FACULTAD DE DERECHO
MAESTRÍA EN DERECHO

ACTUACIÓN DE LOS MINISTERIOS PÚBLICOS ANTE LAS DENUNCIAS Y QUERELLAS EN MATERIA DE DELITOS INFORMÁTICOS EN GUERRERO EN EL 2020.

TESIS

QUE PARA OBTENER EL GRADO DE MAESTRÍA EN DERECHO

OPCIÓN TERMINAL: DERECHO PENAL

PRESENTA:

LIC. JOSÉ LUIS MARTÍNEZ CUEVAS.

DIRECTOR DE TESIS:

M.C. Claudio Flores Seefoó.

TUTOR “CODIRECTOR” ACADÉMICO:

Dr. Saúl Barrios Sagal.

Chilpancingo, Guerrero, 3 diciembre de 2021.

I.- Dedicatoria:

El presente trabajo de investigación está destinado a mis padres Ma. Isabel Cuevas Ocampo y José Luis Martínez Silva por creer en mí, a mi novia la Lic. Silvina García Quezada ya que fue quien me motivo a iniciar con el paso de seguirme preparando y alentarme cuando creía que no podría terminar, de igual manera se les agrade a mis hermanas por su tolerancia, apoyo y comprensión ya que por concluir este gran paso tuve que ausentarme en fechas importantes, finalmente el trabajo concluido es gracias al apoyo académico y emocional de mi director y tutor de tesis que más que mis catedráticos se convirtieron en grandes amigos.

"Siguiendo las instrucciones llegas a donde te esperan, pero cometiendo errores llegas a donde tú quieras"

Anónimo.

II.- Introducción

La presente investigación tiene como fin, identificar si los ministerios públicos dentro del Estado de Guerrero están adecuadamente capacitados para atender las denuncias y querellas en materia de delitos informáticos. Así mismo analizar se analiza una breva comparativa de la atención de como fiscalías de otros Estados están atendiendo el mismo problema y con ello identificar si utilizan en mismo enfoque o estructura en sus corporaciones de procuración de justicia.

Lo anterior referido versa con la adhesión de figuras punibles en el Estado de Guerrero a finales del mes de noviembre del 2019, por lo cual la temporalidad de desarrollo de investigación es en el transcurso del año del 2020.

Las sociedades se transforman conforme a sus necesidades y los nuevos medios de información y comunicación, y estamos de acuerdo en que las TIC transforman de forma radical el espacio de capacidades de las personas (Echeverría, 2008), ya que la sociedad se adapta a los cambios tecnológicos y con ello se desarrollan nuevas conductas las cuales pueden tener una finalidad positiva o negativa en el desarrollo de la misma.

Cuando las TIC se usan en sentido negativo dan apertura a la creación y legislación de los crímenes conocidos como delitos informáticos o ciberdelitos, los cuales se han incrementado por el mayor uso de las tecnologías de información y comunicación, y la problemática existente en la atención a los delitos cibernéticos es debido al aumento de la interacción a través del ciberespacio, tanto que ha llevado a la cooperación y colaboración entre policías cibernéticas y funcionarios del fuero común y federal.

Y relacionar al sujeto activo del delito con la conducta que ocasiona un daño al sujeto pasivo del delito es facultad y obligación del ministerio público, dicha acción versa conforme a sus investigaciones siguiendo el marco jurídico

legal vigente, por tanto, no puede ir más allá de lo que la ley establezca en ese momento, aunque exista certeza de un señalamiento directo del sujeto pasivo.

Por ello es importante saber si, los ministerios públicos están o no adecuadamente capacitados para atender delitos informáticos en Guerrero, México; conocer si se están atendiendo de manera adecuada las denuncias y querellas por delitos informáticos en Guerrero o bien identificar si los delitos informáticos quedan en la impunidad debido a la falta de capacitación o del alcance punible de la legislación vigente.

El fiscal ministerio público es el encargado y facultado para formular imputaciones de delitos cuando algún sujeto de la sociedad cometa una conducta típica, antijurídica y culpable y con ello rompa el orden social, no solo en el entorno físico sino también en el ciberespacio, hablamos de que los ministerios públicos tienen la obligación de aplicar correctamente sus conocimientos para la adecuada formulación de una acusación, contra un sujeto que comete un delito, conducta o incidente informático.

Como académicos del derecho se tiene el deber de analizar las problemáticas reales dentro de la aplicación de las leyes vigentes en el estado, por ello es necesario tener una visión real y objetiva de las actuaciones de los ministerios públicos ante los delitos informáticos, y con ello desde la academia sugerir y proponer nuevas formas ante las cuales se puede atender de mejor forma los delitos informáticos pues con su estudio se identifican los problemas que enfrentan los fiscales ministerios públicos ante la investigación de este tipo de delitos, por ello es importante evaluar la actuación de los ministerios públicos ante las denuncias y querellas en materia de delitos informáticos en el estado de Guerrero.

Conociendo lo anterior, en el presente trabajo de investigación se aborda la problemática planteada con el fin de conocer e investigar los antecedentes de los delitos informáticos en diversas legislaciones a nivel global y local, los delitos

estipulados en los códigos penales locales y con ello hacer una comparativa, así mismo se puede diagnosticar la eficiencia de los Ministerios públicos para atender las denuncias y querellas en materia de delitos informáticos en el estado de Guerrero.

III. Índice:

CAPÍTULO I

Generalidades.

1.1.- Conceptos dentro del lenguaje informático.

El uso y la implementación de la informática entre los seres humanos, nace como consecuencia de la evolución del hombre, de sus necesidades de comunicación y organización en un mundo globalizado a partir del siglo XX.

Diversos autores comentan, que la informática no fue creada por las leyes del orden natural, Morales (2015) sostiene con respecto al origen de la tecnología lo siguiente:

> La tecnología tiene su origen en la evolución del hombre dentro del desarrollo de la convivencia social la construcción de Chinampas el lenguaje de escritura la casa el uso del fuego la agricultura al viajar de un lugar a otro se generó el comercio y con ello el uso del metal para generar moneda y herramientas siendo parte de la ciencia de la información tecnológica.
>
> Dicho lo anterior se puede afirmar que el hombre por naturaleza es un ser social debe crecer con orden y equilibrio en su convivencia con otros seres humanos y esto se logra gracias a la comunicación y en aspecto positivo de la norma de las instituciones gubernamentales militares seguridad pública y procuración administración de justicia. (pp. 3-4).

El posicionamiento antes referido, parece evidente debido a que el ser humano es considerado como un ser social, por tanto, vive bajo las reglas establecidas previamente dentro de una comunidad, un municipio, distrito, Estado o nación, y con las condiciones del siglo XXI podríamos afirmar que la

sociedad actual inclusive se rige bajo una legislación supranacional, hablando de los tratados internacionales que firman los países para la convivencia internacional.

La informática y el mundo cibernético “son todos los cambios de índole cultural que se están generando como consecuencia de la utilización de la informática como medio de información y comunicación” (Gros, 2001, p. 5). han traído indudables ventajas y beneficios en la sociedad actual: dentro de la escuela, trabajo, comercio, comunicación, salud, etc. Las tecnologías de la información y la comunicación facilitan la vida en el mundo contemporáneo y hacen posible concebir la vida que hoy conocemos y desarrollamos a diario.

Investigadores como Argüelles (2016) exponen con respecto a las ventajas proporcionadas por la tecnología respecto en las vías de telecomunicaciones, transparencia y circulación de información y con ello crímenes relacionados con la propia informática.

Por tanto, con lo antes mencionado, es difícil negar que la informática es una herramienta vital en la sociedad actual (sociedades de la información y del conocimiento), aunque no debemos perder de vista que esto puede conllevar a un uso negativo de la misma.

Se ha observado que, a través del uso de la informática surgen nuevas formas de descomposición social y conductas que aprovechan el mal uso de estas herramientas y el derecho no puede ser indiferente al respecto, el avance de la tecnología desarrolla nuevos comportamientos propios del desarrollo humano cuya finalidad es delinquir (Landa, 2017).

Establecido estos dos supuestos es notorio que el derecho informático y el derecho penal están ligados, dado que en ambas ramas del derecho se encuentra involucrada algún tipo de conducta humana, la cual puede

encontrarse descrita en un ordenamiento penal cuando este comportamiento se vuelve lascivo para el resto de población, por lo que el derecho no puede ser omiso ante esto y debe contener en sus ordenamientos legales las conductas que serán punibles para aquellos usuarios que transgredan los derechos tutelados del resto de la población, a través de cuerpos de leyes de índole penal.

Dichas figuras punibles estarán sujetos a un proceso penal, el cual está descrito y contenido dentro del código nacional de procedimientos penales, que obedece a la implementación del sistema penal acusatorio oral, legislado a partir de

La reforma del 18 de junio de 2008 se publicó en el Diario Oficial de la Federación el Decreto por el que se reforman los artículos 16, 17, 18, 19, 20, 21 y 22; las fracciones XXI y XXIII del artículo 73; la fracción VII del artículo 115 y la fracción XIII del apartado B del artículo 123, todos de la Constitución Política de los Estados Unidos Mexicanos (Vázquez, 2019).

El delito informático no nació de manera espontánea y mucho menos del pensamiento de un solo ente. De manera sintetizada **la teoría general del delito informático,** refiere sobre el nacimiento y justificación de esta teoría a su perspectiva en México de esta manera:

> Esta teoría nace con la necesidad de colaborar con una nueva tendencia doctrinal del derecho público, privado, social y globalizado, siendo el caso concreto en México.
>
> Donde a través de ella se vislumbran problemas actuales y concretos, en los cuales la sociedad mexicana se ve afectada a gran escala desde el 2000 hasta el día de hoy (Morales, 2015, p. I).

Para ello en un primer momento debemos definir dos cosas, la definición de delito y como es que puede llegar a involucrarse la tecnología con esta figura jurídica, para ello es imperante tomar el concepto de delito informático desde la perspectiva de los juristas: “aquel que se da con la ayuda de la informática o de técnicas anexas” (Callegari, 1985, p. 115) esta definición consideramos es un tanto limitada dado el supuesto que la informática puede ser utilizada como medio para la comisión de un delito y no la contempla como bien jurídico tutelado.

Por otro lado, Téllez (1996) conceptualiza al delito informático en forma típica y atípica, entendiendo por “la primera a las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin” (p. 461) es decir, las computadoras solo son el medio para la comisión de un delito y “las segundas por las actitudes ilícitas en que se tienen a las computadoras como instrumento o fin” (Téllez, 1996, p. 474).

Esto se puede contraponer con otra definición hecha por Huerta y Líbano (1996) que definen los delitos informáticos como:

> Todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro. (p. 123).

Una vez establecido el concepto de delito informático dentro de la investigación, vuelve importante identificar el antecedente más antiguo de cuando ocurrió el primer delito cibernético o informático.

Existen registros del primer ataque informático en la red o internet, esto nos sirve como punto de referencia y así poder observar la evolución histórica en los delitos informáticos y cibernéticos.

Sin embargo, antes de definir los antecedentes a nivel global tenemos que tener conocimiento de los conceptos de términos relacionados con los delitos informáticos o con los incidentes en el panorama cibernético.

Erróneamente dentro del mundo de la informática se le denomina Hacker al delincuente cibernético, las definiciones más aceptadas en el mundo son las siguientes: “1. m. y f. Inform. pirata informático. 2. m. y f. Inform. Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora” (Real academia, 2020, s.p.) la segunda definición fue aceptada en el 2017 y es con la definición con la que se realizó el trabajo de investigación.

Definido el concepto de hacker, hoy en día los hackers han cambiado de denominación a especialista ético, debemos diferenciar los dos tipos existentes:

Hackers de sombrero negro o black hat**:** Son hackers malintencionados. Se dedican a la búsqueda de vulnerabilidades de seguridad para explotarlas en su propio beneficio. Se dedican también a realizar malware.

Hackers de sombrero blanco o White hat**:** Son los llamados hackers éticos. Suelen ser contratados por alguna compañía para la búsqueda

de vulnerabilidades de seguridad, para detectarlas, conseguir subsanarlas y que la aplicación sea más segura. Estos hackers siempre tienen un fin bien intencionado.

Por tanto, entendamos como: **Hacking** la búsqueda y explotación de vulnerabilidades de seguridad en sistemas o redes (Lucena, 2019, s.p.).

Sin embargo, aun cuando desde la informática han nombrado a los especialistas que encuentren vulnerabilidades en los softwares, en el campo del derecho desde la teoría se ha conceptualizado con un nombre distinto el Cibercrimen se le llama a la "criminalidad asociada al uso de las redes telemáticas (Computerkriminalität), o bien contra los propios sistemas, programas y datos informáticos" (Aboso, 2018, p. 16).

El concepto de hacking no alcanza técnicamente para definirlo como cibercrimen, por ello es más apropiado utilizar etimológicamente el significado e implicación de la conducta para entender los ataques sufridos a una base de datos, por lo que para ello debemos acogernos al concepto de Acceso no Autorizado acceder sin permiso a una base de información de manera indebida, sin autorización o contra derecho (Huerta y Líbano, 1998).

La distinción entre las partes que logran el funcionamiento de un dispositivo es fundamental entenderlo por ello tomamos como referencia las concepciones de la RAE la cual nos dice que Software**:** "es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora" (Real Academia, 2020, s.p.) y Hardware**:** "conjunto de los componentes que conforman la parte material (física) de una computadora" (Real Academia, 2020, s.p.).

Una vez identificados los componentes de un equipo de información y comunicación, es necesario identificar y saber diferenciar las posibles formas de afectar el equipo informático o la propia información, por tanto,

entenderemos dentro de la investigación el concepto de Avast (2019) la compañía especializada en antivirus informáticos su concepto sobre el Malware el cual hace referencia a “cualquier tipo de software malicioso que trata de infectar un ordenador o un dispositivo móvil” (s.p.).

Esta especificación dentro de los delitos informáticos es importante pues dentro de la división y clasificación de malware resulta que existen variedad de sabotajes informáticos, las técnicas más conocidas que permiten cometer sabotajes informáticos son bombas lógicas las cuales producen daño a la base de información de forma posterior a ser infectado el equipo, permitiendo la huida del ciberdelincuente, los cuales son distinto a los gusanos informáticos que se infiltran en programas legítimos para dañar el procesamiento impidiendo volver a su estado original y perdiendo el funcionamiento del mismo (Acurio, 2016).

Por lo anterior referido los fraudes en nuestra legislación penal se encuentran tipificados a nivel federal y nivel local sin embargo, para el contexto técnico cada uno tiene una propia naturaleza forma de dañar el patrimonio informático, por ello es recalcable recabar los tipos de fraudes que existen, el listado de tipos de fraudes informáticos que Acurio (2016) menciona como la técnica del salami, la cual consiste en extraer cantidades financieras diminutas de una cuenta bancaria a otra sin autorización de su titular, además existen las falsificaciones informáticas, las falsificaciones informáticas realizadas con uso comercial y con base en el engaño, las manipulaciones de datos de salida cuyo principal modo se realiza en los cajeros automáticos y el phishing el cual es realizado con la finalidad de robar la identidad de la víctima.

Con los conceptos referidos es posible entrar en el análisis y contexto informático básico, para poder explicar la necesidad de la investigación de la actuación de los ministerios públicos ante los delitos informáticos.

1.2.- Antecedentes de los delitos informáticos a nivel global.

Una vez establecidos algunos términos conceptuales encontramos que los ataques informáticos han tenido presencia desde varias décadas atrás y han estado en constante evolución. Identificando como algunos de estos eventos marcaron la trayectoria del mundo de derecho, por lo cual es de relevancia importante conocer los siguientes antecedentes históricos:

En el año de 1971, los pheakers nombre de que reciben los vulneradores de línea telefónica como John Drapear quien fue un manipulador telefónico, el cual descubrió que mediante un sonido dado con un silbato como premio en cajas de cereal Cap'n Crunch al enlazarlo al tono de las llamadas por cobrar o larga distancia producía los mismos tonos que usaban los conmutadores telefónicos de la época lo cual permitía realizar llamadas sin costo alguno para quien utilizaba este aparato, de forma posterior difundió su descubrimiento mediante el cual por la legislación de la época no era considerado como delito de forma posterior los casos de fraude telefónico aumentaron significativamente en varias partes del mundo (Rinaldi, 2017).

De forma posterior el delito informático evolucionó con la llegada de la automatización de la información de los bancos, Rinaldi (2017) menciona que, en 1973 un empleado de un banco que se desempeñaba como cajero de un banco local de New York utilizó una computadora para causar un daño a la institución financiera pues utilizo una computadora para poder desviar fondos del banco estimados en dos millones de dólares aproximadamente.

Sin embargo, la primera conducta considerada como delito cibernético ya que fue la primera en obtener una condena, es el que realizó Ian Murphy conocido como el capitán Zap, el cual en el año de 1981 ya que hackeo la red de AT&T ya que cambió el reloj interno de la compañía fuera del horario de trabajo de la misma. Por esta razón nació y formo como antecedentes de las

conductas referidas, las violaciones a las redes empezaron a tomarse como figuras delictivas, y como en este caso fue encuadrada como terrorismo, no obstante, solo recibió mil horas de servicio comunitario y una pena corporal de prisión que fue sustituida por libertad condicional por dos años y seis meses, misma penalidad que si se realiza la comparativa con las penas actuales es mucho menos severa (Rinaldi, 2017).

Además, Rinaldi (2017) refiere que el gobierno de Estados Unidos estos antecedentes en el tema de los delitos informáticos o cibernéticos al tener los incidentes informáticos con mayor frecuencia, tomó la iniciativa en 1886 de considerarlas como delitos y en 1988 el congreso consideró estas conductas ilícitas, convirtiendo el hackeo y el robo en algo ilegal, por lo cual los casos disminuyeron, más no fueron erradicados.

En el año de 1988 se lanzó un virus de gusano el cual era auto replicante por Robert T. Morris Jr., dicho virus fue enviado en la ARPANET es decir para aquella época era la precursora del internet, dicho virus se le fue de las manos y terminó por infectar a más de seis cientos mil computadoras aproximadamente, de forma posterior Robert fue condenado a pagar una multa de diez mil dólares y tres años de libertad condicional, misma que si se pone en comparativa con las penalidades de ahora resulta ser mucho menor a las actuales (Rinaldi, 2017).

Sin embargo, estas conductas no pararon, ya que con el mayor uso del internet estas conductas cambiaron y se intensificaron los daños en 1989 se reportó el primer caso conocido de un virus de tipo ransomware a gran escala. El virus referido se caracterizó y presentó como un cuestionario sobre el virus del sida y, una vez descargado, mantenía los datos informáticos de quien lo contestaba como rehenes por quinientos dólares, los cuales solo se liberaban cuando el usuario pagaba la cantidad referida, el caso avanzaba y no era fácil

difundir sobre este problema pues parecía un cuestionario informativo, prosiguió este suceso sin tener detenidos por este problema que afectó a mucha gente de esa época (Rinaldi, 2017).

De forma posterior en el año 1995 sucede que aparecieron por primera vez los llamados macro-virus estos debido a sus propias características son descritos como virus escritos en lenguajes informáticos integrados en aplicaciones las cuales se propagan a sí mismas a otro dispositivo (Rinaldi, 2017).

Estos macro virus se ejecutan cuando se abre la aplicación, como documentos de procesamiento de textos u hojas de cálculo (es decir un documento de office cualquiera), y son una forma fácil para que los hackers puedan enviar el malware.

Esta es la razón por la que la apertura de documentos adjuntos de correos electrónicos desconocidos, pueden ser muy riesgosos y aun en el año 2020 todavía se les considera de alta infección pues estos tipos de virus son difíciles de detectar y son una de las principales causas de infección del ordenador, de las cuales además nos hemos familiarizado con ellos de tal forma que no se nos hacen peligrosos debido a su cotidianidad con la cual se encuentran al navegar en internet.

En otro antecedente global Rinaldi (2017) menciona que en el año de 1997 el FBI informó que más del 85% de las empresas en Estados Unidos habían sido hackeadas, y lo que llamó la atención de este suceso es que la mayoría de las empresas ni siquiera lo sabía y mucho menos acudieron a levantar una denuncia por el hecho, de manera relacionada se investigó a El Chaos Computer Club una organización que hackeaba software y con ello podían hacer transferencias financieras, esto sin que el banco o el titular de la cuenta lo sepan, la víctima se da cuenta solo hasta que el estado de cuenta le

había sido entregado y el banco se excusaba de no ser los culpables, por lo cual muchas personas pierden la confianza en las instituciones bancarias en esos años y que trajo pérdidas millonarias a muchas empresas.

Además, Rinaldi (2017) hace mención que el año de 1999 los delitos informáticos volvieron a poner en la atención de las autoridades ante el lanzamiento del virus Melissa. Este virus se convirtió en la infección informática más agresiva y sin solución rápida aún en la actualidad. El escritor del virus fue acusado de causar un daño de más de ochenta millones de dólares estadounidenses en daños a las redes informáticas y fue condenado a cinco años de prisión.

En un antecedente de delito informático más reciente en el 2000 el número y tipo de ataques en línea crece de manera alarmante para las autoridades de todo el mundo. Mencionando un caso en específico, el minorista de música CD Universe es extorsionado por millones de dólares, esto después de que la información de las tarjetas de crédito de sus clientes fuera publicada en línea, y al mismo tiempo las noticias falsas causan que las acciones de Emulex caigan casi un 50% debido a la desinformación contenida en línea y de los cuales los usuarios evitaron seguir usando (Rinaldi, 2017).

También en el mismo año el virus *I Love You* se propagó a través de internet y fue tanta el auge de este virus que inclusive el entonces presidente de Estados Unidos Bill Clinton afirmó que no usaba ni usaría el correo electrónico para hablar con su hija porque la tecnología no es segura, con ello se detectaba por la ciudadanía que el gobierno de estados unidos no podía controlar de forma alguna la propagación de los virus informáticos.

En un evento más cercano en el año del 2003 SQL Slammer un virus de gusano de propagación se convirtió en el más rápido de la historia esto debido a que logró infectar servidores enteros y creó un ataque de denegación de

servicio, mismo que terminaba por afectar las velocidades a través del internet durante bastante tiempo, el cual no pudo identificarse su ataque de origen. Si nos referimos a la de velocidad de infección, este virus se logró extender a través de casi setenta y cinco mil dispositivos en menos de 10 minutos, los cual volvía para las autoridades un reto fuera de su alcance controlarlo y mucho mayor aún erradicarlo (Rinaldi, 2017,).

En 2007 los casos de hackeo, robo de datos e infecciones de malware se disparan. El número de registros robados y máquinas infectadas aumentan en millones, la cantidad de daños causados en miles de millones, como se puede ver un delito informático no atendido de manera rápida y oportuna puede producir pérdidas económicas y derivar en mayores afectaciones (Rinaldi, 2017).

Los ataques informáticos realizados a nivel federal pueden terminar impactando en la vida cotidiana de las personas, en 2014, la administración de Barack Obama acusó a cinco hackers militares chinos de irrumpir en las redes de las principales corporaciones estadounidenses para desviar secretos comerciales, de esta forma fueron tratados en su proceso:

> Los cargos criminales fueron presentados en la corte federal de Atlanta, donde la compañía tiene su base. La acusación detalla los esfuerzos que los hackers hicieron para cubrir sus huellas, incluyendo el borrado diario de los archivos de registro y el enrutamiento del tráfico a través de docenas de servidores en casi 20 países. En concreto, los cargos que presentaron son: conspiración para cometer fraude informático, conspiración para cometer espionaje económico y conspiración para cometer fraude electrónico (INFOBAE, 2020, s.p.).

Es evidente que el fenómeno del desarrollo tecnológico proporcionó consigo diversas vulnerabilidades en los dispositivos de comunicación en la época, por lo que los países se vieron en la necesidad de empezar a legislar y cuidar su patrimonio informático de los ataques y vulnerabilidades que traían consigo implícitas en los dispositivos de comunicación, por lo que nacieron los Hackers de sombrero blanco o hackers éticos, llamados de esta forma porque las compañías desarrolladoras de software necesitaban brindar confianza a sus usuarios y blindar el uso de sus programas, por ello centraban a hackers profesionales para encontrar vulnerabilidades en sus productos antes de sacarlos al mercado a la venta.

Estos antecedentes han sido tomados en consideración y servido no solo para diferenciar algunas de las diferentes formas de delitos e incidentes informáticos, sino que además permiten entender el amplio espectro de los daños que se pueden producir al no atender de manera adecuada por una figura delictiva.

Los delitos informáticos no son nuevos y siguen evolucionando conforme los dispositivos de comunicación e información tienen mayores usos, por lo cual, al estar hoy en día legislados en la materia penal local, es de importancia que los agentes del ministerio público conozcan los alcances de estas figuras jurídicas vigentes las cuales atentan contra la población sin distinción alguna.

Las repercusiones dentro de los habitantes de un Estado que no contiene contemplados los delitos informáticos de forma idónea, se vuelven vulnerables ante las acciones realizadas por los ciberdelincuentes y, por ende, si estas conductas delictivas evolucionan, el número de victimarios es probable crezcan.

1.3.- Antecedentes de los delitos informáticos en Latinoamérica.

En América latina el uso del internet fue un poco más lento el acceso por parte de la población, no obstante, no significó que los riesgos no estuviesen presentes, ya que al hablar de América latina y conceptualizarse como una región geográfica, se puede establecer que, aunque sea una región amplia, los problemas pueden iniciar desde una zona territorial local limitada, “Cada segundo se crean tres virus informáticos en el mundo, Latinoamérica es de las zonas más afectadas y quedan impunes.” (Tiempo, 2014, s.p.), con respecto a esta afirmación podemos contrastarlas de país a país citando algunos casos.

El sitio web de Delta Asesores retoma que según la Revista Cara y Sello (2018) “durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos” (p.18). No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros son conductas cada vez más usuales en todas partes del mundo.

Esto lo logran a través de clonación de tarjetas bancarias, suplantación de identidad, vulneración y alteración de los sistemas de cómputo, recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas, afectación de los cajeros automáticos, divulgación de contenido sexual o pornográfico entre otras, son conductas cada vez más usuales en todas partes del mundo.

