajar directamente en el procedimiento de investigación o generar errores en herramientas forenses. Para ello, los atacantes requieren de un nivel de conocimiento similar o superior al de los peritos informáticos forenses, así como conocimiento y experiencia con respecto a las herramientas y procedimientos específicos de trabajo que se están aplicando a la investigación.

[146] Derechos digitales. Derechosdigitales.org Ofuscación, me ves/no me ves, Brasil, 2020. Disponibilidad: https://www.derechosdigitales.org/ofuscacion/ Consultado: 08/11/2020.

En este caso, el navegador web anti-forense utiliza un dispositivo portátil, o el navegador web se utiliza en modo privado y se elimina el registro después de la actividad de navegación. El registro contiene la mayor cantidad información sobre el uso de la computadora y el usuario, configuraciones, aplicaciones y dispositivos de hardware en Sistemas operativos Windows. Esta información está categorizada con base al orden en que se ha ejecutado, tales como palabras clave de búsqueda, carpetas a la que se accedió por última vez, aplicaciones de registro y otros.

5.5 Análisis forense en vivo (*live forensics*)

El análisis forense en vivo es una investigación forense que se lleva a cabo cuando el sistema está encendido. Esto se debe a que los datos volátiles se perderán si la computadora se apaga o se reinicia. El análisis se aplica sobre la memoria volátil que es utilizada o almacenada en RAM.[147]

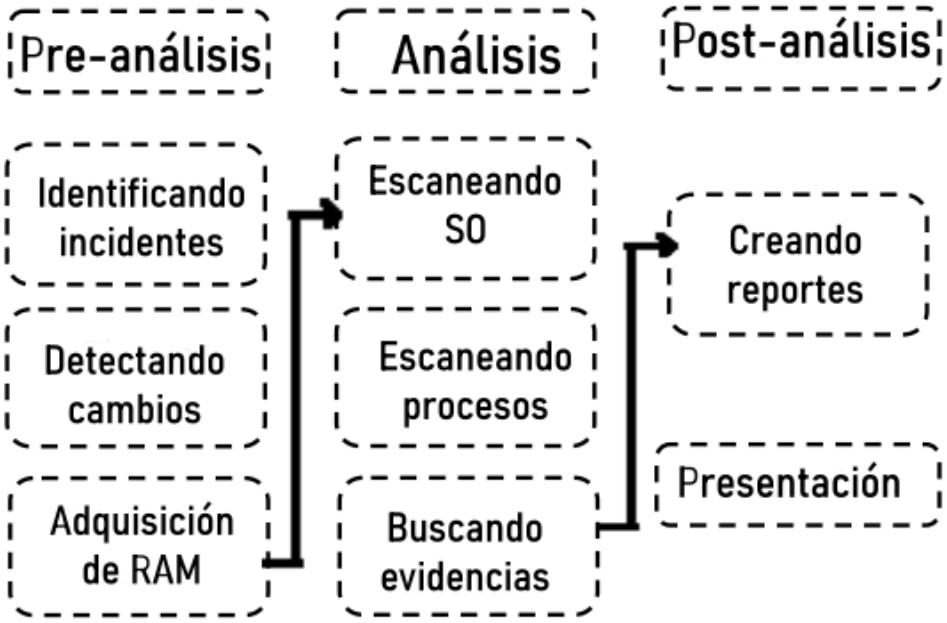
Live Forensics se aplica en una computadora a través de la adquisición y análisis de RAM. La adquisición de RAM aquí es para realizar la captura o creación de imágenes de RAM mediante la herramienta forense de RAM.

Bajo esta metodología, se utilizan tres etapas principales que son el análisis previo, el análisis y el análisis posterior.

[147] Santo Orcero, David. Kali Linux, Madrid, España, 2018, p.176.

Figura No. 1

Metodología del *live forensics*



Fuente: elaboración propia, basada en Santo, *op. cit*., p.186.

5.6 Simulación con Live forensics

La metodología *Live forensics* se comprende mejor, mediante simulaciones. Para ello, se requiere de un equipo de cómputo con sistema operativo Windows, dado que es el más popular. Para el efecto, se requiere un equipo de gama media, considerando que son los más utilizados. Para esta simulación específica, se utilizó un equipo portátil HP, con procesador Core i5, con 4 GB de RAM y 500 GB de HDD. También se utilizó un dispositivo de almacenamiento extraíble de 16 GB, así como el respectivo software forense, tal como se muestra en la tabla siguiente:

Tabla 1

Hardware y software de laptop utilizada para simulación de *Live forensics*

Hardware	Software
Laptop Core i5 4GB RAM	Windows 10 Pro
Flashdrive HP 16 GB	Google Chrome Portable
	Mozilla Firefox Portable
	Internet Explorer Portable
	Browzar Black
	Clean After Me Portable
	Process Monitor Portable
	Volatility Memory Forensic
	WinHex
	DumpIt

Fuente: elaboración propia, basada en el equipo utilizado para simulación.

Con respecto al software, Windows 10 Pro, es el sistema operativo del equipo. Es el SO más reciente y utilizado en los equipos de reciente adquisición. Sin embargo, pueden utilizarse versiones anteriores de Windows, sin ningún problema.

Google Chrome Portable, Mozilla Firefox Portable, Internet Explorer Portable y Browzar Black, son navegadores de internet portables, es decir, no requieren instalación en el equipo, se ejecutan desde el dispositivo de almacenamiento señalado en el hardware.

Clean After Me es un programa portable que se utiliza para limpiar el sistema, luego de ser utilizado para cualquier actividad. Elimina todo rastro en el ordenador, lo que incluye historial, cookies, archivos temporales, contraseñas y vaciado de la papelera de reciclaje. El programa no necesita instalación, por lo que se ejecutará desde el dispositivo de almacenamiento. La herramienta tiene la capacidad de eliminar (limpiar) 26 tipos de

rastros distintos; no obstante, el usuario puede elegir los que desea eliminar y aquellos que desea conservar.[148]

Process Monitor Portable es una herramienta que muestra en tiempo real la actividad en un equipo de cómputo, es decir, lo relacionado con el registro, el sistema de archivos y los procesos activos. Dicho programa, se utiliza generalmente para mostrar qué está sucediendo en el sistema y detectar fácilmente los problemas.[149] Por tal razón, es de mucha utilidad en informática forense, especialmente por lo relacionado con el registro.

Volatility Memory Forensic, es una herramienta muy utilizada en informática forense, debido a que facilita el análisis del contenido de la memoria aleatoria (RAM), encontrar diversos datos como las conexiones de red abiertas, las contraseñas utilizadas, archivos eliminados y, especialmente, el registro de Windows, listas DLL cargadas en cada uno de los procesos, identificación de las propiedades de las imágenes utilizadas, entre otros.[150]

Determinados ataques, intrusiones y actividades ilícitas no dejan rastro alguno en el disco duro, especialmente cuando no se utilizan archivos de texto o multimedia, almacenados en el disco duro. En estos casos, los únicos indicios que es posible encontrar, son los de la memoria RAM, por lo que se requiere de un análisis de la memoria

[148] Clean After Me, uptodown.com Clean After Me, Málaga, España. Disponibilidad: https://clean-after-me.uptodown.com/windows Consultado: 01/10/2021.
[149] Portables Programas, portablesprogramas.com Process Monitor v3.10 Portable, España. Disponibilidad: https://www.portablesprogramas.com/process-monitor-v3-10-portable/ Consultado: 01/10/2021.
[150] Hacking y forensic. Ediciones-eni.com Volatility, España. Disponibilidad: https://www.ediciones-eni.com/open/mediabook.aspx?idR=554bb28fd9f6e0f97724779646d2a3c8 Consultado: 01/10/2021.

volátil y para ello, se utilizan herramientas como Volatility Memory Forensic. Hay varias herramientas de este tipo, cada una con sus respectivas ventajas y desventajas. Las más utilizadas, son la siguientes: Volatility Memory Forensic, DumpIt, FTK Imager, Magnet RAM Capture, F-Response, Live RAM Capturer, Memoryze Redline, entre otras. Lo importante es identificar qué procesos se ejecutaron y cuándo, lo cual puede aportar información muy importante para la investigación.

Mediante este tipo de análisis, es posible obtener las claves y contraseñas que se utilizaron recientemente, para tener acceso a determinadas aplicaciones, perfiles en redes sociales, cuentas de correo, entre otras, las cuales se cargan en la memoria RAM. Además, también se puede acceder a las claves de cifrado, las cuales podrían necesitarse para analizar el disco duro, si este estuviera encriptado.

El problema es, que la memoria RAM es volátil y, cuando se apaga el equipo de cómputo, toda la información contenida en ésta, se pierde. Por tal razón, cuando el equipo está encendido, el análisis en vivo, es el que se denomina *Live* forensics. Sin embargo, si el equipo está apagado, entonces se requiere el proceso denominado "volcado de memoria" o *memory dump*, mediante el cual se realiza una copia de toda la memoria RAM en un momento determinado, para su posterior análisis.[151] En este caso, se denomina análisis post mortem.

[151] Bernal Michelena, David Eduardo. Análisis de volcado de memoria en investigaciones forenses computacionales, Revista Seguridad, No. 31, mayo 2018. México, D. F., DGTIC-UNAM. Disponibilidad: https://revista.seguridad.unam.mx/numero-17/an%C3%A1lisis-de-volcado-de-memoria-en-investigaciones-forenses-computacionales Consultado: 02/10/2021.

DumpIt, es una herramienta popular para realizar volcados de memoria. Sus principales características son la sencillez y la compatibilidad con las distintas versiones del sistema operativo Windows. Es de tipo portable, por lo que no requiere instalación y es ejecutable desde un dispositivo de almacenamiento externo, como una memoria USB.[152]

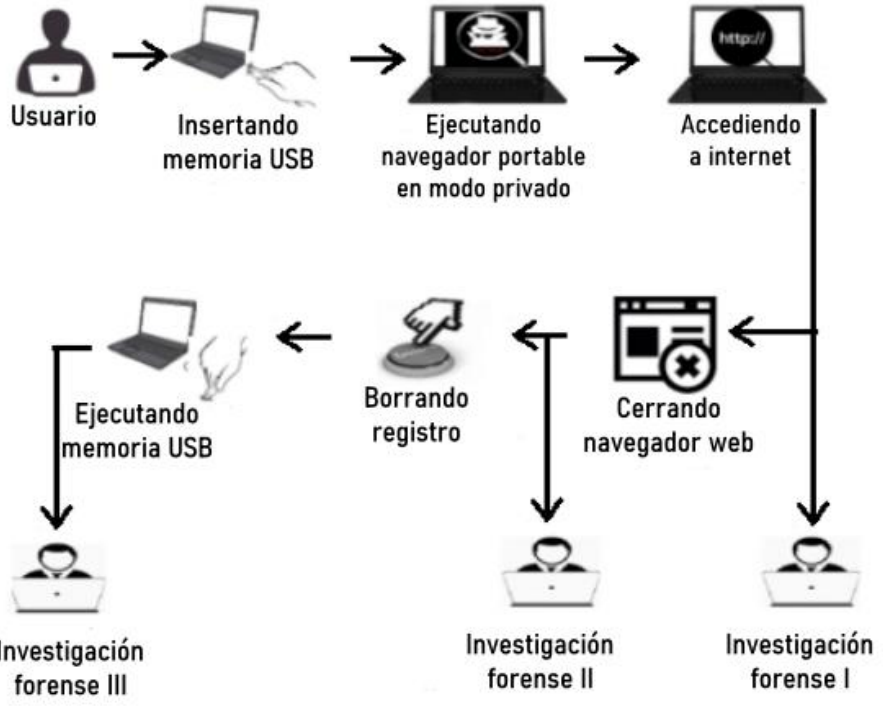
WinHex, es una utilidad de sistema, muy apropiada para la informática forense, debido a que permite la recuperación de archivos, es útil para el peritaje informático, procesar de datos de bajo nivel y seguridad informática. Tiene la capacidad de abrir ficheros, discos y procesos en memoria. Dentro de diversas funciones de este software, las que interesan a la informática forense, son las siguientes: recuperación de archivos, búsqueda de particiones perdidas, clonación de discos, borrado seguro, concatenación o partición de ficheros y edición de la memoria de cualquier proceso.[153]

Las distintas herramientas señaladas, no requieren de procedimientos complejos, simplemente se ejecutan y listo. El estudio simulado se realizó en tres etapas. La primera es cuando el navegador web sigue siendo la forma de adquisición y análisis; la segunda, es cuando el navegador está cerrado y, la tercera, cuando se realiza el análisis anti-forense, usando Clean After Me para eliminar el sistema de registro en la computadora. El proceso se muestra en la figura siguiente:

[152] Mendillo, Vincenzo. Análisis forense de la memoria RAM, Caracas, Venezuela, Universidad Central, 2018, p.19.
[153] Ondata Internacional. Ondataforensic.com Las herramientas de análisis más avanzadas. WinHex. Madrid, España, 2021. Disponibilidad: http://www.ondataforensic.com/tecnologia_winex.php Consultado: 01/10/2021.

