Combate a la Delincuencia Cibernética

Carlos Antonio Vázquez Azuara

saber / trascender

Editorial Universidad de Xalapa
Xalapa, Ver., México, 2012

PRIMERA EDICIÓN

ESTA OBRA FUE REALIZADA POR
EDITORIAL FORO FISCAL S. DE R. L. DE C. V.
SE IMPRIMIÓ EN LA CIUDAD DE XALAPA, VERACRUZ, MÉXICO
EN FEBRERO DEL AÑO 2012, CON UN TIRAJE DE 500 EJEMPLARES
TALLERES Y OFICINAS EN VICENTE GUERRERO
NUMERO 12, DESPACHO 4, COLONIA CENTRO
C.P. 91000
ISBN: 978-607-9066-01-7

SEGUNDA EDICIÓN

ESTA OBRA FUE REALIZADA POR
EDITORIAL UNIVERSIDAD DE XALAPA A. C.
SE IMPRIMIÓ EN LA CIUDAD DE XALAPA, VERACRUZ, MÉXICO
EN AGOSTO DEL AÑO 2012, CON UN TIRAJE DE 1000 EJEMPLARES
OFICINAS EN KILOMETRO 2, CARRETERA XALAPA-VERACRUZ,
FRACCIONAMIENTO ÁNIMAS
C.P. 91190
ISBN: 978-607-8156-08-5

A DIOS TODO PODEROSO Y LA VIRGEN DE GUADALUPE
Por ser el motor que impulsa y mueve mi vida

A MIS PADRES NORABERTHA Y CARLOS ANTONIO
Por haberme dado su vida entera para procurar la mía

A MI HERMANA NORA LUZ
Por haber sido una segunda madre y mi gran bendición

A MI CUÑADO ERIK ROMÁN
Por ser un hermano y un ejemplo de tenacidad y superación

A MI SOBRINO IKIEL
Por ser la alegría de nuestras vidas ¡Dios te bendiga!

A MI PROMETIDA BLANCA ESTELA
Porque en ti encontré a mi verdadero y único amor

Í N D I C E

PREFACIO 13
PRÓLOGO 15
INTRODUCCIÓN 19

CAPÍTULO 1
EL DERECHO BINARIO COMO UNA
NUEVA RAMA DEL DERECHO

1.1. DIVISIÓN, RAMAS DEL DERECHO Y
UBICACIÓN DEL DERECHO BINARIO 24
1.1.1. DEFINICIÓN DE DERECHO 24
1.1.2. EL DERECHO COMO CIENCIA 27
1.1.3. DIVISIONES Y RAMAS DEL DERECHO 30
1.1.4. UBICACIÓN DEL DERECHO BINARIO 33
1.2. EL DERECHO BINARIO Y SU IMPORTANCIA 36
1.2.1. LA ERA DIGITAL 36
1.2.2. REALIDAD VIRTUAL Y REALIDAD MATERIAL 37
1.2.3. ¿POR QUÉ DERECHO BINARIO? 42
1.2.4. CONCEPTO DE DERECHO BINARIO 43
1.3. ÁMBITOS DE ESTUDIO DENTRO
DEL DERECHO BINARIO 44
1.3.1. SOCIOLOGÍA BINARIA 44
1.3.2. DELITOS BINARIOS 44
1.3.3. OFIMÁTICA JURÍDICA 49
1.4. CONCLUSIONES DE ÉSTE CAPÍTULO 51

CAPÍTULO 2
LOS DELITOS INFORMÁTICOS Y CIBERNÉTICOS
A LA LUZ DEL DERECHO COMPARADO

2.1. ARGENTINA 54
2.2. ALEMANIA 54
2.3. AUSTRIA 56
2.4. CHILE 57
2.5. CHINA 58

2.6. ESPAÑA 59
2.7. ESTADOS UNIDOS 61
2.8. FRANCIA 63
2.9. HOLANDA 64
2.10. INGLATERRA 66
2.11. DELITOS INFORMÁTICOS Y CIBERNÉTICOS EN MÉXICO 66
2.12. CONCLUSIONES DE ÉSTE CAPÍTULO 112

CAPÍTULO 3
LA PERSECUCIÓN DE LOS DELITOS CIBERNÉTICOS

3.1. GENERALIDADES 116
3.1.1. DERECHOS FUNDAMENTALES 117
3.1.2. ADMINISTRACIÓN DE JUSTICIA 118
3.1.3. JUSTICIA PRONTA Y EXPEDITA 119
3.2. EL COMBATE A LA CIBER-DELINCUENCIA 123
3.3. IMPLICACIONES EN EL MUNDO GLOBALIZADO 128
3.4. CONSIDERACIONES FINALES DE ÉSTE CAPÍTULO 130

CAPÍTULO 4
ANÁLISIS DE LA INVESTIGACIÓN DE CAMPO RELACIONADA CON LA PERSECUCIÓN DE LOS DELITOS CIBERNÉTICOS

4.1. VALIDACIÓN DE LA MUESTRA Y EL INSTRUMENTO DE RECOLECCIÓN DE DATOS 138
4.2. RESULTADOS OBTENIDOS DE LA APLICACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS MIXTO 162
4.3. SISTEMATIZACIÓN GRÁFICA DE LOS RESULTADOS OBTENIDOS 210
4.4. RECONOCIMIENTO DE LOS DELITOS INFORMÁTICOS Y CIBERNÉTICOS EN VERACRUZ 270
4.5. ALCANCES DE LAS INDAGATORIAS EN TRATÁNDOSE DE DELITOS CIBERNÉTICOS 271
4.6. INTERPRETACIÓN DE LOS RESULTADOS OBTENIDOS 273
4.6.1. INSUFICIENCIA DE LOS TIPOS PENALES PARA LA PERSECUCIÓN DE LOS DELITOS CIBERNÉTICOS 273

4.6.2. FALTA DE INCLUSIÓN DE LOS DELITOS CIBERNÉTICOS EN EL ORDENAMIENTO PUNITIVO ESTATAL 274
4.6.3. DESCONOCIMIENTO Y CONFUSIÓN SOBRE LOS DELITOS INFORMÁTICOS Y CIBERNÉTICOS 275
4.7. CONSIDERACIONES FINALES DE ÉSTE CAPÍTULO 277

CAPÍTULO 5
PROPUESTA DE INCLUSIÓN DE LOS DELITOS BINARIOS EN LA LEY PUNITIVA DEL ESTADO DE VERACRUZ

5.1. ¿POR QUÉ DELITOS BINARIOS Y NO INFORMÁTICOS, CIBERNÉTICOS O ELECTRÓNICOS? 280
5.2. PROPUESTA DE REFORMA AL CÓDIGO PENAL DEL ESTADO DE VERACRUZ 286
5.3. CUESTIONES ANEXAS A LA REFORMA 293
5.4. EXPECTATIVAS DE LA REFORMA 297
5.5. CONSIDERACIONES FINALES DE ÉSTE CAPÍTULO 298

CONCLUSIONES GENERALES 299
REFERENCIAS BIBLIOGRÁFICAS 303
ANEXO 315

PREFACIO

La Universidad de Xalapa, comprometida con el desarrollo científico y la investigación en las diferentes áreas del conocimiento, presenta la obra "***COMBATE A LA DELINCUENCIA CIBERNÉTICA***", bajo el sello editorial de la propia casa de estudios, registrada ante el Instituto Nacional de Derechos de Autor y escrita por el **Dr. Carlos Antonio Vázquez Azuara**, actualmente docente de ésta Universidad y Jefe de las Licenciaturas en Derecho y Ciencias de la Educación.

Con la publicación de ésta obra, aunada a las ya existentes y las que se sigan generando, se busca propagar el nuevo conocimiento que se desarrolla al interior de ésta casa de estudios, así como aquel generado por los catedráticos e investigadores que forman parte de la Universidad de Xalapa y con ello, seguir impulsando la vanguardia científica y presentar obras que sirvan en las aulas para la adquisición de mas y mejor conocimiento y en consecuencia, seguir posicionando a México, en los escalafones de la innovación del conocimiento.