Cabe destacar que un precedente entre ministerio público local y federal importante fue el ocurrido en 2018, el portal de diario Huila informó que en Colombia, se aplicó un operativo en 16 departamentos que permitió desarticular redes criminales señaladas hurtos, estafas y otros delitos por medios electrónicos, identificaron y capturaron a 15 personas que harían parte

de una banda delincuencial la cual se dedicaba a instalar ganchos retenedores en los cajeros electrónicos, esto les permitía quedarse con el dinero en efectivo de sus víctimas, según la investigación, con esta modalidad la banda habría realizado 80 transacciones y se apropió de $64’000.000. dólares (Fiscalía Colombia, 2018)

Las corporaciones de investigación delictiva dentro de Colombia tomaron a los delitos cibernéticos como un problema serio a partir de ese año ya que afectaba a la comunidad cada vez de manera reiterativa, al respecto el portal del periódico de Huila reporta lo siguiente:

> Las ciudades con más denuncias por delitos informáticos son:
> Bogotá: 4.805 denuncias, incremento de 114%.
> Medellín: 1.831 denuncias, incremento de 36.2%.
> Cali: 1.490 denuncias, incremento de 50%.
> Los delitos informáticos que más se cometen son:
> Hurto por medios informáticos y semejantes: 8.817 denuncias.
> Violación de datos personales: 2.180 casos.
> Acceso abusivo a un sistema informático: 2.005 denuncias. (Fiscalía Colombia, 2018, p .1)

De la misma manera el combate contra el crimen informático o cibernético ha tenido resultados ya que en Colombia “la realización de diligencias de registro y allanamiento en Valledupar, Montería y Barranquilla, fueron capturados nueve integrantes de los Ciberceleros” (Fiscalía Colombia, 2018, p. 2). Entre los detenidos está Óscar Peñalosa, alias Boca, un reconocido hacker, en los procedimientos fueron incautados datafonos, tarjetas de entidades bancarias, sim card, celulares, discos duros, entre otros elementos, las detenciones por delitos informáticos han cambiado el paradigma jurídico en Colombia.

Según la investigación, “Los Carceleros o Ciberceleros estarían involucrados en robos virtuales por $2.900’000.000 dólares” (Fiscalía Colombia, 2018 p. 2). Por petición del juez de control de garantías, los presuntos integrantes de esta organización recibieron medidas privativas de la libertad en establecimiento carcelario y el juez de control de garantías ordenó la suspensión del poder dispositivo de cuatro casas y un vehículo, es decir esta organización tenía una estructura sólida para cometer sus ilícitos.

El territorio venezolano no ha sido la excepción a los delitos informáticos uno de los casos de mayor relevancia registrado en Venezuela fueron más atribuidos a la Violación de la privacidad, situando el caso Marval donde la víctima fue Rosmeri Marval, actriz y modelo, fue víctima de hackeo en su cuenta Instagram en el año 2015, utilizaron la cuenta oficial de Marval para estafar a varios usuarios seguidores de la modelo además de insultar a varios seguidores y cuentas asociadas al Instagram de la actriz (Lorca, 2019), si lo podemos equiparar con la legislación mexicana en esa temporalidad, en el caso de haberle ocurrido a un particular cualquiera, la investigación de este hecho no hubiese sido posible atenderlo ya que la suplantación de identidad fue agregado como delito en noviembre del 2019.

En cuestión de Fraudes los delincuentes en Venezuela las autoridades han podido disminuir los delitos informáticos a través de líneas de investigación dirigidas por la División Contra Delitos Informáticos del CICPC, es la encargada de investigar todos los delitos cometidos con el uso de equipos tecnológicos, contemplados en la ley como delitos informáticos. Esta División Contra Delitos Financieros se creó el 07 de octubre de 2003, cuando comenzó el aumento de delitos cibernéticos en el país entre los casos más conocidos se encuentran los responsables conocidos como los Cracker Venezolanos y los magos del cambiazo.

Con lo anterior referido podemos deducir que conforme la tecnología siga siendo una herramienta fundamental para el ser humano, podrá ser vulnerable por los especialistas técnicos los cuales podrían sacar ventaja, por lo que el derecho debe vigilar aquellas conductas que transgredan el patrimonio y derechos de la población en general.

Dentro de este escenario el periódico El Tiempo consiguió una entrevista con especialistas en ciberseguridad de la cual se obtuvieron algunos datos importantes en cuanto a la vulnerabilidad de la población ante los delitos informáticos y la frecuencia de los mismos, por cuanto a Brasil se refiere:

> Brasil es el país más expuesto a los crímenes cibernéticos al haber sido víctima en 2013 de entre 33 y 43% de los ataques en la región indicado por Dmitry Bestuzhev Director del equipo de Investigación y Análisis para América Latina de la empresa rusa de seguridad informática Kaspersky LAB. (El Tiempo, 2014, s.p.),

El panorama en América latina ha sido adverso pues debido a la especialización técnica y la estructura delictiva que poseen los ciberdelincuentes o delincuentes informáticos, muchos de los casos donde la víctima denunciaba se volvió poco probable la localización de algún probable responsable de los delitos informáticos, pues algunos operaban fuera del país donde atacaban o enviaban el contenido obtenido por la conducta delictiva fuera de la territorialidad del país de origen del ataque informático, por lo que la colaboración internacional para resolver este tipo de delitos era indispensable, pero los trámites burocráticos complicaron la labor investigadora.

En otro problema de américa latina era la inexperiencia laboral y limitación económica destinada por el estado para la investigación en esta materia por parte de los agentes investigadores de cada país, por lo que la

mejor solución para tratar de resolver el alto índice delictivo en el campo informático y cibernético fue la creación de los cuerpos investigadores especializados por lo que estos tomaron auge en América latina.

La tipificación a nivel internacional ha crecido entorno a legislar en torno a la informática y los incidentes informáticos, así como en las técnicas de investigación para comprobar con fuentes metodológicas la culpabilidad del ciberdelincuente, respecto a ello en Perú se creó Dirección de Investigación criminal y apoyo a la justicia, en la división de delitos de alta tecnología. Además, en Bolivia también se creó la División de Delitos Informáticos de la Fuerza especial el cual tiene una finalidad similar a la unidad especializada de Perú.

El avance de las unidades especializadas en el Estado de Colombiano está a cargo del grupo de grupo especializado de delitos informáticos, los cuales colaboran con sus laboratorios de computación forense, mismos que están en coordinación con los fiscales para investigar y combatir el crimen en el ciberespacio, que afecte a los habitantes de ese país.

A su vez el Estado Chileno desde el año 2000 ha creado la Brigada Investigadora del Cibercrimen, misma que se ha estado capacitando y combatiendo a los grupos de ciberdelincuentes, colaborando con autoridades de otros países para intentar abarcar bandas que operen fuera del territorio chileno.

Por parte de México, a nivel federal para el combate del crimen cibernético, cuenta con la Policía Cibernética, que actúa como “prevención e investigación de delitos del fuero federal, que a su vez está especializada en delitos de fraudes como el phishing”. (Gamba, 2010, p. 23).

Cabe señalar que de esa temporalidad algunas instituciones han cambiado de nombre sin embargo es importante para la investigación señalar que los delitos informáticos no son nuevos y que han estado presentes y es necesaria su debida atención por parte de los gobiernos.

De tal manera que el panorama que ha existido en América latina en cuanto a víctimas de delincuentes informáticos es muy grande, y genera un daño económico importante Temperini (2013) en su estudio de derecho comparado nos dice:

> De acuerdo a uno de los estudios de mayor relevancia mundial en delitos informáticos, en el cual se han entrevistado más de 13.000 adultos en 24 países, para el año 2012, se calculó que los costos directos asociados con los delitos informáticos que afectan a los consumidores en el mundo ascendieron a US$ 110.000 billones en doce meses. El mismo estudio revela que por cada segundo 18 adultos son víctimas de un delito informático, lo que da como resultado más de un millón y medio de víctimas de delitos informáticos cada día, a nivel mundial. (p.1)

Este trabajo para la época fue indispensable pues proporcionó para el campo del derecho una visión más acertada de las necesidades de la época para atender los delitos informáticos, y a su vez no solo lograr eficacia en la detección de posibles delincuentes, sino que además de ser aplicado podría otorgar certeza jurídica a los gobernados dentro de los países que sufrían una frecuencia excesiva en la vulneración de su patrimonio informático, algunas de las conclusiones de su investigación son las siguientes:

> En base a los resultados obtenidos, es posible afirmar: a) Que, los países latinoamericanos presentan una falta de homogeneización en el ámbito sustantivo de la normativa penal aplicable a los delitos informáticos. b) Que, los países latinoamericanos han optado por

> diferentes posturas en relación a sus formas de regular. Algunos han optado por la sanción de leyes especiales, donde en los casos más destacados incorporan conceptos propios, principios, parte penal material, parte procesal penal, e incluso se han generado los organismos dedicados a su investigación y persecución. Otros tantos países (mayoría) han optado por modificaciones parciales a sus Códigos Penales vigentes, adaptando las figuras penales clásicas a fin de que sea posible su aplicación en los delitos informáticos. (Temperini, 2013, p.12)

Con lo anterior analizado se identifica que el fenómeno de los delitos informáticos y su evolución dentro de américa latina es consistente y existe presencia de ellos en todos los países del sur del continente americano, lo cual vuelve vulnerable a una muy grande cantidad de personas, por lo que las autoridades deben tomar las medidas necesarias para, prevenir, combatir y castigar a los presuntos responsables de la comisión de delitos informáticos.

1.4.- Antecedentes de los delitos informáticos en México.

En México la conexión dentro del internet es importante pues con ella se inicia el momento en el cual nuevas conductas delictivas se desarrollan, por lo cual es importante mencionar que se empezó a trabajar con la interconexión hasta el año de 1986 esto de acuerdo al trabajo de la ITESM donde se puede un artículo de la misma institución mostrar el proceso de la misma implementación de esta tecnología la cual informó que, en México los primeros intentos de interconexión fueron desde los años 70´s y fueron estables hasta 1986 a través de una línea de monterrey al estado de Texas. (Robles, 2007).

Y fue entonces que hasta que un año después en 1987, la UNAM establece su conexión a BITNET a través del ITESM y meses más tarde su propio enlace satelital (satélite Morelos II).

Por tanto, se puede establecer que desde que un equipo informático entra en uso por los habitantes de un estado, haciendo referencia en esta ocasión al Estado mexicano de cierta manera se obliga a si a mismo a proteger los derechos dentro de la informática, por lo que desde algunas décadas atrás recurrió a incluir un cuerpo de leyes enmarcadas a las necesidades de la sociedad en relación con el desarrollo tecnológico e informático.

Este marco jurídico debería tener como característica primordial la prevención de las conductas delictivas de índole informática, así como la punibilidad (sanción) correspondiente, ya que en un primer momento estas conductas quedaban en la impunidad, posteriormente de inicial tuvo aparición en algunos códigos penales locales;

> Con anterioridad a la reforma al Código Penal Federal de 1999, sólo algunos estados de la República, como Sinaloa, Morelos y Tabasco, conscientes de la necesidad de legislar en esta materia, habían incorporado en sus ordenamientos penales normas tendentes a la protección de la información mediante la tipificación del delito informático y del de violación a la intimidad personal.
>
> La inexistencia, hasta antes de 1999, de tipos penales exactamente aplicables a esas conductas ilícitas daba lugar a la impunidad, de manera que resultaba imperativo prever en la ley estas nuevas formas de delincuencia. La magnitud de los daños que esas conductas pueden ocasionar depende de la información que se vulnere, la cual puede tener un fuerte impacto en el desarrollo de la economía y

> la seguridad nacionales, o en las relaciones comerciales, tanto públicas como privadas. (Landa, 2007, p. 241)

Dentro del estudio de los antecedentes encontramos que México como Federación prestó atención de los incidentes informáticos para establecerlos como delitos dentro del catálogo de delitos a nivel federal a través de la reforma de 1999, esta reforma tuvo consecuencias jurídicas de nueva aplicación, pero solo al ámbito Federal dejando fuera las conductas que podrían afectar a las personas dentro del fuero común:

> La iniciativa que presentó el Congreso mexicano y que dio origen a las reformas publicadas en el Diario Oficial de la Federación el 17 de mayo de 1999, propuso adicionar un capítulo al Código Penal Federal para sancionar al que sin autorización acceda a sistemas y equipos informáticos protegidos por algún mecanismo de seguridad, con el propósito de conocer, copiar, modificar o provocar la pérdida de información que contengan. Esta iniciativa dio origen al capítulo denominado Acceso ilícito a sistemas y equipos de informática. (Landa, 2007, p. 241)

Es importante precisar el momento en el cual el país empezó a poner énfasis en la seguridad que existía en el internet, pues a partir de esto el patrimonio informático de los habitantes y del gobierno mismo se vio involucrado en una relación directa y con nuevas necesidades jurídicas, por lo que más adelante se expidieron leyes locales y federales para brindar seguridad jurídica ante la vulneración de la información personal de los dispositivos de la época.

Además, varios códigos locales de las entidades federativas posterior a esta reforma federal dentro del transcurso de 1999 contuvieron dentro de su marco jurídico de forma limitada figuras de los delitos informáticos y otras más no, es decir tardaron tiempo después en contener dichas figuras al margen de

la ley debido a la poca utilidad y limitaciones de los dispositivos electrónicos de comunicación de la época, autores como Landa (2007) que respecto a lo dicho menciono lo siguiente:

> Así tenemos que los códigos penales de Aguascalientes y Tabasco establecen dichas figuras entre los delitos contra la seguridad en los medios informáticos y magnéticos; Baja California, en los delitos contra la inviolabilidad del secreto; Chiapas, Puebla, Querétaro, Zacatecas y Morelos, en los delitos contra la moral pública; Oaxaca, en los delitos contra la moral pública y en los delitos contra la libertad y violación de otras garantías, y Tamaulipas, en los delitos de revelación de secretos y de acceso ilícito a sistemas y equipos de informática. A su vez, el Código Penal para el Distrito Federal contiene una supuesta figura de fraude informático en los artículos 230 y 231, fracción XIV.
>
> Por su parte, los códigos penales de Baja California Sur, Campeche, Chihuahua, Coahuila, Durango, Estado de México, Guanajuato, Guerrero, Hidalgo, Jalisco, Michoacán, Nayarit, Nuevo León, Quintana Roo, San Luis Potosí, Sonora, Tlaxcala, Veracruz y Yucatán no contienen disposición alguna al respecto. (pp. 244-245)

Con lo anterior referido el estado mexicano como parte de las obligaciones que tiene con los gobernado como figura coercitiva al margen dentro de la ley, desde entonces ha buscado tener dentro de su legislación la manera de tener regulados a los infractores dentro del ciberespacio, expertos como Assolini (2019) durante la cuarta Cumbre Latinoamericana de Analistas de Seguridad organizada por Kaspersky refirió:

> Desde el 2014 además de Brasil, ciudadanos y organizaciones de México, Venezuela y Perú son víctimas de entre el 26 % y 36 % de los ataques en la red, añadió además que Brasil, junto a México y Perú,

lidera el desarrollo de este software malicioso que roba datos bancarios de los usuarios en Latinoamérica. (s.p.)

Estos datos porcentuales brindan un panorama de la situación contemporánea del estado de los delitos informáticos que afectan a nivel de américa latina y refieren la importancia y necesidad de definir una tipología delictiva que pueda poder procesar a este tipo de ciberdelincuentes, especializados en fraudes.

Lo anterior referido es concordante con lo dicho por el experto Assolini que está en concordancia con los investigadores Loredo Gonzáles y Ramírez Granados (2013) dentro del cual sostienen lo siguiente:

> A falta de capacidades para regular el contenido en la web, tanto por el volumen de datos, el número de usuarios y problemas de jurisdicción, el crear conciencia del uso responsable de Internet se ha vuelto un punto clave para la convivencia en una sociedad virtual, tanto para los ciudadanos como para empresas. Por ejemplo, cientos de empresas manejan información confidencial de sus clientes y es su responsabilidad asegurar la integridad de la información la cual puede caer en manos de grupos criminales quienes la utilizan para extorsiones telefónicas, suplantación de identidad, espionaje, etc. (p. 50).

En México el antecedente más relevante de forma contemporánea del cual la víctima fue de forma indirecta Estado Mexicano se trata del incidente donde se vio involucrada la paraestatal Petróleos Mexicano (Pemex), un conglomerado de petróleo y gas del estado mexicano, fue golpeado por un ataque de ransomware el cual bloqueó sus servidores, cifró archivos y detuvo algunos trabajos administrativos, dijo la compañía.

> En el secuestro de Pemex, el equipo cibernético ha exigido 565 bitcoins, o aproximadamente $5 millones, pagaderos antes de finales de noviembre para desbloquear los sistemas afectados, según los informes. A partir del jueves 14 de noviembre, los funcionarios de Pemex dijeron que el ataque cibernético estaba "totalmente bajo control", aunque varios empleados afirmaron que las operaciones aún no estaban en funcionamiento como de costumbre, informó CNBC. (Howard, 2019, s.p.)

Con estos antecedentes de delitos informáticos es necesario el análisis y compromiso de las autoridades para involucrarse de mayor forma y con mayor intensidad, en la investigación de los delitos informáticos.

1.5.- Fuentes del derecho en materia de delitos informáticos.

Para el estudio del derecho y la forma en como lo concebimos en la actualidad tiene que partir para su estudio a través de las denominadas fuentes del Derecho es decir que para que un conocimiento sea validado debe de atravesar distintas formas de comprobación utilización y fines, por lo que el derecho informático no es ajeno ni diferente al resto de sus diferentes ramas del derecho pues contiene también sus propias fuentes “podemos encontrar las fuentes históricas reales y formales en relación con las nuevas tecnologías telecomunicaciones y sistemas de almacenamiento” (Morales, 2015, p. 39).

Como sucede en muchos países en México no ha sido distinto el caso, durante el transcurso del tiempo se han detectado diversas formas de descomposición social por el uso de la informática y el internet, de tal manera que en el tiempo contemporáneo se encuentran en mayor crecimiento el número incidencia delictiva por la mayor accesibilidad a dispositivos de comunicación, ya que en los últimos años se ha incrementado el uso de las

tecnologías debido a que ha disminuido el costo de los aparatos de información y comunicación, (Jiménez, 2018).

Por ello ante el incremento de más dispositivos de información y comunicación es necesaria la consulta de las obras precursoras que han sido concernientes en investigar a los delitos informáticos o el cibercrimen, por ello para el estudio de los mismos es necesario recurrir a las fuentes históricas del derecho informático o de aquellas que influyan en el mismo.

Algunos autores refieren que se puede hablar de fuentes formal directa y fuente formal indirecta, tratándose de las directas aquellas normas jurídicas que tienen la observación obligatoria dentro de un territorio en específico que regulen a las tecnologías de información y comunicación, y como fuente indirecta aquellas que aunque no son de aplicación inmediata llevan correlación y han pasado por el proceso legislativo para poder inferir en el derecho informático, las cuales tengan o no vigencia, o por defecto que sean de vigentes en otro territorio (Morales, 2018).

Además, dentro de las fuentes del delito informático existe el debate si puede ser recurrida la costumbre como tal, en el caso concreto creemos que solo será aplicable la costumbre que sea reconocida por la ley, y no la costumbre del sentido común, esto referido en la opinión de Jiménez Rojas la cual nos dice:

> Fuente formal indirecta del derecho informático se debe entender al surgimiento de Los criterios, tradiciones, axiomas, opiniones y Consejos jurídicos que les dan vida, vigencia y permanencia a las instituciones del derecho informático, entre los cuales, Encontramos a la teoría, Costumbre, jurisprudencia y a los principios generales del derecho y estos pueden ser a nivel nacional continental o internacional (Jiménez, 2018, p. 27)

Dentro del estudio del derecho y la sociedad prevalecen algunas teorías filosóficas como la sociología jurídica, el realismo jurídico y la filosofía analítica jurídica, debido a que en cuanto hace a la sociología jurídica se entiende que el motivo de su sentido para utilizar y construir un nuevo conocimiento parte del objeto del estudio, es decir de la sociedad misma en el entorno en el cual viven, los medios climáticos del territorio, partiendo de la población hasta el gobierno por lo que se entiende que de una comunidad a otra, las necesidades y comportamiento dentro de la comunidad de sus individuos y así como de manera colectiva varían de población o población.

Por lo cual esta teoría que estudia el comportamiento humano puede ir en su estudio desde un sujeto de manera individual hasta el estudio del comportamiento de una sociedad misma debido a que las necesidades con el paso del tiempo cambian, y en virtud de que las condiciones no son las mismas de una década a otra o de una década en un siglo, por lo que esta herramienta para el derecho se vuelve fundamental para el desarrollo de la epistemología, por lo cual no puede dejarse fuera el enfoque teórico aplicable a los delitos informáticos.

Es importante que sea cual sea la Fuente de la cual emane conocimiento sobre el delito informático, se debe de tener en cuenta la naturaleza del conocimiento extraído y el entorno al cual será aplicable pues si bien es cierto que el derecho es un conjunto de normas, estas finalmente serán aplicables a una sociedad, por lo que no podemos decir que la norma vigente es la única fuente reconocida para el estudio del delito informático, esta deducción está basada en el comentario al respecto por Morales (2018) el cual dice:

> El derecho informático es ciencia, por el principio interdisciplinario, esto es, adquiere el carácter conceptual, teórico y práctico en relación con otras ciencias, como son la sociología, economía, política, administración, se informática, pedagogía, criminología, psicología contabilidad criminalística balística turismo historia gastronomía ciencias militares y policiacas etcétera. (p. 74)

Por ello con el uso de la tecnología surgen nuevas ramas dentro del mismo derecho informático, pues la tecnología propicia al surgimiento de nuevas conductas y necesidades y con ello el usuario se ve únicamente limitado por los lineamientos legales vigentes ya sea que estos sean a nivel local, estatal, federal o en su defecto internacional.

Las fuentes del derecho informático son importantes a considerar pues a partir de ellas se formarán los manuales de actuación y estrategias de combate al delito informático por ello, saber la dimensión de la misma ayuda a una mejor comprensión del panorama ante el cual los ministerios públicos se enfrentarán al desarrollar sus actividades investigativas.

CAPÍTULO II.

Relación de los delitos informáticos con el sistema penal acusatorio.

2.1.-Figuras consideradas como delitos informáticos a nivel local.

Para el análisis idóneo figura del delito debemos recordar su origen el cual proviene del latín *delinquere*, que significa, dejar, abandonar, alejarse del buen camino, una vez entendido esto no podemos iniciar de la definición del delito con una definición a nivel local de cualquier entidad federativa, debemos partir de la definición del orden Federal, esto recordando que las leyes no se pueden contravenir entre sí mismas, por lo que dentro del Código Penal Federal define al delito dentro del artículo 7 el cual a la letra dice: “Artículo 7o.- Delito es el acto u omisión que sancionan las leyes penales” (Código Federal, 2020 p. 5).

Con respecto a esto se deduce que todas las acciones u omisiones a un supuesto jurídico previsto en la ley penal, será considerada la conducta contraria a derecho, por tanto, será punible y será acreedor el autor de dicha conducta a una sanción correspondiente a la establecida dentro del mismo código, de tal manera va de la mano de la teoría positivista en relación al delito, “sustancialmente podemos considerar delito como una conducta típica antijurídica y culpable”. (castellanos, 2012, p. 171)

Con lo anterior referido se encuentra concordancia entre la teoría del derecho positivo y el contenido de la norma jurídica penal vigente dentro del territorio mexicano, lo cual posibilita el hecho de crear una figura más amplia dentro de las entidades federativas entendiéndose así, que la palabra de definición delito puede ampliarse al tratarse de un suceso especial, ya sea que esta definición se adapte de manera optativa u obligatoria por las

entidades federativas a través de una ley especial, refiriéndose a la adhesión de figuras delictivas correspondientes a delitos informáticos.

Lo referido en el párrafo anterior viene a contexto en un breve análisis comparativo de las diferentes leyes especiales que tenemos dentro de nuestro marco jurídico en el territorio mexicano, con lo cual se establecen figuras las cuales son punibles ante la ley y sancionadas por el estado para quienes incurran en estas conductas por acción u omisión, en este mismo sentido que podría ser la solución más práctica para agilizar la inclusión de los delitos informáticos en un solo capitulado especial a nivel Federal o en cada entidad, y con ello desaparecer la obesidad legislativa, como lo refieren algunos autores:

> El delito informático se encuentra descrito de igual manera en leyes especiales en diversas materias, por ejemplo: los delitos ecológicos descritos en la Ley Federal de responsabilidad ambiental; los delitos de trata de personas descritas en la ley general para prevenir, sancionar y erradicar los delitos en materia de trata de personas y para la protección y asistencia a las víctimas de estos delitos; así como otros delitos y faltas descritos en la ley de migración; Ley Federal contra la delincuencia organizada, ley de instituciones de crédito, Ley General de organizaciones y actividades auxiliares del crédito, ley del mercado de valores, ley general de instituciones y sociedades mutualistas de seguros, Ley Federal de instituciones de fianzas, ley de los sistemas de ahorro para el retiro, ley para regular las actividades de las sociedades cooperativas de ahorro préstamo, ley de sociedades de inversión, ley de ahorro y Crédito popular, ley de uniones de crédito, etc. Produciendo incertidumbre en los gobernados. (Morales,2015, p. 76)

Lo anterior referido concuerda de manera recurrente al mencionar la creación de una figura jurídica la cual se conoce como delito, la cual se encuentre en el código penal en lugar de una ley especial, ya que no se encuentra un capítulo especial de delitos informáticos a nivel Federal.

Esta medida es sugerida por académicos que en respuesta a la necesidad de la sociedad de que se legisle una ley especial ante el aumento del delito informático, por ejemplo, la ley Olimpia, esto se logró siguiendo el proceso legislativo que se conoce dentro del territorio mexicano, dicha situación es descrita de la siguiente manera:

> De manera recurrente, en el ámbito académico, existe la inquietud entre los noveles egresados de la Licenciatura en Derecho, para considerar como probable objeto de investigación el tema de los Delitos Informáticos, es decir, sugieren su inclusión, ya sea en el Código Penal Federal o en uno de carácter estatal, en razón a que perciben la ausencia de un Capítulo o un delito con tal denominación. (Piña,2015, p. 7)

Cabe mencionar que un delito informático aparece desde cuando una persona se apropia ilegalmente de información confidencial almacenada en un computador, en un correo electrónico, en un dispositivo móvil o USB, pero debe cumplir con el supuesto de que esta conducta se encuentre contenida dentro del marco legal punible donde se esté llevando a cabo la conducta.