Figura No. 2

Etapas del estudio simulado



Fuente: elaboración propia, basada en estudio simulado.

En la simulación, cada navegador web portable, se utilizó en modo privado, utilizando diferentes palabras clave en cada navegador, para el acceso a Internet, tal como se muestra en la tabla siguiente:

Tabla 2

Navegadores, actividades y claves

Navegador portable	**Actividad en la que se utilizó el navegador portable (Clave)**
Google Chrome	Google – Ironman – Imágenes – Correo de Yahoo
Internet Explorer	Google – Batman – Imágenes- Facebook
Mozilla Firefox	Google – Spiderman -Imágenes– Twitter

Browzar Black	Google – Xman – Imágenes – Correo de Google (Gmail).

Fuente: elaboración propia, basada en estudio simulado.

Cada actividad de navegación realiza una búsqueda en Google con diferentes palabras clave en todos los navegadores web. Lo mismo ocurre con la actividad de la cuenta, también diferente en cada navegador web.

5.7 Análisis y resultados de la simulación

Antes de iniciar el análisis, es necesario detectar las incidencias y cambios en el sistema, lo cual se puede realizar con la adquisición de memoria por medio de la herramienta DumpIt, para obtener una copia del archivo de la memoria RAM. Entonces, se procede al análisis, para encontrar evidencia de un navegador web usando Volatility Memory Forensic y WinHex.

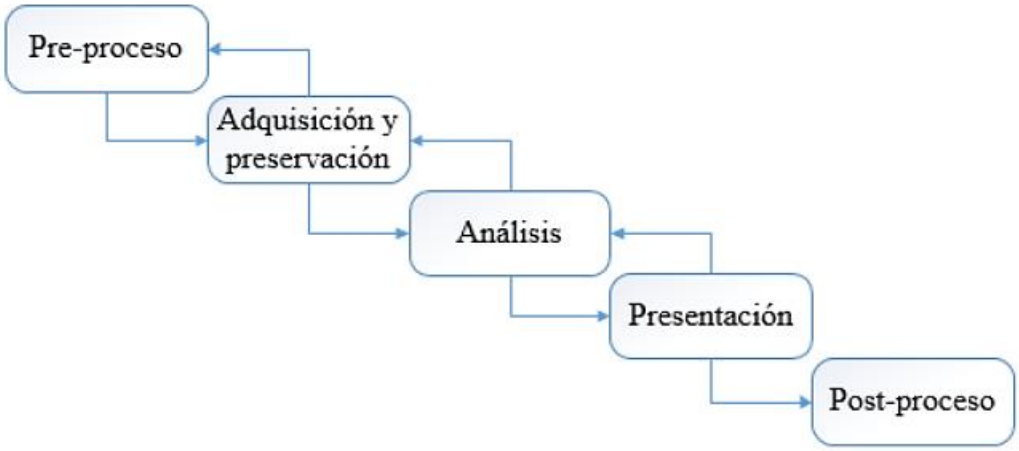
5.7.1 Modelo - Generic Computer Forensic Investigation Model -GCFIM-

Es importante aclarar que, para la simulación, se utilizó el *Generic Computer Forensic Investigation Model* -GCFIM-, que constituye el resultado de una investigación que realizó Yunus Yusoff y sus colaboradores. Consistió en una revisión y análisis de los modelos de análisis e investigación forense, utilizados en el periodo 1985-2011. A partir de los resultados se descubrió la existencia de cinco fases comunes en todos los

modelos, que son precisamente las que dan origen al modelo GCFIM.[154] Las fases, son las siguientes:

Figura No. 3

Fases del Modelo GCFIM



Fuente: elaboración propia, basada en Cano (2009).

- Pre-proceso: Esta fase es fundamentalmente de tipo preparatorio. Se debe garantizar que el personal a cargo, cuente con la preparación y experiencia adecuada, así como contar con las herramientas de análisis requeridas y que funcionen como es debido.
- Adquisición y preservación: Esta fase incluye los subprocesos de identificación y recolección de la evidencia en la escena del delito, además de realizar el transporte y almacenamiento adecuados, con el nivel de seguridad apropiado, para garantizar que los datos no sean alterados.

[154] Cano Martínez, Jeimy. Computación forense. Descubriendo los rastros informáticos, México, D.F., Alfa Omega Grupo Editor, S.A., de C.V., 2009, p.171.

- Análisis: Consiste en el examen minucioso de las evidencias. Además, se realiza una clasificación de las mismas, en función de su importancia para la investigación. Incluye desechar la información que no está vinculada de ninguna manera con el caso.
- Presentación: Hace referencia a la preparación de la documentación vinculada con la investigación: resultados del análisis, hipótesis, reportes, entre otros.
- Post-proceso: Se refiere a la presentación de los informes ante un tribunal judicial, como apoyo para dilucidar lo vinculado con el delito que se ventila. Por otra parte, incluye la devolución de la evidencia a su propietario, en buenas condiciones, cuando esto sea procedente.

5.7.2 Análisis previo

a) Incidentes e identificación de cambios

La detección de incidentes o cambios en el registro se realiza con Volatility Mmeory Forensic.

Tabla 3

Detección de cambios en el Registro

Navegador	Proceso	Localización
Internet Explorer.exe	RegQueryValue	HKCU\Software\ Microsoft\Windows\ CurrentVersion\Internet Settings\5.0\LowCache\ Cookies\CachePrefix
Internet Explorer.exe	RegOpenValue	HKCU\Software\ Microsoft\Windows\ CurrentVersion\Internet

		Settings\5.0\LowCache\ History
Internet Explorer.exe	RegCloseValue	HKLM\SOFTWARE\ Microsoft\Windows\ CurrentVersion\Internet Settings\5.0\Cache\ History
firefox.exe	RegQueryValue	HKCU\Software\ Microsoft\Windows\ CurrentVersion\Internet Settings\Connections\ DefaultConnectionSettings
firefox.exe	RegCloseValue	HKCU\Software\ Microsoft\Windows\ CurrentVersion\Internet Settings\Connections
firefox.exe	IRP_MJ_READ	C:\pagefile.sys
chrome.exe	RegOpenKey	HKLM\Software\ Microsoft\Windows NT\ CurrentVersion\Time Zones\SE Asia Standart Time\Dynamic DST
chrome.exe	FASTIO_ WRITE	C:\Users\User PC\ AppData\Local\Temp \GoogleChromePortable\ Deafult\Cache\data_1
chrome.exe	IRP_MJ_READ	C:\pagefile.sys
Browzar Black 2000.exe	RegOpenKey	HKLM\SOFTWARE\ Microsoft\Cryptography\ Offload
Browzar Black 2000.exe	RegCloseKey	HKLM\SOFTWARE\ Microsoft\Cryptography\
Browzar Black 2000.exe	RegQueryKey	HKLM\SOFTWARE\ Policies\Microsoft\ Cryptography\

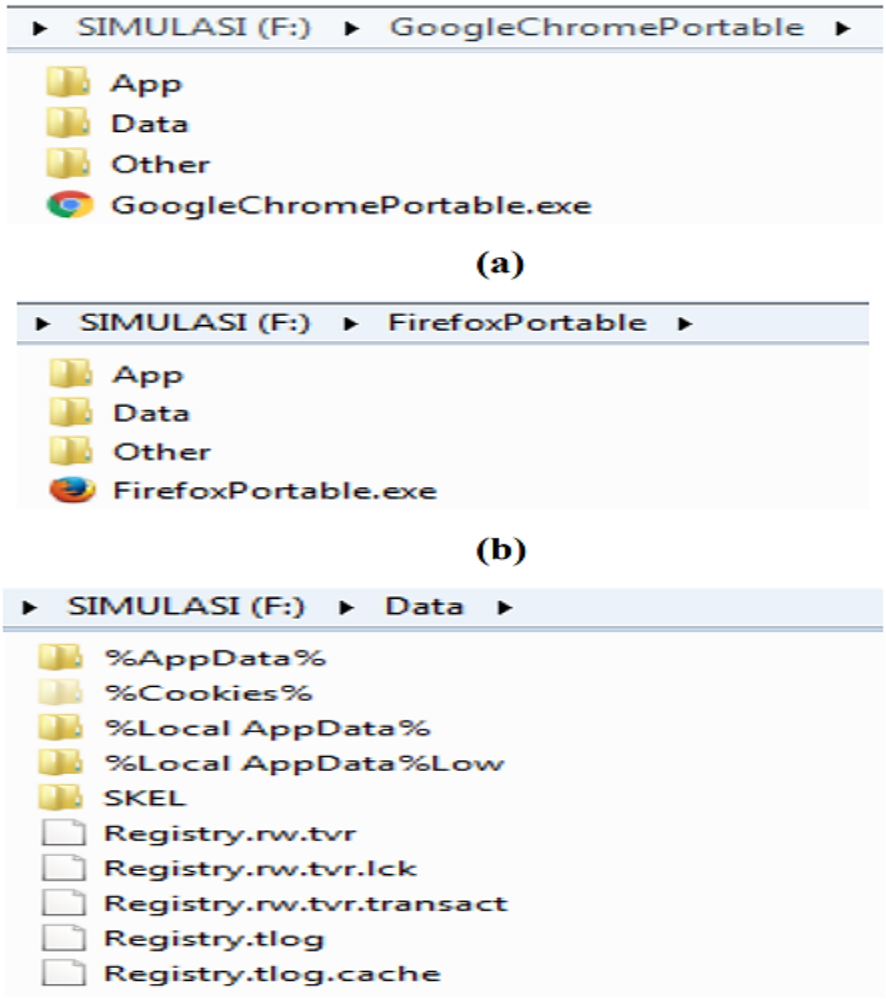
Fuente: Elaboración propia, basada en estudio simulado.

En la tabla anterior, se detecta un solo cambio en el registro del sistema y es el uso de Browzar que sobrescribe datos utilizados por Internet Explorer, es muy importante esto, como referencia para un análisis posterior.