PRÓLOGO

El **Dr. Carlos Antonio Vázquez Azuara**, en su obra "***COMBATE A LA DELINCUENCIA CIBERNÉTICA***", ha desarrollado una serie de postulados teóricos, que fundamentan lo que denomina "derecho binario", el cual, dadas sus características, se vislumbra como una nueva rama del derecho, cuyo objeto de estudio, entre otros aspectos, es la regulación jurídica de la realidad virtual.

Asimismo, el "derecho binario" del que nos habla el autor, va más allá del derecho informático, pues parte de un campo de estudio más amplio y el establecimiento de nuevas áreas del conocimiento que se desprenden de los postulados teóricos que fundamentan esta nueva rama del derecho.

De igual modo, en ésta obra, se advierte una investigación de campo, realizada por el Dr. Azuara, que revela una serie de rezagos que existen en la administración de justicia en tratándose de los "delitos binarios", comenzando por el desconocimiento e incluso la falta de reconocimiento y por ende de tipificación, de este tipo de delitos.

También, se presenta un estudio comparado entre países y entre los Estados de la república mexicana, con relación a los delitos informáticos para establecer las diferencias y coincidencias que existen en este tipo de delitos en las diversas legislaciones del país y el mundo.

El Dr. Azuara, establece una propuesta de reforma al Código Penal de Veracruz, para incluir los "delitos binarios", haciendo revelaciones interesantes, tales como el establecimiento de la propiedad y la posesión binaria, la incorporación de delitos binarios que no se basan en los tradicionales, el reconocimiento jurídico de la realidad virtual, entre otras aportaciones.

El autor, nos deja claro, el camino tan amplio que aún falta por recorrer en materia de derecho binario, los retos que involucra la era digital y las deficiencias que existen en la regulación jurídica de la realidad virtual y propone una reforma que si bien es cierto, no pretende resolver los rezagos existentes en el combate a la delincuencia cibernética, igual de cierto es, que funge como parte aguas para continuar perfeccionando los mecanismos jurídicos que hasta el momento parecen ser insuficientes para resolver los problemas social- jurídicos que se suscitan con relación a las nuevas tecnologías e Internet.

En el mismo orden de ideas, el autor, parte del reconocimiento del derecho como ciencia y lo define desde una perspectiva de la teoría tridimensional del derecho, argumentando que el derecho como ciencia social, debe necesariamente, atender a los problemas que la sociedad enfrenta con base en la pobre regulación jurídica de Internet y de las nuevas tecnologías.

De igual forma, nos habla acertadamente sobre la sociología binaria, entendiéndose por tal, la que se desarrolla a través de las redes sociales, por tanto se habla de una socialización que transforma la manera de interrelacionarse, que dadas las nuevas tecnologías, no requiere contacto físico o comunicación frente a frente, sino que todo se concreta a un código binario.

También, el autor, nos habla sobre la ofimática jurídica, enfatizando con ello, el auxilio que las nuevas tecnologías brindan al estudio y evolución del derecho, refiriendo un campo de estudio muy interesante que también se desprende de los postulados teóricos que fundan el “derecho binario”.

Finalmente, en su propuesta de reforma, establece la necesidad de una mayor sanción al “delincuente binario”, en virtud de tener éste último, un grado de temibilidad mayor, es decir, al ser una persona mas

preparada y con conocimientos sobre las nuevas tecnologías e internet, puede causar un grado mayor de daño y dado el caso de la virtualidad de los hechos, existe una menor posibilidad o mayor dificultad para fincar responsabilidad y por ende, mayor dificultad para imponer una eventual sanción.

Es así, como el Dr. Carlos Antonio Vázquez Azuara, nos presenta en ésta obra, una serie de postulados teóricos y una investigación de campo muy completa, que representa un sendero de investigación novedoso, que se ha tocado en otras áreas del conocimiento, pero hasta el momento de una forma muy hermética, pero en ésta obra, se plasma un campo de estudio tan amplio como el derecho mismo y permite que en posteriores investigaciones, se tenga un panorama completo sombre la regulación jurídica de la realidad virtual y nos deja abierta la puerta para establecer mas y mejores mecanismos normativos, para resolver los problemas social-jurídicos que de forma cotidiana enfrenta el hombre común, cuando con un solo clic, se puede ingresar a un nuevo mundo que a la fecha se sigue explorando y tratando de regular a paso lento.

Sin duda, la presente obra, será referencia obligada para quienes estudian la regulación jurídica de internet y las nuevas tecnologías y sin duda, se convertirá en una fuente de conocimiento en un área que promete mucho, para la generación de nuevo cocimiento.

Marzo de 2012
Mtro. Carlos Antonio Vásquez Gándara
Mtro. Víctor Manuel Vásquez Gándara

INTRODUCCIÓN

Hoy en día, nos encontramos inmersos en una era digital, llena de avances tecnológicos, que no solo han facilitado la vida del hombre, sino también, han hecho dependiente al ser humano de tales avances. Los dispositivos celulares, computadoras portátiles, tablas digitales y el acceso de todos ellos a internet, han sido uno de los avances tecnológicos más significativos del siglo, permitiendo al hombre incursionar en una nueva era que trae consigo nuevos retos que enfrentar y nuevas normas que establecer.

La era digital, ha generado que gran parte de la población, tenga dos realidades que vive de forma cotidiana y de manera simultánea, esto es, la realidad material y la realidad virtual, la primera de las mencionadas, se regula con la serie de ordenamientos jurídicos que ya conocemos y que nos han regido desde tiempos inmemoriales, transformándose constantemente, para adecuarse a las exigencias de dicha realidad, pero la realidad virtual, en cambio, surge recientemente con el auge de las nuevas tecnologías e internet, permitiendo al usuario que desarrolle su vida cotidiana en un espacio virtual que en el caso de internet, es conocido como el ciberespacio; éste último, no tiene una regulación jurídica actualmente y todo lo que en la realidad virtual acontece, es terreno fértil como objeto de estudio del derecho y es en este sentido, que surge el "Derecho Binario", entendiéndose como "la rama del derecho que se encarga del estudio de las normas que regulan la relación entre los individuos basada en su realidad virtual y de ellos con dicha realidad, así como el estudio de las normas que regulan la conducta de los individuos basada en las nuevas tecnologías e Internet".

El "Derecho Binario" entonces, enfoca su atención a uno de los campos de acción jurídica menos estudiados por los juristas, muy a pesar que en México, en 2012, "el número de usuarios de Internet fue de 40.6 millones de personas, cifra que supera en un 14 por ciento a los 34.9

millones de 2011"[1] y Veracruz, en 2012, "es el cuarto estado del país respecto de conexión y usuarios de Internet, sólo por detrás del Distrito Federal, Nuevo León y Jalisco"[2].

Pero el "Derecho binario", funge como sustento doctrinario de la propuesta principal mencionada en líneas posteriores y que se desprende de lo resultados que arroja el estudio de campo que respalda ésta investigación y el cual revela el rezago existente en tratándose del combate a la delincuencia cibernética.

Para la comprensión de los delitos basados en las nuevas tecnologías y la internet, se presenta un estudio comparado de legislaciones de todo el mundo a fin de advertir en sus respectivos códigos penales las diferencias o coincidencias para la regulación jurídica de los delitos actualmente conocidos como informáticos, pero también se realiza un estudio comparativo entre legislaciones de los Estados, a fin de conocer las coincidencias y discrepancias con relación a la regulación jurídica de los referidos delitos informáticos.

Es así, que al explicar el "Derecho binario", se establece una antesala teórica para el tema principal que resulta ser el combate a la delincuencia cibernética, cuestión que según los datos estadísticos aportados en la investigación de campo que se presenta, aún encuentra innumerables rezagos, debido en gran parte, a la carencia de tipificación de lo que se denomina "Delito Binario".