Por ello es sumamente importante para las autoridades y ministerios públicos el estar informado sobre las acciones que se consideran delito informático ya que, no todas las conductas que dañen propiedad informática de una persona significa que esté tutelada como un derecho o quien realice esta conducta sea merecedor a un castigo punible:

> La doctrina del Derecho de la Informática, ha identificado tres alternativas de solución para hacer frente al problema jurídico que representa la sociedad informatizada, mismas que consisten en: 1) la actualización de la legislación, 2) la evolución jurisprudencial; y, 3) la redacción de leyes de carácter particular. Amén de ello, ha registrado los fenómenos que, por una parte, distorsionan las instituciones jurídicas y por otra, erosionan el ejercicio de los derechos y libertades fundamentales. (Piña, 2015, p. 1)

El contenido referido implica que las autoridades deben atender de cierta forma las lagunas del derecho vigente, pues existe la confusión entre delito informático y el delito clásico, la principal diferencia existente es que el delito informático vulnera la información y el dato privado de otra persona, mientras que el delito clásico informático es el ilícito realizado a través de medios electrónicos.

También se puede encontrar que dentro de los delitos informáticos el sujeto activo y pasivo juegan un papel con connotaciones o características, distintas al delito clásico o tradicional:

> Los sujetos activos. Las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y puede ocurrir que por su situación laboral se encuentra en lugares estratégicos donde se maneja información de carácter sensible. Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que le diferencia entre sí la naturaleza de los delitos cometidos. (Velázquez, 2007, s.p.).

Por otro lado, establece que el sujeto pasivo del delito informático es de vital importancia identificarlo, así como las características propias de este tipo

de víctimas, pues no solo son consideradas afectadas las personas físicas sino también las morales pueden ser vulneradas:

> En primer término, tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.
>
> El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos. (Acurio, 2016, pp. 18-19).

En un ejemplo práctico se puede decir que los correos e-mail donde se solicita dinero no deben ser considerados como un delito cibernético o informático pues en este supuesto sólo se ocupa como un medio por el cual se comete un delito clásico, pues podría equipararse el medio del correo como a través de una hoja o un intermediario.

Por ello al crear una figura o ley especial de delitos informáticos se debe considerar a los delitos informáticos con determinadas características, y en los estados que contemplan delitos informáticos las figuras son adheridas en el código penal local sin tener la atención en el tecnicismo desde la informática, complica la labor de investigación para el Ministerio público, por ello debe no legislarse con el uso único que le damos solo dentro del mundo del derecho, a la informática.

> La criminalidad informática está rodeada de una serie de términos y de conceptos que no son de fácil comprensión si no se está habituado a ellos. Por esta razón, la legislación —tanto sustantiva como procesal— ha de ir en sintonía con esta terminología. (Arocena y Esparza,2016, p. 67).

Debido a la discrecionalidad del acto delictivo con la cual se realizan estas conductas, ha tenido dado como resultado el nacimiento de la informática forense, misma que auxilia a los ministerios públicos para la investigación de este tipo de delitos que deben tener para su comisión conocimientos técnicos, por tanto, las aplicaciones de técnicas científicas y analíticas permiten identificar datos de prueba de forma licita dentro de un proceso penal. (DragonJar, 2015).

Un problema histórico de importancia en esta problemática al conceptualizar al delito informático es que los teóricos en México no se logran poner de acuerdo para formular un concepto único o al menos aproximado sobre el cual deba versar los delitos informáticos. “Los juristas mexicanos, no se ponen de acuerdo en la concepción y definición cuando abordan el tema de los delitos informáticos”. (Levet, Espinoza, Macgluf, Fragoso, 2019, p. 11)

Este problema se puede identificar que viene desde la teoría jurídica, la atención de los delitos informáticos no logra ponerse en los reflectores para su estudio por parte del derecho para poder llevar la discusión de uniformidad de criterios y enfoques con ello de forma procedente legislar de manera adecuada y con ello ofrecer una herramienta procesal más apta al ministerio público para poder investigar los delitos informáticos.

Las figuras delictivas de delitos informáticos ya operan en diferentes países del mundo, y debido a que en nuestro sistema de justicia penal se rige por el principio de inocencia la atención de delitos informáticos en México a nivel local se ve rebasada por la legislación, ya que no se puede actuar sin

legalidad por parte del estado o de los ministerios públicos, pues todas sus actuaciones deben estar fundadas y motivadas en la ley.

Con esto referimos que las imputaciones hechas por el estado a través de los ministerios públicos a los ciudadanos, deben estar siempre dentro del marco legal vigente y debidamente fundamentada, respetando la legalidad en concordancia con el máximo ordenamiento legal en México, el cual está establecido debidamente en el artículo 14 constitucional, el cual refiere sobre la legalidad con la que las autoridades del Estado Mexicano deben conducirse (Constitución, 2020).

De acuerdo al texto constitucional referido no se puede atribuir un castigo a una persona sin que esta conducta se encuentre contenida en un texto punible vigente y comprobable únicamente bajo un tribunal competente, y esto va acorde a los principios teóricos de la teoría positivista en donde analógicamente se presume que no hay delito sin ley o tipo penal previo a la conducta realizada si esta no está legislada y condenada como punible, esto de acuerdo al principio doctrinal:

> nullum crimen nulla poena sine lege: Este es un principio legal básico que ha sido incorporado al Derecho penal internacional, prohibiendo la creación de leyes ex post facto que no favorezcan al imputado. *(Anselm, 1801, s.p.).*

Con lo anterior podemos referirnos de igual manera al artículo 16 constitucional el cual nos refiere de los procedimientos a seguir por asuntos del orden criminal, es decir que para la atención de delitos informáticos en el ámbito local es necesario su implementación en los códigos penales locales.

Las leyes procedimentales deben contener los medios adecuados a seguir por los fiscales ministerios públicos, esto con la finalidad de no violentar los derechos de los probables responsables de un delito informáticos

afectando sus derechos de libertad consagrados en el 16 constitucional que establece que solo podrán ser sujetados los gobernados a los actos de molestia por una investigación solo aquellos que sean por un mandamiento escrito y por una autoridad competente, de lo contrario no solo puede violarse los derechos humanos y procesales de una persona sino que además, la autoridad por actuar por analogía puede ser acreedora a una sanción por abuso de poder.(Constitución, 2020).

Es decir que la constitución protege los derechos humanos de todas las personas que se encuentren en el territorio mexicano, por tanto, no podrán ser molestados por ninguna autoridad sin una orden de aprehensión o causa legal que lo ordene, también el artículo 16 menciona:

> Toda persona tiene derecho a la protección de sus datos personales**,** al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. (Constitución, 2020, p. 45).

De la misma manera la constitución protege el derecho a la información de los datos personales y a mantenerlos en reserva o secrecía si es la decisión del gobernado, y de igual manera establece sólo las formas en las cuales se podrán disponer de ellos, además es reiterativa al mencionar que sin un una orden de aprehensión y proceso con principio de inocencia no se podrá condenar a una persona. (Constitución, 2020,)

Finalmente establece la propia constitución que las comunicaciones están protegidas y que no podrán ser violadas por una investigación de una autoridad sin una orden para hacerlo, sin embargo, el ministerio público necesita dar una causa justificada para ello:

> Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley. (Constitución, 2020, pág. 50).

Señalado esto debe por ende la ley o norma jurídica aplicable al caso, reunir el requisito indispensable de ser tácita y explícita para poder ser aplicable, pues de lo contrario la autoridad incurre en actos jurídicos con características autoritarias e ilegales con los gobernados.

En México ha existido delitos informáticos aun antes del desarrollo de la red 4.0 o Tecnologías de Cuarta Generación, aún antes de que se implementara en la constitución la reforma al sistema penal del 2008 donde cambia el paradigma del sistema de justicia penal mexicano.

Al respecto de lo anterior referido, se implementó en el territorio del país un único procedimiento penal el cual es predominantemente oral, es decir que se tiene en la realidad presente del territorio mexicano averiguaciones previas dentro de los juzgados aún en proceso o no concluidos, con el cambio de sistema penal cambió la denominación de las averiguaciones previas a carpetas de investigación, este cambio no han resuelto el problema al que arrastra a la sociedad con las afectaciones que sufren por los delitos informáticos, por lo que el objeto de estudio incluye las herramientas dentro de la ley en el código nacional de procedimientos penales, para determinar la eficacia de este proceso penal y el desarrollo del procedimiento.

El sistema de administración de justicia penal anterior a la reforma del 2008 el ministerio público era denominado como Autoridad, y este sistema

dejaba sin actuación a la víctima y la mera confesión del imputado era suficiente para la condenatoria del mismo por el juez, contrario con el sistema acusatorio que se implementó de manera forzada por los estados en el 2016 derivado de la reforma del 2008 es caracterizado por sustentar las imputaciones y sentencias sobre las pruebas ofrecidas para sustentar las mismas, de esta manera ambos sistemas no contemplan la dificultad del encuadre legal de las figuras dentro de sus marcos de investigación debido a la naturaleza específica de estos delitos informáticos.

Realizando una comparación entre el ordenamiento legal que ha tenido México en materia de delitos informáticos y algunos aplicados por otros países se puede identificar un rezago en la legislación mexicana en comparación con otros países Alemania desde 1986 contempla delitos informáticos en su legislación, Australia desde 1987 en su marco penal también contiene delitos informáticos, otro de los países europeos que tiene desde hace más de dos décadas este tipo de delitos es Francia desde 1988, además conforme el internet fue avanzando en la década de los 90s países como Holanda en 1991 y Holanda en 1993 adicionaron sus primeras figuras punibles en su legislación, por su parte en el continente americano chile en 1993 y estados unidos en 1994 fueron los primeros precursores en atender este tipo de delitos. (Acurio, 2016).

En México las primeras legislaciones con características de protección del patrimonio informático misma que entró en vigencia hasta el 24 de marzo de 1997 en la Ley Federal del derecho de Autor, dado que la misma fue publicada el 24 de diciembre de 1996 la cual pretendía proteger que los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito.

De tal manera es interesante recalcar que algunos estados dentro del territorio mexicano se preocuparon durante este periodo para legislar en

materia de delitos informáticos dentro de su ordenamiento local, pero solo el Estado de Sinaloa contiene en su marco legal un capitulado denominado como tal “DELITOS INFORMÁTICOS”, con el cual se buscó ofrecer protección a la población de este tipo de conductas ilícitas dentro del ordenamiento jurídico Código Penal del Estado de Sinaloa, el cual dice;

> Título Décimo "Delitos contra el patrimonio" Capítulo V Delito Informático Artículo 217. Comete delito informático, la persona que dolosamente y sin derecho:
>
> I. Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información;
>
> II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.
>
> Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa. (Código Sinaloa, 1997, p. 35)

Con respecto a esta figura dentro de la legislación en Sinaloa, se encuentra en comparación con los alcances tecnológicos de la actualidad rebasada, esto en cuanto al tecnicismo de los dispositivos que existen en la actualidad, esto basado en la definición que tenemos dentro de la investigación de delito informático, así como el alcance del tecnicismo de los dispositivos con el cual se realiza su funcionamiento, no obstante, este ordenamiento reconoce como bien jurídico tutelado el patrimonio informático.

En México las legislaciones a pesar de que han coexistido el nivel local y Federal no ha existido una armonía en un mismo sentido sobre el contenido requerido para atender de manera uniforme en todo el país a los delitos informáticos, por lo cual dificulta para los Fiscales Ministerios Públicos la investigación de conductas delictivas de colaboración entre corporaciones dentro del territorio mexicano y mucho más fuera del mismo.

Esta afirmación debe ser considerada pues el país actualmente en cuestión tecnológica vive de manera casi uniforme en cuanto al avance tecnológico, por lo que tener un capitulado único donde contenga previstos los nuevos avances tecnológicos en la Telemática beneficiaria a todos, esta afirmación del avance tecnológica concuerda con la opinión del Investigador Temperini que dice:

> El incremento de tecnología disponible, tanto para el delincuente como las víctimas, combinado con el escaso conocimiento o información sobre cómo protegerse de los posibles delitos que se pueden sufrir a través de las nuevas tecnologías, otorga a los delincuentes las llaves a las puertas de un inmenso campo fértil de potenciales víctimas de ataques. (Temperini, 2013, s.p.).

Los fiscales ministerios públicos se encuentran en desventaja ante las diferentes formas que se desarrollan a diario, y no pueden negarse a recibir una denuncia por lo cual pueden superar las figuras de crimen informático a las capacidades de investigación de un ministerio público.

2.2.- Procedimientos aplicables en el sistema adversarial con los delitos informáticos.

En México el panorama jurídico vigente en el área penal tuvo su origen a partir de la reforma constitucional/penal del 8 de junio del año 2008, dicha reforma no solo modificó el proceso penal y el procedimiento dentro del

mismo, esta reforma implicó un cambio dentro de todo el sistema penal como tal, es decir que dicha reforma implicó una transformación profunda dentro de las instituciones, personal administrativo, nombramientos, jerarquías y reglas procedimentales.

A través de dicha reforma las atenciones a los delitos serían atendidos con mayor celeridad jurídica, además otorgaría a los gobernados mayor certeza jurídica, por lo que dicha reforma al sistema acusatorio penal devolvería la confianza en las instituciones y corporaciones encargadas de la procuración, administración e impartición de justicia.

La implementación de un nuevo sistema de justicia penal implica retos y reacciones en la sociedad en la cual será aplicada la funcionalidad del propio sistema, puesto que a menudo surge el cuestionamiento sobre las comparativas entre el sistema que entra en vigor con aquel que se queda abrogado o derogado por el transcurso del tiempo y las necesidades de la población.

A su vez es necesario cuestionarse si de un sistema a otro se logró un cambio y con ello una transformación entre la atención de los delitos que son tratados por las autoridades, este análisis implica identificar si existe una evolución en el propio sistema o identificar si se trata de una simulación en la impartición de justicia penal en México.

Cabe mencionar que el referido sistema penal en México se encuentra en transición a pesar de estar implementado el inicio y vigencia de su operatividad en el año del 2016 a nivel nacional, y que algunos estados iniciaron con este sistema desde unos años antes, como el caso del estado de Morelos, y en otros como el estado de Guerrero entró en operaciones hasta el año 2016, donde a pesar de encontrarse en el año del 2020 siguen aún procesos abiertos anteriores al 2016.

Es decir que el estado de guerrero se encuentra en operaciones de ambos sistemas y que poco a poco la transición de un sistema a otro está ocurriendo y es necesario hacer la comparativa en el caso que nos ocupa, saber si los delitos informáticos han sido atendidos en su debida manera tanto en un sistema como en otro, pues recordemos que toda comisión de un delito denunciado y no condenado, es sinónimo de impunidad.

La transición e implementación de un sistema jurídico a otro distinto en México no ha sido satisfactorio para algunos académicos pues consideran ha sido deficiente, con careciente falta de personal que no practique los abusos del viejo sistema y pueda dar un servicio de calidad, dando como resultado un sistema sin recursos, con la opacidad de los niveles estatal y federal, dando como resultado un sistema carente de aceptación social. (Ramírez, 2018).

El objeto de estudio de los delitos informáticos en relación al sistema acusatorio penal acusatorio y oral vigente en el territorio mexicano no ha terminado de realizarse, pues visto desde la visión legislativa los avances tecnológicos no están siendo contemplados de manera procedimental ya que como hemos referido con antelación los delitos informáticos tienen que tener su debida atención debido a su origen y características propias, pero dentro de la cual refiere que si ha intentado el poder legislativo intención de reformar e incluir un tratamiento distinto a los delitos informáticos, así como la forma adecuada de tratarlos desde la perspectiva técnica.

Es decir, los cibercriminales están usando a su favor las debilidades propias del equipo de información y comunicación, combinándolas con la evolución de la misma, ya que con ello se dificulta entender quién es el responsable principal por la seguridad de un equipo de información.

Aunque en México pareciera que no hay interés mínimo en combatir el cibercrimen en la cámara de diputados se ha enviado un dictamen para incluir

a los delitos informáticos, el cual fue publicado en la gaceta parlamentaria número 5013 del 26 de abril de 2018 particularmente en el anexo XII de dicho órgano de difusión. (Levet, Espinoza, Macgluf, Fragoso, 2019)

Este dictamen pretendía anexar en las reglas procedimentales obtención de evidencias digitales de forma licita y en tiempo real, sin violar los datos personales o privacidad de las personas, sin embargo, no fue aceptado. (Levet, Espinoza, Macgluf, Fragoso, 2019).

No obstante en México los fiscales ministerios públicos se encuentran con un reto jurídico importante en su labor de indagatoria de este tipo de incidentes o conductas delictivas que no se encuentran registradas en un solo ordenamiento legal, en México es el caso donde algunos de sus delitos se encuentran contemplados en leyes especiales, y no en los códigos penales federal o local, lo cual dificulta el encuadre exacto de una conducta delictiva para poder desarrollar una acusación formal ante un tribunal competente.

Con lo anterior dicho es notorio que el poder legislativo necesita auxiliar al poder judicial y ejecutivo para la atención de los delitos informáticos dado que su atribución y facultad vigilar por la adecuada legislación que formule la protección de los derechos humanos de los gobernados y con esto el estado pueda ofrecer seguridad jurídica a los mismos.

Para esto es necesario reforzar los ordenamientos penales de forma adecuada de manera sintética, y no recurrir a la acción conocida como obesidad legislativa, la cual consiste en expedir leyes especiales para cada caso específico, con ello se evita aumentar el problema del exceso de leyes que se generan por tener leyes no concretas y extensas:

> La multiplicidad de leyes es algo que lastima a las repúblicas. Las leyes, cuando son muchas, no causan otra cosa que trastornos y

> complejidades. Muchas leyes se olvidan y en ese olvido no pueden respetarse, por lo que se desprecian. La sencillez de la ley produce su admiración y respeto. La abundancia de leyes, su desprecio e ignorancia. Cuando hay muchas leyes, se contradicen unas a otras, y hacen nacer diversas interpretaciones u opiniones maliciosas, de donde nacen los litigios y las desavenencias. (Saavedra, 2003, s.p.)

Las leyes son cambiantes pero en ningún momento pueden dejar ciudadano esté fuera del amparo de la ley, además produce efectos negativos dentro de las instituciones encargadas de la investigación de delitos pues se crean confusiones, pérdidas de tiempo por mal encauzar una investigación o la dilatación de gestión investigadora, además de un mal uso de recursos en la investigación de delitos por parte del ministerio público, y las policías que colaboran en la investigación de delitos informáticos en colaboración con los ministerios públicos.

No sólo encontramos que el poder legislativo Federal no ha puesto énfasis en la atención y tratamiento adecuado de los delitos informáticos al no contemplarlos en una sola ley, sino que además encontramos que el Poder Ejecutivo Federal de igual manera en su agenda de trabajo para la seguridad tampoco tiene contemplado o al menos referido, el énfasis en voltear a ver el campo informático y las conductas que se desarrollan de manera constante a diario dentro de todo el territorio nacional.

Lo cual nos refiere que el estado Mexicano y las normas que emanan de él, no va en concordancia con los avances tecnológicos que sufre la población dentro del Siglo XXI dado que debido a la espacialidad y naturaleza de los delitos informáticos, las diferentes formas que nos ofrece la telemática, bases de datos y demás medios de comunicación y almacenamiento pueden no encontrarse dentro de la territorialidad y jurisdicción del Estado Mexicano, por

lo que esto nos habla de la vulnerabilidad de las leyes mexicanas ante el fenómeno de la ciberdelincuencia el cual está delimitado a todo el mundo.

En referencia con el periodo presidencial actual correspondiente del 2019 al 2024 no contempla en su plan de desarrollo, la atención de los delitos informáticos o cibernéticos, por lo cual la discusión en las aulas de las universidades y foros para estudiosos del derecho es importante. (Levet, Espinoza, Macgluf, Fragoso, 2019).

Con lo anterior referido se puede prever que no bastará con crear una ley con un enfoque literal o específico, es necesario que para que el ministerio público logre una efectividad en su investigación, la ley con la que trabaje y sustenta sus acusaciones es necesario se encuentre sustentada en un real conocimiento del campo por parte del legislativo al momento de crear los tipos penales o leyes especiales correspondientes a los delitos informáticos.

Además, en cuanto hace al contenido del código nacional de procedimientos penales, no establece un mecanismo en el cual los ministerios públicos puedan actuar de forma idónea para la investigación de estas conductas delictivas llamadas delitos informáticos.

Esto conlleva a la premisa de replantearse la teoría del delito informático y adecuarla a las nuevas necesidades tecnológicas con las cuales se cuenta en la actualidad las cuales llegaron de forma permanente en el modus vivendi de las personas, volviéndose con ello una necesidad a mediano plazo el repensar nuevas formas de conceptualizar este tipo de delitos y debido a el daño que ocasionan y la forma en que el estado las persiga al ser punibles.

2.3.- Tratamiento de los delitos informáticos por las fiscalías de los Estados.

Respecto al registro de los porcentajes de incidencia delictiva el INEGI a través de la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) 2018 establece tres puntos importantes:

> Se estima en 25.4 millones el número de víctimas de 18 años y más en el país durante el 2017.
>
> El 35.6% de los hogares del país contó con al menos un integrante como víctima del delito.
>
> En 93.2% de los delitos no hubo denuncia, o bien, la autoridad no inició una averiguación previa o carpeta de investigación (INVIPE, 2018, p. 1).

Como se ve referida en dicha información, no se precisa si existe una incidencia delictiva en cuanto a delitos informáticos por lo cual es importante que los estados conozcan el grado de incidencia delictiva que están teniendo en materia de delitos informáticos.

El panorama dentro del territorio mexicano legislación local se encuentra poco trabajada por lo que lo vuelve tierra fértil para la comisión de delitos informáticos ya sea de sujetos activos del delito dentro del territorio nacional o fuera de él, respecto a esto es importante mencionar que en estadísticas privadas si se está contemplando a manera de estudio la forma de prevención de este delito debido a que cuando es dañado el patrimonio informático el ciudadano no encuentran la forma idónea interponer una querella o denuncia ante una autoridad competente por este vacío legal de delitos informáticos dentro del cual el sitio INFOBAE refiere el 10 junio de 2019 lo siguiente:

> México es el país que más fraudes cibernéticos registra en América Latina. Datos de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), muestran que

> **cada** hora se cometen 463 delitos de esta naturaleza en operaciones por comercio electrónico y banca móvil.
>
> Entre 2017 y 2018, 8 de cada 10 empresas en el país sufrieron al menos un ataque una vez al año, según la consultora de seguros Towers Watson. Por su parte, el año pasado se reportaron un promedio de 333.000 mil casos al mes, lo que significó un **crecimiento del 37%** con respecto al año anterior. (INFOBAE, 2019, p. 3)

Los datos mencionados hablan del crecimiento de delitos informáticos, y del daño económico que está provocando entre las empresas, con ello se puede ver la inseguridad mediante la cual están expuestas las personas morales y físicas en su patrimonio. Donde sí se habla del daño económico que en México generan este tipo de delitos el crecimiento va de los **276,000 en 2013, a 3.1 millones en 2018 y que USD 2 billones** en el año del 2019. (INFOBAE, 2019)

Pero no todo es alrededor de las empresas, las personas sufren la suplantación de identidad sin saberlo, esto con el motivo de darle usos delictivos a la información personal o bancarias de las personas a quien roban sus datos personales, por ello se ha hecho común la redirección a través de enlaces que envían a sitios maliciosos, los cuales son enviados por correo, y redes sociales o de mensajería social. (INFOBAE, 2019).

Encontramos interesante lo referido por este sitio web contrastado con las estadísticas del INEGI ya mencionadas con anterioridad ya que si bien es cierto en ambas se muestra un estimado de las afectaciones delictivas, las estadísticas del INEGI solamente abarcan a delitos comunes reconocidos por la ley, mientras que en la referida por el sitio web INFOBAE contiene dentro de ella la cifra oscura aproximada de las empresas sufren por delitos informáticos.

De tal modo que aún queda en incertidumbre jurídica saber el porcentaje de las afectaciones de los delitos informáticos hacia las personas físicas, debido al alto número de dispositivos de comunicación que se maneja por persona, en un ejemplo hipotético se puede referirse a que por cada persona mayor de 18 años contiene al menos un teléfono celular, una computadora, tableta, Smart TV, etc. Con este caso hipotético debe surgir la necesidad de cuantificar cuántas personas están acudiendo a las fiscalías de las diferentes entidades federativas a denunciar un delito informático o si sus afectaciones están siendo atendidas de manera adecuada.

Con base en lo referido en el párrafo anterior, se considera necesario un breve análisis a la ley que regula los delitos informáticos de manera vigente en al menos 3 entidades federativas por lo cual se analizó el contenido del código penal del código penal del Estado de Morelos, Código penal del Estado de Guerrero, y Código penal del Estado de Querétaro que a la letra refiere:

CÓDIGO PENAL DEL ESTADO DE MORELOS:

CAPÍTULO VIII DE LOS DELITOS INFORMÁTICOS NOTAS: REFORMA VIGENTE. - Vigencia: 2010/10/21. ARTÍCULO *148 quarter. - Comete el delito informático, la persona que dolosamente y sin derecho: I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red; III. Haga uso de la red de Internet utilizando cualquier medio para realizar actos en contra de las personas o cosas, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, para

perturbar la paz pública o que atente contra el orden constitucional; y IV. Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa. (Código, Morelos, 2020, p. 122).

En este código local del estado de Morelos si tiene como tal un capítulo el cual hace referencia a la punibilidad del delito informático o del cibercrimen, además prevé diferentes formas de dañar al bien informático de una persona, en cambio en el estado de Guerrero van encaminados a la pornografía, la suplantación de identidad y la difusión de imágenes o videos no consentidos con contenido sexual, los cuales no fueron agregados hasta el 2019 y si bien es cierto que en el código penal del estado de Guerrero no cuenta con un capítulo especial denominado como delitos informáticos la entidad si está vigilando de cierta forma este fenómeno.