El análisis de los registros de Windows, permite reunir información valiosa con respecto a los parámetros del SO, el software que está instalado en el equipo, los dispositivos de almacenamiento que se conectaron, los dispositivos instalados y fechas de creación, modificación y acceso de carpetas y archivos. Todo esto es esencial para el investigador informático forense, puesto que puede ayudar a encontrar evidencias de un delito.

Figura No. 4

Google Chrome Portable, (b) Mozilla Firefox Portable, (c) Internet Explorer Portable



Fuente: Elaboración propia, basada en estudio de simulación.

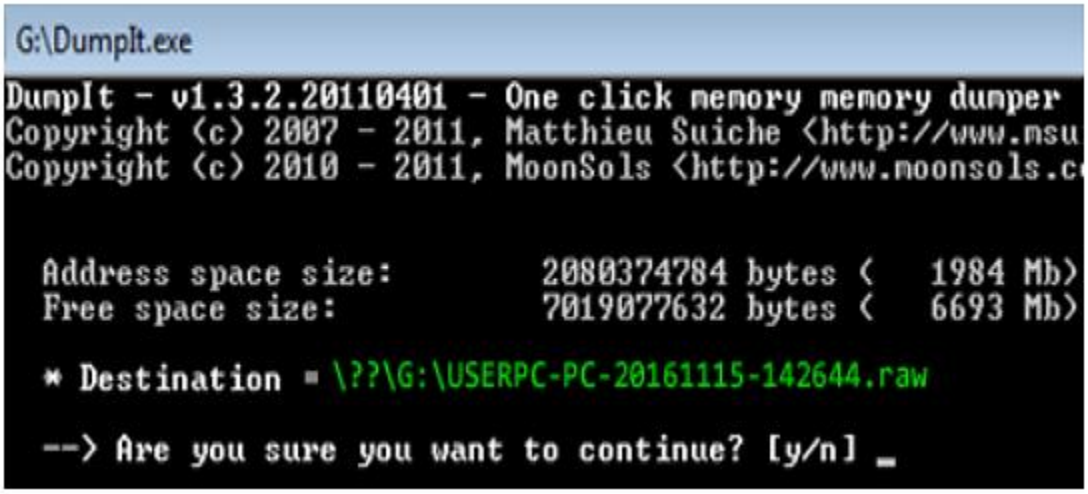
Cuando Internet Explorer, Google Chrome y Mozilla Firefox Portable ejecutado, hay cambios para crear nuevos archivos en la unidad USB que se muestra en la Figura 3a, 3b y 3c.

b) Adquisición de RAM

La adquisición de RAM, como ya se indicó, se realiza con DumpIt. Los resultados de la adquisición se obtienen en un archivo con extensión .raw, tal como se aprecia en la figura siguiente:

Figura No. 5

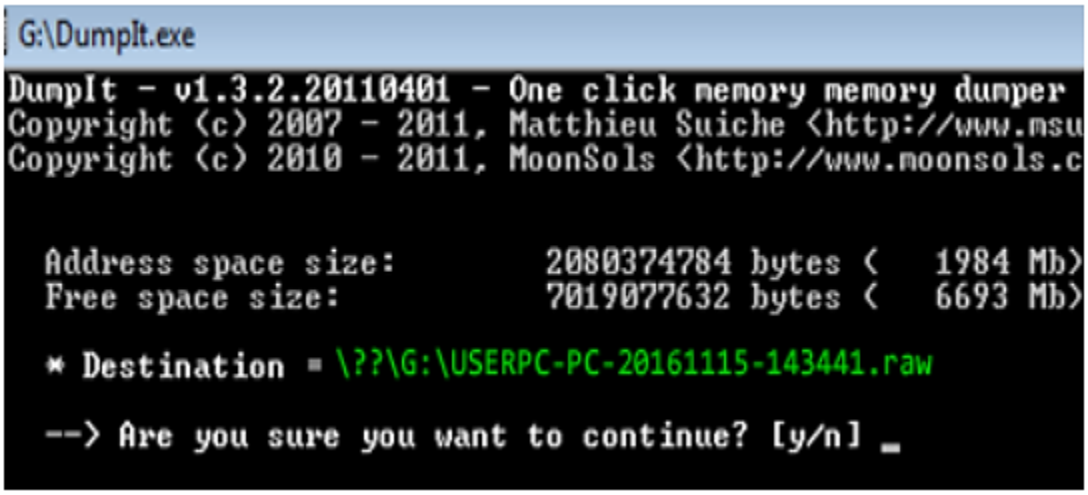
Adquisición de RAM I



Fuente: Elaboración propia, basada en estudio simulado.

Figura No. 6

Adquisición de RAM II



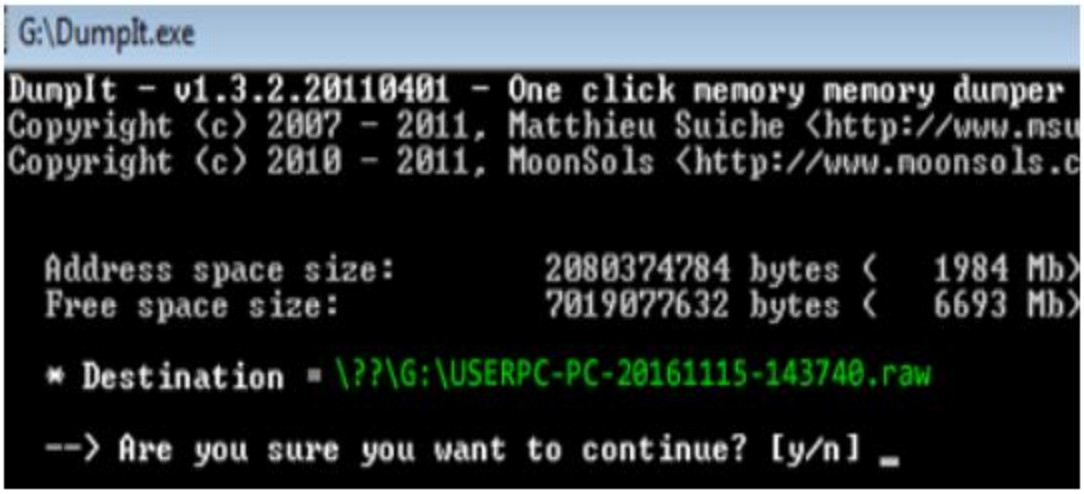
Fuente: Elaboración propia, basada en estudio simulado.

En la adquisición de la primera RAM, se genera una imagen de archivo denominado USERPC-PC-20161115-142644.raw, el cual se almacena automáticamente en la unidad USB donde se ejecutó DumpIt.

Además, se generan archivos de imágenes en el controlador USB que ejecuta DumpIt, tal como se muestra en la figura anterior, específicamente el archivo USERPC-PC-20161115-143441. Mientras que, en la tercera adquisición de RAM, se genera otro archivo, tal como se muestra en la figura siguiente:

Figura No. 7

Adquisición de RAM III



Fuente: Elaboración propia, basada en estudio simulado.

El tamaño del espacio de direcciones en las tres imágenes, muestra el tamaño de la RAM a adquirir, la cual equivale a 2.080.374.784 bytes (1984 Mb), redondeados a 2 GB. La adquisición de la memoria RAM es fundamental; puesto que, con ello se obtiene todo lo que está almacenado temporalmente; es decir, todo lo relacionado con procesos y archivos abiertos o utilizados recientemente.

c) Búsqueda de evidencia digital

La búsqueda de evidencia digital se puede realizar de dos maneras: con Volatility Memory Forensic y con WinHex. La primera opción, se muestra en la siguiente tabla:

Tabla 4

Evidencia digital de Internet Explorer usando Volatility Memory Forensic

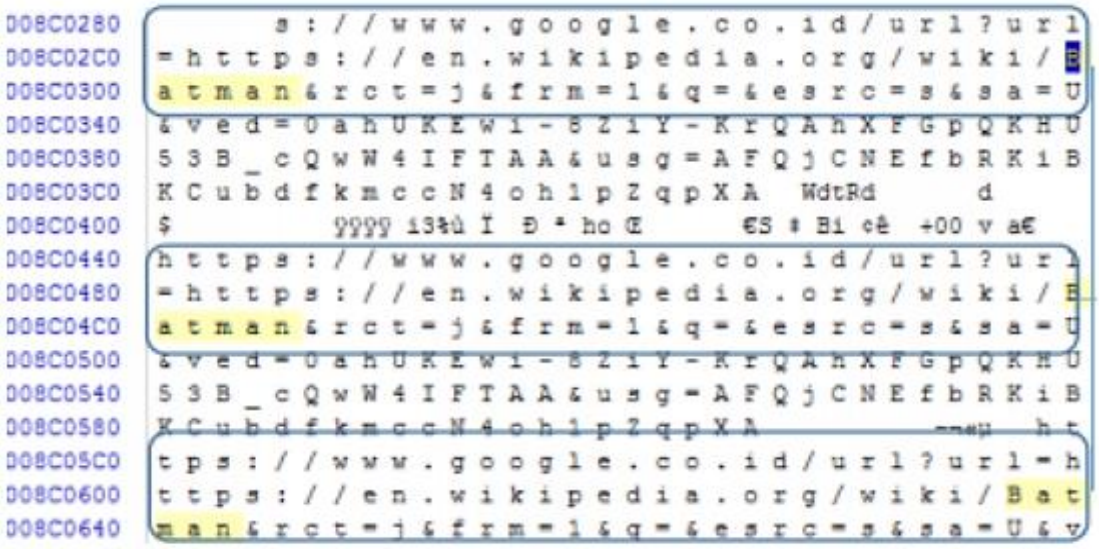
Análisis I	Análisis II	Análisis III
Proccess : 4416 Internet Explorer	Proccess : 4416 Internet Explorer	Not found
Location:Visited User PC@https: //www.google. co.id/search?hl= id&source=hp& biw=&bih=&q= xman&gbv=1	Location:Visited User PC@https: //www.google. co.id/search?hl= id&source=hp& biw=&bih=&q	
Last accessed: 2021-10-02 14:20:20 UTC+000	Last accessed: 2021-10-02 14:20:20 UTC+000	

Fuente: Elaboración propia, basada en estudio simulado.

El análisis significa que el software de proceso ID 4416 que se ejecuta es Internet Explorer, y hay nueva información sobre el historial de accesibilidad y cuándo se produce el acceso. Esto es importante, puesto que no importa si el usuario eliminó el historial de navegación, aquí aparecerán los datos que se necesitan. Como se puede apreciar, en la tabla aparecen los sitios web a los que se tuvo acceso, la fecha y la hora. En este sentido, será fácil descubrir los sitios utilizados por un delincuente para contactar a la víctima y perpetrar el hecho delictivo. Ahora bien, utilizando el segundo método, mediante WinHex, se obtiene lo siguiente:

Figura No. 8

Búsqueda con WinHex

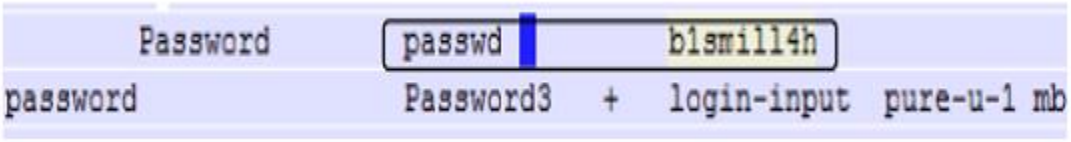


Fuente: Elaboración propia, basada en estudio simulado.