El estudio de campo en la presente obra, consiste en la aplicación de un instrumento de recolección de datos mixto, dirigido a las autoridades

[1] Según las cifras del Estudio de Hábitos de los Usuarios de Internet en México 2012.
[2] Dato revelado por el director de Telecomunicaciones en el Estado de Veracruz, en febrero de 2012, previo a la presentación del Congreso "Día Internacional de las Comunicaciones con el tema Las Mujeres y Las Niñas en las Tecnologías de la Información y las Telecomunicaciones", que se celebraría en Mayo de 2012, en el mismo Estado.

de administración de justicia en Veracruz, aplicado a una muestra de 4 de 7 subprocuradurías que representan al Estado, dos de la zona centro, una de la zona sur y una de la zona norte, asimismo, se escogió una muestra aleatoria de 56 agencias y dependencias, que representan el 18.67% de la población total de 300 agencias.

De las 56 agencias mencionadas como muestra, se entrevistaron a sus respectivos funcionaros adscritos a las mismas, es decir, un representante por agencia, lo que nos da un total de 56 personas entrevistadas, entre las que se incluyeron oficiales de mesa, agentes del ministerio público y agentes de la agencia veracruzana de investigación.

Los resultados obtenidos de la aplicación del instrumento de recolección de datos mixto referido con antelación, nos revela la necesidad de incorporar al ordenamiento punitivo de Veracruz, el "Delito Binario", entendiéndose por tal, "la comisión de un acto antijurídico, antisocial, típico, culpable y punible basado en los delitos tradicionales o independientes de estos, cometidos con el uso de las nuevas tecnologías y/o el Internet, como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante, pudiendo causar una afectación o no, a la propiedad y/o posesión binaria de que se trate".

Finalmente, se establece una propuesta de reforma al Código Penal de Veracruz, para lograr una mayor eficacia en el combate a la delincuencia cibernética.

CAPÍTULO 1
EL DERECHO BINARIO COMO UNA NUEVA RAMA DEL DERECHO

1.1. División, ramas del Derecho y ubicación del Derecho Binario

El Derecho como una ciencia, indudablemente, requiere estar en constante transformación, adaptándose a los cambios que de forma consuetudinaria se generan en el entorno social y jurídico, lo cual a su vez propicia que se tengan que perfeccionar las áreas del conocimiento y es por ello, que como resultado de transformaciones, que se han generado con el estallamiento de la era digital, surge el Derecho Binario, como una nueva rama del derecho, que tiende a enfocar su estudio a la regulación jurídica del individuo relacionada con las nuevas tecnologías y el Internet.

Pero el Derecho Binario, a su vez, analiza otros ámbitos de estudio como lo son la sociología binaria y los delitos binarios, que son sub-disciplinas que surgen a la par de la concepción de esta nueva rama del derecho, pero que también obedecen a sus áreas fundadoras como lo son la sociología y el derecho penal.

El Derecho Binario, tiene la expectativa de posicionarse como un área del conocimiento sin precedentes, pues como se advertirá en páginas posteriores, va a estudiar la realidad virtual que prácticamente todos los individuos llevan aparejada con la realidad material, solo que la primera de las mencionadas, aún encuentra múltiples deficiencias en cuanto a su regulación jurídica.

1.1.1. Definición de Derecho

Para poder hablar de la división y las ramas del derecho, es importante primero definir qué es el Derecho y para lo cual, nos encontramos con diversos postulados teóricos que intentan proyectar una definición para su concepto, sin embargo, esto no es nada fácil, tal y como lo refirió en su momento Immanuel Kant, en su obra: Crítica de la Razón Pura, al

afirmar que "Los juristas buscan todavía una definición para su concepto del derecho". Pero la dificultad no radica evidentemente en la comprensión del derecho sino en que la realidad avanza a pasos agigantados, mientras que la vanguardia jurídica intenta alcanzarla a paso lento, por tanto, se advierte como las diversas concepciones del derecho que se han venido proyectando a través de teóricos de la talla de Miguel Reale, García Máynez, Luis Recasens Siches, Norberto Bobbio, entre muchos otros, ya son insuficientes para abarcar el gran campo actual del derecho.

Una de las definiciones más acuñadas sin duda es la que advierte al derecho como "un orden concreto, instituido por el hombre para la realización de valores colectivos, cuyas normas -integrantes de un sistema que regula la conducta de manera bilateral, externa y coercible- son normalmente cumplidas por los particulares, y en caso de inobservancia, aplicadas o impuestas por los órganos del poder público"[3].

Sin embargo, las definiciones que más han perdurado por sus alcances, son aquellas acuñadas por autores que respaldaron sus postulados en la teoría tridimensional del derecho, atendiendo a tres aspectos fundamentales del derecho, como lo son: "el hecho, el valor y la norma", o lo que resulta ser "la validez, la justicia y la eficacia" respectivamente; Pues bien, dicha teoría tridimensional del derecho, fue ampliamente estudiada por Eduardo García Máynez y Miguel Reale entre otros destacados juristas y refería una convivencia entre los postulados provenientes del iusnaturalismo, iuspositivismo y el realismo sociológico.

[3] García Maynez, Eduardo, "Filosofía del Derecho", Porrúa, México, 1989

La "Teoría Tridimensional del Derecho"[4] aborda aspectos de la constitución del mismo partiendo de un sentido justo y valorativo, formalmente valido y eficaz, por tanto, definiendo al derecho como "una integración normativa de hechos según valores"[5]

Por una parte el Iusnaturalismo, en su carácter universal, supremo y eterno, nos dice que la norma debe estar dotada de un aspecto justo, moral y valorativo, y que es inherente al ser humano, mientras que el Iuspositivismo, concibe a la norma solo por cuanto hace a que es emitida por órganos competentes, formalmente valida y expresando la voluntad del legislador, y por último, el Iusrealismo o realismo sociológico, advierte a la norma aplicada al hecho, y concibe su eficacia por cuanto hace a que resuelve problemas sociales.

Es así, que dichas corrientes, que generalmente se excluyen una de la otra y más aún, niegan entre sí la razón de su existencia, originan que se analice al derecho desde un aspecto tridimensional, exponiendo que el derecho, no debe atender únicamente a un aspecto justo, o formalmente válido o eficaz, si no que puede y debe poseer la interacción de todos esos atributos derivados de las corrientes filosóficas citadas con antelación.

Pues bien, atendiendo a la teoría tridimensional del derecho, se presenta una definición del derecho, pero incorporando además otro aspecto a la definición, que es la verificación científica de los conocimientos jurídicos.

Es así que podemos definir al Derecho como la serie de conocimientos susceptibles de verificación científica, que se encargan de estudiar la regulación de las relaciones entre individuos y su interacción en

[4] Reale, M. (1997), Teoría Tridimensional del Derecho (Trad. A. Mateos), Madrid, Editorial Tecnos. (Original en portugués, 1994).
[5] Reale, M., Teoría Tridimensional del Derecho, op. Cit., pág. 98

sociedad, mediante un orden normativo revestido de un aspecto justo y valorativo, formalmente valido y eficaz.

1.1.2. El Derecho Como Ciencia

De la definición presentada en el punto anterior, se puede advertir claramente que se habla de una serie de conocimientos susceptibles de verificación científica, lo cual a su vez genera una pregunta de debate obligada: ¿Es el Derecho una Ciencia?

La respuesta se vislumbra aparentemente complicada, pero antes de dar respuesta, se debe aclarar que existen corrientes encontradas, ya que mientras algunas afirman que el derecho no es una ciencia, otras fundamentan lo contrario, pero para el caso de la presente investigación, se expresará que el derecho dependiendo del fundamento de sus postulados, en ocasiones adquiere el carácter de ciencia y en ocasiones únicamente se advierte como una proyección sistematizada de conocimientos teóricos.

Es decir, contradiciendo un poco a Shakespeare, con su famoso “ser o no ser”, en el caso que nos ocupa, podemos expresar que el derecho tiene supeditado su carácter de científico al hecho de que los conocimientos que proyecta provengan de un método científico cuyos resultados sean susceptibles de verificación científica y ojo que no referimos comprobación científica, sino verificación, toda vez que en ciencias sociales, no es posible una rígida comprobación, pero si una verificación en el laboratorio de las áreas humanísticas que resulta ser la sociedad. El derecho por tanto en ocasiones puede ser advertido como ciencia y en ocasiones no.