Haciendo la comparativa de la entidad Guerrerense respecto a su marco legal de delitos informáticos con la legislación contenida dentro del código penal del estado de Querétaro, encontramos que tampoco tiene un capitulo denominado como delitos informáticos, sin embargo, esta legislación penal contempla figuras punibles distintas a las contenidas en el estado de Morelos y Guerrero, textualmente refiere lo siguiente:

CÓDIGO PENAL DEL ESTADO DE QUERÉTARO:

TÍTULO SÉPTIMO DELITOS CONTRA LA INVIOLABILIDAD DEL SECRETO Y EL ACCESO ILÍCITO A SISTEMAS DE INFORMÁTICA (Ref. P. O. No. 24, 22-IV-11) CAPÍTULO I REVELACIÓN DE SECRETO (Ref. P. O. No. 24, 22-IV-11) ARTÍCULO 159.- A quien teniendo conocimiento de un secreto, o estando en posesión de un documento, grabación, filmación o cualquier otro objeto que se le hubiese confiado, lo revele o entregue, sin consentimiento de quien tenga derecho a

otorgarlo y que pueda causar daño para cualquier persona, se le aplicará prisión de 3 meses a un año y hasta 20 días multa o trabajo en favor de la comunidad hasta por tres meses. Si el que divulgare el secreto, documento, grabación, filmación u objeto, lo hubiera conocido o recibido por razón de su empleo, cargo, profesión, arte u oficio, la pena de prisión será de uno a 5 años, hasta 50 días multa y suspensión en sus funciones de 2 meses a un año. ARTÍCULO 159 BIS. El que para descubrir los secretos o vulnerar la intimidad de otro, sin el consentimiento de éste, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación, se le impondrán de seis meses a tres años de prisión y de cien a trescientos días multa. CAPÍTULO II ACCESO ILÍCITO A SISTEMAS DE INFORMÁTICA ARTÍCULO 159 TER. Al que, sin autorización, por cualquier medio ingrese a sistemas informáticos, destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos protegidos o no por algún sistema de seguridad, se les impondrán seis meses a dos años de prisión y de cien a trescientos días multa. protegidos o no por algún sistema de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos o no por algún sistema de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa. Las penas señaladas en el párrafo anterior se aplicarán a aquellos que, teniendo autorización para ingresar al sistema informático, hagan uso

> indebido de la información, para sí o para otro. ARTÍCULO 159 QUATER. Al que, sin autorización, por cualquier medio ingrese a sistemas informáticos, destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos del Estado, protegidos o no por algún sistema de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos o no por algún medio de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido o no por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a setecientos cincuenta días multa. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en cualquier empleo, puesto, cargo o comisión de carácter público. (Queretaro,2020, p. 44).

Este de gran observancia mencionar que código penal del estado de Querétaro no cuenta con un capítulo especial de delitos informáticos, sin embargo, cuenta con amplia categoría de delitos informáticos y su forma detallada de prever la comisión de un delito es apropiada solo para el acceso no autorizado, lo cual dará ventajas a la acreditación de los delitos en comparación con los estados de Guerrero y Morelos por parte de los ministerios públicos para poder realizar su trabajo de investigación de forma idónea.

Dentro del breve análisis entre 3 legislaciones distintas de cada uno de los estados, se puede analizar y deducir que la capacidad en cuanto al funcionamiento indagatorio por parte de la fiscalías es distinto debido a que la legislación de cada estado contempla como bien jurídico tutelado a la información de las personas, sin embargo varía la denominación y definición de la conducta penal, por tanto se prevé de cierta manera formas distintas en las cuales los dispositivos de comunicación a través del internet son utilizados por las personas y la interacción que realizan con ellos, sin embargo no es uniforme la legislación en cuanto al tipo penal.

Con esto podemos identificar que la acción investigadora de un estado a otro se puede ver impedida ya que los ministerios públicos se encuentran capacitados en cuanto al lenguaje jurídico y técnico de su legislación local, sin embargo la forma adecuada de investigación que deben integrar dentro de los parámetros que establezca el código Nacional de Procedimientos Penales es general para proceder con la forma adecuada de imputación hacia un sujeto que infrinja el capitulado de los delitos del fuero común del Código Penal de la entidad.

De tal forma que la legislación que de Querétaro y Morelos la cual se diferencian en el tecnicismo limitado y con fines distintos con lo cual se abre la posibilidad de investigación por parte de los agentes de ministerio público, pero a la vez se dificulta la colaboración para investigar un delito ya que entre un estado y otro cambian de manera total el sentido de los artículos y legislaciones penales.

En cierta manera están relacionados en el estricto sentido de que el estado castiga el mal uso de las tecnologías de información y comunicación, por lo que las conductas que no se encuentren previstas en los códigos penales no podrán apoyarse de las figuras conocidas como delitos

equiparados para poder imputar de forma de alguna una conducta penal a un ciudadano.

Finalmente encontramos que la legislación dentro del estado de Guerrero no resulta ser retrasada debido a que se reconoce la información como bien jurídico tutelado en algunos de sus artículos, ya que para la ley dentro del Estado de Guerrero la informática no solo sirve como el medio para cometer un ilícito sino que también puede ser el bien jurídico transgredido, de tal manera que los ministerios públicos estarán limitados sólo en las reglas procedimentales que establezca el código nacional de procedimientos penales para imputar un delito ya que dicha legislación como se ha referido no contiene un capítulo especializado en la indagación y comprobación de delitos informáticos.

Debido a que el Ministerio Público actúa en representación del estado tendrá que manejarse bajo los estatutos de la ley de lo contrario podría incurrir en responsabilidades administrativas y penales en el caso de intentar formular una acusación contra un probable responsable por la comisión de un delito por simple analogía, o por no respetar las formas procedimentales para la obtención de prueba, pues no presentara una acusación basada en supuestos jurídicos que la ley contemple como ilegales, sino como una forma subjetiva por parte del ministerio público a cargo de la investigación lo cual sería violatorio de los derechos humanos de los ciudadanos.

2.4.- El funcionamiento de la policía en colaboración con los ministerios públicos.

El ámbito espacial de la investigación de delitos en términos jurídicos se le denomina jurisdicción y sirve para la organización de operación del estado,

con ello queremos decir qué una corporación solamente podrá investigar un delito dentro de su jurisdicción o territorio asignado.

Lo anterior referido entra en conflicto con el desarrollo de las nuevas tecnologías puesto que cuando éstas se utilizan en un sentido negativo o con intención de lacerar el bien jurídico tutelado de alguien más, y para este hecho no necesariamente se tiene que encontrar presencialmente el sujeto activo del delito dentro del mismo espacio geográfico que el sujeto pasivo del delito, por ello es importante estudiar y descubrir nuevas formas de investigación sin vulnerar los derechos de las personas, y a la vez que estas formas ayuden a los cuerpos del orden público evaluar si sus estrategias son efectivas en el combate al crimen cibernético.

Con lo referido nos lleva al hecho de que estas investigaciones realizadas por el ministerio público no sólo se limitan a un municipio, estado o país, sino que este fenómeno es de ámbito internacional, por lo que para su estudio debemos usar el sentido de la complejidad dialéctica interdisciplinario, como lo establecen autores como Leonardo, Rodríguez, Pascal, Rodríguez (2015) en su obra pensamiento complejo y ciencias de la complejidad:

> De este modo, se consolidan y expanden redes internacionales de cooperación y de investigación en sistemas complejos, cuyas líneas de trabajo comprenden tanto las ciencias físico-naturales, las ciencias de la computación y la matemática, como las ciencias sociales, incluyendo la antropología y la arqueología. De esta manera, asistimos a la configuración de un espacio de investigación de vocación verdaderamente transdisciplinar. (p. 191)

En México, la policía ministerial, estatal, o la nueva corporación denominada Guardia nacional funge un papel determinante en el trabajo del ministerio público pues podríamos denominarlos como los brazos operativos

de los ministerios públicos, es tanto así que desde él se buscó la colaboración de los 3 niveles de gobierno para la investigación de los delitos el cual se llamó, Convenio de Colaboración que celebran la Procuraduría General de la República, la Procuraduría General de Justicia Militar y las Procuradurías y Fiscalías Generales de Justicia de las entidades federativas, esto buscando a la colaboración entre instituciones.

Además, a través de la colaboración se busca subsanar dificultades de investigación, entre otros factores como son la espacialidad, limitantes de conocimientos, también cómo pueden ser la carga laboral o el presupuesto económico que el estado les brinde para la realización de estas actividades, dicho de esta manera la colaboración no es solamente una mera intención de ayudarse entre corporaciones si no es el fin que el estado busca para su perfeccionamiento.

Los policías generalmente son las primeras autoridades en tener conocimiento o llegar a la escena del crimen, por lo que estas autoridades deben estar al tanto de las reglas de operatividad a las cuales el ministerio público está sujetado para la investigación adecuada de un ilícito, pues de no hacerlo cuando los policías no actúan bajo los protocolos establecidos se dañan los derechos humanos de los presuntos responsables, lo cual pone en peligro la acusación sustentada del ministerio público ante el juez de control constitucional..

Las carencias de las corporaciones policiacas no han sido subsanadas aun con la implementación del nuevo sistema acusatorio, por lo que es poco recomendable a las corporaciones su baja efectividad en la investigación de campo de los delitos, es decir que si bien para la investigación de un delito común como el homicidio donde se ocupa gasolina, personal humano y material para asistir a la atención de dicho suceso, para la investigación de un

delito informático vuelve más problemática la investigación de la misma por las carencias materiales y logísticas de las corporaciones dadas sus limitadas instalaciones proporcionadas por el estado.

Desafortunadamente, las modificaciones normativas no han venido acompañadas de un impulso económico para las policías, y ello, se deduce que nuestros policías viven una situación crítica porque la mayoría ni siquiera cuentan con el piso mínimo para realizar sus funciones: su vida profesional transcurre con jornadas laborales irracionales y salarios muy bajos; y, en algunas corporaciones, deben pagar por sus uniformes, municiones o por la reparación de las patrullas, por lo que conociendo estas limitantes debemos profundizar en la búsqueda reiterada de modelos los cuales sirvan para salir de esta crisis social.

En México las policías cibernéticas citando el caso de la ciudad de México las líneas de acción la Policía de Ciberdelincuencia Preventiva realiza:

- Monitoreo de redes sociales y sitios web en general.

- Pláticas informativas en centros escolares e instituciones de la Ciudad de México, con el objetivo de advertir los delitos y peligros que se cometen a través de internet, así como la forma de prevenirlos, creando una cultura de autocuidado y civismo digital.

- Ciber Alertas preventivas las cuales se realizan a través del análisis de los reportes recibidos en las cuentas de la Policía de Ciberdelincuencia Preventiva.

Y en base al gran número de tareas que deben realizar para auxiliar al ministerio público, por tanto, también las policías cibernéticas deben estar capacitadas y financiadas con el equipo adecuado para poder realizar sus funciones de operatividad e investigación de delitos.

Por otro lado, ver una buena policía inspira confianza desde la sociedad la cual es quien debe denunciar los actos delictivos, aunque de acuerdo con esto el INEGI refiere que la falta de cultura para denunciar sigue siendo un fenómeno recurrente de lo cual refiere:

> Debido al problema que representa la denominada “cifra negra” (registro de delitos) en los registros administrativos de delitos, las encuestas de victimización se constituyen en la alternativa para hacer la aproximación más apegada a la realidad del fenómeno de la delincuencia. Las encuestas de victimización, a pesar de su enorme valor para proporcionar información sobre la victimización de personas, hogares o empresas del sector privado, no permiten medir delitos en los que no hay una víctima directa o donde la víctima no es una persona (delitos sin víctima identificable), tales como el lavado de dinero, el tráfico de drogas, de armas o de personas, entre otros. Así, las encuestas de victimización, como es el caso de la ENVIPE 2018, captan únicamente delitos que afectaron de manera directa a las víctimas y que ocurrieron durante 2017 a hogares y a personas de 18 años y más, integrantes de los hogares. (ENVIPE, 2018, s.p.).

Por lo que, al enfrentarse al cambio de un sistema penal, como ha sido el caso concreto del sistema vigente en el territorio mexicano, debe tenerse contemplada también de igual manera, las corporaciones encargadas de la seguridad, es decir las autoridades de campo, debido a que por su naturaleza, estas deben estar capacitadas para afrontar de forma directa el crimen y tomar las medidas pertinentes para salvaguardar el bien jurídico tutelado de ser posible o en su defecto para la persecución adecuada del probable responsable.

Conforme a esto dentro de un artículo de la Revista semestral del Consejo de Coordinación para la Implementación del Sistema de Justicia Penal encontramos una serie de supuestos y recomendaciones a considerar para poder atender los delitos informáticos, las cuales son las siguientes:

> b)En la actualidad, con los avances tecnológicos, se presentan nuevos retos y nuevos tipos penales, los hechos delincuenciales cada vez son más elaborados y complejos, el espionaje, infiltración, tecnología de punta en armamento y recursos, y nuevas tácticas de terrorismo por parte de la delincuencia común organizada, puso en entre dicho el estado de derecho en diferentes latitudes del país, y demostró que para la delincuencia del futuro se necesita policía del futuro, lamentablemente durante mucho tiempo no se logró competir a la altura de las ventajas de los delincuentes.
>
> c) La inadecuada aplicación de los incentivos federales a los municipios, ya que no siempre se utilizan para fomentar las políticas de prevención del delito, o mejoramiento de armamento y equipo, desviándose del objetivo primordial al que van enfocados. (SEGOB, 2016, pp. 9-10).

Con ello podemos deducir con seguridad que la policía dentro de cualquiera de sus variantes reconocidas en el estado mexicano debe estar relacionada con la terminología de los delitos informáticos, y capacitación para atender a la víctima en el momento en el que se encuentre como primer respondiente de una afectación por cualquier variante de un delito informático.

Por esta razón el ministerio público debe tener policías capacitados de acuerdo con la labor investigativa que realizan en sus investigaciones de campo, ya que sus informes serán con lo que los ministerios públicos fortalezcan sus teorías del caso o bien sus acusaciones.

2.5.- Investigación de los delitos informáticos con apego a los derechos humanos.

La reglamentación de la investigación de un ilícito debe de estar contemplada dentro del código Nacional de procedimientos penales que regula todas las formas de investigación para sustentar la comprobación de un hecho punible, de esta manera es el ministerio público quien deberá acatarse única y exclusivamente a las normas establecidas en dicho código para poder sustentar una acusación imputable a un ciudadano, ya que de salirse de estas normas o en su defecto tomar atribuciones excesivas pueden los ministerios públicos recaer en formas de transgresión a los derechos humanos o procesales del ciudadano por lo cual el ministerio público debe de ser consciente y diligente en actuar en la investigación de un hecho delictivo.

La transgresión de los derechos humanos es importante que los ministerios públicos no incurran en ella debido a que pueden ser acreedores de sanciones de tipo pecuniario, administrativo o penal dependiendo de la relevancia o importancia de la manipulación de sus actos de investigación.

Las recomendaciones hechas por los organismos de derechos humanos hacia las actividades realizadas por una autoridad responsable siempre son apegadas al marco legal vigente dentro de los derechos reconocidos por los códigos locales federales o la Constitución, aún en los tratados internacionales de los que el estado mexicano sea parte por lo cual es importante la capacitación adecuada y conocimiento del ministerio público para realizar cualquier acto de investigación con relación a los delitos informáticos.

Es distinta la recomendación que hace un organismo de derechos humanos a las resoluciones dictadas por un órgano jurisdiccional de primera o segunda instancia, por lo cual los ministerios públicos deben vigilar que sus

actuaciones vayan acorde con lo establecido en las normas procesales contenidas dentro del código Nacional de procedimientos penales, ya que los órganos jurisdiccionales o los organismos que vigilan los derechos humanos podrían detener la acusación o el resultado de pruebas que afecten los derechos procesales del imputado de un delito informático debido o que no fueron recabadas dentro del marco legal vigente por lo cual el ministerio público como, organismo encargado y facultado para la investigación de ilícitos debe de aplicar la coerción sólo cuando sea necesario y con causa justificada de lo contrario podría como resultado dejar sin efectos las actuaciones que realice durante la investigación.

En México el marco legal vigila el cumplimiento del respeto de los derechos humanos a partir de la reforma del 2011 la cual cambió el paradigma procesal para las autoridades en cuanto a la visión investigativa que tenían, México con esta reforma se adhiere a los lineamientos que otros países ya tenían contemplados con anterioridad a la declaración de los derechos humanos, lo cual fortaleció su relación con otros Estados, debido al reconocimiento de la identidad jurídica de los gobernados. (Vuanello, 2011)

Con lo anterior referido es importante tomarlo en consideración pues los ministerios públicos no solo deben vigilar que los imputados no sufran violaciones a sus derechos humanos o procesales, sino que además deben tener en consideración que su actuar debe no transgredir a la víctima, es decir debe vigilar que sus actos de investigación sea neutrales pero eficientes para aclarar un hecho delictivos y de esta forma delimitar responsabilidades de manera objetiva sin favorecer a las partes, ya que de ninguna forma debe actuar por analogía o uso de razón, es decir todas sus actuaciones deben estar fundadas y motivadas.

De tal forma al tratarse de la investigación de un delito informático requiere especial atención y forma de investigación, ya que el daño causado a la víctima no es detectable de manera instantánea en algunos casos, la red informática ha potenciado formas de criminalidad, debido a la fácil difusión de virus, programas y archivos personales (Vuanello, 2011).

Con lo anterior referido es importante determinar que la informática no solo es un medio de información y que no solo a través de este medio se pueden cometer delitos del orden común,

Asimismo, la posibilidad de intercambiar informaciones a distancia multiplica las posibilidades de atentar contra bienes jurídicos, que en palabras de Pérez (1998) involucra los siguientes:

> 1º La intimidad, la imagen, la dignidad y el honor de las personas.
>
> 2º La libertad sexual, al permitir la propagación de imágenes o informaciones que entrañen formas de exhibicionismo, provocación sexual, o fomenten la pornografía entre menores de edad.
>
> 3º La propiedad intelectual e industrial, el mercado y los consumidores.
>
> 4º La seguridad nacional y el orden público. (p.728)

De igual manera las leyes procesales y sustantivas no pueden limitar a la informática pues podría considerarse como coartar la libertad de la información o a su vez la libertad de expresión por lo cual las investigaciones de los ministerios públicos deben delimitar muy adecuadamente esta línea entre los propios derechos humanos, ya que dentro del ciberespacio se constituye un entorno libre, mismos que los estados no deben limitar en el libre desarrollo humano. (Vuanello, 2011).

Por último, debemos tomar en cuenta que el ministerio público como órgano investigador no puede quedarse en la negativa de investigar hechos

que transgredan la tranquilidad de los gobernados por lo cual es necesario que evolucione el derecho al mismo tiempo que la tecnología.

Esto en relación a que ya se ha dicho que el derecho es la ciencia encargada de la regulación de la conducta externa del hombre, y el uso de la informática poco a poco deja de depender del hombre para llevar a cabo su funcionamiento por lo cual es importante que se contemplen los avances tecnológicos en la búsqueda comprobación de delitos.

Además, es importante para las propias instituciones públicas blindarse a sí mismas y a sus empleados de posibles ataques cibernéticos ya que el estado no puede verse endeble o frágil ante los embates delictivos de un cumulo de personas.

CAPÍTULO III.

Especialización de los ministerios públicos nivel estatal.

3.1.- Fiscalías especializadas para atención de delitos informáticos en México.

La funcionalidad de los ministerios públicos está determinada en base a la facultad de tener la dirección de la investigación de un hecho delictivo, sin embargo, su actuación está limitada por su jurisdicción y la competencia en que son asignados, de esta manera se entiende que no es posible para un ministerio público investigar de forma física fuera de su área asignada, por ello el derecho penal debe adecuarse a la tecnología actual.

Para todas las labores de investigación de un ilícito, el ministerio público tiene la facultad de solicitar una colaboración de investigación con su similar el cual se encuentre adscrito a otra jurisdicción, estas colaboraciones deben estar siempre sustentadas y motivadas en la ley penal vigente.

Con lo anterior referido se entiende que, para el acto de investigación de delitos informáticos, el ministerio público del fuero común debe conocer sobre la materia penal pero además debe conocer con exactitud la información exacta de lo que pedirá a través de su colaboración a su similar de otra jurisdicción ya que, en dichas colaboraciones, la autoridad no podrá ir más allá o realizar actividades investigativas más de lo que la autoridad que suscriba la colaboración solicite.

De tal manera es importante que los delitos informáticos sean investigados por ministerios públicos capacitados y especializados en la materia, de esta forma algunos estados han creado fiscalías especializadas para la atención de delitos informáticos, algunas como la fiscalía de la CDMX, Fiscalía de Tabasco, Fiscalía de Yucatán y la Fiscalía de Chihuahua.

No obstante, aunque sean fiscalías especializadas aparentemente encaminadas a combatir los delitos informáticos cada una atiende las principales problemáticas que hay en su estado, lo cual complicaría desde el funcionamiento las colaboraciones entre fiscalías especializadas.

En una segunda problemática para la colaboración sería el tipo penal, ya que no basta con solicitar una colaboración indicando el delito o presunta sospecha por la cual se realice la colaboración investigativa, sino que además tendría por principio que ser tipificada la conducta en ambos estados como punible para que no existiese problema para realizar la diligencia colaborativa, ya que por principio la autoridad que realice la colaboración vigilará no incurrir en abusos de autoridad o bien terminar transgrediendo un derecho de un presunto responsable al realizar dicha colaboración que le ha sido solicitada.

Las diferencias de las fiscalías especializadas se vuelven notorias desde las denominaciones de sus nombres y prosiguiendo a sus actividades, por ejemplo, haciendo la comparativa de la Fiscalía General del Estado de Tabasco que crea la Unidad de Investigación de Delitos Informáticos hace diferencia con la Fiscalía General de Justicia de la Ciudad de México (FGJ-CDMX) que creó la Unidad de Atención de Ciber delitos de Violencia de Género, dicha denominación va encaminada a tratar de forma distinta problemáticas relacionadas con delitos informáticos pero con problemas de fondo y enfoques distintos.

Entonces si existe dicha diferencia, en cuanto a la denominación y tratamiento de delitos informáticos, complica de forma parcial las acciones investigativas de los ministerios públicos, en palabras de Ernestina Godoy Ramos Titular de la Fiscalía General de Justicia de la Ciudad de México,

> Hemos diseñado un proceso que va a tener que ser probado en la práctica, vamos a tener que trabajar de manera muy coordinada con los

> jueces y lo estamos haciendo de la mano con las mujeres que han sido víctimas de este delito, desde el momento en que reciben una denuncia de ese tipo solicitan la interrupción, el bloqueo de páginas, y la circulación de fotos o videos de la presunta agraviada, se ha establecido una vinculación directa con los responsables de Facebook, Twitter y WhatsApp, que son los más comunes para poder estar en condiciones de realizar estas primeras medidas de protección, los delitos cibernéticos son un reto para los sistemas jurídicos nacionales porque no tienen fronteras, la jurisdicción es universal y afectan bienes intangibles como son los datos de información electrónica. El internet da al delincuente anonimato al utilizar herramientas informáticas avanzadas para ocultar su identidad y las pruebas para comprobarlo son difíciles de recabar, más cuando el delito se ha cometido en otra jurisdicción distinta a la de la víctima. (Proceso Editorial, 2020, s.p.).

Es decir que a pesar de que las fiscalías especializadas a pesar de tener como enfoque lo delitos informáticos, sus tratamientos y delitos de interés se vuelven diversificados, no obstante, haciendo una comparativa con otras fiscalías especializadas como por ejemplo la de robo de vehículos, el enfoque y tratamiento es similar, situación que no ha sido uniforme en cuanto a los delitos informáticos.

Otra comparativa visible de forma inicial en el nombre pero que abarca en las funciones y finalidades del combate al crimen de delitos informáticos se puede mencionar en la Fiscalía General del Estado de Tabasco, que crea la Unidad de Investigación de Delitos Informáticos, que se diferencia con Fiscalía General de Justicia de la Ciudad de México (FGJ-CDMX) que creó la Unidad de Atención de Ciber delitos de Violencia de Género las podemos poner en comparativa con La Fiscalía General de Estado de Yucatán mediante la Unidad Especializada en Delitos Cibernéticos y la Especializada en Combate

al Secuestro (UECS), o con la fiscalía del Estado de Chihuahua que tiene la Dirección de Análisis de Evidencia Digital e Informática Forense que es parte de la Dirección General del Centro Estatal de Información Análisis y Estadística Criminal, de dicha forma la estructura de cada una hace notoria de cada una solo va determinada a atender delitos específicos que si bien son informáticos no los atienden de forma general, sino que atienden un enfoque preferencial.

Con lo anterior referido se observa que la primera (fiscalía de tabasco) crea una fiscalía para atender delitos informáticos de forma general y que sus ministerios públicos pudieran estar capacitados para conocer un amplio catálogo de delitos informáticos debido a la denominación del nombre de dicho nombre asignado a la referida fiscalía especializada.

Se puede identificar que la segunda fiscalía (Fiscalía de la CDMX) es una unidad especializada para atender asuntos relacionados con la violencia de género en la población concentrada en la territorialidad de la CDMX pero que están sus directivos y personal conscientes de que los victimarios no precisamente pueden encontrarse dentro de su jurisdicción.

En tanto en la tercer fiscalía especializada (Fiscalía del estado de Yucatán) tiene la ardua tarea de investigar delitos informáticos donde la informática cumple como el medio por el cual se realizan otros tipos de delitos del fuero común como es el secuestro, apartándose así de delitos informáticos generales y atendiendo una causa especializada y de forma justificada, es por ello que la denominación establece de forma clara cuál es el fin de la creación de dicha fiscalía especializada y la forma en que puede colaborar con otros estados.

Por último en el Estado de Chihuahua la Dirección de Análisis de Evidencia Digital e Informática Forense es parte de la Dirección General del

Centro Estatal de Información Análisis y Estadística Criminal tiene una finalidad distinta a las anteriores, este departamento sirve sólo como medio de coadyuvancia y su objetivos es encaminado a las funciones de recabar y analizar información a través de medios electrónicos y de telecomunicaciones para elaboración de informes técnico/forenses con el fin de establecer vínculos y coadyuvar con las autoridades competentes a la resolución de investigaciones es decir los ministerios públicos del fuero común.

En relación con otros estados existen algunos que no contienen fiscalías especializadas en la atención de delitos informáticos en sus fiscalías generales del estado, pero han elaborado la creación de cuerpos de seguridad denominados policías cibernéticas mismas que han tomado el rol de vigilantes en la seguridad pública como medio de prevención del delito informático y coadyuvan a las agencias del ministerio público del fuero común para el perfeccionamiento de las investigaciones sobre delitos informáticos.

Pudiendo referir el caso de la Fiscalía del estado de Jalisco que actúa en coordinación con la policía cibernética, asesorando a la ciudadanía con los procedimientos necesarios para levantar una denuncia en el supuesto de ser víctima de un delincuente cibernético, y de auxiliar a los ministerios públicos en sus actuaciones mediante colaboraciones. (Fiscalía del Estado Jalisco, 2020).

Otro ejemplo de la colaboración entre ministerios públicos con cuerpos de seguridad del estado es la Unidad Cibernética de la Comisión Estatal de Seguridad Pública (CES) Morelos, la cual coadyuva en la identificación de conductas delictivas dentro del espacio del internet para asesorar a la población y fomentar la cultura de la denuncia donde a través de las tecnologías de información y comunicación se atente contra la información de las personas.