La figura anterior muestra que los resultados del análisis encontraron el historial, y lo que que se ha hecho es acceder a Google para búsqueda de información. Se ingresó al sitio de Wikipedia y se buscó el término “Batman”. Si se tratara de un delincuente que busca niños o niñas de determinada edad con fines de secuestro, sus búsquedas aparecen con WinHex y se entendería cómo hizo para encontrar a determinada víctima. Ahora bien, resulta que en el historial de navegación, el usuario ingresó a Facebook y allí mantuvo contacto con la víctima de secuestro, pero no se puede ingresar al perfil, porque tiene contraseña, como todos los perfiles en redes sociales. Una vez más, resalta la importancia de WinHex, puesto que revela las contraseñas que se han utilizado en el equipo de cómputo que es objeto de análisis, tal como se muestra en la siguiente imagen:

Figura No. 9

Revelar contraseñas con WinHex



Fuente: Elaboración propia, basada en estudio simulado.

Se puede encontrar la cuenta de contraseña utilizada para iniciar sesión en una red social específica, pero solo se encuentra en la primera y segunda simulación, antes de que antiforensic elimine el registro. De la misma manera, es posible encontrar las cuentas de correo utilizadas y su respectiva contraseña, tal como se muestra en la imagen siguiente:

Figura No. 10

Detectando cuentas de correo y contraseñas

Fuente: Elaboración propia, basada en estudio simulado.

Tal como se puede apreciar, en la imagen aparece la cuenta de correo a la que se tuvo acceso desde el equipo de cómputo y su respectiva contraseña, con lo que será

sumamente fácil acceder a la misma. WinHex también permite recuperar los archivos que fueron eliminados con la intención de no dejar rastros. Aunque para ello existen diversos programas, igual de eficaces, tales como: Recuva, Asistente de recuperación de datos de EaseUS. Puran File Recovery, Disk Drill, Glary Undelete, SoftPerfect File Recovery, Wise Data Recovery, entre otros.

Utilizando esta metodología es posible encontrar las evidencias necesarias para clarificar un delito en el que se utilizó internet o las redes sociales. En el caso del delito de secuestro, es posible encontrar los sitios web visitados, las palabras clave de búsqueda, los perfiles en redes sociales con sus respectivas contraseñas, las cuentas de correo con sus contraseñas, la recuperación de archivos eliminados, entre otros. Obviamente, existen otros métodos; sin embargo, la intención de esta investigación no es agotar la temática, sino ofrecer una alternativa, con sus respectivos procedimientos y herramientas, para poner en evidencia las ventajas de la misma.

CAPÍTULO VI

PRESENTACIÓN, ANÁLISIS Y DISCUSIÓN DE RESULTADOS

6.1 Presentación de resultados

6.1.1 Cuestionario No. 1

Dirigido a miembros de la Unidad de Antisecuestros de la Policía Nacional Civil -PNC- (34 investigadores).

¿Ha recibido alguna capacitación o especialización sobre el delito de plagio o secuestro? Especifique.

- Todos coinciden en señalar que han recibido el Curso Avanzado de Investigación Criminal en casos de Plagio o Secuestro, impartido en Bogotá, Colombia.
- También señalan los siguientes cursos: Incursión para el rescate de víctimas de secuestro y/o rehenes en cautiverio; IX Congreso Internacional de lucha contra el secuestro; Antisecuestros y antiextorsiones; Asesoría en gerencia de crisis para la negociación en plagio o secuestro.

¿Cómo las redes sociales han facilitado a los secuestradores la obtención de datos de las posibles víctimas?

- Por la publicación de actividades familiares en las redes.
- Las redes sociales son fuentes abiertas y en la cultura guatemalteca se tiene la costumbre de publicar información personal y familiar, la cual es aprovechada por los delincuentes.

- Por medio de la publicación de fotografías y datos personales que revelan la capacidad económica de un individuo o de su familia.
- Fotografías, datos personales, direcciones, números telefónicos, ubicación, bienes inmuebles y económicos.
- Las víctimas plasman información personal, abierta al público.
- En muchas ocasiones, de manera inconsciente, publicamos situaciones o actividades, lo cual no deberíamos hacer.
- Las personas publican en las redes toda la información relacionada con ellos y su familia.
- En sus perfiles, la gente publica datos vitales de información que los hacen vulnerables a este fenómeno criminal.
- Hay dos maneras: la primera es que la gente publica mucha información personal en redes sociales; la segunda, es que se dejan engañar por los intereses que muestran los malhechores en alguna red social.
- Por medio de datos e información muy específica, publicada en redes sociales.
- Por la publicación de datos personales y abiertos a todo público.
- Las redes sociales facilitan a los delincuentes la tarea de crear un perfil de la víctima y su familia.
- La mayoría de las personas publican información personal y constantemente hacen publicaciones donde indican su ubicación, los lugares que frecuentan y otros.
- A la mayoría de la gente le gusta presumir lo que tiene en redes sociales, suben fotos de sus vehículos, casas y viajes, para demostrar que tienen dinero.
- Por la inmadurez e ignorancia de la gente, al publicar su información personal.

- Por medio de citas a través de las redes sociales. Precisamente, en la Mesilla, en el municipio de La Democracia, Huehuetenango, hubo 6 casos de secuestro con esta modalidad, donde contactaron a las víctimas en redes sociales con un perfil falso, luego acordaron una cita y terminaron siendo secuestrados.
- La gente no es consciente del peligro que corre, revelando información personal.

¿Cuáles son los medios más utilizados por los secuestradores para obtener la información de sus víctimas?

- 23, de los 34 encuestados (68%), señalan que el medio más utilizado por los secuestradores, son las redes sociales: Facebook, WhatsApp, Instagram, Tik Tok y Twitter.
- Otros medios señalados, son los siguientes: Amigos, compañeros, familiares, trabajadores, conocidos, vecinos, pareja, ex pareja, privación de libertad de un familiar par obtener información, vigilancia estática.

¿Por medio de quién, los secuestradores obtienen mucho más fácil información de sus víctimas?

- Los más señalados por los investigadores, son los familiares, especialmente los menores de edad. Luego, están los trabajadores, vecinos, amigos y las fuentes abiertas (redes sociales).

¿Qué red social que utilizan los delincuentes, mucho más fácil para entrar en contacto con las posibles víctimas de secuestro?

- El 89% responde que Facebook. Luego, señalan a WhatsApp, Tik Tok, Instagram y Messenger.

¿Con qué herramientas TI (Tecnologías de la Información), cuentan en el departamento para dar seguimiento e investigación a este tipo de delitos donde están involucradas las redes sociales?

- 30 investigadores (88%), no respondieron esta pregunta, quizá porque ellos no forman parte de la división que se encarga de la informática forense, sino de los secuestros como tal. Los cuatro que respondieron, indican lo siguiente: análisis e inteligencia criminal, existe personal específico que se encarga de ello, algunas plataformas, software de rastreo satelital.

¿Tienen un protocolo de investigación exclusivo cuando se comete un delito de plagio y secuestro, donde se utiliza como plataforma una red social?

- 21 investigadores (62%), indican que sí cuentan con un protocolo; 6 (18%), responden que no cuentan con un protocolo; 6 (18%), no respondieron la pregunta y 1 (2%), responde que sí cuentan con un protocolo, pero es empírico.

¿Existe algún procedimiento para la indagación de un perfil de una red social con fines investigativos?

- 30 investigadores (90%), indican que sí existe un procedimiento. De ello se encarga la unidad de Delitos Informáticos del DEIC, también conocida como Ciber-Crimen. 2 (6%), indican que no existe ningún procedimiento; 1 (2%), no respondió la pregunta y 1 (2%), indica que no hay un procedimiento específico, cada uno actúa con base a sus conocimientos y experiencia.

¿Se sigue un protocolo de asesoría para la víctima o familiares de la víctima, al momento que la División tiene conocimiento de un delito de plagio y secuestro?

- 33 investigadores (98%), indican que sí se sigue un protocolo de asesoría para la víctima o familiares de la misma, a través del Departamento de Gerencia de Crisis, quienes están especializados para dicha tarea. 1 (2%), no respondió la pregunta.

¿Cuáles son algunos de los factores por los cuales los criminales u organizaciones criminales, cometen el delito de plagio o secuestro en Guatemala?

- 31 investigadores (91%), indican que el factor económico es determinante para cometer el delito de plagio o secuestro. Casi siempre, se busca un beneficio económico. 3 (9%), no respondieron la pregunta.

¿Qué red social ha sido la más utilizada para cometer el delito de plagio o secuestro?

- 22 investigadores (65%), indican que la red más utilizada para cometer el delito de plagio o secuestro, es Facebook. 7 (21%), indican que WhatsApp, pero aclaran que esta exige un mayor nivel de confianza entre víctima y victimario; 5 (14%), no respondieron la pregunta.

6.1.2 Cuestionario No. 2

Para miembros de la Sección contra Delitos Informáticos de la Subdirección General de Investigación Criminal de la Policía Nacional Civil -PNC- (7 investigadores).

¿Ha recibido alguna capacitación o especialización sobre cibercrimen y el uso de la tecnología para la investigación criminal?

- Los 7 investigadores (100%), indican que, efectivamente, han recibido capacitaciones y especializaciones sobre cibercrimen. Señalan el uso de las TIC´s en el ámbito investigativo, OSINT, Informática Forense, e Investigación de Delitos Informáticos, Cibercimen y Ciberterrorismo.

¿Cómo cree que la tecnología ha ayudado a las entidades del sector justicia a agilizar sus procesos investigativos?

- Agilización de procesos.
- Las TIC's constituyen la mayor fuente de información.
- Muchos trabajadores de la justicia desconocen las TIC's, no saben cómo utilizarlas.
- Ha facilitado la individualización de los sindicados de diversos delitos.
- Modernización de equipo y procedimientos.

¿Considera que Guatemala cuenta con la tecnología necesaria para la investigación del delito de plagio y secuestro?

- De los 7 investigadores encuestados, 4 responden que no se cuenta con la tecnología necesaria; 2 responden que sí, y uno responde que sí, pero aclara que solo en parte.

¿Cómo cree que las redes sociales han facilitado a los delincuentes la obtención de información específica de sus posibles víctimas?

- Es la manera más fácil, puesto que la mayoría de las personas acostumbran publicar información sensible y datos personales.

- Las redes sociales son medios para conectar gente, los usuarios son los que no toman las precauciones respectivas.
- La mayoría de los delincuentes las utilizan para obtener información.
- Los usuarios no saben utilizar las redes, ni resguardar sus datos.
- Por la ignorancia de los usuarios con respecto a la vulnerabilidad que representa el hecho de compartir información personal.
- Utilizando el método OSINT[155] e ingeniería social[156].
- Por medio de la publicación indebida de información y datos personales.

¿Qué red social considera que es mucho más vulnerable para la obtención de la información personal de las víctimas?

- De los 7 investigadores encuestados, 5 responden que Facebook.
- Uno indica que las redes sociales son seguras, el problema es que los usuarios no saben utilizar la configuración de privacidad al compartir información en las mismas.
- Uno responde que las redes sociales no son vulnerables, sino el ser humano que, por ignorancia o descuido, no sabe utilizarlas. Si se habla de seguridad o vulnerabilidad, ningún sistema es seguro.

¿Qué red social ha sido la más utilizada para cometer el delito de plagio o secuestro?

- De los 7 investigadores encuestados, 5 responden que Facebook; uno de ellos aclara que es la red que más se presta para la ingeniería social.

[155] Open Source Intelligence (en español Inteligencia de Fuentes Abiertas). Hace referencia a una serie de técnicas y herramientas para recopilar información pública, correlacionar los datos y procesarlos.
[156] Serie de técnicas que utilizan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.