Por tanto, resolviendo el dilema sobre si el derecho es o no una ciencia, es necesario primero dilucidar ¿Qué es una ciencia? Y sabiendo esto con claridad, se podrá entonces saber si el derecho es o no una ciencia, y para para dar respuesta a la pregunta anterior sin entrar a

tediosas definiciones, podemos decir que ciencia, es aquella serie de conocimientos debidamente organizados y sistematizados que son susceptibles de comprobación y/o verificación a través de un método científico, siendo este último aquel que permite la obtención de resultados relativamente incuestionables.

La importancia de que los postulados jurídicos proyectados por los doctrinarios del derecho, tengan rigor científico, radica en el hecho de que tales postulados adquirirán el carácter de conocimiento científico y por ende difícilmente sean cuestionables, de lo contrario, los conocimientos en esta materia, podrían enfrascarnos en debates interminables en la constante búsqueda de la verdad sin obtener nunca una aproximación más exacta y para muestra de lo expresado en éste párrafo, podemos poner un ejemplo utópico: Si cuando Albert Einstein, expresó su fórmula de $E=mc^2$, hubiera existido otra persona que hubiera afirmado que en realidad la formula correcta era $E=mc^3$, quizás ambos individuos, se hubieran enfrascado en interminables debates teóricos tratando de demostrar con argumentos que tenían la razón y quizás hubieran existido corrientes que apoyaran a uno u otro respectivamente sin finalmente dar la respuesta correcta ninguno de los dos, pero el debate nunca pudo existir siquiera, porque Albert Einstein, fue a su laboratorio y demostró que su fórmula era correcta a través de un método científico y con la presentación de resultados evidentes… pues bien, esto también ocurre en el derecho, solo que nuestro laboratorio, como decíamos anteriormente, es la sociedad, por tanto los conocimientos del derecho tendrán más aproximación a la verdad si se encuentran revestidos de rigor científico proveniente de la verificación a través de un método de la misma naturaleza, pero cuando esto no ocurre, el derecho pasa de un plano de ciencia a un plano de disciplina del conocimiento, pero no por ello, reiteramos, menos valioso.

Damos pues, respuesta a la pregunta: ¿Es el Derecho una Ciencia? La respuesta, tal y como veníamos anticipando anteriormente, es que sí es

una ciencia, pues cuenta con métodos científicos capaces de presentar resultados, que se acreditan en el laboratorio de las ciencias humanísticas (la sociedad), propiciando en consecuencia, conocimientos susceptibles de verificación científica, sin embargo, cuando esto no ocurre, el derecho se queda en un plano de postulados teóricos sin rigor científico, lo cual no demerita el enriquecimiento que han aportado los juristas eminentemente teóricos, ya que tal y como sabemos la filosofía no es una ciencia, sin embargo, es considerada por la comunidad científica como la madre de todas las ciencias, por tanto y partiendo de éste orden de ideas, tengan rigor científico o no los postulados jurídicos que se plantean en las grandes páginas del orbe del derecho, son indudablemente valiosos para el perfeccionamiento del ámbito jurídico.

Para sustentar el carácter de ciencia del derecho se puede advertir lo siguiente:

La ciencia dice Luis Villoro, "es un cuerpo de saberes, antes que un conocimiento, le importa la objetividad… la objetividad de su justificación le permite ser una garantía de verdad para cualquier sujeto que tenga acceso a sus razones"[6]

Pero la ciencia va más allá, puesto que requiere una verificación científica en caso de las ciencias sociales, a través de un método de la misma naturaleza.

Por otra parte, tal y como lo manifiesta Carlos Muños Rocha, el problema epistemológico de la ciencia jurídica radica en que se ha reducido la investigación del derecho al análisis lógico normativo sin incursionar en los otros aspectos que conforman al derecho lo cual implica una visión parcial del mismo[7]

[6] Villoro Luis, Creer, saber, conocer, Siglo XXI, México, 2004, p. 224.
[7] http://www.juridicas.unam.mx/publica/librev/rev/jurid/cont/20/pr/pr31.pdf

Asimismo, al iniciarse la década de los cincuenta, Alf Ross y Norberto Bobbio se propusieron la construcción de una Ciencia Jurídica que tuviera todos los atributos necesarios para hacerla acreedora del título de "verdadera ciencia", y en ambos casos, sobre una base empírica[8]

Por lo anterior, se puede afirmar que el Derecho es una ciencia, siempre que sus conocimientos sean susceptibles de verificación científica en la sociedad, a través de un método de la misma naturaleza.

1.1.3. Divisiones y Ramas del Derecho

La Ciencia del Derecho, para su mejor comprensión, debe en todo momento proyectarse ante los estudiosos del ámbito jurídico, de una forma organizada que permita un entendimiento claro de los conocimientos en cuestión, por tanto existen dos grandes divisiones del derecho, que son el derecho interno y el derecho internacional, este último se integra por dos grandes ramas del derecho, que son el Derecho Internacional Público y el Derecho Internacional Privado, por su parte el Derecho Interno se subdivide a su vez en tres grandes divisiones que son el Derecho Público, el Derecho Privado y el Derecho Social.

El Derecho Interno, es la parte del derecho que mediante las divisiones que a su vez lo constituyen (público, privado y social), regula mediante normas, las relaciones de los individuos que integran un determinado grupo social constituido como un Estado y también regula las relaciones de aquellos con el Estado mismo.

[8] Mabel García, Silvana, el derecho como ciencia, Invenio, vol. 14, núm. 26, Universidad del Centro Educativo Latinoamericano, Rosario, Argentina, junio 2011, pp. 13-38

En lo concerniente al Derecho Internacional, se puede definir como la totalidad de reglas sobre las relaciones (soberanas) de los estados, organizaciones internacionales y otros sujetos de derecho internacional entre si, incluyendo los derechos y deberes de los individuos relevantes para la comunidad estatal (o parte de esta)[9]

Asimismo, cuando hablamos de Derecho Público, como parte del Derecho Interno, se puede definir como aquel que regula la relación entre los particulares y el Estado, teniendo como ramas de su competencia el Derecho Constitucional, el Derecho Administrativo, el Derecho Penal, el Derecho Procesal, entre otras ramas del derecho, incluyendo las de reciente concepción.

En lo relativo al Derecho Privado como parte del Derecho Interno, es aquel que regula la relación entre los particulares, teniendo como ramas que lo constituyen al Derecho Civil y al Derecho Mercantil.

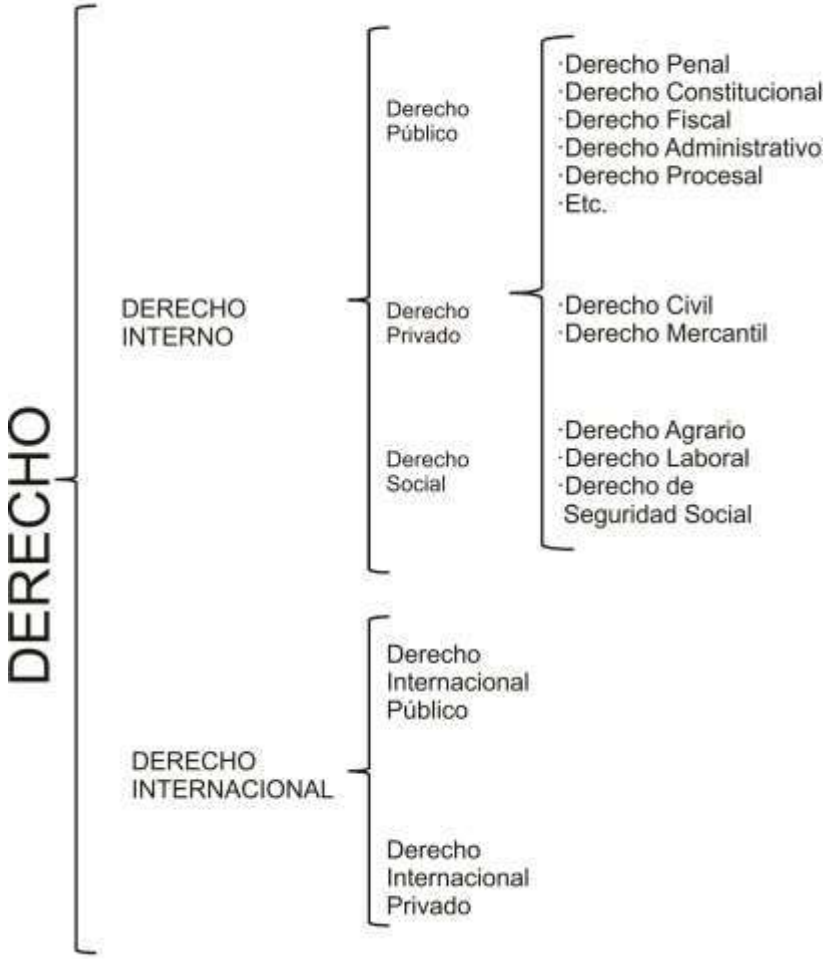
En lo relativo al Derecho Social, como parte del Derecho Interno, es aquel que regula el actuar de los particulares en su desempeño cotidiano partiendo del grupo social al que pertenecen, teniendo como ramas de su competencia el Derecho de Seguridad Social, el Derecho Agrario y el Derecho Laboral.