Por su parte el Gobierno del Estado de México, a través de la Secretaría de Seguridad del Estado de México, creó dentro de sus cuerpos de seguridad de prevención del delito la Unidad de Prevención e Investigación Cibernética, esta Unidad tiene como objetivo prevenir, atender y combatir incidentes informáticos cometidos a través de medios digitales, como fraude, extorsión, robo de identidad, explotación sexual, acoso, maltrato animal, venta de sustancias prohibidas y armas entre otros.

Decir esta unidad de policía cibernética por su denominación y actividades parece ser ampliamente capacitada, pero únicamente podrá actuar salvo la denuncia de una persona, por lo cual es importante que los ministerios públicos conozcan de la materia para realizar las colaboraciones de manera idónea y en los tiempos procesales pertinentes.

Una de las primeras unidades de policía cibernética formada el 3 de abril de 2013 en la ciudad de México, con la finalidad de prevenir, por medio del monitoreo y patrullaje en la red pública, cualquier situación constitutiva de un delito y ayudando a la población en la orientación de presentar una denuncia o querella según se tratare de la afectación a quien contacte a dicho cuerpo de seguridad.

Por su parte dentro del territorio del estado de Guerrero para corroborar la existencia de alguna fiscalía especializada, se solicitó un informe a la Fiscalía General del estado de Guerrero, donde al tener respuesta del requerimiento, fue esta fiscalía no cuenta con una agencia especializada actualmente en delitos informáticos.

Sin embargo, al investigar a fondo esta entidad se detectó que la misma cuenta con una policía cibernética, dicho cuerpo de seguridad funciona de en forma de prevención y de forma colaborativa con las agencias del ministerio público del fuero común para atender y erradicar las conductas delictivas

dentro del territorio del estado de Guerrero, donde además en dicho estado a partir del 2020 se incluyen tipos penales donde se contempla las conductas delictivas por medio de medios informáticos o inclusive es el mismo bien informático el que puede ser vulnerado dando con ello un avance considerable en materia de delitos informáticos.

Con lo antes mencionado cabe referir que a nivel federal existe para auxiliar a la Fiscalía General de la República la Coordinación para la Prevención de Delitos Electrónicos de la División Científica de la Policía Federal, es decir que de forma parcial se está avanzando en el combate del delito informático, ya que con la creación de las policías cibernéticas el ministerio público puede tener un margen más amplio de investigación.

Además, la Guardia nacional también está encargada de la prevención del delito cibernético e informático debido a que han realizado campañas para la concientización y prevención del delito:

> El Instituto Federal de Telecomunicaciones (IFT) y la Guardia Nacional realizarán la Semana de Conferencias de Ciberseguridad 2021, que tienen como objetivo promover el uso y aprovechamiento de las Tecnologías de la Información y Comunicaciones (TIC) de manera responsable, así como compartir con los usuarios información útil que les permita protegerse ante riesgos, amenazas y ataques cibernéticos. (Guardia Nacional, 2020, s.p.).

Las fiscalías especializadas en delitos informáticos son una realidad y deben tener su importancia por parte de los estados, debido a que el internet y sus conductas no se restringen a un espacio reducido a su entorno territorial, darles a los delitos informáticos una debida atención es una necesidad que la sociedad requiere.

3.2.- Capacitación para la investigación de delitos informáticos.

El ministerio público como ente encargado de la dirección de la investigación de un hecho delictivo debe conocer de forma genérica las diferentes formas de recabar de medios de prueba para poder sustentar su teoría del caso contra un probable responsable.

Dichos medios de prueba tienen que versar en su obtención de manera licita, sin violar con o sin el consentimiento los derechos de las personas involucradas en un hecho delictivo, de tal forma que los elementos policiacos o servidores públicos encargados a su coadyuvancia no se vean forzados a realizar actuaciones contrarias a derecho.

> En cuanto a la licitud, está directamente ligado con la forma y modo de obtención de los textos o su fuente o el elemento. Es decir, los elementos de la comunicación están protegidos por la privacidad y en ciertos casos legales con autorización judicial se podrán aportar al proceso e incluso se podrán aportar por una de las partes intervinientes en la conversación, siempre y cuando la persona le quite el velo constitucional de protección y sirva dicha prueba para su juicio. (Valencia, 2020, pág. 10).

Con lo anterior referido se puede detectar que para los delitos informáticos el ministerio público debe tener en cuenta siempre los momentos procesales oportunos para solicitar los medios de prueba pertinentes, por ello saber del tiempo en el cual una prueba en materia informática puede borrarse o modificarse resulta de manera importante para las partes y sobre todo para el propio ministerio público, pues con ello evitaría caer en responsabilidades por omisión de investigación, las autoridades del rango y ramo que conozcan o se actualicen, en temas digitales con finalidad de construir la jurisprudencia (Valencia, 2020).

La necesidad para el ministerio público de estar relacionado con el lenguaje informático resulta importante pues se debe recordar que en materia penal no existe la suplencia de la queja para las partes, es decir que si el ministerio público comete un error en el lenguaje técnico al momento de una acusación y las partes pudieran hacerlo notorio y verse favorecidas o perjudicadas según sea el caso en él se encuentren o el momento procesal donde ocurrieron dichas confusiones de términos técnicos.

El análisis y tratamiento de la evidencia digital es importante para el ministerio público ya que se vuelve el receptor de los equipos de cómputo asegurados en la comisión de un delito informático por ello la conservación de la evidencia digital se vuelve importante ya que el equipo de cómputo por sí mismo no representa un medio de prueba de un hecho ilícito, para el ministerio público se vuelve indispensable poder relacionar la información contenida en dicho equipo con el desarrollo de su teoría del caso y la forma en que dicho equipo de cómputo fue utilizado para transgredir a otra u otras personas y con ello poder lograr una adecuada imputación o acusación.

También se hace referencia al tratamiento de evidencia digital contenida en teléfonos, pudiera parecer que a simple vista se trata del mismo mecanismo, sin embargo, no es así, el equipo de cómputo se caracteriza por ser un equipo más fijo el cual pudiera no ser de uso personal para una sola persona, en cambio el teléfono celular existe una probable seguridad de que dicho equipo funciona para una sola persona debido a que es un dispositivo de comunicación más personal.

Debido a la necesidad de poder relacionar la conducta con el daño y el responsable de la misma, dentro de la ciencia penal para desarrollar una investigación efectiva de aplicar las ciencias forenses, como en este caso sería aplicable la informática forense, con ello la especialización de peritos en

la materia han tenido que ser capacitados de forma adecuada ya que por la exactitud y modo de la comisión del delito es importante la preparación y experticia del perito se vuelve importante, ya que será de quien pueda fiarse el ministerio público. (Zambrano, Dueñas, Macías, 2016).

Además de lo mencionado la preservación de la evidencia digital en un dispositivo celular se vuelve más complejo debido a que por las propias características del celular puede destruirse con mayor facilidad o en contrario sensu pudiera verse asegurado con mayor facilidad debido a que este se encuentra normalmente en posesión inmediata del victimario, por lo cual el aseguramiento del dispositivo celular como el acceso al mismo debe cumplir con los protocolos adecuados iniciando con la cadena de custodia, ya que en todo momento se debe tener en consideración por el ministerio público que no podrá inspeccionar dicho aparato móvil hasta que el probable responsable se encuentre debidamente registrado como detenido y se hayan girado los oficios a las coordinaciones forenses necesarios.

Un tercer punto que es el de mayor atención por los misterios públicos es el de la preservación de pruebas en internet, debido a que, de no estar capacitados de forma adecuada, pudiera darse el caso que dejara de lado la prueba dentro de su investigación, o en su defecto dejar en la impunidad el acto delictivo ya que no podría relacionar el medio de prueba con el presunto delincuente.

A su vez el ministerio público deberá solicitar las colaboraciones con la policía cibernética si es que hubiera un departamento dentro de su jurisdicción o solicitar la colaboración para evitar que la víctima objeto de un re victimización constante, recordando que es incierto saber si un contenido fue borrado por completo de la red de internet, por ello el tiempo en el que se

solicite la colaboración a las policías cibernéticas resulta crucial para las víctimas.

Esto último punto referido nos lleva al punto cuatro que es el dictamen pericial, debido a que el ministerio público como se ha referido debe tener el conocimiento del lenguaje técnico en al menos conceptos básicos, saber preservar las evidencias digitales en equipos de cómputo, dispositivos celulares o móviles e internet, esto con la finalidad de que en el momento que solicite un dictamen pericial, sea con una indicación clara de que es lo que deberá analizar de forma exacta el experto informático.

De acuerdo a lo que el ministerio público solicite en su dictamen pericial tendrá a su disposición una metodología realzada por el experto para realizar la tarea encomendada, donde este experto dará a forma de lista las conclusiones realizadas y se las comunicará al ministerio público, por ello si el ministerio no es certero en su petición de lo que se pretende indagar en un dispositivo, equipo de cómputo o internet será en vano que realice muchas series de dictámenes o bien solicitará dictámenes que no contribuirán con su teoría del caso y que pudieran darle herramientas al victimario para quedar en impunidad su acto delictivo.

Como una muestra en cuanto a las capacitaciones de los ministerios públicos del fuero común al solicitar información en cuanto a la capacitación de los ministerios públicos sobre los elementos de la fiscalía general del estado de Guerrero, se solicitó informes para saber si su personal había sido actualizado en algún curso para atender de forma adecuada delitos informáticos, respondiendo a la petición hecha de forma rápida y positiva, se informó que durante el 2020 se han impartido cinco cursos y durante el 2021 no se ha impartido cursos de esta índole, adjuntando la tabla con los nombres y número de ministerios públicos que participaron en dichas capacitaciones.

2020	SECAP(Sistema Electrónico para el Control de Averiguaciones Previas)	16 de julio
	Conferencia: BNAVIM (Banco Nacional de Datos e Información sobre Casos de Violencia contra k las mujeres).	17 de julio
	Plataforma México, conceptos Generales	29 de julio
	Actualización y Capacitación de las Nuevas Herramientas de la APP de la Fiscalía Gral. del Estado.	13 de agosto
	Curso de capacitación en materia de Inteligencia Patrimonial y Económica	14 al 19 de Diciembre
2021	-	0

IMAGEN 1: Información solicitada a la Fiscalía del estado de Guerrero.

En relación con los cursos proporcionados en la tabla anterior se puede observar, que los agentes del ministerio público del estado de Guerrero, conforme al título de los mismos cursos se puede deducir que no van encaminados al conocimiento de las figuras delictivas adicionadas en el código penal en el 2019 correspondientes a los delitos de divulgación no consentida de imágenes o videos íntimos o sexual, usurpación de identidad o usurpación de identidad equiparada, con lo cual hace ver que la capacitación no es la idónea para la atención de los delitos informáticos que se tienen contemplados en el código penal local vigente.

De las capacitaciones proporcionadas por la fiscalía del estado de Guerrero a sus elementos ministerios públicos se solicitó el desglose total de sus asistentes para saber cuántos ministerios públicos fueron capacitados en estos cursos, con lo cual obtuvimos la siguiente respuesta:

2020	SECAP(Sistema Electrónico para el Control de Averiguaciones Previas)	67 MPS
	Conferencia: BNAVIM (Banco Nacional de Datos e Información sobre Casos de Violencia contra k las mujeres).	34 MPS
	Plataforma México. conceptos Generales	44 MPS
	Actualización y Capacitación de las Nuevas Herramientas de la APP de la Fiscalía Gral. del Estado.	48 MPS
	Curso de capacitación en materia de Inteligencia Patrimonial y Económica	32 MPS
2021	-	0

IMAGEN 2: Información solicitada a la Fiscalía del estado de Guerrero.

Es importante recordar que en el estado de Guerrero los delitos informáticos como el sexting, (Ley Olimpia), la usurpación de identidad y la usurpación de identidad equiparada, fueron anexados a finales del año 2019, por lo cual demuestra que el estado de Guerrero capacito casi de forma inmediata a sus elementos para poder atender dichas figuras delictivas en la entidad, sin embargo, que esta misma capacitación fuera más apta para el tratamiento adecuado de estos delitos.

Es importante hablar sobre el número de casos denunciados en el año 2020 y 2021, por ello se solicitó a la Fiscalía General del Estado de Guerrero la información al respecto al número de denuncias o querellas interpuestas en esas temporalidades, dándonos como resultado la información correspondiente al año del 2020 y parcialmente hasta el mes de marzo del 2021, la cual está en la siguiente tabla:

DELITO	2020	2021
Sexting (Ley Olimpia) tanto para mujeres como para hombres.	84	27
Pornografía.	5	3

IMAGEN 3: Información solicitada a la Fiscalía del estado de Guerrero.

Respecto a esta información es notable que el delito informático afecta a las personas sin importar el sexo, por ello la prevención y el combate al delito informático es importante dentro de la sociedad actual, ya que en el 2020 fueron en total 84 denuncias o querellas, sin embargo se puede contra polarizar con el año del 2021 ya que en solo 3 meses se obtuvieron 27 es decir, que en ese breve periodo de tiempo se llevaban más de un cuarto respecto a las cifras del 2020, y que tentativamente de seguir con ese mismo nivel aproximadamente se tendrían 108 denuncias o querellas por lo menos al concluir el 2021.

Por último y de forma no menos importante es que el ministerio público sepa identificar el problema que se le presente y recurra a una figura punible idónea para sustentar su acusación, ya que debe identificar cuando se están presentando ante él, datos de pruebas manipuladas o fabricadas para crear una falsa acusación, y de no comprobar su autenticidad del hecho caería en responsabilidades administrativas o penales por omisión.

Con la capacitación adecuada se procura la naturaleza y rol inicial del ministerio público el cual consiste en esclarecer los hechos reales y con ello buscar castigar a un verdadero probable responsable, ya que no siempre se da el caso de que quien denuncia es la víctima, pues pudiera darse el caso de que alguien abusando de la buena fe la institución recurra a falsas acusaciones para transgredir a otra persona.

3.3.- Importancia del financiamiento de las fiscalías para atención de delitos informáticos.

El presupuesto en materia de seguridad pública se vuelve importante debido a que la es el inicio de las medidas preventivas del delito, por tanto el financiamiento de las fiscalías locales que son las encargadas de la investigación de las conductas ilícitas y daño causado es lo idóneo para evitar que los delincuentes se multipliquen y operen en la impunidad, no obstante, es necesario referir que dicho financiamiento no se especifica exactamente cómo será distribuido dentro de las fiscalías generales de los estados, o bien dentro de los cuerpos de seguridad pública por lo que es viable desarrollar una nueva investigación de acuerdo al financiamiento en las corporaciones de justicia.

En el caso que nos ocupa las policías cibernéticas cumplen con roles de coadyuvancia con los ministerios públicos sin embargo no están del todo financiadas, “las entidades federativas no cuentan con capacidades de Policía Cibernética robustas por la austeridad”. (Economista, 2017), por ello se vuelve necesario que el primer financiamiento sea para las policías cibernéticas pues se encargan del primer combate contra el crimen cibernético que es la prevención del delito informático a través de sus portales oficiales.

> El 40% de las entidades cuentan con Unidades de Policía Cibernética, de ellas, sólo 10% cuenta con la infraestructura y capacidades mínimas para su operación. La falta de cultura de seguridad informática de la población y el incremento de los delitos cibernéticos han generado la necesidad de impulsar una reforma legislativa en materia de delitos cibernéticos. (SEGOB, 2014, p.195).

Se vuelve importante esta referencia debido a que como se ha mencionado, no todos los estados contienen una fiscalía especializada en

delitos informáticos, por lo cual los ministerios públicos se tienen que apoyar en dichas corporaciones de seguridad pública para mantener el combate al crimen informático, ya que el caso pudiera agravarse si en dicho estado no solo no cuente con una fiscalía especializada o con ministerios públicos sin estar adecuadamente capacitados en materia de delitos informáticos, sino que también no cuente con una adecuada policía cibernética que les pueda ayudar en la coadyuvancia para eliminar contenido en la red de forma preventiva del delito.

Por ello el financiamiento respecto a delitos informáticos a las fiscalías generales de los estados, no solo implica que puedan atender de mejor forma y con mayor efectividad los delitos e incidentes informáticos, implicaría poder lograr un margen estadístico real y actual de la situación de sus propios estados en materia de delitos informáticos, con ello de forma posterior solicitar una adecuación legislativa en sus códigos penales locales ya que actualmente no se cuenta con dicho padrón informático de los ciberdelincuente potencialmente peligrosos, y además se requiere mayor colaboración internacional en materia de delitos informáticos con otros países. (SEGOB, 2014)

Dichos indicadores o padrón de registro de delincuentes informáticos como se menciona, no solo daría una perspectiva internacional para la investigación de delitos informáticos con otros países, sino que de forma directa implica la confiabilidad del sector social en las instituciones, pues la cifra negra de delitos informáticos con ello pudiera verse al menos de forma parcial por la población y con ello generar una mayor cultura de la prevención del delito informático.

En otro sentido el financiamiento sobre delitos informáticos a las fiscalías de los estados conlleva a un entendimiento y colaboración de forma

más uniforme entre los distintos ministerios públicos que se encuentren a lo largo del territorio de sus respectivos estados, y con ello sería más viable poder comprobar ante los jueces encargados de los órganos jurisdiccionales el tipo penal con el cual es imputada una persona, ya que al entender el lenguaje técnico empleado por parte de los ministerios públicos al momento del desarrollo de las audiencias dentro del proceso penal conlleva a una acusación basada en el conocimiento del hecho ilícito en relación con el lenguaje técnico.

De esta manera al ser capacitado el ministerio público se enfocará más en el acto investigativo y dejaría de lado su preocupación por incurrir en un acto de omisión investigativa por el desconocimiento del lenguaje o funcionamiento técnico, dejando de ser un problema tanto para el ministerio público como para el operador jurisdiccional y reconociendo de esta manera por el estado la información como un bien jurídico tutelado.

> El empleo de este medio acarrea un singular problema para el investigador, para el Juez Penal, debido a la dificultad probatoria que su empleo para tales fines produce, es de observar con ello que la tecnificación de medios analizada, no está aparejada con la capacitación necesaria en los órganos jurisdiccionales existiendo la posibilidad de que el delito cometido bajo tales circunstancias quede impune. (Cárdenas, 2014, p. 63).

No financiar a las fiscalías en materia de delitos informáticos y que a su vez estos no realicen una investigación adecuada de un hecho delictivo trae como consecuencia la impunidad y con ello abre la puerta para que el ciberdelincuente cometa estas conductas de forma más reiterada y con mayor impacto para las probables víctimas, ya que el estado abandona con ello su poder coercitivo y permite que se lesione el estado de derecho, que además

pudiera el estado mexicano ser sancionado por un organismo internacional por dejar al descubierto los derechos de las víctimas dentro de una investigación.

En comparación con el estado mexicano pudiera contra polarizarse la situación del país de Perú, donde existe una ley especial de delitos informáticos y que nuestro sistema de impartición de justicia es de forma parcialmente similar en cuanto a sus figuras:

> TERCERA. Coordinación interinstitucional de la Policía Nacional del Perú con el Ministerio Público la Policía Nacional del Perú fortalece al órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, la Policía Nacional del Perú centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad. (Congreso República de Perú, 2013, s.p.)

Con lo antes referido se observa que en dicho país también se está llevando una estrategia contra el delito informático y donde el principal ente encargado de la investigación y dirección del combate contra los delitos informáticos es el ministerio público.

Dicha comparativa nos sirve para reafirmar la postura del investigador donde es importante el financiamiento y la capacitación constante del ministerio público para combatir los delitos informáticos pues estos no están delimitados a su comisión por una jurisdicción exacta y que conforme mayor se investigue puede verse una mayor complejidad en cuanto a identificar el victimario, el grado de participación del mismo, y los medios utilizados para transgredir a la víctima.

Finalizando con este punto de la investigación es necesario referir que el financiamiento debe consistir en mejor equipo de cómputo y de conectividad a internet, impartición de cursos de manera gratuita al personal encargado bajo el ministerio público es decir las secretarias y mecanógrafas, ya que son las auxiliares del ministerio público para la generación de oficios en la investigación y sus actuaciones no deben contravenir la ley.

Además, dicho financiamiento permite que las investigaciones lleven su formalidad y con ello se evitan las violaciones al gobernado ya que en el artículo 7 y 16 de la constitución de los estados unidos mexicanos establecen la libertad de imprenta privada y la garantía de inviolabilidad domiciliara y comunicaciones privadas el Habeas Data. (GERALDES DA CUNHA, 2011)

Es decir que si bien es cierto que el Ministerio público es el encargado de dirigir la investigación de un ilícito este tiene siempre que seguir las formalidades de la ley y sobre todo será el propio estado el encargado de proveer el financiamiento para que estas investigaciones sean de calidad.

Lo anterior referido versa en el hecho que no necesariamente se necesita que el sujeto activo del delito tenga a su alcance de tecnología de vanguardia, esto dificulta para el ministerio público la investigación pues no puede determinar un perfil delictivo por un estatus económico el del victimario. “Desde el enfoque de los ciberdelincuentes, resulta necesario distinguir entre los medios financieros que requieren para cometer un delito informático”. (MAYER, 2016, s.p.)

Los Ministerios Públicos no pueden elevar las estadísticas contra el delito informático si estas figuras punibles no se encuentran contempladas de forma idónea en la ley, tampoco si no cuentan con la infraestructura necesaria para la indagación de estos delitos.

El financiamiento idóneo debe tener como finalidad el combate contra la impunidad y la protección a la información, se vuelve necesario mayor financiamiento a mayor número de población debido a que se vuelve mayor el rango de búsqueda del presunto delincuente informático.

CAPÍTULO IV

Resultados del apartado de percepción de seguridad en internet

4.1.- Resultados.

La percepción de la realidad por parte de las personas respecto a los delitos informáticos es importante debido a que es a ellos en quienes afectan las consecuencias de las conductas realizadas por los ciberdelincuentes.

Para atender este punto, se realiza una encuesta utilizando como medio de contacto y recolección de respuestas a las redes sociales, esto con la finalidad de obtener participantes que contesten por voluntad propia, además permite tener un muestreo más amplio dentro del Estado tomando en consideración las limitantes económicas dentro de la investigación.

En consecuencia, la realización de un sondeo en base a la perspectiva de las personas que utilicen dispositivos de comunicación y almacenamiento con acceso a internet es necesario, tanto para conocer sus hábitos de navegación como las medidas de ciberseguridad que utilizan al navegar en el ciberespacio y en base a ello poder saber la vulnerabilidad que tienen al usar las tecnologías de información y comunicación.

El número de participantes en dicho sondeo fue de 362 en el cual participaron 235 mujeres es decir el 64.9 %, el 34.5% de hombres que significó 125 participantes, cabe destacar que 2 participantes es decir el 0.2% prefirieron no mencionar su sexo, respecto a ello el cuestionario estuvo abierto a participantes desde los 12 años auxiliados de un tutor y a los mayores de 18 sin excepción de edad.

El dato referido al número de participantes toma relevancia pues se visualiza una buena participación voluntaria, lo cual habla que las personas

tienen un gran interés en que las tecnologías de información y comunicación sean sometidas a su estudio y con ello se determinen mejores formas de protección o a su vez identificar los hábitos comunes que tienen con otras personas.

En base a ello obtuvimos una respuesta por parte de los participantes de las edades comprendidas entre los 19 a 25 años siendo así 38.1% del total de los participantes los cuales significaron 138 de ellos, en segundo lugar, un rango de edad comprendida entre los 26 a 35 años fue del 28.2%, es decir 101 participantes, finalmente la menor población fueron el 1.1% con 4 participantes.

El porcentaje de la edad de los participantes en la encuesta se vuelve interesante pues nos habla de que las generaciones que están llegando a la edad adulta se van preocupando cada vez más por sus hábitos y seguridad que deben tener en cuenta al usar las tecnologías de información y comunicación ya que se ven mayormente involucradas con las mismas.

Dicha afirmación no es de sorprenderse debido a que como se ha referido en el trabajo de investigación, la sociedad cada vez más inmiscuye en sus actividades cotidianas el mayor uso de las tecnologías de información y comunicación, lo que da como resultado social que seamos más dependientes de la tecnología y, por tanto, como también se ha referido, vayan surgiendo nuevas conductas que atenten contra el bien jurídico informático.

Por lo visto en los resultados de la encuesta, se puede afirmar que 347 de los participantes es decir el 95.9% utilizan un dispositivo de comunicación personal como lo es el celular, y entre ellos los días en donde se conectan a internet con mayor habitualidad de navegación son los días viernes 65.7%, lunes 62.2%, sábado 54.1% y 50.6%, superando el 50% del número total de los participantes en estos días la mitad de los participantes los días donde se

conectan en el ciberespacio, con la respuesta de los participantes podemos analizar que un gran número de personas se encuentra realizando acciones dentro del ciberespacio en la mayoría de la semana, por lo cual también se encuentran dentro del campo de acción de los delincuentes cibernéticos.

Es importante señalar que la probabilidad que tiene una persona de ser víctima de algún delito informático aumenta por pasar más tiempo en el ciberespacio, y en la encuesta toma relevancia saber que 123 participantes mencionan estar conectados todo el día, lo cual significa que al menos 34% del total de participantes tienen una alta convivencia con las ciberamenazas.

Además, como se ha referido las redes sociales son el sitio más inseguro dentro del ciberespacio ya que no hay una autoridad que las regule como tal, ya que solo se ha regulado el contenido, sin embargo, el 48.9% es decir 177 están conectados en el mayor medio de ataque de delincuentes cibernéticos, es decir en redes sociales y mensajería instantánea lo cual nos da un panorama de muestra del alto índice delictivo que puede no estar siendo atendido.

Por otro lado, los participantes refieren que el principal motivo de que los usuarios permanezcan en redes sociales es debido a los sistemas de mensajería instantánea siendo el 40.6% es decir 147 participantes afirman que es el principal motivo por el cual se conectan en internet; el segundo motivo principal es el de ver y compartir memes y videos en las mismas redes sociales lo que nos sigue dando una muestra del grado de vulnerabilidad en el que se encuentran los participantes de la encuesta.

Aun cuando los propios participantes refieren no sentirse seguros en las redes sociales, el 66.9 % del total de los participantes percibe que la suplantación de identidad es el mayor riesgo que tienen; como segundo riesgo les preocupa que te roben la contraseña y como tercer riesgo visible

consideran que la infección de virus el dispositivo de comunicación, sin embargo, esto no los limita a dejar de usarlas, por lo que el regular a las redes sociales pudiera ser una alternativa para disminuir las posibles amenazas dentro del ciberespacio para sus usuarios.