- Dos, indican que WhatsApp es la red más utilizada para cometer el delito de plagio o secuestro.

¿Se sigue un protocolo cuando se comete un delito de plagio o secuestro en cualquier plataforma de cualquier red social?

- Los 7 investigadores encuestados indican que sí se sigue un protocolo. Aclaran que esto obedece a que las redes sociales tienen políticas de privacidad y requisitos para brindar información. En estos casos, se sigue el protocolo de solicitud de información por emergencia.

¿Qué clase de equipos informáticos y electrónicos cuenta la sección de delitos informáticos para la reconstrucción, obtención y extracción de la evidencia digital?

- De los 7 investigadores encuestados, 5 indican que cuentan con UFED[157], y dos afirman que, además de UFED, también cuentan con Ultrakit.[158]

¿Qué tipo de evidencias han podido obtener cuando se comete un delito de plagio o secuestro en las redes sociales?

- Los siete investigadores encuestados indican que han encontrado evidencia digital: imágenes, video, audio, mensajes de texto, información de registro, información de transacciones, ubicaciones, direcciones IP, geolocalización, fecha

[157] (Universal Forensic Extraction Device), un dispositivo que se utiliza para la extracción y decodificación de la información de la gran mayoría de teléfonos del mercado, y que se emplea comúnmente en las investigaciones de la informática forense.

[158] Es un kit de bloqueadores contra escritura, clonadores, adaptadores y conectores para su uso en la adquisición forense de imágenes de prácticamente cualquier disco duro o dispositivo de almacenamiento.

y horario de conexión, conversaciones, números de teléfono asociados a cuentas, entre otros.

6.2 Análisis de resultados

A través de la informática forense, se realizan investigaciones vinculadas con cualquier delito o crimen donde esté involucrada la tecnología informática, para recolectar las pruebas o evidencias necesarias para identificar y juzgar a los implicados en el mismo.

La tecnología informática, especialmente las computadoras, tablets, celulares e internet, son utilizados para cometer diversos delitos. Para algunos de estos delitos, la tecnología informática e internet, son indispensables, tales como grooming (seducción en línea), sexting (mensajes sexuales), sextortion (chantaje sexual), cyberbullyng (ciberacoso), phishing (robo de identidad) o malware (programa malicioso). En otros delitos, tales como el plagio o secuestro, la tecnología informática e internet, no son indispensables; no obstante, pueden utilizarse para facilitar la búsqueda e identificación de posibles víctimas, incluso, ayudan a concertar citas o encuentros, donde se ejecuta el delito.

En el caso de internet, son específicamente las redes sociales las que más se utilizan en este tipo de delitos. Por esta razón se eligió este tema de investigación, puesto que, la universalización de las redes sociales obliga a estudiarlas y analizar su participación en el desarrollo de conductas delictivas, para esto es necesario la integración de estas herramientas al proceso investigativo como fuente de información en la búsqueda de actos con características de ser delitos para que permita mitigar esta

problemática que se vive a diario en estos medios de interacción digital. Estas redes sociales propician medios para que la ardua labor investigativa pueda ser llevada a cabo de manera científica, es por ello que, es imprescindible la utilización de las mismas en la búsqueda de información para el esclarecimiento de hechos criminales, particularmente en el caso del delito de plagio o secuestro.

En este sentido, la investigación se realizó con la pretensión de ofrecer información amplia y científica sobre el tema de las redes sociales y su vinculación con el secuestro, como herramienta para la investigación criminal, para que personas particulares o instituciones interesadas en la materia puedan enriquecer sus conocimientos.

En primer lugar, se realiza un análisis de las nuevas tendencias delictivas que han encontrado un espacio propicio en las redes sociales para llegar a sus víctimas. La comunicación ha avanzado a lo largo de la historia de la humanidad, a través de diversos métodos e instrumentos, hasta llegar a internet y las redes sociales. Con las redes sociales, llegaron nuevos delitos y los que ya existían, replantearon sus estrategias para aprovechar las nuevas tecnologías. El anonimato intrínseco de las redes sociales contribuye a la ejecución de comportamientos socialmente recriminados. Delitos como el bullyng y el acoso, que se circunscribían al ámbito escolar o a la vecindad, ahora se realizan en las redes sociales. Y han surgido nuevos delitos, como los denominados delitos informáticos o ciberdelitos.

Por otra parte, en delitos antiguos como el plagio o secuestro, se crearon nuevos métodos y técnicas, ante las inmensas posibilidades que ofrecen las redes sociales. Este

delito, que consiste en poner a la persona en una condición determinada que impide la libertad de locomoción en su totalidad o parcialmente, de acuerdo a las limitaciones impuestas por el sujeto activo, se ha incrementado en virtud de las redes sociales, incluso han surgido nuevos tipos de secuestro, como el secuestro de información privilegiada y el secuestro virtual.

Las redes sociales les dan tanto poder a los delincuentes, que muchas veces ni siquiera necesitan acercarse a alguien físicamente para conseguir lo que quieren. Les basta tener un poco de información personal y un número de teléfono y hacen lo que se conoce como “secuestro virtual”, el cual no es otra cosa que una moderna forma de extorsión.

Desde este enfoque, las redes sociales constituyen un arma de doble filo, puesto que pueden ser aprovechadas por los delincuentes para facilitar la identificación de posibles víctimas, también constituyen una herramienta fundamental en la investigación criminal y forense. En este sentido, ha surgido una nueva área o disciplina en la criminalística: la informática forense, donde se combinan elementos vinculados con el derecho y la informática para la recopilación, análisis e interpretación de datos de sistemas informáticos, redes, comunicaciones inalámbricas y dispositivos de almacenamiento internos o extraíbles, para que se admitan como pruebas en los tribunales de justicia.

Estas redes sociales propician medios para que la ardua labor investigativa pueda ser llevada a cabo de manera científica, es por ello que, es imprescindible la utilización

de las mismas en la búsqueda de información para el esclarecimiento de hechos criminales, particularmente en el caso del delito de plagio o secuestro.

Por tal razón, las unidades de investigación de estos delitos que involucran las redes sociales, deben recibir una preparación específica en plagio o secuestro, pero también en informática forense. En este sentido, los miembros de la Unidad de Antisecuestros de la Policía Nacional Civil -PNC-, han recibido capacitaciones y especializaciones en el extranjero, específicamente en Colombia. De la misma manera, los miembros de la Sección contra Delitos Informáticos de la Subdirección General de Investigación Criminal de la Policía Nacional Civil -PNC-, se han especializado en la materia. Esto es necesario, porque los delincuentes mejoran sus técnicas o adoptan nuevas, de acuerdo a la evolución de la informática en internet.

Los secuestradores se valen de la información desplegada en redes sociales como arma para seleccionar a sus víctimas y hacer más fácil el poder llegar a ellas. Basta con entrar al perfil de una persona en Facebook, Twitter, Instagram, entre otras, para darse cuenta que la gente hace varias publicaciones vinculadas con su trabajo, profesión, estatus económico, lugares y restaurantes que visita, el vehículo que posee y mucho más. Sin pensarlo, se convierten en una presa fácil de extorsión o secuestro. Más aún si tiene un negocio propio, son el blanco preferido de los delincuentes.

Según la opinión de los investigadores encuestados, las redes sociales facilitan a los delincuentes la obtención de datos de sus posibles víctimas, debido a que los usuarios de las mismas no son cautos y publican información personal variada, que puede ser

utilizada para perfilarlo como una posible víctima de plagio o secuestro. A la vez, señalan que el medio más utilizado por los delincuentes en la actualidad, para cometer un secuestro, son las redes sociales, por su uso extensivo y generalizado. Dentro de las redes sociales, la más utilizada en el delito de plagio o secuestro, es Facebook, porque ésta se presta más para la ingeniería social.

En las redes sociales se observa cómo cientos de jóvenes publican fotografías de sus viajes, propiedades, actividades, mejores amigos o los nombres de sus padres, e incluso datos específicos, como colegios, universidades, gimnasio y hasta su dirección personal. Los nuevos equipos telefónicos con tecnología de punta tienen acceso a todo tipo de aplicaciones que permiten que se divulgue todo lo que hace a cada minuto, hasta permiten subir fotos del lugar en donde está y con quién se encuentra.

Sin embargo, es importante destacar que el problema no lo constituyen las redes sociales en sí mismas, sino los usuarios que no perciben el riesgo de publicar información sensible o confidencial. Por otra parte, no saben utilizar la configuración de seguridad de las mismas, para la publicación de datos o material multimedia. Desde el ámbito de la informática, todos los equipos y sistemas son inseguros y vulnerables; con mayor razón, las redes sociales que suelen ser públicas y facilitan la interacción.

De acuerdo con los investigadores, los secuestradores obtienen mucho más fácil información de sus víctimas, a través de los familiares, especialmente los menores de edad, los trabajadores, vecinos, amigos, y todo ello se puede hacer a través de las redes sociales. Puesto que, en el delito de secuestro, casi siempre se busca un beneficio de

tipo económico, los delincuentes buscan a personas con buenos puestos de trabajo, salarios altos y que muestren un estilo de vida cómoda.

Cuando la división encargada de este tipo de delitos, es informada de un secuestro, se sigue un protocolo en general; sin embargo, si en el delito estuvieron vinculadas las redes sociales, el protocolo a seguir es distinto, puesto que cada una de las redes sociales tiene sus propias normas y políticas de privacidad, por lo que se sigue el protocolo de solicitud de información por emergencia. También, se sigue un protocolo de asesoría para la víctima o familiares de la víctima, por medio del Departamento de Gerencia de Crisis, quienes se encargan de dicha tarea.

En Guatemala se cuenta con tecnología para la investigación del delito de plagio y secuestro, cuando están involucradas las redes sociales. Con respecto a equipos informáticos y electrónicos cuentan con las herramientas UFED y Ultrakit, las cuales se utilizan para la reconstrucción, obtención y extracción de la evidencia digital. También se utiliza el método OSINT; sin embargo, éste también es utilizado por algunos delincuentes para la recopilación, correlación y procesamiento de información.

Con estas herramientas, se obtiene la evidencia digital, la cual hace referencia a archivos multimedia, conversaciones, direcciones IP, geolocalización, historial de conexión, información de registro, transacciones, entre otras. Dicha tecnología constituye una ayuda importante para el sector justicia, puesto que permite la agilización de procesos y encontrar más información y con menos recursos.

Se han dado varios casos de secuestros donde se utilizan las redes sociales. El 28 de abril del año 2011, agentes de la Policía Nacional Civil capturaron a un individuo en la ciudad de Guatemala, sospechoso de haber secuestrado y asesinado a dos adolescentes, a quienes contactó por medio de Facebook, según información de La Prensa, en su versión digital.[159]

El 23 de abril del año 2018, agentes de la Policía Nacional Civil, capturaron a 3 hombres, sindicados de haber secuestrado a una joven en Gualán, Zacapa, según información consignada en la edición virtual de Prensa Libre. Se trata de una banda que contactaba a las víctimas por medio de Facebook, para luego secuestrarlas y exigir dinero a los familiares a cambio de no asesinarlas.[160]

El 18 de junio del año 2021, fue aprendido un individuo en el departamento de Suchitepéquez, quien pretendía secuestrar a una niña de 12 años, a quien contactó por medio de redes sociales, según información de Prensa Libre, en su edición digital.[161]

[159] La Prensa, laprensa.hn Cae en Guatemala presunto asesino de caso Facebook. Guatemala, 2011. Disponibilidad: https://www.laprensa.hn/mundo/cae-en-guatemala-presunto-asesino-en-caso-facebook-HBLP356274 Consultado: 07/11/2021.