A continuación se presenta un esquema para reflejar lo anteriormente expuesto:

[9] Herdegen Matthias, Derecho Internacional Publico, UNAM, México, 2005, p. 3

CUADRO 1

DIVISIONES Y RAMAS DEL DERECHO



1.1.4. Ubicación del Derecho Binario

El Derecho Binario, como una nueva rama del derecho y del cual se hablará ampliamente en líneas posteriores, se ubica dentro de la división del Derecho Interno, pero también dentro de la división del Derecho Internacional.

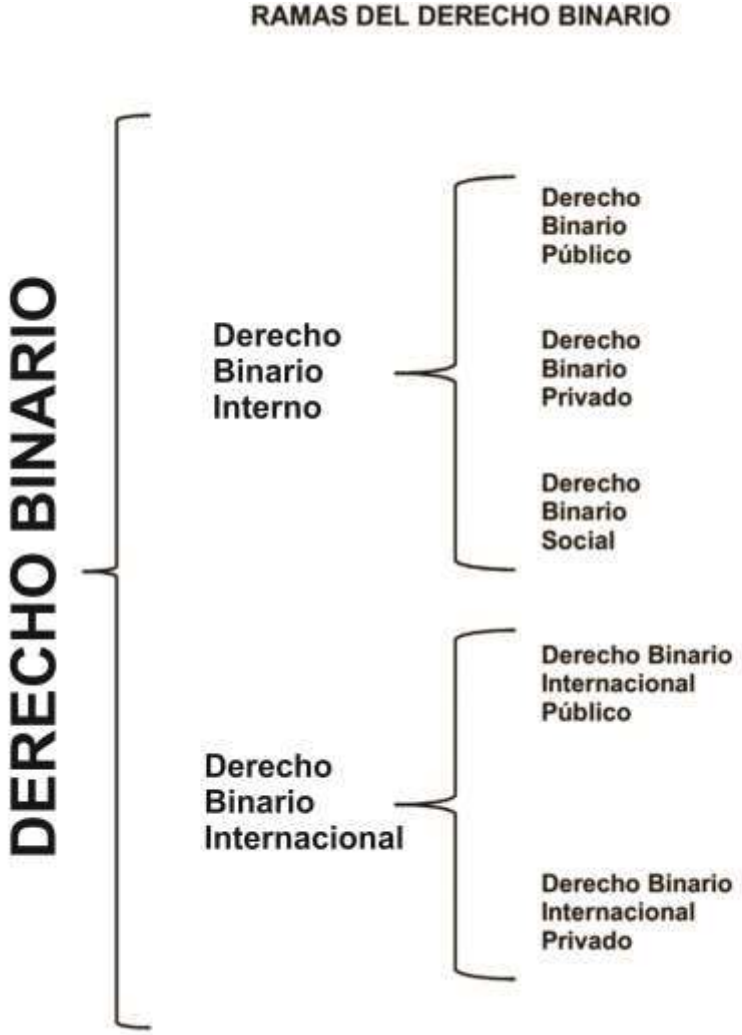
Se ubica dentro del Derecho Interno y a su vez dentro del Derecho Público, en virtud de que por su naturaleza tiene que ver con la regulación de las relaciones entre los particulares y el Estado, pero también dentro del Derecho Privado, toda vez que tiene que ver con la regulación de las relaciones entre particulares y finalmente también se ubica dentro del Derecho Social pues tiene que ver con la regulación del actuar de los particulares en su desempeño cotidiano partiendo del grupo social al que pertenecen, por tanto resulta correcto establecer que el Derecho Binario, forma parte del derecho interno en sus tres subdivisiones.

De igual modo, resulta importante destacar que el Derecho Binario, también se ubica dentro del Derecho Internacional, pues también tiene que ver con sus dos ramas, es decir, con el estudio de las normas que regulan las relaciones entre los Estados, entendiendo por Estados, aquellos entes conformados por territorio, población y gobierno y por ende también tiene relación con el estudio de las relaciones entre los Estados y los sujetos de derecho internacional.

De lo anterior, se puede comprender entonces, que el Derecho Binario, por la naturaleza de su campo de estudio, se ubica dentro del Derecho Interno y Dentro del Derecho Internacional, en consecuencia, esto origina que el Derecho Binario, tenga a su vez diversas ramas, como lo son: Derecho Binario Público, Derecho Binario Privado, Derecho Binario Social, Derecho Binario Internacional Público y Derecho Binario Internacional Privado.

En líneas posteriores, se tendrá una comprensión completa de cómo el Derecho Binario, en virtud de su campo de estudio, tiende a relacionarse prácticamente con todas las ramas del derecho que existen y por tanto, es imprescindible que se subdivida a su vez en otras ramas, las cuales para una mejor comprensión, se presentan en el siguiente cuadro:

CUADRO 2


RAMAS DEL DERECHO BINARIO
DERECHO BINARIO
Derecho Binario Interno
Derecho Binario Público
Derecho Binario Privado
Derecho Binario Social
Derecho Binario Internacional
Derecho Binario Internacional Público
Derecho Binario Internacional Privado

1.2. El Derecho Binario y su importancia

1.2.1. La era digital

Para comenzar con este apartado, valdría la pena hacernos una pregunta, ¿qué es la era digital?, para entender esto, es necesario remontarse al inicio de la edad contemporánea, que es el periodo histórico comprendido entre el inicio de la Revolución Francesa hasta la actualidad. Esto es un total de 223 años, entre 1789 y 2012 dividido en acontecimientos históricos bien definidos y marcados por el avance tecnológico constante iniciado con la Revolución Industrial, así como por las mayores guerras conocidas en la historia de la humanidad; esta época, se puede diferenciar de las que le anteceden, entre muchos otros aspectos, por el surgimiento de las nuevas tecnologías, el surgimiento de las computadoras, la Internet y en suma, el surgimiento de la era digital.

Si volteamos a nuestro alrededor, no es difícil advertir, que nos encontramos inmersos en un mundo digital, totalmente diferente, plagado de avances tecnológicos que facilitan la vida del hombre pero a la vez, lleno de retos, que nos obligan al conocimiento y a la vez genera nuevos cambios y mayores transformaciones, entre las cuales, definitivamente se encuentran las de tipo jurídico y hay autores que plantean la posibilidad de contemplar al ser humano ya no únicamente como el Homo Sapiens Sapiens, sino como el Homo Ciber Sapiens, término acuñado por Nicholas Negroponte, en su obra “Ser Digital”, para catalogar al ser humano inmerso en la era digital.

Las Nuevas tecnologías se entrelazan con la modificación de distintos componentes del régimen jurídico, de valores, principios, conceptos, normas reguladoras; con la aparición de nuevas modalidades en la creación del derecho y con cambios de puntos de vista sobre sus

fuentes, su naturaleza y contenido, sus modos de organización y funcionamiento[10].