En cuanto a la palabra ciberseguridad la mayoría de los entrevistados lo asocian con la vigilancia, con la policía cibernética o el internet seguro, es decir no existe conocimiento exacto de la cultura de la ciberseguridad entre los participantes, sin embargo, tienen una idea de que el internet debe ser seguro, no obstante, algunos piensan que está involucrado con la seguridad del Estado o la seguridad que el mismo debería brindar dentro del ciberespacio para que este sea un medio seguro.

Sin embargo, aun cuando no conozcan sobre la ciberseguridad, si están conscientes que existen ciberdelitos en internet pues la mayoría refiere conocer algún tipo de ciberdelito, en este sentido identifican como delito a la vulneración de datos personales en primer lugar, los fraudes en segundo y el robo de identidad en tercer lugar.

Además, las personas que integraron la muestra, consideran que entre las aplicaciones que más utilizan, las más seguras son las de paquetería de ofimática de office como Word, Excel o Powerpoint, mismas que no necesariamente requieren acceso a internet, sin embargo, puede aún existir peligro a utilizarlas si se utilizan con contenido al internet (como el office 365), en ese sentido afirman que son inseguras las aplicaciones como Facebook o WhatsApp identificadas como redes sociales que necesitan para su funcionamiento la conectividad directa al ciberespacio.

Como se ha referido, entre los participantes el celular es el principal medio por el cual se conectan en internet, menos del 27.1% no tiene un antivirus en sus celulares instalado y toman como principal medio de

protección no abrir enlaces desconocidos; contrario a el uso de la computadora donde 242 de participantes (66,9 %) si utiliza un antivirus en sus computadoras, tomando en cuenta esto el celular y la computadora son los medios mas importantes.

En esa misma percepción los participantes consideran como las aplicaciones más inseguras en primer lugar a Facebook, WhatsApp e Instagram; en segundo lugar, los videojuegos en línea son considerados como los más inseguros y en tercer lugar los participantes no consideran seguras a las aplicaciones de banca en línea.

Aun cuando las aplicaciones bancarias en línea no son consideradas como confiables por los participantes, el 74,6% ha realizado alguna compra en línea, dando como principal método de pago el deposito en un banco o en una tienda de comercio denominada OXXO con el 34%, lo cual habla de que menos de la mitad de los participantes no tiene confianza en la realización de pagos por banca móvil o seguridad para proporcionar sus datos de su tarjeta de crédito o débito, por miedo a ser víctimas de un fraude.

Al preguntar sobre los motivos por los cuales no tienen seguridad en este tipo de aplicaciones, mencionan que el robo de información, o el exceso de información de datos personales del usuario que las mismas aplicaciones piden para su uso significa un riesgo latente pues no saben quién tendrá acceso a ellas o porque no hacen nada contra el robo de su identidad y que se ha sabido que las aplicaciones venden esa información a otros sitios.

El 51.1% de los entrevistados, mencionan que ellos o algún familiar han sido víctimas de un ciberdelito, con ello refieren que la usurpación de identidad es el primer delito del cual han sido víctimas; en segundo lugar, colocan a la divulgación de imágenes o videos con contenido sexual; y como tercero el

acceso no autorizado a sus cuentas, con lo cual son coherentes con sus respuestas en los cuestionamientos anteriores.

El porcentaje referido en el párrafo anterior vuelve interesante analizar cifra negra de delitos no denunciados, pero a la vez esta información de las víctimas y las denuncias van acorde con la información de denuncias realizadas por delitos informáticos en el Estado de Guerrero, esto en base a la información solicitada a la Fiscalía del Estado de Guerrero, sin embargo, los participantes no mencionaron si denunciaron por lo que podríamos estar hablando de una cifra negra bastante amplia.

Lo anterior referido es preocupante puesto que solo el 10.5% de los participantes refieren saber dónde denunciar o con que instancia acudir si son víctima de un delito cibernético el cual es ante el ministerio público, el 72.1% es decir 261 personas acudirían con la policía cibernética, corporación que no es la indicada para atender o tomar su denuncia o querella para perseguir a los ciberdelincuentes, esta corporación como se ha dicho sirve solo para orientar a la población sobre cómo mantenerse seguro al navegar en internet, y el 13.8% desconoce a donde recurrir a denunciar si son víctimas de una delito en el ciberespacio, con lo cual habla de la vulnerabilidad por desconocimiento de las personas ante este tipo de conductas delictivas.

Además de acuerdo la percepción de los participantes aun cuando no acudirían con la autoridad indicada para denunciar un delito cibernético el 70.7% es decir, 256 participantes, mencionan que no es efectiva la autoridad para atender los delitos informáticos, en este caso tratándose de los ministerios públicos.

Lo anterior referido puede decirse que no existe confiabilidad en la figura de los ministerios públicos dentro del Estado de Guerrero por parte de la sociedad pues como se ha referido no buscarían denunciar debido a que no

tienen confianza en la institución donde laboran, dicha desconfianza como se ha referido se transforma en una cifra negra, pues la sociedad está dejando de denunciar y con ello se deja en la impunidad a las víctimas de un delito cibernético o informático y por tanto, también quedan exentas de una reparación del daño.

Con base en la percepción negativa que les han otorgado a los ministerios públicos, al cuestionarles que calificación les asignarían del 1 al 10 a las autoridades encargadas de los delitos informáticos, es decir, los ministerios públicos, más del 50% de la población del cuestionario refirió darle calificación de menos de 5, con lo cual confirma y refleja el nivel de desconfianza que tiene la población a los ministerios públicos que son los encargados de darle la directriz a la investigación de los delitos informáticos del fuero común dentro del Estado de Guerrero.

En relación a los resultados obtenidos se vuelve de importancia el contenido legislado y vigente en las leyes y códigos punibles, dado que al menos en el Estado de Guerrero tenemos legislados delitos informáticos mismos que no están siendo denunciados por los ciudadanos según los resultados de la encuesta realizada en el presente trabajo.

Además, el contenido legislativo vigente se vuelve importante no solo para el ministerio publico sino también para la propia sociedad debido a que es en ellos en quienes se aplica la norma, además propicia a que si una conducta no está regulada como punible o castigable, un ente de la sociedad aproveche esta situación para poder actuar con total libertad y sin recriminación punible alguna, debido a que esta conducta no sería castigada con una pena, ya que como se ha dicho en el trabajo de investigación, para que el ministerio público pueda acusar debe existir la conducta como punible de forma previa a la comisión o realización de la misma.

Además, debemos seguir teniendo en cuenta que el derecho penal debe tenerse en cuenta como el último recurso del estado para hacer valer una norma, y no debe ser utilizado como medida de prevención del delito, ya que quienes infringen la norma con acreedores a una pena, así mismo los infractores de la norma estarán obligados a la reparación del daño, pero esto únicamente puede llegar a suceder si la presunta víctima denuncia y se logra condenar al presunto imputado.

Por otro lado, teniendo en cuenta que los participantes de la encuesta han mencionado en casi su totalidad que cuentan con un dispositivo de información y comunicación, para el Estado debe verse en una tarea primordial el atender las conductas delictivas o incidentes informáticos que suceden dentro de su jurisdicción, por lo cual de buena manera se tendría que impulsar a través del congreso del estado por decreto la creación de una fiscalía especializada en delitos informáticos.

Dicha fiscalía debería contar con poder de atracción para los delitos de estas características que ocurran dentro del estado, pues de esta manera las personas tendrían conocimiento básico de donde interponer una denuncia o querella de este tipo de delitos pues como se ha reflejado en el resultado de la encuesta realizada pues solo el 10.5% sabe ante qué organismo puede denunciar o promover una querella de forma adecuada donde, además dichos funcionarios públicos encargados de ese organismo son los únicos facultados para atender todos los delitos de orden común.

Por otro lado, la creación por derecho de dicha fiscalía especializada en delitos informáticos al tener concentrados todos los delitos informáticos en el Estado de Guerrero correspondientes al fuero común, daría paso a que los delitos informáticos competentes al fuero federal sean remitidos de forma inmediata, esto con la finalidad de garantizar los derechos procesales de la

víctima y para agilizar la investigación en curso por cualquier delito informático que no sea competente de la fiscalía del Estado de Guerrero.

Lo anterior mencionado es con la finalidad de no dejar en la cifra negra de impunidad a las víctimas, pues muchas de ellas desconocen que la conducta por la cual han sido objeto es de índole y jurisdicción Federal, además de que reprochan al Estado local el daño que les han ocasionado, dicha percepción negativa que se tiene sobre las autoridades locales con la creación de dicha fiscalía especializada en delitos informáticos, cambiaría el enfoque y percepción negativa que la sociedad tiene pues se transmitiría el mensaje de que los delitos informáticos se empiezan a tomar con la seriedad requerida.

Además, para el estado de Guerrero volvería más económica la capacitación del personal encargado de investigar delitos informáticos pues en vez de capacitar a todos los ministerios públicos del Estado de forma paulatina se centraría en la capacitación de un cumulo de fiscales agentes ministerios públicos especializados así como de agentes ministeriales, ya que de acuerdo a la información proporcionada por la misma Fiscalía del Estado de Guerrero del 2020 a 2021 solo se habían impartido 6 cursos para actualizar a su personal.

Teniendo en cuenta que los delitos informáticos no solo se encuentran contenidos en el código penal local de cada entidad o el código penal federal, hay que mencionar que los delitos informáticos en México se encuentran en leyes especiales las cuales mencionan penas para quienes hagan mal uso de los instrumentos de información y comunicación o bien en las bases de datos, como ejemplo la ley de protección de datos personales en posesión de los particulares, Ley de instituciones de Crédito, Ley del mercado de Valores, por citar unos ejemplos, por tanto la tipología de delitos informáticos a nivel local y

nivel federal deben estar adecuadamente asignadas en sus competencias y jurisdicciones territoriales.

Además, se debe tener en cuenta para el Estado de Guerrero que tiene que tener en consideración que otras entidades locales tienen figuras punibles de delitos informáticos con las que no cuenta, lo que conlleva tarde o temprano a necesidad de legislarlos debido a que el delincuente informático no tiene jurisdicción física para la comisión del delito o bien no puede limitarse a un área geográfica para atacar, por lo que puede existir la posibilidad de que gente que se encuentre en el Estado de Guerrero se encuentre siendo víctima de delincuentes que se encuentren operando fuera del territorio del Estado, por lo cual se vuelven importantes las colaboraciones de investigación interestatales, y para ello sus casos deben estar centralizados en una fiscalía especializada con la finalidad de aprovechar de mejor forma los recursos humanos y financieros.

Finalmente, el presente trabajo de investigación estaba inicialmente destinado a realzarse un estudio comparativo en las diferentes entidades, sin embargo, considerando las limitaciones geográficas, financieras, pandémicas por el problema de salud actual, se tomó la decisión de darle un giro de forma local, donde solo se tomaría en cuenta el estado de Guerrero, dejando con ello abierta la investigación y poder continuar con ella en investigación para obtener un grado doctoral.

CONCLUSIONES

En base al contenido de la investigación obtenemos como primera conclusión que se necesita un mayor interés a nivel local en el estado de Guerrero para atender los delitos informáticos, esto debido a que se ha identificado que la mayoría de los Estados del territorio mexicano no cuentan con fiscalías especializadas en delitos informáticos, y Guerrero es uno de ellos.

Además de lo anterior, cabe mencionar que la legislación penal local entre los Estados no está sincronizada en su contenido punible, es decir no está acorde para poder realizar investigaciones conjuntas complicando así la colaboración entre los fiscales ministerios públicos de las fiscalías de diferentes Estados, imposibilitando así una investigación efectiva. Lo que se traduce en no encontrar al culpable de una conducta punible, por lo tanto, la víctima queda en vulnerabilidad y sin su derecho a la reparación del daño y obtención de justicia.

Los cuerpos especializados en investigación de delitos informáticos no están siendo contemplados para auxiliar al ministerio público e inclusive los mismos ministerios públicos carecen de una capacitación adecuada, tal es el caso de la fiscalía del estado de Guerrero, ello limita la perspectiva del ministerio público para entender la conducta punible y el alcance de las afectaciones que estas pueden tener esto significa que al momento de estudiar la conducta para encuadrarla y presentar una acusación, no se puede realizar de forma idónea, por ende no se estará atendiendo de manera adecuada y se verá reflejado más tarde en los índices de impunidad o de carpetas de investigación no judicializadas por falta de elementos para presentar el caso ante el juez de control.

De acuerdo con la investigación realizadas y los datos obtenidos de la misma fiscalía del Estado, podemos concluir que los ministerios públicos no cuentan con la infraestructura necesaria para poder realizar una investigación adecuada y técnica sobre los delitos informáticos, carecen de un presupuesto especial asignado para la investigación de los mismos, esto significa un impacto o una limitante en sus recursos para poder indagar de forma proactiva dentro del espacio cibernético lo cual se traduce de forma negativa en impunidad.

A través de la investigación realizada, se observó la perspectiva negativa que la sociedad tiene sobre la atención e investigación de los ministerios públicos hacia los delitos informáticos, debido a que no creen que exista certeza en la capacitación o interés de las autoridades para la investigación de este tipo de delitos y/o conductas, otorgándoles una calificación de índole negativo en cuanto a la confiabilidad que existe ante los entes facultados para la investigación de delitos como lo son los Ministerios públicos.

Por lo anterior se puede describir que la atención de la Fiscalía del estado de Guerrero hacia los delitos informáticos si se está llevando a cabo, sin embargo, es necesario reforzar ciertas estrategias o métodos para mejorar la eficiencia en el tratamiento y atención a las denuncias o querellas en delitos informáticos, a continuación, se proponen algunas ideas para atender a esta problemática detectada por el presente trabajo de tesis.

PROPUESTAS

En base a los resultados obtenidos y una vez que se han formulado conclusiones, lo idóneo es sugerir soluciones en forma de propuesta al problema planteado, por lo cual, siendo coherentes con el contenido de la investigación, mencionamos las siguientes:

1.- La capacitación de los Ministerios Públicos debe ser constante en materia de delitos informáticos, incluyendo conocimientos técnicos y jurídico acorde a la dinámica social, es decir que esta capacitación vaya dirigida a la funcionabilidad de los dispositivos de información y comunicación, el desarrollo de la conducta del delincuente informático y el conocimiento de los elementos de la tipología de los delitos informáticos.

2.- Desde el Congreso del Estado, se sugiere que impulsen la creación de fiscalías especializadas en delitos informáticos, o en su defecto equipos especializados para casos especiales donde se atiendan este tipo de incidentes delictivos, con la finalidad de obtener patrones o modus operandi de bandas de ciberdelincuentes y con ello lograr una sola línea de investigación y evitar con ello el desgaste del aparato estatal de indagación delictiva dentro de la fiscalía para no duplicar información que pudiera pertenecer a un mismo delincuente informático o grupo organizado que opere a través de las tecnologías de la información y comunicación.

3.- Incrementar la cooperación entre Fiscalías Generales de los Estados dentro del territorio mexicano, con la finalidad de ampliar la investigación de manera colaborativa, expandiendo la perspectiva y así fortalecer al Estado para que sea más eficaz el poder coercitivo ante ciberdelincuente, y que además disminuya los trámites burocráticos de colaboración jurisdiccional se

siguen interponiendo como limitantes dentro de una investigación de delitos informáticos.

4.- Con la colaboración de las Fiscalías Generales de los Estados de la República Mexicana seria propio enviar a todos los congresos una propuesta de reforma en los códigos penales locales para incluir un capitulado denominado “Delitos Informáticos” y con ello lograr la uniformidad de figuras punibles en todo el país, con ello se lograría que la colaboración se fortaleciera y se lograría evitar duplicidad de investigación y con ello mayor eficiencia en la búsqueda de ciberdelincuentes.

5.- Otorgar mayor financiamiento destinado para la investigación de los delitos informáticos, ya sea otorgados por el nivel estatal o gestionarlos a nivel federal debido a la importancia de estas conductas punibles. Dicho financiamiento estaría destinado a equipos de información y comunicación, informática forense, internet de alta velocidad y auxiliares de mesa de investigación, vehículos para movilidad, así como las herramientas tecnológicas adecuadas.

ANEXOS.

Hábitos de navegación en internet y percepción de la atención a Delitos Informáticos

Con la finalidad de responder la pregunta de la presente investigación, mediante un instrumento electrónico, se aplicó un cuestionario con una serie de preguntas de tipo cualitativo principalmente, donde se abordan temas de conectividad, hábitos en internet y percepción de seguridad en entornos digitales, así como la percepción de eficiencia de las autoridades encargadas de atender los delitos informáticos.

La muestra fue aleatoria y por invitación a ciudadanos del estado de Guerrero principalmente. Las preguntas combinan respuestas de tipo dicotómico, escalas tipo Liker y tres preguntas abiertas para conocer el sentir y la experiencia de las personas en materia de Delitos informáticos.

Lo anterior se eligió para dar más agilidad a los participantes además de facilitar la interpretación de los resultados.

La encuesta se divide a su vez en tres sectores: 1) Datos personales y de conectividad, 2) hábitos de navegación y 3) percepción de seguridad en internet.

El instrumento electrónico se realizó con los formularios de google para ser socializado mediante las redes sociales de estudiantes de 4º año de licenciatura de la Facultad de Derecho, en primera instancia y docentes de nivel licenciatura y posgrado principalmente.

Con esta estrategia se reunieron un total de **362 participaciones** obtenidas desde distintos lugares del estado de Guerrero.

ANEXO I

RESULTADOS DE LA ENCUESTA

Resultados de la primera sección.

La muestra obtenida incluye a **235 mujeres** y **125 hombres**, que representan un **64.9%** y **34.5%** respectivamente (Gráfico 1)

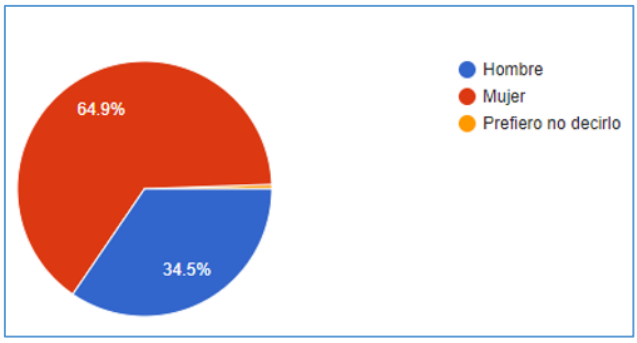


Gráfico 1. Distribución de la muestra por sexo.

La edad de las personas que respondieron el cuestionario se concentra principalmente entre los **19 y 25 años de edad (38.1%)** seguido del rango comprendido entre los **26 a 35 años (28.2%).** Esto confirma la población objetivo: estudiantes y docentes de nivel licenciatura y posgrado.

Además, otros rangos de edad que se incluyen en la muestra son de **36 a 50 años (19.9%)** y jóvenes de **15 a 18 años (7.7%).**

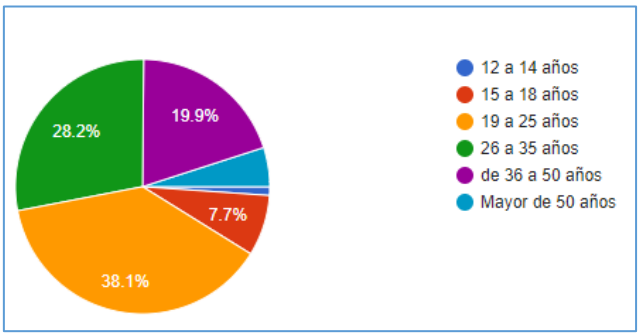


Gráfico 2. Rangos de edad de la muestra.

La ocupación de la mayoría de los entrevistados corresponde con la población objetivo, 182 personas son **estudiantes**, 62 son **docentes**, 55 **empleados de gobierno** y 31 son **empleados de empresa privada**.

1. Estudiantes (**50.3%**),
2. Docentes (**17.1%**),
3. Empleado de gobierno (**15.2%**),
4. Empleado en empresa privada (**8.8%**).

En lo que respecta a la formación académica, se corresponde con la muestra elegida puesto que más del 60% de las personas que respondieron son de **licenciatura**, 18% de **posgrado** y el 17% pertenecen a la comunidad de **bachillerato**.

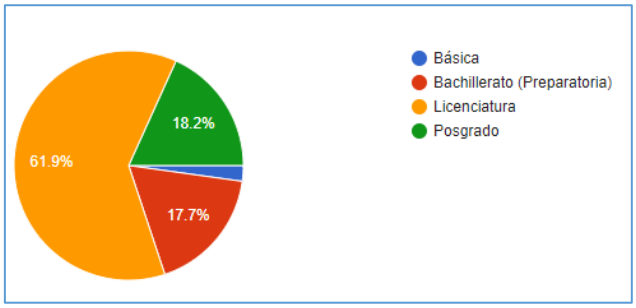


Gráfico 3. Formación académica de la muestra.

Con esto culmina la sección de datos personales de las personas que respondieron la encuesta, es de resaltar que, como se esperaba, la mayor parte de la muestra corresponde a la comunidad académica de licenciatura.

Resultado de la segunda sección.

En la segunda sección llamada: hábitos de navegación en internet, se les preguntó a los participantes si contaban con conexión a internet en casa, 327 personas respondieron que si representando el 90.3% de la muestra.

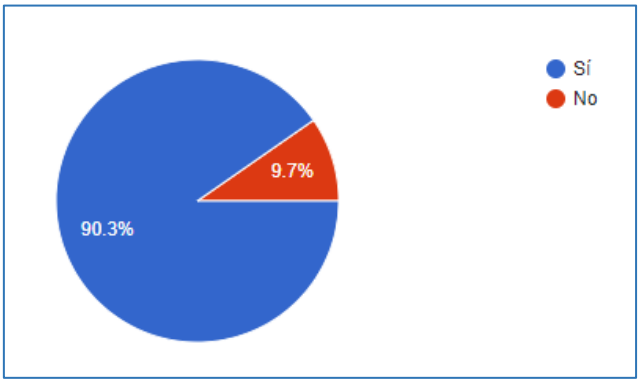


Gráfico 4. Conectividad, ¿Cuenta con conexión a internet en casa?

Los principales dispositivos que utilizan para acceder a internet son: Smartphone, Laptop, Smart TV y computadora de escritorio.

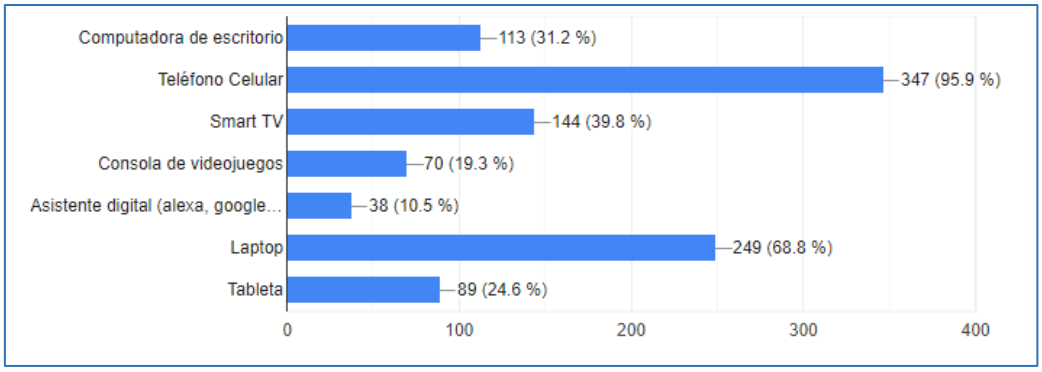


Gráfico 5. Dispositivos que utilizan para acceder a internet.

Se les hizo la pregunta ¿cuáles son los días que más se conecta? A lo que la mayoría respondió que los **viernes**, **lunes** y **sábado** (Gráfico 6).

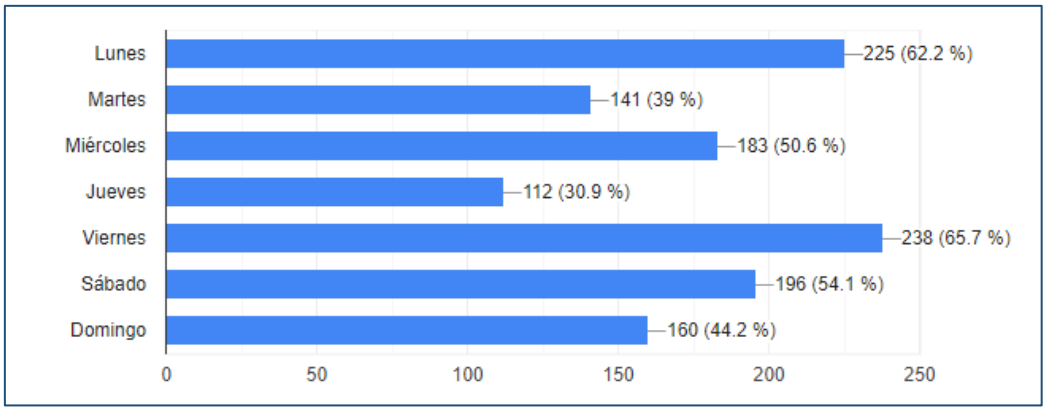


Gráfico 6. ¿Cuáles son los días que más se conecta? Elija tres días principales.

Además, se les pidió responder el horario que suelen conectarse, a lo que 123 personas que representan el **34% respondieron que todo el día están conectados**, un segundo bloque de 81 personas **(22.4%) respondió que se conecta de 8 a 11 de la noche**, caso contrario, un **2.8% manifestó que se conectan en el horario de 6 a 9 de la mañana** (Gráfico 7).

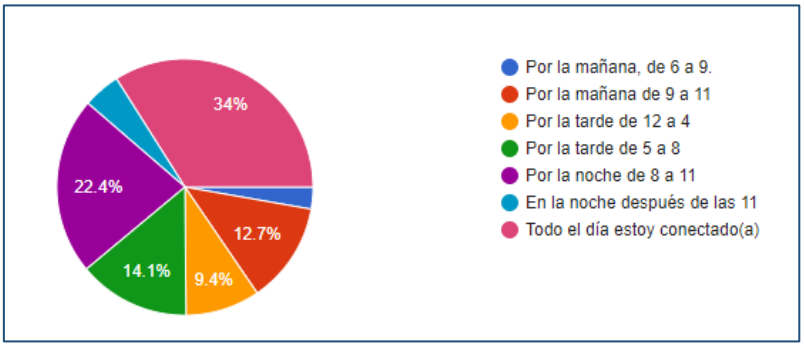


Gráfico 7. Respuestas a la pregunta ¿En qué horario suelen conectarse a internet?