[160] Morales, Mario, Prensa Libre, *op. cit.*

[161] Ortega Juan, Carlos. Prensalibre.com Hombre habría enviado mensajes inapropiados a niña por redes sociales para intentar raptarla. Guatemala, 2021. Disponibilidad: https://www.prensalibre.com/guatemala/comunitario/hombre-habria-enviado-mensajes-inapropiados-a-nina-por-redes-sociales-para-intentar-raptarla/ Consultado: 07/11/2021.

6.3 Discusión de resultados

Se cumplieron con los objetivos de la investigación, puesto que, luego de comparar la teoría con la información recopilada a través de las encuestas dirigidas a los expertos en plagio o secuestro e informática forense, se puso en evidencia lo siguiente:

- Efectivamente, con el auge y expansión de internet y las redes sociales, han surgido nuevas tendencias delictivas y los delitos antiguos han encontrado un espacio propicio para implementar nuevas estrategias para llegar a las víctimas, incluso la tipología de ciertos delitos, se ha ampliado.

- Se demostró, desde la teoría y con los aportes de los expertos encuestados, que el uso de las redes sociales es irrenunciable como herramienta en la investigación criminal y forense, puesto que los ciberdelitos utilizan como plataforma esencial a las redes sociales. Sin embargo, otros delitos también se valen de las redes como instrumento para la ingeniería social o para perfilar y llegar a las posibles víctimas.

- Se demostró que las redes sociales son utilizadas para la comisión del delito de plagio o secuestro, de tres maneras: como fuente de información para perfilar posibles víctimas; como medio para la ingeniería social; y como medio para obtener información de terceras personas sobre los individuos que interesan a los delincuentes.

- Finalmente, por medio de la teoría y la información recopilada en las encuestas, se describen los procedimientos que utilizan los peritos en informática forense en

Guatemala y otros procedimientos que no son exclusivos de esta disciplina, pero que son eficaces para determinadas tareas que facilitan la individualización de los delincuentes y la obtención de evidencias.

CONCLUSIONES

Actualmente, con las redes sociales han surgido nuevos delitos, tales como grooming, sexting, sextortion, cyberbullyng, phishing y otros. No obstante, también los viejos delitos han encontrado en las redes sociales un espacio propicio para llegar a sus víctimas, tales como el plagio o secuestro, donde éstas son muy importantes para perfilar a las víctimas.

Las redes sociales constituyen una herramienta invaluable en la investigación criminal y forense, puesto que agilizan los procesos y permiten la recopilación de información que no sería posible por otros medios o tomaría más tiempo y recursos.

En el delito de plagio o secuestro, las redes sociales son utilizadas para perfilar a las posibles víctimas, de tres maneras: la primera es a través de las fotografías y videos de propiedades, vehículos, viajes, lugares que frecuentan y datos personales publicados por los usuarios. La segunda es mediante la ingeniería social, que consiste en engañar a los usuarios incautos para que compartan datos confidenciales. La tercera, es la información que se puede obtener de las posibles víctimas por medio de familiares (especialmente menores de edad), amigos, conocidos o trabajadores, a través de las redes sociales.

Para la investigación del delito de plagio o secuestro a través de las redes sociales, se utilizan diversas herramientas y procedimientos, tales como UFED, Ultrakit y método OSINT. Otras herramientas fáciles de utilizar, son los navegadores web portables, Clean After Me, Process Monitor Portable, Volatility Memory Forensic, DumhIt y WinHex, las cuales se utilizan para realizar volcados de memoria RAM, recuperación de archivos

eliminados, recuperación de cuentas de correo, perfiles en redes sociales y contraseñas utilizadas, recuperar historial de navegación, entre otros.

RECOMENDACIONES

Se recomienda al Ministerio de Gobernación y Ministerio de Educación, lanzar campañas en redes sociales sobre los peligros y amenazas que éstas suponen para las personas de todas las edades, especialmente para los niños y jóvenes e informar cómo protegerse.

Se recomienda a los estudiantes y profesionales de la criminalística, formarse y actualizarse en la metodología y herramientas de informática forense, puesto que, en la actualidad, las redes sociales e internet, son una herramienta invaluable en la investigación criminal y forense.

Se recomienda a las universidades, instituciones no gubernamentales y empresas de telefonía, realizar campañas de sensibilización en el uso adecuado de las redes sociales, especialmente en lo vinculado a la información publicada y la configuración de seguridad, para no ser víctimas de diversos delitos, especialmente, del delito de plagio o secuestro.

Se recomienda a las universidades, formar a los futuros peritos en criminalística en la aplicación de las herramientas y procedimientos actuales de la informática forense, para estar a la vanguardia con respecto a los desafíos que presenta la tecnología informática e internet.

REFERENCIAS

Bibliográficas:

Aboso, Gustavo E. & Zapata, María F. Cibercriminalidad y derecho penal. Montevideo, Uruguay, Ed. Euros Editores, 2006.

Acurio Del Pino, Santiago. Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0, Quito, Ecuador, Instituto Nacional de Tecnología de la Información, 2015.

Arrona-Palacios, Arturo; Banda-Cruz, Daniel Alberto; Guevara-López, Carlos Alejandro; Villarreal-Sotelo, Karla El secuestro en Tamaulipas y sus repercusiones. CienciaUAT, vol. 6, núm. 2, octubre-diciembre, 2011, pp. 70-74 Universidad Autónoma de Tamaulipas, Ciudad Victoria, México.

ASOBANCARIA, Secuestro de información o “Ramsonware”: una amenaza para todos, Cartagena, Colombia, Asobancaria, 2017.

Azuela Fllores, José Ignacio; Baltazar Romero, Isabel; Jiménez Almaguer, Karla Paola; Ochoa Hernández, Magda Lizet; Jiménez Torres, Nadia Huitzilin Tipología de usuarios de redes sociales en México: ¿creadores o espectadores? Investigación y Ciencia, vol. 23, núm. 65, mayo-agosto, 2015, pp. 59-72 Universidad Autónoma de Aguascalientes Aguascalientes, México.

Barreira, R.; Pinheiro, V.; Furtado, V. Un marco para el análisis forense digital basado en el etiquetado de roles semánticos. En Actas de la Conferencia Internacional IEEE 2017 sobre Inteligencia e Informática de Seguridad: Seguridad y Big Data, ISI 2017, Beijing, China, 22–24 Julio 2017; pp. 66–71.

Barrére Cambrún, Martín. Análisis Forense Informático. Automatización de Procesamiento de Evidencia Digital. Montevideo, Uruguay, UDR, 2010.

Barrio Fernández, Ángela & Ruiz Fernández, Isabel. Los adolescentes y el uso de las redes sociales. En International Journal of Developmental and Educational Psychology, Vol. 1, No.3, España, 2014, p.571-576.

Boyd, D. M., & Ellison, N. B, Sitios de redes sociales: Definición, historia y erudición. Diario de la computadora, Mediated Communication, Vol. 13, No. 1, Michigan, Estados Unidos, 2007.

Calderón Martínez, A. T. Teoría del delito y juicio oral, 23ª. Ed. México, D. F., Departamento de Investigaciones Jurídicas de la UNAM, 2012.

Cano Martínez, Jeimy José. El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas, Bogotá, Colombia, Ediciones UNIANDES, 2010.

Carneiro, Roberto; Toscano, Juan Carlos & Díaz, Tamara. Los desafíos de las TIC para el cambio educativo, Madrid, España, Fundación Santillana, 2021.

Cauhapé-Cazaux, Eduardo. Apuntes de derecho penal guatemalteco. La teoría del delito. Guatemala, Fundación Myrna Mack, 2003.

Cea Jiménez, A. D. Los delitos en las redes sociales: aproximación a su estudio y clasificación, Madrid, España, CPC, 2012.

Centro de Documentación, Información y Análisis. Delito de secuestro: (Segunda Parte). Estudio de Derecho Comparado Interno (32 códigos penales locales) y a Nivel Internacional (8 países) y Opiniones Especializadas. México, D. F. Cámara de Diputados, LX Legislatura, 2008.

Conti, N. J. Secuestro coactivo. Buenos Aires, Argentina, Asociación Pensamiento Penal, 2008.

Couso García, Fernando. El informe pericial criminológico como herramienta de protección de los derechos fundamentales de víctimas y victimarios (Tesis de pregrado). Bilbao, España, Universidad del País Vasco, 2020.

Cruz Quintero, Gloria Esperanza. Importancia de la informática forense, Bogotá, Colombia, Universidad Piloto de Colombia, 2016.

Deitel, P. & Deitel. Ajax, Rich Internet Aplications y Desarrollo Web para programadores. Madrid, España, Ediciones Anaya Multimedia, 2008.

Escobar de León, Luis Eduardo, Manejo de la cadena de custodia en la recolección de evidencia digital (Tesis de pregrado), Quetzaltenango, Guatemala, Universidad Rafael Landívar, 2017.

Fernández Teruelo, J. G. La sanción penal de la distribución de pornografía infantil a través de Internet, Boletín de la Facultad de Derecho de la UNED, 20, España, 2002

Flores Cueto, Juan José; Morán Corzo, Jorge Joseph & Rodríguez Vila, Juan José. Las redes sociales, Lima, Perú, Unidad de Virtualización Académica de la Universidad de San Martín de Porres, s.f.

Flores Salgado, Lucerito. Derecho Informático, México, D. F., Editorial Patria, 2009.

Gil Urdiciain, Blanca. Manual de lenguajes documentales. Gijón, España: Trea. 2004.

González Rus, J. J.: “Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos”, en Revista de la Facultad de Derecho de la Universidad Complutense, 12, 1986, p. 107-164.

Guardia de Viggiano, Nisla V. Lenguaje y comunicación, San José, Costa Rica, CECC/SICA, 2009.

Gómez, José & Fedor, Simón. La Comunicación, *Revista Salus*, vol. 20, núm. 3, septiembre-diciembre. Venezuela. Universidad de Carabobo, 2016.

Góngora Pimentel, G. Evolución del poder Judicial y las decisiones del Poder Judicial de la Federación en la materia, México, D. F., Porrúa, 2003.

Hurtado Guapo, Ma Antonia; Fernández Falero, Ma del Rosario. Reconciliando las tipologías de usuarios de internet. Razón y Palabra, núm. 89, marzo-mayo, 2015 Universidad de los Hemisferios Quito, Ecuador

Hütt Herrera, Harold. Las redes sociales: una nueva herramienta de difusión. Reflexiones, Vol. 91, No. 2, San José, Costa Rica, 2012, pp. 121-128.

Ibáñez Gómez, Fernando & Esteban, Miguel Ángel. Análisis de los ataques piratas somalíes en el Océano Índico (2005- 2011): evolución y modus operandi, Zaragoza, España, Universidad de Zaragoza, 2013.

Jiménez Ornelas, R. A. El secuestro, uno de los males sociales del mexicano. México, D. F., Departamento de Investigaciones Jurídicas de la UNAM; 2010.

Lima Malvido, María de la Luz. Delitos Electrónicos. Academia Mexicana de Ciencias Penales, Editorial Pomia, México, 2018.

Londoño Rojas, Edna Margarita. La interdisciplinariedad de la informática forense en la era digital, Bogotá, Colombia, UNIPILOTO, 2015.

López Delgado, Miguel. Análisis forense digital, España, 2007.

López Molina, Keren Hapuc & Vindell Olivas, Juan Carlos. Laboratorio de computación forense para el Departamento de Criminalística de la Policía Nacional de Nicaragua (Tesis de pregrado), Managua, Nicaragua, UNAN, 2011.