Asimismo, se debe tener presente que una de las aportaciones más importante en materia digital, es la Internet, a través del correo electrónico, páginas web, negocios cibernéticos, redes sociales y redes en general en todo el mundo entre otros muchos usos. Un aspecto que debe destacarse, es que los usuarios de la Internet, o conocidos también como cibernautas, en un inicio, fueron empíricos en el uso de las nuevas tecnologías, pero actualmente, se recibe instrucción en esta materia en las escuelas desde la educación básica.

1.2.2. Realidad virtual y realidad material

Tal y como en su momento, Pitágoras afirmó que, todo es una realidad numérica, todo se puede contar, todo se puede medir, en el mismo orden de ideas, es procedente afirmar que todo es una realidad jurídica, es decir, todo está regulado por normas, de manera directa o indirecta y todos estamos supeditados a ciertos lineamientos normativos y siguiendo el mismo orden de ideas, todo es una realidad digital, pues hoy el individuo en su mayoría, no puede concebir su vida sin el apoyo de las nuevas tecnologías, entendiéndose por estas últimas los recientes desarrollos tecnológicos y sus aplicaciones, pero esto a su vez, trae como consecuencia un gran reto, pues nos encontramos en el desarrollo de la era digital, que debe regularse por normas que aún están en proceso de perfeccionarse, debiendo tomar en cuenta que el hombre actualmente vive dos realidades al mismo tiempo, la realidad virtual y la realidad material.

La realidad material, es la que vivimos de forma cotidiana, tangible y palpable, desempeñando actividades sociales, familiares, emocionales,

[10] Kaplan, Marcos, Ciencia, Estado y Derecho en la Tercera Revolución, UNAM, México, 2000.

laborales, de recreación entre otras y las cuales están reguladas por los diversos ordenamientos normativos que imperan en cada país.

La realidad virtual, es una realidad que vivimos a la par de nuestra realidad material, es intangible y transportable, basada en un código binario y en muchos casos es una realidad en la que interactuamos la mayor parte de nuestro tiempo y refiere aquella donde realizamos todas nuestras actividades sociales, familiares, emocionales, laborales, de recreación, entre otras, mediante las nuevas tecnologías y la Internet, sin embargo, en esta realidad los ordenamientos jurídicos que salvaguardan nuestros derechos, aún son endebles y carentes de eficacia.

Para poder comprender cómo la mayoría de los individuos, nos desenvolvemos en una realidad virtual y en una realidad material, de forma simultánea, atenderemos al siguiente ejemplo:

Una persona, se levanta a las siete de la mañana con apoyo de su televisor previamente programado para encenderse solo, telefonea a su trabajo que no podrá apersonarse por cuestiones de salud, pero que atenderá sus pendientes por la vía del correo electrónico, inmediatamente se arregla y desayuna en su domicilio, posteriormente se dirige a su estudio, donde enciende su computadora, en la cual se conecta a Internet y comienza a enviar correos electrónicos a diversos clientes y comienza a sostener charlas por medio de un software de conversación con otros prospectos a clientes… inicia una videoconferencia con algunos conocidos de la oficina y realiza algunos depósitos, mediante transferencias bancarias electrónicas por la Internet, una vez hecho esto, levanta el teléfono y ordena una pizza, posteriormente, ingresa a la red social de su preferencia y comienza a charlar por medio de ésta red social con su novia con la que se expresa diversas frases de amor y quedan pendientes para ir al cine al día siguiente, asimismo, para desesterarse un rato, pone una película en la

web, escucha un poco de su música favorita, finalmente ya entrada la noche, envía algunos mensajes de celular y se dispone a dormir para comenzar un nuevo día.

¿Qué advertimos del ejemplo anterior?, muy simple, en la realidad material del sujeto en cuestión, sólo vemos a un tipo que se levantó de su cama, se sentó la mayoría del día frente a la computadora y entrada la noche se retiró a dormir, esa fue su realidad material, pero en su realidad virtual, este sujeto, satisfizo sus necesidades laborales, emocionales, sociales y de recreación, y jamás lo vimos salir de su casa. Quizás éste no sea el caso de las mayorías, pero la verdad, es que típicamente combinamos nuestra realidad material, con nuestra realidad virtual, pero si esto es así ¿cuál es el problema?, es decir, la vida es más sencilla y cómoda.

El problema radica en la regulación jurídica de nuestra realidad virtual pues tal y como se menciona con antelación, esta realidad que todos vivimos, carece de ordenamientos jurídicos que la puedan regular eficazmente y por ende, es complicado que se salvaguarden nuestros derechos en este tipo de realidad y para comprender esto mejor, vamos a un ejemplo utópico:

Si en este momento, la tecnología nos permitiera llegar a Marte, y resultara que quisiéramos comenzar a poblar aquel planeta, lo primero que haríamos, sería resolver los problemas que impidieran el desarrollo de la vida humana como la conocemos en la tierra, y si de alguna forma lográramos resolverlos, lo primero que haríamos sería tratar de reproducir la vida que tenemos en la tierra en aquel planeta, pero este intento resultaría inútil porque al tratar de implementar las leyes que conocemos en la Tierra en Marte, se generaría un caos, porque para empezar la ley de la gravitación universal de la tierra, no obedece a la gravedad que hay en Marte, la ley de protección de la flora y la fauna en la tierra, no tendría sentido en aquel planeta puesto que ni siquiera se habría establecido el tipo de flora y fauna, la ley de la oferta y la

demanda, carecería de alcance puesto que lo que se vende en la tierra quizás no sería vendible en aquel planeta y en suma, las leyes de todo tipo, naturales, sociales etc., tendrían que adaptarse a las condiciones de aquel planeta y si se quisiera que las leyes que funcionan en la tierra, funcionaran igual en aquel planeta, habría un verdadero problema, lo que se necesitaría sería crear nuevas leyes y adaptar las que ya tenemos a las nuevas condiciones del nuevo planeta.

Pues bien, lo mismo pasa con la realidad virtual, el problema se hace evidente, cuando queremos utilizar las leyes que nos regulan en la realidad material, para que nos regulen en la realidad virtual, es lo mismo que en el ejemplo anterior, las leyes que funcionan en la tierra deberían adaptarse al planeta rojo para que pudieran sernos de utilidad, y aplicado a la realidad virtual y material, las leyes deben adaptarse a esa nueva realidad que tenemos los individuos para que funcionen adecuadamente y por ende puedan ser salvaguardados nuestros derechos.

Por ejemplo, si se realiza una compraventa en mi realidad material, simplemente hay que apersonarse al lugar donde radica el negocio del vendedor, se advierte el objeto de la compra, se realiza un contrato verbal con un consentimiento expreso de ambas partes, el comprador, entrega la cantidad de dinero requerida y el vendedor entrega el objeto de la compra y ante esto existen dos testigos que acompañan al comprador. Esto se encuentra regulado perfectamente por las leyes civiles relativas a las obligaciones.

Ahora bien, si éste supuesto lo lleváramos a cabo en nuestra realidad virtual, nos metemos a la página de compras por Internet de nuestra preferencia, contactamos a un vendedor, le enviamos datos por correo electrónico al igual que él nos envía sus datos, advertimos el objeto de la compra por fotos, realizamos un contrato que ni es “verbal” ni es “no verbal”, sino binario, en el que expresamos nuestra voluntad de

efectuar la compraventa y finalmente mediante una trasferencia bancaria electrónica, depositamos a la cuenta del vendedor la cantidad de dinero y él se compromete en un breve termino a mandarnos por servicio de envío el objeto de la compraventa. Hasta éste momento se sigue pensado que toda esta actividad, se encuentra perfectamente regulada por las leyes civiles relativas a las obligaciones.

Pero aquí es donde se da el problema, porque creemos que las leyes que funcionan en nuestra realidad material, tendrán la misma eficacia en nuestra realidad virtual y no es así.