Los usuarios de internet de la muestra, respondieron que se conectan a internet y se mantienen online de la manera siguiente:

- De 1 a 2 horas conectados 19.6%
- De 2 a 5 horas conectados 29%
- Más de 5 horas 27.3%
- Todo el día en internet 21%

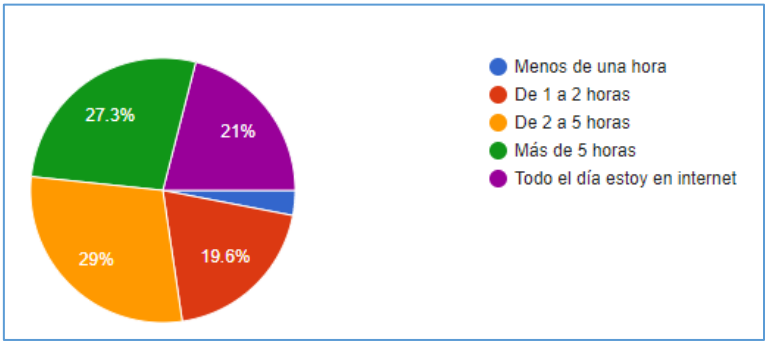


Gráfico 8. Respuestas de la pregunta ¿Cuántas horas suele estar conectado(a) en internet?

Lo anterior nos sirve de indicador de la importancia que tiene el conocer los hábitos de navegación pues la respuesta más frecuente de las personas es que se conectan **5 horas durante el día** al servicio de internet para **diversas actividades** como las que se indican a continuación en orden de mayor frecuencia en las respuestas:

- Revisan sus redes sociales 36.5%
- Consumen contenido multimedia 16.3%
- Utilizan chats 12.4%
- Revisan su correo electrónico 11.9%
- Realizan videoconferencias 10.5%

Cabe mencionar que algunas otras actividades con menor frecuencia incluyen **trabajo en línea**, **compras por internet** y **jugar en línea**.

A la pregunta ¿Cuál es su dispositivo favorito para conectarse a internet?, 318 personas respondieron que **se conectan a través de un teléfono celular** o Smartphone, lo que corresponde con la pregunta 2 mencionada anteriormente.

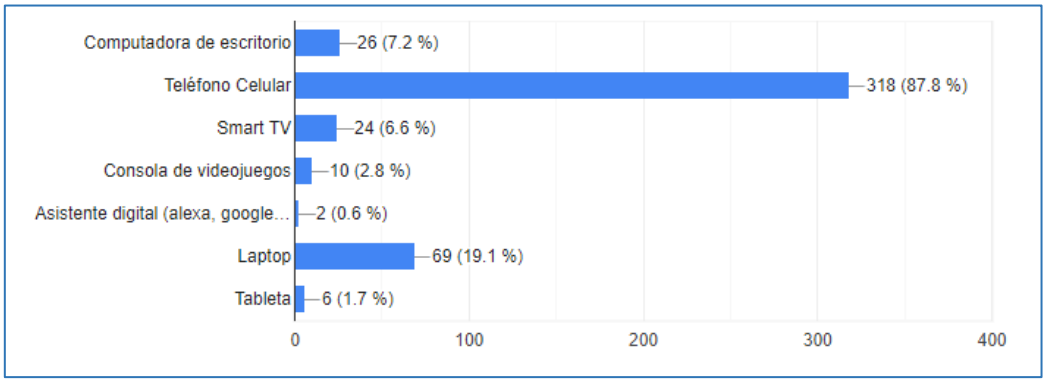
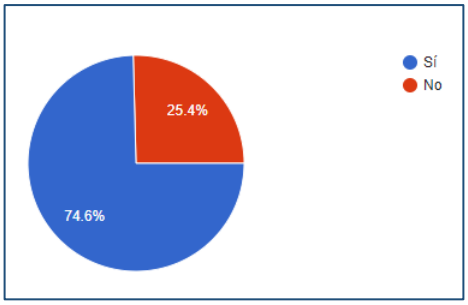


Gráfico 9. Dispositivo favorito para conectarse a internet.



En la pregunta 8 se les plantea la interrogante ¿Has realizado compras por internet? Y la gran mayoría un **74.6% respondió que sí compran online** (270 personas).

Gráfico 10. Respuestas si han comprado en internet o no.

Posteriormente se le pregunta acerca del método de pago elegido para realizar sus compras, Las principales respuestas son: 123 personas respondieron que pagan **a través de depósitos en Oxxo o en banco (34%)**, 79 personas pagan por medio de **transferencia bancaria (21.8%)**, 73 personas utilizan para pagos la **tarjeta de débito (20.2%)** y 53 personas utilizan **tarjeta de crédito (14.6%)** al realiza sus compras.

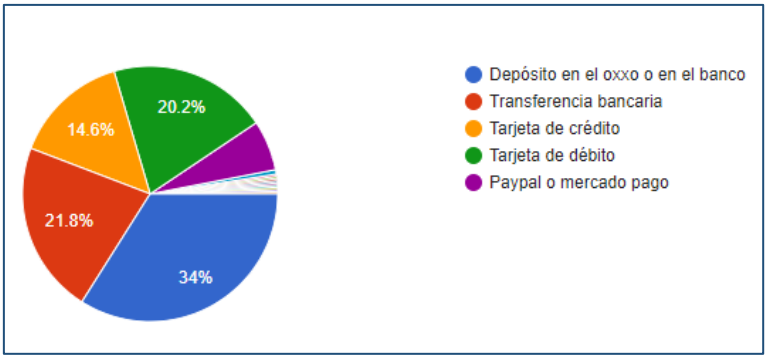


Gráfico 11. Método preferido para pagar las compras realizadas en internet.

La pregunta 9 es la primera relacionada con la percepción de seguridad, en este caso al comprar en línea, se les pregunta que respondan en una escala del 1 al 5, donde 1 es *"nada seguro"* y el 5 es *"muy seguro",* los entrevistados respondieron lo siguiente:

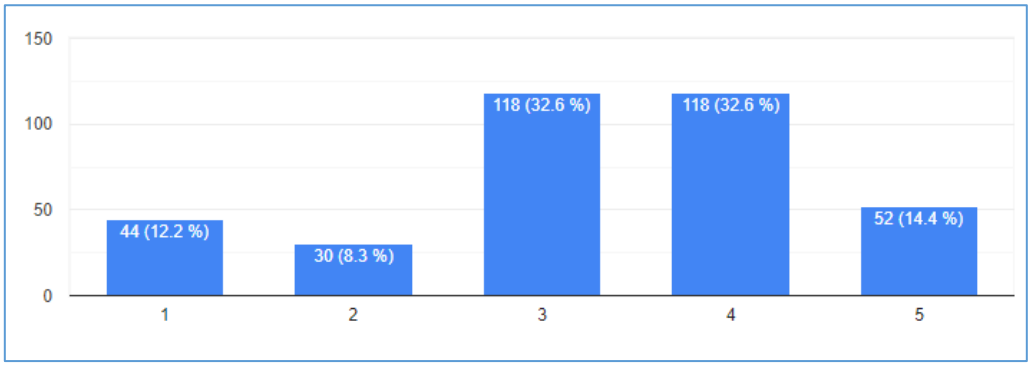


Gráfico 12. Distribución de la percepción de seguridad, más cercano a 5 es mejor.

Como podemos apreciar en el gráfico 12, la mayoría de las personas se sienten seguras de comprar por internet.

Agrupando las calificaciones 3, 4 y 5 se tiene un total de 288 respuestas que representan el **79.6% de personas que consideran seguro comprar en internet**.

Cabe mencionar el **14.4% manifiesta sentirse muy seguro** de comprar en internet y el **12.2% considera que no es nada seguro** este tipo de compra.

Para conocer los hábitos cotidianos de navegación que las personas tienen en el ciberespacio, se retoma que la mayoría respondió estar en redes sociales (véase página 6) y en el reactivo 11 se les preguntó acerca de las actividades realizadas en estas plataformas, obteniendo los siguientes resultados:

La mayoría con un **40.6% respondió que envía mensajes**, un **20.7% ve y comparte videos**, un **16.6% ve y comparte memes** (imágenes, frases o videos generalmente graciosos) y un **16.3% lo utiliza para actividades escolares o laborales**.

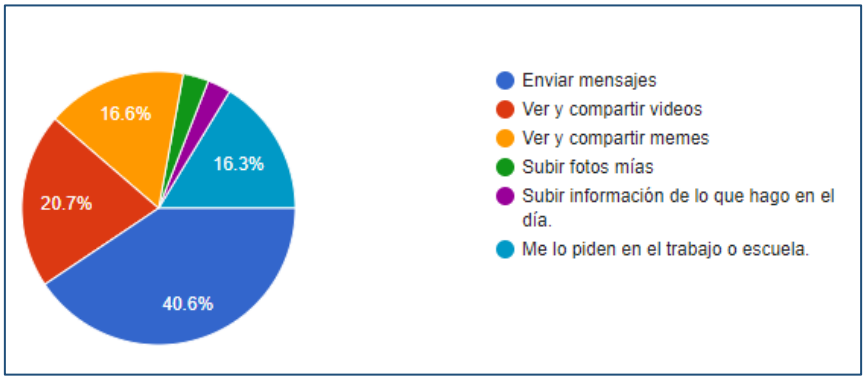


Gráfico 13. Actividades realizadas por los usuarios de redes sociales.

Cabe mencionar un punto muy importante en temas de seguridad en redes sociales, un **3% manifiesta subir fotos personales** y un **2.8% sube información de su día a día** o información de las actividades que hace durante el día.

Consecuentemente, la pregunta 12 le pide medir la percepción de seguridad al navegar en redes sociales en una escala de 1 al 5, donde 1 es “nada seguro” y 5 representa “muy seguras”.

A pesar que la mayoría con un 47.8% responde de manera neutral ni seguro ni inseguro, los resultados conjugados de la opción 1 y 2 tienden una **percepción de inseguridad con un 36.5%** y solamente un **2.2% manifiesta que las redes sociales son seguras**.

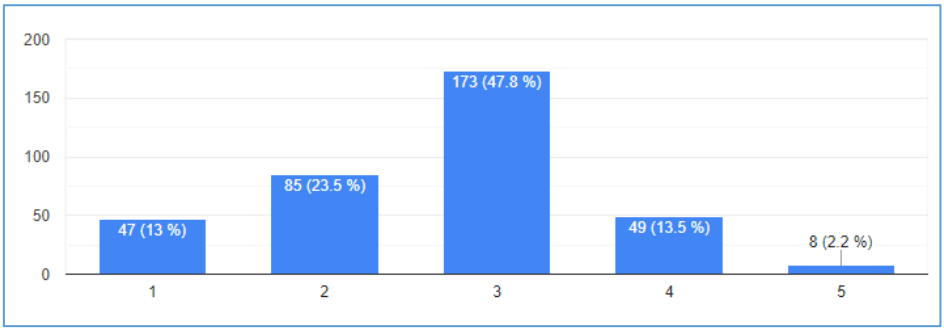


Gráfico 14. Percepción de seguridad en redes sociales, más cercano a 5 es más seguro.

Para finalizar esta sección, en el reactivo 13 se pregunta acerca de los riesgos que las personas perciben en las redes sociales, permitiendo más de una respuesta con lo que se obtuvieron los siguientes resultados:

- un 66.9% de las personas consideran que puede haber suplantación de identidad,
- Un 43.6% considera a la extorsión como un riesgo latente,
- Un 41.7% responde que se corre el riesgo de tener la adicción a las redes sociales,
- El 31.5% manifiesta que existe riesgo de que les roben la contraseña,
- Un 31.2% considera un riesgo el infectar con algún virus su dispositivo y,
- El 10.8% contestaron que el bullying (ciber acoso) es un riesgo en redes sociales.

Los demás resultados no son significativos, pero cabe mencionar que hubo dos respuestas más en el instrumento electrónico: “robo de datos personales” y “divulgación de información sensible” relacionadas con la privacidad e intimidad.

Cabe aclarar que, al permitir varias respuestas, no se obtiene un 100% en la suma de las respuestas y solo se registran en la interpretación las respuestas de mayor frecuencia.

Resultados de la tercera sección

En la tercera y última sección, se incluyen algunas preguntas abiertas para sondear los conceptos que identifican las o los entrevistados referente a la seguridad en internet (ciber seguridad).

La *pregunta 14* pide responder lo primero que piensan al escuchar la palabra **ciberseguridad**, la mayoría de las respuestas incluyen las palabras clave:

- En primer lugar, se obtienen respuestas que incluyen la palabra **seguridad** en la red o internet, lo cual es evidente por la naturaleza de las preguntas.
- En segundo lugar, mencionan la palabra **internet** o **redes**, haciendo alusión al entorno digital de la seguridad.
- La tercera palabra que identifican las personas que respondieron la encuesta es **navegación**, que de manera intuitiva se refiere a utilizar internet.
- En cuarto lugar, las palabras utilizadas en las respuestas tienen que ver con los **datos**, **información**, **datos personales** que los usuarios de internet proporcionan y otorgan en las plataformas digitales para poder hacer uso de ellas.
- Finalmente, los usuarios identifican a la **policía cibernética** y redes sociales como partes fundamentales de la navegación en internet.

Los resultados de esta pregunta indican que el usuario de internet identifica correctamente el significado de cibernético como aquellos procesos inmersos en entornos digitales que proporcionan los dispositivos telemáticos conectados a internet principalmente.

La *pregunta 15* sigue la misma dinámica, pero incluyendo ahora la palabra **ciberdelito**, las palabras clave obtenidas en las respuestas fueron:

- En primer lugar, y de manera evidente, asocian la palabra ciberdelito con **delitos**, **ilegal**, **crimen** o **amenazas.**
- En segundo lugar, de manera natural identifican a **internet** como el medio donde se cometen estos incidentes.
- La palabra **redes sociales** es la tercera más utilizada en las respuestas, confirmando los hábitos de navegación observados en este trabajo.
- En cuarto lugar, definen una serie de delitos o conductas asociadas al ciberdelito, siendo **fraude, robo, extorsión y hackeo** las más utilizadas por las personas que respondieron el formulario.
- Por último, asocian al ciber delito con la palabra **información, datos personales, leyes, reglas, normas y seguridad**.

Con los resultados de esta pregunta, se confirma que el usuario de internet que respondió este cuestionario, conceptualiza al ciberdelito en el mismo sentido que lo hace la presente investigación.

En la *pregunta 16*, se le pide que identifique a la principal amenaza que existe al navegar por internet, un **38.7% respondió que es la vulneración de datos personales**, un **26% identifica a los fraudes**, **14.9% responde que el robo de identidad** es la amenaza principal y un **9.7% identificó a la pornografía** como amenaza.

Con un menor porcentaje de respuestas, el **6.6% manifiesta que los virus** son la principal amenaza, el **3% responde que el robo de dinero** lo es, y **1.1% identifica espionaje** por parte del gobierno.

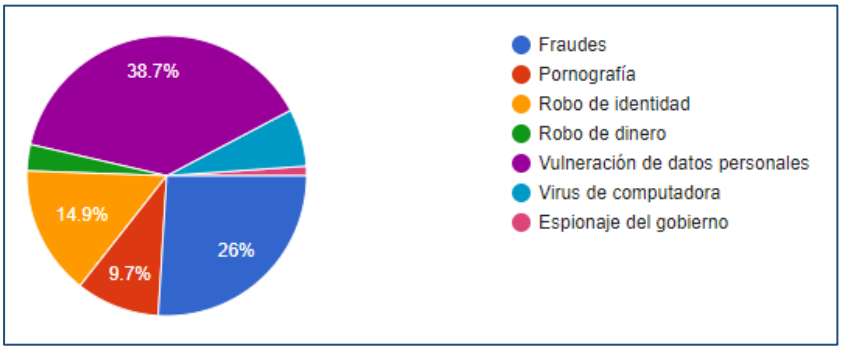


Gráfico 15. Principales amenazas identificadas al navegar por internet.

En un ejercicio de confianza se le pide a las personas que respondieron el instrumento electrónico que indicaran las tres aplicaciones que **más confianza** les dan, a continuación se enlistan en orden de mayor a menor, a las aplicaciones en las que confían:

1. Aplicaciones ofimáticas (**Word, Excel, Powerpoint**),
2. Aplicaciones de mensajería instantanea (**Whatsapp, Mesenger y telegram**),
3. Redes sociales (**facebook, twitter, instragram y youtube**) y,
4. El navegador Chrome y la banca en línea.

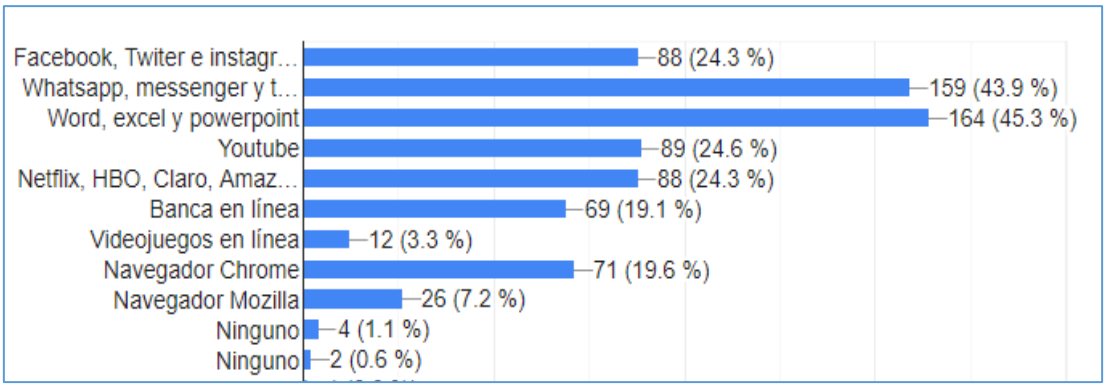


Gráfico 16. Aplicaciones en las que más confían los usuarios de internet.

También se pregunta por las acciones que realizan para mantenerse seguros al navegar en internet con su teléfono celular (*pregunta 18*) y con su computadora o laptop (*pregunta 19*) a lo cual respondieron lo siguiente:

Acciones de seguridad en teléfono celular (enlistándolos en orden de mayor cantidad de respuesta):

1. No abro páginas que no conozco
2. Evito pulsar en enlaces desconocidos
3. Evito instalar aplicaciones que no conozco
4. Mantengo mi vida privada
5. Instalo un antivirus
6. Actualizo mi software
7. Cambio mi contraseña al menos una vez al año y,
8. Uso contraseñas diferentes en las aplicaciones.

Acciones de seguridad en computadora o laptop (enlistándolos en orden de mayor cantidad de respuesta):

1. Instalo un antivirus,
2. Evito entrar a páginas poco seguras,
3. Mantengo con contraseña mi dispositivo,
4. Respaldo mi información regularmente,
5. Limpio el caché una vez al mes,
6. Compro licencias originales
7. Analizo mi equipo una vez al mes,
8. Cambio contraseñas regularmente
9. Instalo un adblock que evite ventanas emergentes.

Para finalizar con los dispositivos, la *pregunta 20* busca la respuesta acerca de ¿qué dispositivo consideras más seguro para navegar en internet? Y las respuestas con mayor frecuencia son:

1. Teléfono celular Android con un **34.3%**,
2. Computadora personal (Windows o Linux) con un **32.3%**,
3. Teléfono celular Iphone, tuvo **13.8%** de las respuestas y,
4. Computadora Apple (Mac) un **9.7%.**

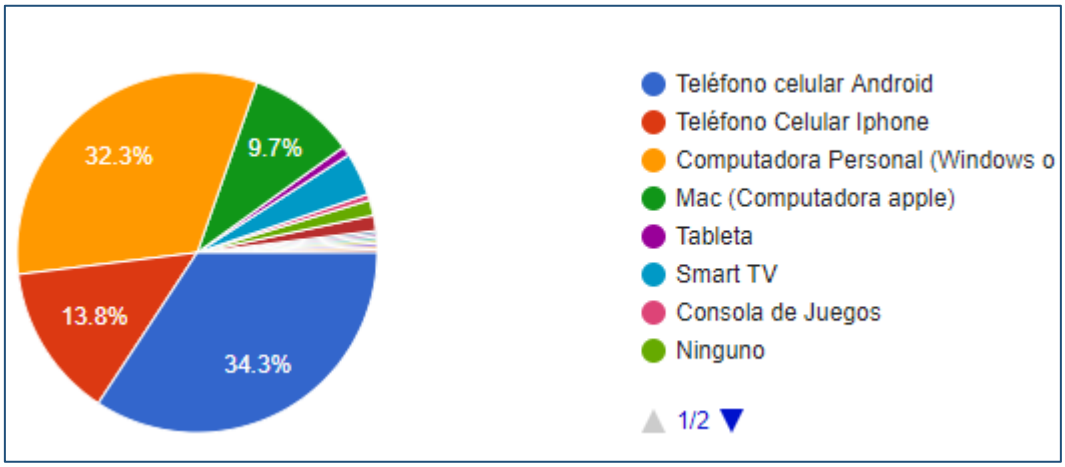


Gráfico 17. Dispositivos que los usuarios consideran más seguros para navegar en internet.

Para contrastar la pregunta 17 y confirmarla se pide en la *pregunta 21* que indique tres de las aplicaciones a las que **no les tiene confianza**, las respuestas se enlistan de mayor a menor frecuencia:

1. No confían en Redes sociales Facebook, twitter e Instagram
2. Desconfían de videojuegos en línea
3. No tienen confianza de la banca en línea
4. Desconfían de los navegadores, tanto Chrome como mozilla
5. No confían en youtube y,
6. Desconfían de plataformas digitales como Netflix, HBO, Claro video y Amazon Prime.

La razón de esta **desconfianza** se aborda en la *pregunta 22*, dejándola como pregunta abierta a las y los entrevistados permitiéndoles externar sus inquietudes de manera libre.

Las palabras claves y frases más frecuente obtenidas para poder interpretar el sentir de las personas fueron las siguientes:

- Primeramente, la palabra **información** es la que más mencionan en las respuestas.
- La Segunda palabra más utilizada es **personal**, haciendo alusión a la información y datos personales que pueden estar expuestos en las aplicaciones que utilizan en internet.
- En tercer lugar, mencionan a la **vulnerabilidad, hackeo y acceso fácil**, refiriéndose a la intención que tienen algunas personas de apropiarse de la información de manera no autorizada
- En cuarto lugar, mencionan a **robo** y **virus**, como dos elementos de riesgo en el uso de las aplicaciones que utilizan al navegar en internet.
- Finalmente, las respuestas utilizan las palabras, **privacidad**, **seguro** y **desconocido**, danto a entender en sentido tanto positivo como negativo, del uso de internet y la desconfianza que se tiene al quedar expuesto en entornos virtuales.

Con estas respuestas, se obtiene un panorama general acerca de las preocupaciones que tienen los usuarios que utilizan diversas aplicaciones al conectarse al servicio de internet

Las últimas preguntas se centran en los delitos informáticos o ciberdelitos y su atención por parte de las autoridades competentes.

De manera expresa la *pregunta 23* plantea si los entrevistados o algún conocido o familiar ¿ha sido víctima de un ciberdelito? A lo que un **51.1% respondió que sí** y un **48.9% contestó que no.**

Poco más de la mitad de las personas conocieron a alguien afectado o fueron víctimas de alguno de los siguientes delitos:

- 24.8% Por usurpación de identidad,
- 15.9% Divulgación de imágenes o videos (íntimo o sexual),
- 15% Acceso no autorizado por desconocidos,
- 8.9% Acoso u hostigamiento,
- 5.6% Acceso no autorizado por conocidos,
- 4.2% Pornografía,
- 4.2% Borrado intencional de información,
- 3.3% Sexting.

La instancia a que las y los entrevistados acudirían para denunciar o reportar un delito informático es:

- 72.1% Policía cibernética
- 13.8% No lo sabe
- 10.5% Ministerio público
- 1.9% Un abogado.

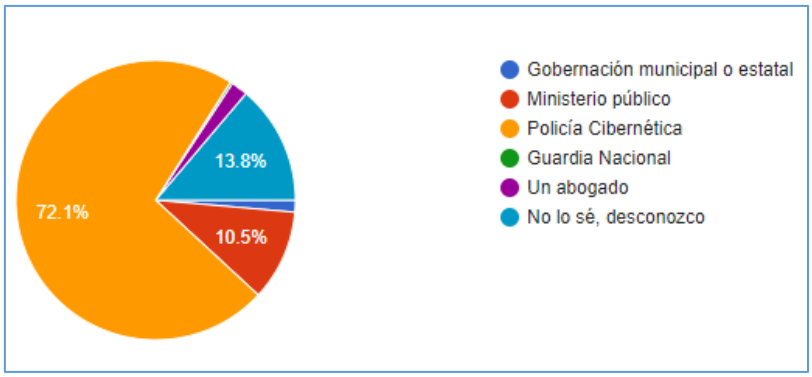


Gráfico 18. Respuesta a la pregunta, ¿Ante qué instancia acudirían para denunciar un delito cibernético?

Para culminar este trabajo tenemos dos preguntas que abordan directamente al tema de estudio que responde a la actuación de los ministerios públicos respecto a delitos informáticos.

La *pregunta 26* mide la percepción que tienen los ciudadanos entrevistados al plantear: ¿Consideras que la autoridad es efectiva en atender los delitos informáticos o delitos que ocurren en el ciberespacio (internet)?

Los resultados obtenidos indican que 7 de cada 10 personas piensan que la autoridad **no es efectiva (70.7%)** mientras que 3 de cada 10 personas piensan que si es efectiva (29.3%).

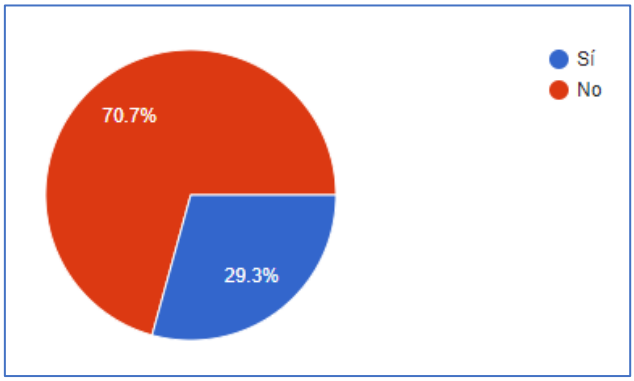


Gráfico 19. Percepción de efectividad que tienen las personas entrevistadas.

Se debe resaltar que el la percepción de las y los entrevistados, para corroborar esta percepción se deben analizar de manera directa los resultados de las autoridades competentes.