Maldonado Escobar, Carlos Alejandro. Herramientas forenses de análisis digital para la obtención de información aplicado a ordenadores y dispositivos móviles (Tesis de pregrado), Quetzaltenango, Guatemala, Universidad Rafael Landívar, 2020.

Martin Serrano, Manuel. Evolución e historia en el desarrollo de la comunicación humana. Extraído de Teoría de la comunicación. La comunicación, la vida y la sociedad. Madrid: McGraw-Hill Interamericana de España, 2007.

Meluk, E. El secuestro, una muerte suspendida. Su impacto psicológico. Bogotá, D.C., Uniandes, 1988.

Mendillo, Vincenzo. Análisis forense de la memoria RAM, Caracas, Venezuela, Universidad Central, 2018.

Ministerio de Defensa. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio, Madrid, España, Ministerio de Defensa, 2010.

Ministerio Público Fiscal. El Ministerio Público Fiscal de la nación recomienda algunas precauciones para evitar ser víctima de los denominados “secuestros virtuales”, Buenos, Aires, Argentina, Procuraduría General de la Nación, 2014.

MINTIC. Seguridad y privacidad de la información, Bogotá, Colombia, 2016.

Molina, B., Agudelo, M., De los Ríos, A., Builes, M., Ospina, A., Arroyave, R. et al. El secuestro: su repercusión en las creencias y en la estructura de relaciones en un grupo de familias antioqueñas. Revista Colombiana de Psiquiatría, 32(1), 27-50, 2003.

Monge Orejel, Brenda Leticia. El delito de secuestro sancionado con la pena de muerte pone en mayor riesgo la vida de las víctimas (Tesis de pregrado), Guatemala, Universidad de San Carlos de Guatemala, 2006.

Muñoz Arango, C. E. El delito del secuestro. Anuario de Derecho N° 48, Págs. 178 -186, 2019.

Muñoz Conde, F. Teoría General del Delito. Valencia, España, Tirant lo Blanch, 1991.

Neira Brunetti, Bernardo. El delito de secuestro y el secuestro terrorista, Santiago, chile, Universidad Andrés Bello, 1997.

Observatorio Nacional Ciudadano. Análisis integral del secuestro en México. Cómo entender esta problemática, México, D. F., 2014.

Observatorio Nacional de las Telecomunicaciones y de la SI. Las redes sociales en internet, España, ONSI, 2011.

Oficina de las Naciones Unidas contra la Droga y el Delito. Manual de lucha contra el secuestro. Viena, Austria, ONU, 2006.

Oficina de las Naciones Unidas Contra la Droga y el Delito. Manual sobre la investigación Del delito de trata de personas. Guía de autoaprendizaje, San José, Costa Rica, UNODC, 2010.

Organización de las Naciones Unidas. Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos. Revista Internacional de Política Criminal, 1994.

Ortiz, Emanuel. Evidencia Digital: Fundamentos aplicables para el abordaje de la Examinación Forense. Boston, Massachusetts, Estados Unidos, RedCiber, 2019.

Ortiz Pradillo, Juan Carlos. La investigación del delito en la era digital, Madrid, España, 2014.

Parababire, Carmen. Perspectiva sociológica del secuestro express como una nueva modalidad de delito caso estudio: municipio Naguanagua Estado Carabobo año 2012 y el primer periodo del 2013 (Tesis de pregrado). Carabobo, Venezuela, Universidad de Carabobo, 2013.

Pax Christi. La industria del secuestro en Colombia ¿Un negocio que nos concierne? Utrecht, Holanda, Pax Christi Holanda, 2016

Pérez Beristain, M. A. Esteganografía de la información en nuestra vida. En Logos No. 2, Vol. 7, No. 14, México, D. F., 2020.

Pineda, Billy Alexander. Estado situacional de la educación secundaria ante el uso de redes sociales digitales, Guatemala, Universidad de San Carlos de Guatemala, Dirección General de Investigación, 2020.

Pinto, María. Manual de clasificación documental. Madrid, España: Síntesis, 1997.

Ramírez Estrella, Alex Guillermo, La prueba electrónica: los medios electrónicos como recurso para la práctica de la prueba (Tesis de postgrado), Guayaquil, Ecuador, Universidad de Santiago de Guayaquil, 2016.

Romeo Casabona, Carlos María. Poder informático y seguridad jurídica. Madrid, España: FUNDESCO, 1988.

Romero Castro, Martha; Choez Chele, Miguel Angel; Álava Mero, Christian José, et, al. La informática forense desde un enfoque práctico, Manabí, Ecuador, Área de Innovación y Desarrollo, 2020.

Rowley, J. E. La organización del conocimiento: una introducción a la recuperación de la información. Hampshire, Inglaterra: Ashgate, 1992.

Sain, Gustavo. Delito y nuevas tecnologías: Fraude, narcotráfico y lavado de dinero por internet, Buenos Aires, Argentina, Editores del Puerto, 2012.

Santo Orcero, David. Kali Linux, Madrid, España, 2018.

Segarra-Saavedra, J. e Hidalgo-Marí, T. Viralidad e interacción. Análisis del engagement de los diez anuncios más vistos en YouTube en España en 2016, Icono 14, volumen 16 (1), pp. 47-71, 2018.

Téllez Valdez, Julio, (1987). Derecho Informático. México, D. F.: Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, 1987.

Toc López, Sandra Dominga. Estudio sobre el delito de secuestro en la sociedad guatemalteca (Tesis de pregrado), Guatemala, Universidad de San Carlos de Guatemala, 2007.

Uña Juárez, Octavio & Hernández Sánchez, Alfredo. La sociología, Madrid, España, Esic, 2004.

Yang, Y., Saladrigas Medina, H., & Torres, Ponjuán. El proceso de la comunicación en la gestión del conocimiento. Un análisis teórico de su comportamiento a partir de dos modelos típicos, Revista Universidad y Sociedad, Vol. 8, No. 2, Cuba, Universidad de Cienfuegos, 2016, p. 165-173.

Legislación:

Asamblea Nacional Constituyente. Constitución Política de la República de Guatemala, 1985.

Congreso de la República de Guatemala, Decreto Numero 17-73, Código Penal, 1973.

Electrónicas:

Areitio Bertolín, Javier. Conectronica.com, Seguridad forense, técnicas antiforenses, respuesta a incidentes y gestión de evidencias digitales, España, 2009. Recuperado de: https://www.conectronica.com/tecnologia/seguridad/seguridad-forense-tecnicas-antiforenses-respuesta-a-incidentes-y-gestion-de-evidencias-digitales. Consultado el: 15/10/2021.

Bassini, Andrés Eduardo. derechopenalonline.com El perito informático y la prueba pericial, Argentina, 2013. Disponibilidad: https://derechopenalonline.com/el-perito-informatico-y-la-prueba-pericial/ Consultado: 10/10/2021.

Bernal Michelena, David Eduardo. Análisis de volcado de memoria en investigaciones forenses computacionales, Revista Seguridad, No. 31, mayo 2018. México, D. F., DGTIC-UNAM. Disponibilidad: https://revista.seguridad.unam.mx/numero-17/an%C3%A1lisis-de-volcado-de-memoria-en-investigaciones-forenses-computacionales Consultado: 02/10/2021.

Bienpensado.com, Gómez, David, Social Media no traduce redes sociales, Bogotá, Colombia, 2012. Disponibilidad: https://bienpensado.com/que-es-social-media-y-su-diferencia-con-las-redes-sociales/ Consultado el 19/08/2021.

Bryson, Joanna. Bbvaopenmind.com La última década y el futuro del impacto de la IA en la sociedad, España, Grupo BBVA, 2022. Recuperado de:

https://www.bbvaopenmind.com/articulos/la-ultima-decada-y-el-futuro-del-impacto-de-la-ia-en-la-sociedad/ Consultado el 16/02/2022.

Capacitarte. capacitarte.org ¿Qué es el ciberdelito? Buenos Aires, Argentina, 2021. Disponibilidad: https://www.capacitarte.org/blog/nota/que-es-el-ciberdelito Consultado: 29/08/2021.

Ciberseguridad, ciberseguridad.com Perito informático forense y judicial, España, 2019. Disponibilidad: https://ciberseguridad.com/servicios/perito-informatico/ Consultado: 11/10/2021.

Ciberseguridad. Ciberseguridad.com Evidencia digital, 2021. Disponibilidad: https://ciberseguridad.com/servicios/analisis-forense/evidencia-digital/#Funcionamiento Consultado: 27/10/2021.

Clean After Me, uptodown.com Clean After Me, Málaga, España. Disponibilidad: https://clean-after-me.uptodown.com/windows Consultado: 01/10/2021.

Consejo de Europa, coe.int Convenio de Ciberdelincuencia. Estrasburgo, Francia, 2021. Disponibilidad: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm Consultado el 30/09/2021.

Correduría Inteligente. Mpmsoftware.com Redes Sociales: definición y características, España, 2019. Disponibilidad: https://www.mpmsoftware.com/es/blog/redes-sociales-definicion-y-caracteristicas/#:~:text=Personalizaci%C3%B3n,un%20grado%20elevado%20de%20privacidad. Consultado el 20/08/2021.

Derechos digitales. Derechosdigitales.org Ofuscación, me ves/no me ves, Brasil, 2020. Disponibilidad: https://www.derechosdigitales.org/ofuscacion/ Consultado: 08/11/2020.

El Fisco. Elfisco.com Revista nº 151. El crimen organizado y las nuevas tecnologías, Argentina, 2020. Recuperado de: http://elfisco.com/articulos/revista-no-151-el-crimen-organizado-y-las-nuevas-tecnologias Consultado el: 15/10/2021.

Fintech School, escuelafintech.com Las funciones del perito informático, España, 2019. Disponibilidad: https://escuelafintech.com/que-es-perito-informatico/ Consultado: 11/10/2021.

García, Luis. Onretrieval.com El Investigador Forense y la pérdida de datos. España, 2021. Disponibilidad: https://onretrieval.com/el-investigador-forense-y-la-perdida-de-datos/ Consultado: 12/10/2021.

GCF Global. edu.gcfglobal.org.es ¿Qué es una URL? España. Disponibilidad: https://edu.gcfglobal.org/es/como-usar-internet/que-es-una-url/1/ Consultado: 03/10/2021.

González, Yolanda. protecciondatos-lopd.com La informática forense en la investigación de delitos, Madrid España, Grupo Atico34, 2020. Recuperado de: https://protecciondatos-lopd.com/empresas/informatica-forense/ Consultado el 13/10/2021.

Hacking y forensic. Ediciones-eni.com Volatility, España. Disponibilidad: https://www.ediciones-eni.com/open/mediabook.aspx?idR=554bb28fd9f6e0f97724779646d2a3c8 Consultado: 01/10/2021.

Herranz, Arantza. Xataka.com Soy perito informático y estos son algunos de los casos más surrealistas en los que he trabajado. España, 2020. Disponibilidad: https://www.xataka.com/seguridad/soy-perito-informatico-estos-algunos-casos-surrealistas-que-he-trabajado Consultado: 12/10/2021.

Indubitado. Indubitado.com Informática forense: resumen. España, 2021. Disponibilidad: https://indubitado.com/2021/informatica-forense-resumen/ Consultado: 12/10/2021.

Informática Forense. https://duartecarito.wixsite.com Fases en la informática forense. Colombia, 2015. Disponibilidad: https://duartecarito.wixsite.com/eportafolioforense/single-post/2015/05/18/fases-en-la-informatica-forense Consultado: 27/10/2021.