En ambos casos se da la compraventa, solo que en la realidad material, puedo incoar acción por incumplimiento de contrato y en un momento dado también acción por fraude, incluso aportando el dicho de testigos, pero en la realidad virtual, si el vendedor no entrega el objeto de la compra, lo único que se puede demostrar es que se hizo una trasferencia de dinero y que existe el anuncio de un objeto en Internet para su venta, pero ¿cómo se demuestra todo lo que originó el acto que hoy es perjudicial al comprador?, si lo único que ocurrió materialmente hablando fue el transcurso de largas horas frente a la computadora… ¿qué evidencia tengo?, ¿las páginas web y las cuentas de correo?, ¿dónde dicen las leyes vigentes que tengan algún alcance y valor probatorio?, ¿cómo las vinculo al individuo del cual de por si casi no tengo datos?, ¿cómo demuestro que la cuenta de correo es de su propiedad?, ¿cómo le doy alcance y valor probatorio a lo acontecido en el ciberespacio?, si existían testigos, ¿qué van a declarar?, ¿Qué vieron a un individuo frente a la computadora?, ¿de quién es la competencia para conocer del caso?.

El mismo acto jurídico, realizado en diferentes realidades, no se puede salvaguardar mediante las mismas normas, es necesario crear nuevas y mejores normas para la realidad virtual, es decir, para los nuevos retos de la era digital, y es aquí donde entra el Derecho Binario.

1.2.3. ¿Por qué Derecho Binario?

Muchos intentos han existido para establecer una rama del derecho que se encargue de estudiar la relación de esta ciencia con la era digital, y los intentos originales de los que se tiene conocimientos parten del derecho informático y del derecho cibernético, así como de la informática jurídica, esta última como ciencia auxiliar, pero tales conceptos, no alcanzan a comprender todo el campo de estudio que involucra la relación del derecho con las nuevas tecnología y la internet, por tanto, resulta indispensable que la ciencia del Derecho contemple dentro de sus diversas áreas de estudio, una rama que logre satisfacer y encausar los conocimientos del derecho al ámbito de la era digital y es por ello que surge el Derecho Binario.

El Derecho Binario, se denomina como tal, puesto que, el único enlace que existe entre el hombre y la era digital, es un código denominado código binario, es decir, aquel constituido por unos y ceros, de ahí que se denomine binario. Pues bien, el Código Binario, permite a los medios digitales comprender las instrucciones dadas por el ser humano, es decir, es el lenguaje específico que se necesita para que un ordenador comprenda las instrucciones dadas por la parte humana. Cuando vemos en nuestro monitor un documento de un procesador de textos común y se advierte una hoja, con regla y márgenes, lo que estamos viendo evidentemente es para comprensión de los ojos del usuario, pero la realidad, es que lo que vemos en un trasfondo es una secuencia de unos y ceros.

Por tanto, al ser el Código Binario, el único medio que permite la manifestación de la era digital tal y como la conocemos, es que resulta correcto denominar a la nueva Rama del Derecho de la que se viene hablando, como Derecho Binario.

1.2.4. Concepto de Derecho Binario

El Derecho Binario, es la rama del derecho que se encarga del estudio de las normas que regulan la relación entre los individuos basada en su realidad virtual y de ellos con dicha realidad, así como el estudio de las normas que regulan la conducta de los individuos basada en las nuevas tecnologías e Internet.

El anterior concepto, da la pauta para un campo de estudio tan amplio como el derecho mismo, es decir, todo aquello que llevemos a cabo en nuestra realidad virtual, debe ser regulado también por normas eficaces para este entorno y dichas normas, son objeto de estudio del Derecho Binario, así como la consecuencia que estas tengan sobre la vida del individuo.

El Derecho Binario, también es conceptualizado desde una perspectiva tridimensional, toda vez que, en la definición anterior, cuando nos referimos a normas, nos referimos a una perspectiva que atiende a tres enfoques: Normas justas y valorativas, normas eficaces y normas formalmente válidas.

Cuando se habla del derecho binario atendiendo a normas justas y valorativas, se entiende que las mismas, deben estar constituidas desde una óptica iusnaturalista.

Cuando se habla del derecho binario atendiendo a normas eficaces, se entiende que las mismas, deben estar constituidas desde una óptica iusrealista.

Cuando se habla del derecho binario atendiendo a normas formalmente válidas, se entiende que las mismas, deben estar constituidas desde una óptica iuspositivista.

El Derecho Binario, encuentra apoyo por otras ciencias auxiliares del Derecho como lo es la Informática jurídica, siendo ésta, "la técnica interdisciplinaria que tiene por propósito la aplicación de la informática (entiéndase computadoras) para la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de dicha información, necesarios para una toma de decisión con repercusiones jurídicas[11]

1.3. Ámbitos de estudio dentro del derecho binario

1.3.1. Sociología Binaria

La sociología binaria, es la rama de la sociología que se encarga del estudio de la interacción entre los individuos y de éstos con su entorno social, mediante las nuevas tecnologías y el internet.

Esta rama de la sociología, surge de la manifestación del Derecho Binario, pues ahora, la manera de interrelacionarse ya ha pasado de un plano material a un plano virtual, es decir, se pueden hacer amigos, relaciones de pareja, incluso enemistades con personas a las que nunca se les ha visto jamás sino únicamente mediante un código binario que se traduce en un lenguaje que podemos entender satisfactoriamente.

1.3.2. Delitos Binarios

Es indudable que los delincuentes en aras de un mundo globalizado e inmerso en las nuevas tecnologías, han encontrado nuevas y mejores formas de delinquir, las cuales a su vez son más difíciles de sancionar, por ser más complicado arribar a la tan anhelada verdad histórica de los hechos.

[11] Téllez Valdés, Julio, Derecho informático, UNAM, México, 1991

Definición de Delito Binario:

Se entenderá por delito binario, la comisión del acto antijurídico, antisocial, típico, culpable y punible basado en los delitos tradicionales o independientes de estos, cometidos con el uso de las nuevas tecnologías y/o el Internet, como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante, pudiendo causar una afectación o no, a la propiedad y/o posesión binaria de que se trate.

En consecuencia, los delitos binarios, pueden ser de tres tipos:

1. Basados en los delitos tradicionales
2. Independientes de otros delitos
3. En perjuicio de la propiedad y/o posesión binaria

Por propiedad binaria, se entiende, el derecho que se tiene de uso, goce, usufructo y disfrute sobre bases de datos, sistemas de red, carpetas de información, archivos, programas, cuentas de correo electrónico, cuentas de redes sociales, sitios de internet, espacios virtuales y toda aquella información digital o sitios digitales, resguardados en el ciberespacio o en algún medio de almacenamiento, sin que necesariamente se tenga la posesión de las misma.

Por posesión binaria, se entiende el derecho que se tiene de uso, goce, usufructo y disfrute sobre bases de datos, sistemas de red, carpetas de información, archivos, programas, cuentas de correo electrónico, cuentas de redes sociales, sitios de internet, espacios virtuales y toda aquella información digital o sitios digitales, resguardados en el ciberespacio o en algún medio de almacenamiento, sin que necesariamente se acredite la propiedad de las mismas.

De la definición de delito binario, podemos deducir que, dicho acto puede involucrar la comisión de los delitos tradicionales, entendiéndose

por estos, los delitos tipificados como tales en los ordenamientos punitivos vigentes, pero mediante el uso de las nuevas tecnologías y/o el Internet, como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante para perpetrar dicho acto. La comisión a la que se refiere la definición anterior, puede ser por acción, o por omisión.

De igual forma, cuando se habla del uso de las nuevas tecnologías y el Internet, nos referimos a tres perspectivas de los Delitos Binarios: como un medio o canal para cometer el acto delictivo, como el objetivo o finalidad del acto delictivo y como el soporte o coadyuvante del acto delictivo.

Como un medio o canal para cometer el acto delictivo.- se refiere a la utilización de las nuevas tecnologías y/o el Internet, como el hilo conductor entre el sujeto activo y el sujeto pasivo del delito tradicional, por ejemplo, atentos a lo dispuesto en el Código Penal vigente en Veracruz, en su numeral 173 que a la letra dice: “Las mismas sanciones previstas en el artículo anterior, se aplicarán a quien amenace a otro con causarle un mal futuro en su persona o derechos, o en la de otra con la que tenga algún vínculo. Este delito se perseguirá por querella”, pues bien, si un individuo amenaza a otro enviándole un correo electrónico, está utilizando las nuevas tecnologías y/o la internet para cometer un acto delictivo en contra de otro sujeto.