En el gráfico 20, se realiza un cruce de información entre aquellos que respondieron que ellos, un conocido o familiar ha sido víctima de delito y aquellos que responden que la autoridad NO es efectiva, en este cruce podemos apreciar que piensan que **la autoridad no es efectiva independientemente si han sido víctimas o no de un delito.**

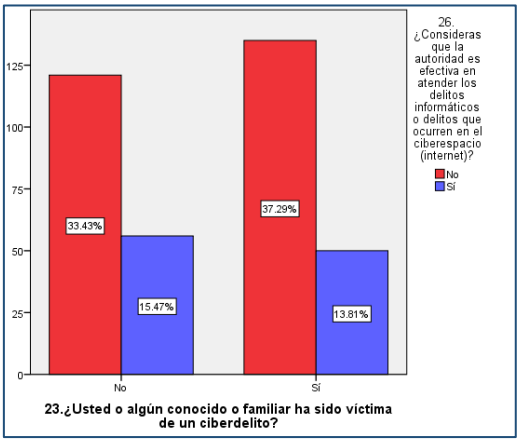


Gráfico 20. Cruce de información entre las preguntas 23 y 26.

Finalmente, se les pidió a las y los entrevistado que calificaran a la autoridad en una escala del uno al diez, donde el 1 representa una calificación mala (**reprobado**) y el 10 una calificación muy buena (**aprobado**).

El promedio de calificación que le otorgan a la autoridad competente es de **5.1 puntos**, que se puede traducir en una calificación neutral, si sólo tomamos en cuenta la naturaleza de la pregunta, pero analizando el contexto social y escolar donde el 7 es la mínima calificación aprobatoria, entonces la autoridad evaluada obtuvo en realidad una calificación reprobatoria.

Haciendo un sencillo ejercicio estadístico se agrupan las calificaciones obtenidad en el rango del 1 a 6 (quartil 60) se tiene el **69% de las respuestas**, mientras que en las calificaciones del 7 al 10 representan un 31%.

La mayor cantidad de respuestas la obtuvo la calificación de 5 y la que menor frecuencia de respuestas tiene es la calificación de 10.

La distribución de las respuestas se pueden observar en el gráfico 21.

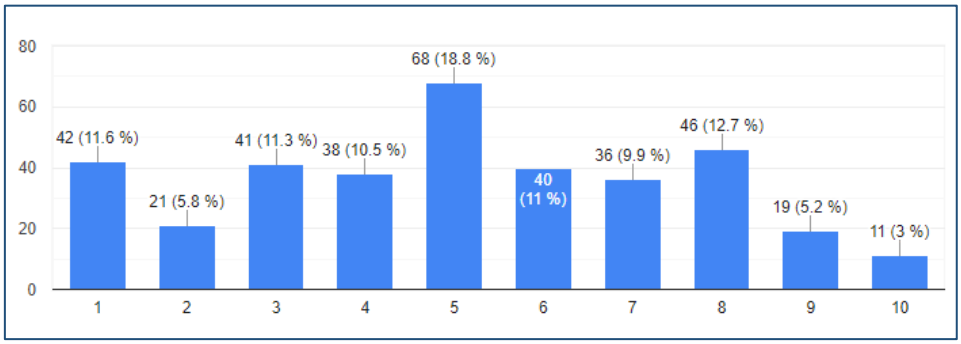


Gráfico 21. Calificación que los entrevistados les otorgan a las autoridades encargadas de atender delitos informáticos.

Con la finalidad de tener cifras reales de la situación actual de los delitos informáticos dentro del Estado de Guerrero, se solicitó a la Fiscalía del Estado de Guerrero, a través de la Unidad de Transparencia y Acceso a la Información dichas cifras, misma dependencia que nos respondió de manera rápida y favorable.

La información solicitada fue de gran ayuda en el trabajo de investigación debido a que sustento la hipótesis planteada al inicio del misma, además aporto información vital en la investigación como saber el número de denuncias realizadas en el 2020 y 2021 de delitos informáticos, el número y nombre de capacitaciones realizadas por los ministerios públicos para atender delitos informáticos, entre otros cuestionamientos.

ANEXO II

INFORMACIÓN SOLICITADA A LA FISCALÍA DEL ESTADO DE GUERRERO

Fiscalía General del Estado de Guerrero.
Órgano Interno de Control
Unidad de Transparencia y Acceso a la Información Pública.

OFICIO: FGE/OIC/UTAI/494/2021.

Chilpancingo, Guerrero, a 30 de junio del

"2021, Año de la Independencia"

C. JOSE LUIS MARTINEZ CUEVAS.
PRESENTE.

Con fundamento en el artículo 150, de la Ley número 207 de Transparencia y Acceso a la Información Pública del Estado de Guerrero, hago referencia a su solicitud de información de fecha 21 de mayo, recibida a través de Oficialía de Partes de esta Unidad.

Derivado de los oficios números: FGE/VFINV/2283/2021, de la Vicefiscalía de Investigación, FGE/IFCP/0309/2021, del Instituto de Formación y Capacitación Profesional, FGE/VCAPJ/DGRHyDP/0665/2021, de la Dirección General de Recursos Humanos, FGE/DGPA/139/2021, la Dirección General de Presupuesto y Administración, al respecto notifico a usted la información rendida por dichas áreas.

1.- ¿Cuántas denuncias han tenido en el año del 2020 y 2021 de los siguientes delitos?

R:

DELITO	2020	2021
Sexting (Ley Olimpia) tanto para mujeres como para hombres.	84	27
Pornografía.	5	3
Usurpación de Identidad.	16	10
Usurpación de Identidad Equiparada.	27	11

En relación a los delitos de Grominng (Ciberacoso Sexual Infantil por internet), Ciberbulling (Ciber Acoso), Phishing (Suplantación de Identidad, Fraudes), Ransomware (secuestro de Información), no se encontraron registros, por lo tanto es aplicable el siguiente criterio emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Respuesta igual a cero. No es necesario declarar formalmente la inexistencia. En los casos en que se requiere un dato estadístico o numérico, y el resultado de la búsqueda de la información sea cero, éste deberá entenderse como un dato que constituye un elemento numérico que atiende la solicitud, y no como la inexistencia de la información solicitada. Por lo anterior, en Términos del artículo 42 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el número cero es una respuesta válida cuando se solicita información cuantitativa, en virtud de que se trata de un valor en sí mismo.

Resoluciones

•RDA 2238/13. Interpuesto en contra de la Procuraduría General de la República. Comisionada Ponente María Elena Pérez-Jaén Zermeño.
•RDA 0455/13. Interpuesto en contra del Instituto Nacional de Migración. Comisionado Ponente Ángel Trinidad Zaldívar.
•RDA 4451/12. Interpuesto en contra de la Procuraduría Federal de la Defensa del Trabajo. Comisionada Ponente María Elena Pérez-Jaén Zermeño.
•RDA 2111/12. Interpuesto en contra de la Presidencia de la República. Comisionada Ponente María Elena Pérez-Jaén Zermeño.
•4301/11. Interpuesto en contra de la Secretaría de Comunicaciones y Transportes. Comisionada Ponente Sigrid Arzt Colunga.

2.- ¿Cuántos cursos de capacitación en materia de delitos informáticos se han impartido al personal de la Fiscalía del Estado de Guerrero en el año 2020 y 2021?

R:

2020	6 capacitaciones
2021	0

3.- ¿Nombres de los cursos que tomaron los ministerios públicos para capacitación de delitos informáticos o cibernéticos en el año del 2020 y 2021?

R:

2020	SECAP(Sistema Electrónico para el Control de Averiguaciones Previas)	16 de julio
	Conferencia: BNAVIM (Banco Nacional de Datos e Información sobre Casos de Violencia contra k las mujeres).	17 de julio
	Plataforma México, conceptos Generales	29 de julio
	Actualización y Capacitación de las Nuevas Herramientas de la APP de la Fiscalía Gral. del Estado.	13 de agosto
	Curso de capacitación en materia de Inteligencia Patrimonial y Económica	14 al 19 de Diciembre
2021	-	0

4.- ¿Numero de Ministerios Públicos que participaron en estos cursos relacionados con delitos informáticos?

R:

2020	SECAP(Sistema Electrónico para el Control de Averiguaciones Previas)	67 MPS
	Conferencia: BNAVIM (Banco Nacional de Datos e Información sobre Casos de Violencia contra k las mujeres).	34 MPS
	Plataforma México, conceptos Generales	44 MPS
	Actualización y Capacitación de las Nuevas Herramientas de la APP de la Fiscalía Gral. del Estado.	48 MPS
	Curso de capacitación en materia de Inteligencia Patrimonial y Económica	32 MPS
2021	-	0

5.- De los Ministerios Públicos en función actualmente ¿Cuántos son hombres y cuantos son mujeres?

R:

- 294 hombres MP
- 285 mujeres MP

6.- ¿Qué mecanismo o protocolo especializado implementa la Fiscalía para atender el delito contemplado en el artículo 187 de difusión no autorizada de imágenes y videos no autorizada?

R: No existe mecanismo o Protocolo especializado en esta Fiscalía para atender el delito contemplado en el artículo 187 en difusión no autorizada de imágenes y videos no autorizada.

7.- ¿Que mecanismo o protocolo especializado implementa la Fiscalía para atender el delito de Grooming (ciberacoso sexual infantil por internet)?

R: No existe mecanismo o Protocolo especializado para atender el delito de Grooming (Ciberacoso sexual infantil por internet)

8.- ¿Tiene la Fiscalía del Estado de Guerrero un presupuesto asignado de forma especial para atender delitos informáticos?

R: Al respecto le informo a usted que esta institución no cuenta con un presupuesto asignado con el rubro "DELITOS INFORMATICOS"

9.- ¿La Fiscalía tiene una agencia especializada para atender delitos informáticos en el estado, (cuál es el nombre de ser afirmativa la respuesta)?

R: Actualmente la Fiscalía General del Estado no cuenta con una Agencia Especializada para atender Delitos Informáticos en el Estado.

Gracias por ejercer tu derecho de acceso a la información.

ATENTAMENTE.
TITULAR DE LA UNIDAD DE TRANSPARENCIA
Y ACCESO A LA INFORMACIÓN PÚBLICA.

FISCALÍA GENERAL
DEL ESTADO DE GUERRERO
ÓRGANO INTERNO DE CONTROL
UNIDAD DE TRANSPARENCIA Y ACCESO
A LA INFORMACIÓN PÚBLICA
CHILPANCINGO DE LOS BRAVO, GRO.

LIC. FABIOLA RAMÍREZ BENÍTEZ.

C.c.p. Mtro. Jorge Zuriel de los Santos Barrila.- Fiscal General Del Estado.- Para su superior conocimiento.- Presente.
C.c.p.- Mtra. Iliana Liborio Díaz.- Contralora Interna y Presidenta del Comité de Transparencia y Acceso a la Información Pública de la FGE. - Para su conocimiento. – Presente.

FRB*barn

REFERENCIAS:

Acurio del Pino, S, (2016), Delitos Informáticos: Generalidades. México. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

ABOSO, G. E. Derecho penal cibernético, Buenos Aires, B de F, 2018.

Alonso, L. A., y Esparza Leibar, I. (2017). Los retos procesales de la criminalidad informática desde una perspectiva española. Novum Jus, 11(1), 39-72. https://doi.org/10.14718/NovumJus.2017.11.1.2 ***https://novumjus.ucatolica.edu.co/article/view/1427/1906***

Agustina, J. R. (2021). *Nuevos retos dogmáticos ante la cibercriminalidad ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma?* Estudios Penales y Criminológicos. https://www.researchgate.net/profile/JoseAgustina/publication/352397866_Nuevos_retos_dogmaticos_ante_la_cibercriminalidad_Es_necesaria_una_dogmatica_del_ciberdelito_ante_un_nuevo_paradigma_in_press/links/60c8364a299bf108abd971ea/Nuevos-retos-dogmaticos-ante-la-cibercriminalidad-Es-necesaria-una-dogmatica-del-ciberdelito-ante-un-nuevo-paradigma-in-press.pdf

Anselm Von Feuerbach P. J. (1801) *Lehrbuch des gemeinen in Deutschland gültigen peinlechen Rechts* (Tratado del Derecho penal común vigente en Alemania) Alemania. *Revista de Derecho Penal y Procesal Penal*, (2), 3–25. https://csl.mpg.de/en/publications/paul-johann-anselm-von-feuerbach-y-su-tratado-de-derecho-penal-comun-vigente-en-alemania-1801spanische-ubersetzung-von-p/

Assolini F. (2019) *Kaspersky registra 45 ataques por segundo en América Latina*. Sitio noticias de Kaspersky Latinoamerica-Argentina.

https://latam.kaspersky.com/blog/kaspersky-registra-45-ataques-por-segundo-en-america-latina/15274/

Argüelles Arellano, M. del C. (2016). *Retos de la legislación informática en México. Computación y Sistemas*, pág.827. 20(4), 827-831. https://doi.org/10.13053/cys-20-4-2515

Avast. Belcis I. (2019) *¿Qué es el Malware?* Sitio oficial Avast Company. https://www.avast.com/es-es/c-malware#:~:text=%C2%BFQu%C3%A9%20es%20el%20malware%3F&text=Malware%20es%20un%20t%C3%A9rmino%20general,objetivos%20de%20un%20modo%20diferente.

Bernárdez Cabello y Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva frente a las ciberamenazas", 116., 2015, ISBN 9788490852576, págs. 111-123 Idioma: español http://digital.casalini.it/3053113

Callegari, N. (1985) Delitos informáticos, Revista de la Facultad de Derecho de la UBP, Colombia. pág. 112-118. https://revistas.upb.edu.co/index.php/derecho/article/view/5140

Cárdenas G. (2014) Delitos Informáticos y Rol, DIVINDAT segunda parte. http://repositorio.caen.edu.pe/bitstream/handle/caen/67/3%20Delitos%20informaticos%20y%20rol%20DIVINDAT%20-%202%20parte.pdf?sequence=3

Carrasco Solís J. y Saucedo Rangel A. (2016) *INFORME ESTADO DE MORELOS Sistema Acusatorio Adversarial*, *SEGUIMIENTO DE LOS PROCESOS DE IMPLEMENTACIÓN DE LA REFORMA PENAL EN MÉXICO.* https://biblioteca.cejamericas.org/bitstream/handle/2015/5477/informe

morelos_sistemaacusatorioadversarial.pdf?sequence=1&isAllowed=y

Castellanos Tena, F. (1959) *Lineamientos Elementales de Derecho Penal, Jurídica Mexicana, 1ºa Edición,* México.

Código penal del estado de Guerrero, (2020) *CÓDIGO PENAL DEL ESTADO DE GUERRERO,* H. congreso del estado de Guerrero, 2020. Artículo 217. http://www.ordenjuridico.gob.mx/Estatal/GUERRERO/Codigos/GROCOD07.pdf

CÓDIGO PENAL DEL ESTADO DE MORELOS, (2021) Articulo 148 Quarter. Consejería Jurídica del Poder Ejecutivo del Estado de Morelos. http://marcojuridico.morelos.gob.mx/archivos/codigos/pdf/CPENALEM.pdf;c

Código penal del estado de Querétaro (2020) *CÓDIGO PENAL DEL ESTADO DE QUERÉTARO*, H. congreso del estado de Querétaro. Artículo 159. http://legislaturaqueretaro.gob.mx/app/uploads/2016/01/COD004.pdf

Constitución Política de los Estados Unidos Mexicanos (2020) H. cámara de Diputados. http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Constitucion_Politica.pdf

Código Penal Federal de los Estados Unidos Mexicanos. (Código Federal). http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_Penal_Federal.pdf

CÓDIGO PENAL PARA EL ESTADO DE SINALOA (1997) Congreso local de Sinaloa.

http://laipsinaloa.gob.mx/images/leyes/archivos/pdf/CODIGO%20PENAL.pdf

CONDUSEF (2019). *FRAUDES CIBERNÉTICOS Y TRADICIONALES, SHCP.* https://www.condusef.gob.mx/documentos/comercio/FraudesCiber-4toTrim2019.pdf

Congreso de la República de Perú. (2013) "*LEY Nº 30096, LEY DE DELITOS INFORMÁTICOS*".https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Delta Asesores (2018) *Ley de Delitos Informáticos en Colombia,* Delta Asesores blog. https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

DragonJar,(s.f.) *Laboratorios: Informática Forense, Introducción y Contenido,* dragonjar.org.https://www.dragonjar.org/laboratorios-informatica-forense-introduccion-y-contenido.xhtml

El Tiempo. (2014) *Cada segundo se crean tres virus informáticos en el mundo.* El tiempo Noticias. https://www.eltiempo.com/archivo/documento/CMS-14402815

ENVIPE (2018) *ENCUESTA NACIONAL DE VICTIMIZACIÓN Y PERCEPCIÓN SOBRE SEGURIDAD PÚBLICA*. INEGI.BOLETÍN DE PRENSA NÚM. 425/18 https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2018/EstSegPub/envipe2018_09.pdf

ESTRADA GARAVILLA M.(2008)DELITOS INFORMÁTICOS, http://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080526_32.pdf

Fiscalía General de Colombia (2018) *Boletín 24230, Fiscalía* General de la Nación de Colombia. Departamento de Comunicación y Legislación. s.p. https://www.fiscalia.gov.co/colombia/seccionales/capturadas-121-personas-por-delitos-informaticos/

Fiscalía General del Estado de Jalisco. (2017) *Policía Cibernética.* https://fiscalia.jalisco.gob.mx/content/policia-cibernetica-0#:~:text=La%20Fiscal%C3%ADa%20del%20Estado%20a,de%20que%20la%20Polic%C3%ADa%20Cibern%C3%A9tica

Gamba J., (2010) *Panorama del derecho informático en América Latina y el Caribe.* Comisión Económica para América Latina y el Caribe (CEPAL) https://repositorio.cepal.org/bitstream/handle/11362/3744/1/S2009865_es.pdf

García, Rolando (2006). *Sistemas complejos. Conceptos, método y fundamentación epistemológica, de la investigación interdisciplinaria*. Barcelona, Editorial Genisa.

GERALDES DA CUNHA LOPES T. M. (2011) "*Las recientes reformas en materia de protección de datos personales en México"*, Anuario Jurídico y Económico Escurialense, XLIV (2011) 317-334 / ISSN: 1133-3677, https://dialnet.unirioja.es/descarga/articulo/3625376.pdf

Howard Kass, D. (2019) *Ataque a PEMEX, Ransomware* MSSP Alert https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/pemex-recovery-update/

Huerta Miranda, M. y Líbano Manzur C., Los Delitos Informáticos, Editorial Jurídica Cono Sur. 1996.

INFOBAE. (2020) *Estados Unidos acusó a cuatro militares chinos por el hackeo de Equifax*, Departamento de prensa y noticias internacionales Infobae. https://www.infobae.com/america/eeuu/2020/02/10/estados-unidos-acuso-a-cuatro-militares-chinos-por-el-hackeo-de-equifax-la-filtracion-de-datos-mas-grande-de-la-historia/

INFOBAE (2019) México, el país con más fraudes cibernéticos en América Latina, Departamento de prensa y noticias internacionales Infobae https://www.infobae.com/america/mexico/2019/06/10/mexico-el-pais-con-mas-fraudes-ciberneticos-en-america-latina/#:~:text=M%C3%A9xico%20es%20el%20pa%C3%ADs%20que,comercio%20electr%C3%B3nico%20y%20banca%20m%C3%B3vil.

Jiménez Rojas J. R. (2016) **DELITOS INFORMÁTICOS EN MÉXICO**, Revista Bimestral. No. 26, febrero - marzo, ISBN:1 251 478, 1 251 477. https://revista.seguridad.unam.mx/sites/default/files/revistas/pdf/26_RevistaSeguridad-Emulacion_con_honeypots.pdf

La Línea política Redacción (2020) *ATENDER COMPLEJIDADES EN LA INVESTIGACIÓN DE DELITOS QUE VIOLENTAN INTIMIDAD DE LAS MUJERES EN EL CIBERESPACIO, RETO DE LA FGJCDMX, Línea Política, Columna 3. México.* https://lineapolitica.com/atender-complejidades-en-la-investigacion-de-delitos-que-violentan-intimidad-de-las-mujeres-en-el-ciberespacio-reto-de-la-fgjcdmx/

Landa Duran, G.M. (2007), *Los delitos informáticos en el Derecho penal de México y España*. Revista del Instituto de la Judicatura Federal. https://www.ijf.cjf.gob.mx/publicaciones/revista/24/r24_9.pdf

Leonardo G., Rodríguez Z., Pascal R., Paula G. (2015) *pensamiento complejo y ciencias de la complejidad,* universidad autónoma metropolitana, México pp.191

Levet Rivera C. E, Espinoza Maza J. de J., Macgluf Issasi A., Fragoso Terán J.M.(2019) *La inconclusa Reforma al Código Penal Federal en Materia de Delitos Informáticos*, Interconectando Saberes ISSN: 2448- 8704 pp.7-18 https://is.uv.mx/index.php/IS/article/view/2628

Loredo Gonzáles J. A. y Ramírez Granados A. (2013)" Delitos *informáticos: su clasificación y una visión general de las medidas de acción para combatirlo"* Facultad de Ciencias Físico Matemáticas Universidad Autónoma de Nuevo León San Nicolás de los Garza, Nuevo León, México. PP. 44-51. Sitio web http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Lucerna Herrera, C. (2019) *Que es el haking*, OpenWebinars https://openwebinars.net/blog/que-es-el-hacking/

Mayer S. (2016) "La importancia de evitar delitos informáticos". https://sites.google.com/site/equipo8delitosinformaticos/ensayo-sobre-la-importancia-de-evitar-delitos-informaticos

Medina Gómez, D. (2020). *Los delitos cibernéticos y los problemas a enfrentar. Hechos y Derechos*, 1(55). Instituto de Investigaciones Jurídicas, UNAM, México. https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/14381/15543

Morales Ortiz, J. O. (2015). *Teoría General del Delito Informático*. Centro de Capacitación Científico Tecnológico Laboral, primera edición, México.

Piña Libien H. R. (2016) *Los Delitos Informáticos previstos y sancionados en el Ordenamiento,* Orden Jurídico, versión virtual y digitalizada México. http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf

Pérez Luño A. E. (1998) *Internet y el Derecho,* Orden Jurídico, versión virtual y digitalizada México. .https://dialnet.unirioja.es/descarga/articulo/248265.pdf

Proceso Editorial. (2020) *La Fiscalía de la CDMX crea unidad especial para atender ciber delitos sexuales.* Revista Proceso, México. https://www.proceso.com.mx/nacional/cdmx/2020/8/27/la-fiscalia-de-la-cdmx-crea-unidad-especial-para-atender-ciberdelitos-sexuales-248399.html

Ramírez Martínez, B. (2018). *El sistema de justicia penal acusatorio: diagnóstico, crítica y propuestas.* Hechos y Derechos, s.p. https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/12419/14026

Real Academia Española. (s.f.) *Diccionario de la Real Academia Española, RAE. Es* https://dle.rae.es/j%C3%A1quer#TLIznqw

Real Academia Española. (s.f.) *Diccionario de la Real Academia Española, RAE. Es* https://dle.rae.es/software

Real Academia Española. (s.f.) *Diccionario de la Real Academia Española, RAE. Es* https://dle.rae.es/hardware?m=form

Rinaldi, P. (2017) *¿DE DÓNDE VIENE EL DELITO CIBERNÉTICO? ORIGEN Y EVOLUCIÓN DEL DELITO CIBERNÉTICO, LE VPN* https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

Robles Garay, O. A. (1999) *Evolución de internet en américa latina y el caribe.* ITESM, Campus Monterrey, México. SIMPOSIO LATINOAMERICANO Y DEL CARIBE: LAS TECNOLOGÍAS DE INFORMACIÓN EN LA SOCIEDAD. AGUASCALIENTES, págs. 257-264 https://interred.files.wordpress.com/2007/02/evolucion_de_internet_en_america_latina_y_el_caribe.pdf

Saavedra Fajardo (2003) *El problema del exceso de leyes,* Contrapeso. http://contrapeso.info/2003/el-problema-del-exceso-de-leyes/

SEGOB. (2014) *CURSO DE ESPECIALIZACIÓN PARA INTEGRANTES DE LAS UNIDADES DE POLICÍA CIBERNÉTICA,* Secretaria de Gobernación. https://www.gob.mx/cms/uploads/attachment/file/236695/PRP_-_10.pdf

SEGOB. (2016) *Revista Nuevo Sistema de Justicia Penal,* Revista semestral del Consejo de Coordinación para la Implementación del Sistema de Justicia Penal, Número 8,9. Volumen X.https://www.gob.mx/cms/uploads/attachment/file/53039/Revista_NSJP_X.pdf

SEGOB. Guardia Nacional (2020). Comunicado de Prensa 859, Secretaria de Gobernación. https://www.gob.mx/guardianacional/prensa/arranca-la-campana-nacional-antifraude-cibernetico-que-impulsan-la-guardia-nacional-y-las-unidades-de-policia-cibernetica-del-pais?idiom=es

Valencia Álvarez A. (2020) Revista de la Facultad de Derecho Veracruzana, ISSN en trámite, Veracruz, México. https://www.uv.mx/derecho/files/2019/04/Revista-de-la-Facultad-de-Derecho-No-3-Impacto-de-los-delitos-informaticos-en-la-sociedad-actual.pdf

Vázquez Marín, Ó. (2008). *La implementación de los juicios orales en el sistema de justicia penal mexicano: ¿qué sigue después de la reforma constitucional?* Reforma Judicial. Revista Mexicana de Justicia, 1(12). México, s.p. doi :http://dx.doi.org/10.22201/iij.24487929e.2008.12.8732

Velázquez Elizarraras J. C. (2007) *El estudio de las relaciones jurídicas internacionales, aplicación del Derecho Internacional*. Universidad Autónoma de México.

Vuanello R. (2011) *La cibercriminalidad como atentado a los derechos humanos de los más jóvenes, Rev. Crim. vol.53 no.1 Bogotá junio 2011.* http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082011000100004

Téllez Valdés, J. (1996) *Los Delitos informáticos. Situación en México*, Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida,

Temperini Ignacio, M.G. (2013) *Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra.* http://conaiisi.unsl.edu.ar/ingles/2013/82-553-1-DR.pdf

Torres Ruiz, P. (S.A.) *ASPECTOS GENERALES DE LOS DELITOS INFORMÁTICOS Y EL COMBATE A LOS MISMOS*, Orden Jurídico.

http://ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/TorresRuiz.pdf

Zambrano Mendieta J. Dueñas Zambrano K.I. Macías Ordoñez L.M. (2016) *Delito Informático. Procedimiento Penal en Ecuador, dom. Cien., ISSN: 2477-8818 Vol. 2, núm. esp. Ago., 2016, pp. 204-215.* https://dialnet.unirioja.es/descarga/articulo/5761561.pdf