Ionos, ionos.es ¿Qué son los navegadores? España, 2020. Disponibilidad: https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/que-es-un-navegador/ Consultado: 08/11/2021.

Landinez Olaya. A. Tratamiento del secuestro en los medios escritos el tiempo y el nuevo siglo, 2001. Disponibilidad: http// intellectum.unisaba.edu.co:8080/jspui/bitstream/108186317/1/126696.Pdf Consultado: 10/09/2021.

Latto, Nica. Avast.com Navegación privada: cómo activar o desactivar el modo de incógnito, España, 2021. Disponibilidad: https://www.avast.com/es-es/c-guide-to-private-browsing#gref Consultado: 03/10/2021.

Lazcano, Patricio & Montes, Carlos. Latercera.com Así funciona un ransomware, el virus que tiene en jaque a Banco Estado y es la principal ciberamenaza en Chile, Chile, 2020. Disponibilidad: https://www.latercera.com/que-pasa/noticia/asi-funciona-un-ransomware-el-virus-que-tiene-en-jaque-a-bancoestado-y-es-la-principal-ciberamenza-en-chile/7C5WJ2LOVZFDNAGV636LJ4WQYQ/ Consultado: 12/10/2021.

Lemontech blog blog.lemontech.com Evidencias digitales: significado, objetivo y tratamiento, Perú, 2021. Disponibilidad: https://blog.lemontech.com/evidencias-digitales/ Consultado: 08/11/2021.

Lifeder.com, Montano, Joaquín, Medios de comunicación antiguos y sus características, España, 2021. Disponibilidad: https://www.lifeder.com/medios-de-comunicacion-antiguos-y-sus-caracteristicas/, consultado el 18/08/2021.

Manage Engine. Manageengine.com Análisis forense de redes con NetFlow Analyzer, 2021. Recuperado de: https://www.manageengine.com/latam/netflow/analisis-forense-de-redes.html Consultado el: 15/10/2021.

Matesanz, Vanesa. Xataka.com ¿Cómo se llega a ser el perito informático que analiza los discos duros de Bárcenas? España, 2016. Disponibilidad: https://www.xataka.com/ordenadores/como-se-llega-a-ser-el-perito-informatico-que-analiza-los-discos-duros-de-barcenas Consultado: 12/10/2021.

Mintic, enticconfio.gov.co Ciberextorsión por medio de secuestros de perfiles digitales. Colombia, 2020. Disponibilidad: https://www.enticconfio.gov.co/poder-digital/ciberextorsion-mediante-secuestro-de-perfiles-digitales Consultado: 18/09/2021.

Morales, Mario, prensalibre.com Usaron perfil falso de Facebook para secuestrar a joven; PNC los captura Guatemala, 2018. Disponibilidad: https://www.prensalibre.com/ciudades/zacapa/usaron-perfil-falso-de-facebook-para-secuestrar-a-joven-pnc-los-captura/ Consultado: 27/10/2021.

MRInternacional S.A. newsinamerica.com Guatemala sufrió más de 25 millones de intentos de ciberataques en la primera mitad del año, 2020. Recuperado de: https://newsinamerica.com/pdcc/tecnologia/2020/guatemala-sufrio-mas-de-25-millones-de-ciberataques-en-la-primera-mitad-del-ano/ Consultado el 12/10/2021.

Netinbag. netinbag.com ¿Cuál es la diferencia entre informática forense y recuperación de datos?, España, 2020. Disponibilidad:

https://www.netinbag.com/es/internet/what-is-the-difference-between-computer-forensics-and-data-recovery.html Consultado: 15/10/2021.

Ondata Internacional. Ondataforensic.com Las herramientas de análisis más avanzadas. WinHex. Madrid, España, 2021. Disponibilidad: http://www.ondataforensic.com/tecnologia_winex.php Consultado: 01/10/2021.

Onieva, David, softzone.es Navegadores. Usa Internet de forma más segura con estos navegadores portables, España, 2021. Disponibilidad: https://www.softzone.es/programas/navegadores/navegadores-internet-portables/ Consultado: 01/11/2021.

Owaida, Amer. Welivesecurity.com Contraseñas: 5 errores comunes que deberías evitar, España, 2020. Recuperado de: https://www.welivesecurity.com/la-es/2020/05/07/errores-comunes-crear-contrasenas/ Consultado el: 14/19/2021.

Perito Legal. Peritolegal.es Perito informático: la solución a tu caso con medios digitales. España, 2020. Disponibilidad: https://peritolegal.es/wp-content/uploads/2020/11/Perito-informatico-.-La-solucion-a-tu-caso-con-medios-digitales.pdf Consultado: 12/10/2021.

PJ Group, peritojudicial.com Las 11 habilidades clave de un perito, España, 2020. Disponibilidad: https://peritojudicial.com/11-habilidades-clave-perito/ Consultado: 11/10/2021.

Portables Programas, portablesprogramas.com Process Monitor v3.10 Portable, España. Disponibilidad: https://www.portablesprogramas.com/process-monitor-v3-10-portable/ Consultado: 01/10/2021.

Rd Station, rdstation.com Redes sociales, España 2020. Disponibilidad: https://www.rdstation.com/es/redes-sociales/ Consultado: 20/08/2021.

Redacción Tecnósfera, eltiempo.com Ramsomware: aumenta el delito de secuestro de datos, Colombia, 2021. Disponibilidad: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ransomware-riesgos-del-secuestro-de-datos-y-consejos-para-evitarlo-609194 Consultado: 20/10/2021.

Román, Ricardo, ricardoroman.cl Las redes sociales online llegan, poco a poco, al móvil, Chile, 2007. Disponibilidad: http://www.ricardoroman.cl/2007/09/08/las-redes-sociales-online-llegan-poco-a-poco-al-movil/ Consultado el 19/08/2021

Semymas, semymas.com Riesgos de compartir información personal en redes sociales, España, 2018. Disponibilidad: https://semymas.com/riesgos-informacion-personal/ Consultado: 20/08/2021.

Sophos, Los ataques perpetrados contra las redes sociales crecen un 70%, España, 2021. Disponibilidad: https://www.sophos.com/es-es/press-office/press-releases/2010/02/security-report-2010.aspx, Consultado el 20/08/2021.

Tarlogic Security Experts. Tarlogic.com Ransomware o cómo quedarse sin empresa en unas horas, España, 2021. Recuperado de: https://www.tarlogic.com/es/blog/ataque-ransomware-en-horas/ Consultado el 12/10/2021.

Thesocialmediafamily.com Conoce las redes sociales más utilizadas (2021). España. Disponibilidad: https://thesocialmediafamily.com/redes-sociales-mas-utilizadas/ Consultado el 29/08/2021.

Toc López, S. Estudio sobre del delito de secuestro, 2007. Disponibilidad: http: //biblioteca.usac.edu.gt/tesis/04/04_6808.pdf Consultado: 10/09/2021.

Torres, Enrique. Cyta.com.ar Informática forense: el camino de la Evidencia digital, Buenos Aires Argentina, 2020. Recuperado de: http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/informatica_forence.htm Consultado el 13/10/2021.

Unidad Editorial Internet, S. L., elmundo.es Un 'secuestro tigre' en Irlanda se salda con un botín de siete millones de euros, España, 2009. Recuperado de: https://www.elmundo.es/elmundo/2009/02/27/internacional/1235752696.html Consultado el 02/09/21.

Unitypromotores.com Unitypromotores. Consejos de seguridad en Redes Sociales, Guatemala, 2020. Disponibilidad: https://www.unitypromotores.com/consejos-seguridad-redes-sociales/ Consultado el 19/08/2021.

Welivesecurity. welivesecurity.com/la-es ¿Qué son las técnicas antiforenses? España, 2015. Disponibilidad: https://www.welivesecurity.com/la-es/2015/07/02/tecnicas-anti-forenses/ Consultado: 03/10/2021.

ANEXOS

Universidad Rafael Landívar
Tradición Jesuita en Guatemala

INSTRUMENTOS

CAMPUS SAN ROQUE GONZÁLEZ DE SANTA CRUZ S. J.
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE

Fecha: _____

Boleta No._____

CUESTIONARIO PARA MIEMBROS DE LA UNIDAD ANTISECUESTRO DE LA PNC

Título de la Investigación: Análisis del uso de las redes sociales como herramienta en la investigación criminal y forense en Guatemala en los delitos de plagio o secuestro.

Instrucciones: Por favor, responda las siguientes preguntas de acuerdo a sus conocimientos y experiencia.

1. ¿Ha recibido alguna capacitación o especialización sobre el delito de plagio o secuestro? Especifique.

2. ¿Cómo las redes sociales han facilitado a los secuestradores la obtención de datos de las posibles víctimas?

3. ¿Cuáles son los medios más utilizados por los secuestradores para obtener la información de las víctimas?

4. ¿por medio de quien los secuestradores obtienen mucho más fácil información de sus víctimas?

5. ¿Qué red social considera que utilizan los delincuentes mucho más fácil para entrar en contacto con las posibles víctimas de secuestro?

6. ¿Con que herramientas TI (Tecnologías de Información) cuentan en el departamento para dar seguimiento e investigación a este tipo de delitos donde están involucradas las redes sociales?

7. ¿Tienen un protocolo de investigación exclusivo cuando se comete un delito de plagio y secuestro donde se utiliza como plataforma una red social?

8. ¿Existe algún procedimiento para la indagación de un perfil de una red social con fines investigativos?

9. ¿Se sigue un protocolo de asesoría para la víctima o familiares de la víctima al momento que la División tiene conocimiento de un delito de plagio o secuestro?

10. ¿Cuáles son algunos de los factores por los cuales los criminales u organizaciones criminales cometen el delito de plagio o secuestro en Guatemala?

11. ¿Qué red social ha sido la más utilizada para cometer el delito de plagio o secuestro?

CAMPUS SAN ROQUE GONZÁLEZ DE SANTA CRUZ S. J.
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE

Fecha: _____

Boleta No._____

CUESTIONARIO PARA MIEMBROS DE LA SECCIÓN CONTRA DELITOS INFORMÁTICOS DE LA SUBDIRECCIÓN GENERAL DE INVESTIGACIÓN CRIMINAL DE LA PNC.

Título de la Investigación: Análisis del uso de las redes sociales como herramienta en la investigación criminal y forense en Guatemala en los delitos de plagio o secuestro.

Instrucciones: Por favor, responda las siguientes preguntas de acuerdo a sus conocimientos y experiencia.

1. ¿Ha recibido alguna capacitación o especialización sobre cibercrimen y el uso de la tecnología para la investigación criminal?

2. ¿Cómo Cree que la tecnología ha ayudado a las entidades del sector justicia a agilizar sus procesos investigativos?

3. ¿considera que Guatemala cuenta con la tecnología necesaria para la investigación del delito de plagio o secuestro?

4. ¿Cómo Cree que las redes sociales han facilitado a los delincuentes la obtención de información específica de sus posibles víctimas?

5. ¿Qué red social considera que es mucho más vulnerable para la obtención de la información personal de las víctimas?

6. ¿Qué red social ha sido la más utilizada para cometer el delito de plagio o secuestro?

7. ¿se sigue un protocolo cuando se comete un delito de plagio o secuestro en cualquier plataforma de cualquier red social?

8. ¿Qué clase de equipos informáticos y electrónicos cuenta la sección de delitos informáticos para la reconstrucción, obtención y extracción de la evidencia digital?

9. Qué tipo de evidencias han podido obtener cuando se comete un delito de plagio o secuestro cuando en las redes sociales?