Como el objetivo o finalidad del acto delictivo.- se refiere a las nuevas tecnologías y/o el Internet, como el receptor de la actualización del tipo penal que se configure, por ejemplo, atentos a lo dispuesto por el Código Penal vigente en Veracruz, en su numeral 226, que a la letra dice: “A quien, en perjuicio de tercero, por cualquier medio destruya o deteriore una cosa, total o parcialmente ajena o propia, se le impondrán de seis meses a ocho años de prisión y multa hasta de ciento cincuenta días de salario”. De éste supuesto jurídico, si una persona con dolo,

introduce a un ordenador una memoria USB, con un virus que lo desconfigura, con toda la intención de que esto ocurriera, está utilizando las nuevas tecnologías y/o el Internet como el objetivo o finalidad del acto delictivo.

Como soporte o coadyuvante del acto delictivo.- se refiere a la utilización de las nuevas tecnologías y/o el Internet, como apoyo para la consumación del acto ilícito sin ser necesariamente un medio o la finalidad, por ejemplo, atentos a lo dispuesto por el Código Penal Federal, en su numeral 424, que a la letra dice: "Se impondrá prisión de seis meses a seis años y de trescientos a tres mil días multa: "III. A quien use en forma dolosa, con fin de lucro y sin la autorización correspondiente obras protegidas por la Ley Federal del Derecho de Autor". De éste supuesto delictivo, podemos poner un claro ejemplo, ya que si un individuo descarga una obra reservada, esto no representa ningún problema, pues no es con ánimo de lucro, pero si después hace entrega del disco duro que posee el ordenador, para que otro imprima la información y la distribuya con ánimo de lucro, entonces el que descargó la información, no utilizó las nuevas tecnologías y/o el Internet como un medio o canal, pues sólo descargó y almacenó información, tampoco utilizó las nuevas tecnologías y/o el Internet como el objetivo o la finalidad, pues nunca dañó ningún ordenador, pero si utilizó las nuevas tecnologías y/o la internet como un soporte o coadyuvante, para que se cometiera el acto ilícito. En este caso, el que descargó la información y entregó el disco duro, fungiría como cómplice y el receptor del disco duro, sería el autor material, al mismo tiempo sería el que utilizó las nuevas tecnologías y/o la internet como soporte o coadyuvante del acto delictivo. En el mismo orden de ideas, esta perspectiva de los delitos binarios, se actualiza cuando se utilizan discos duros, para el almacenamiento de información que posteriormente es utilizada para la comisión de actos delictivos, siendo el puro almacenamiento un acto que por sí solo no constituye un delito, pero que si será un soporte o coadyuvante para actos ilícitos futuros.

Este tipo de delitos, de hecho, se encuentran reconocidos actualmente como delitos cibernéticos y de derecho, se encuentran tipificados como delitos informáticos entendiéndose por estos, “actitudes ilícitas en que se tienen a las computadoras como instrumento o fin" (concepto atípico) o las "conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" (concepto típico)”[12] y algunas acepciones han intentado llamarlos delitos electrónicos, pero ninguno de los términos descritos con antelación se aproxima a la realidad de este tipo de delitos, pues no se reconoce aún que nos encontramos en presencia de un actuar que involucra más allá de la informática, de la cibernética y de la electrónica, es decir, hablamos de un nuevo panorama paralelo al que ya conocemos constituido por un código binario que usamos de manera cotidiana y por tanto, existe una división muy clara de delitos, los delitos tradicionales y los delitos binarios, siendo que los primeros nos causan afectación en nuestra realidad material y siendo que los últimos nos causan una afectación a nuestra realidad virtual y material.

Definición de delincuente binario:

Consecuencia de los razonamientos anteriores, los delincuentes binarios, son aquellos que cometen un acto determinado como delito binario, dotados de conocimientos sobre el uso de las nuevas tecnologías y/o el internet, utilizándolos como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante, para la comisión del acto antijurídico, antisocial, típico, culpable y punible, lo cual infiere un mayor grado de temibilidad y por tanto una dificultad mayor para su aprehensión y por ende dichos actos involucran una mayor sanción.

[12] Ibídem, p. 82

1.3.3. Ofimática Jurídica

Un concepto que se pretende acuñar en la presente investigación, es el de ofimática jurídica, el cual se definirá a continuación, no sin antes definir primero que es la ofimática *per se.*

Pues bien, ofimática, es "el conjunto de técnicas, aplicaciones y herramientas informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionados"[13], es decir, es todo aquel software que permite la optimización de las funciones realizadas por los individuos.

Partiendo de este razonamiento, la ofimática jurídica, no es otra cosa que "La serie de conocimientos que comprende el estudio y utilización del software y hardware, común o especializado, al servicio del derecho y con el fin de optimizar, facilitar y coadyuvar con las funciones de los estudiosos y profesionistas del derecho".

De la anterior definición, se desprende lo que es el software común y el especializado, el segundo de los mencionados, se da en gran parte de las disciplinas que el hombre conoce y el derecho no es la excepción, ya que se entiende por software especializado aquel que requiere aparte de los conocimientos básicos en computación, conocimientos de otras disciplinas para su utilización y por software común se entiende aquel que de forma cotidiana utilizamos para facilitar las labores de nuestra vida y que no necesariamente requiere otro tipo de conocimientos que no sean los básicos en computación, para su utilización.

[13] http://www.alegsa.com.ar/Dic/ofimatica.php

A continuación, algunos ejemplos y comparaciones:

TABLA 1

SOFTWARE COMÚN	SOFTWARE ESPECIALIZADO			
	DERECHO	**DISEÑO GRÁFICO**	**ARQUITECTURA**	**CONTABILIDAD**
Microsoft Word	IUS	Photo Shop	AutoCAD	Sistematic
Microsoft Excel	FACES 4	Corel Draw	Scribus	Contabilidad GL
Microsoft Windows	Sv3DVision	Ilustrator	ALBA	Jazz Stock 5.0
Windows Media Player	Legis Pro	Indesign	Crossroads	Ciad

Como se puede advertir en la tabla anterior, el individuo inmerso en la era digital, utiliza diverso software para llevar a cabo su vida cotidiana y típicamente accede a programas comunes como los mencionados con antelación, pero cuando entramos al estudio de alguna disciplina especializada, ésta requiere software especializado y por tanto, la utilización del mismo, previos conocimientos sobre la materia, por ejemplo, el IUS, es un software que solamente los abogados pueden comprender en cuanto hace a sus alcances al igual que el AutoCAD para los arquitectos, que para su utilización involucra conocimientos previos de ciertas disposiciones relativas a la arquitectura.

La ofimática jurídica, como disciplina auxiliar del derecho, es un área de estudio que compete al derecho binario.

1.4. Conclusiones de éste capítulo

De los razonamientos vertidos a lo largo del presente capítulo, se puede arribar a los siguientes puntos concluyentes:

1. El Derecho es una ciencia, por cuanto hace a que sus conocimientos son susceptibles de verificación científica, de lo contrario, se queda en un plano de disciplina teórica, mas no por ello, menos valiosa.

2. El Derecho Binario, es una nueva rama del derecho, que es necesario reconocer y comenzar a estudiar, puesto que su campo de estudio, involucra un nuevo mundo, el mundo digital, la realidad virtual, de los cuales actualmente sólo podemos ver una reminiscencia, pero que en pocos años, será lo más estudiado del derecho.

3. El jurista de la nueva era digital, deberá adaptarse a los cambios y transformaciones de un mundo regido por el código binario, para lo cual deberá trasladarse de las letras a los bits y de los libros a la internet y en suma romper con el obsoleto esquema del abogado de las letras y pasar al esquema del abogado de los unos y los ceros.

4. Por su importancia, trascendencia y amplio campo de estudio, el Derecho Binario, se ubica tanto en el derecho interno como en el derecho internacional, dando esto como con secuencia a su vez diversas ramas que constituyen al Derecho Binario.

5. En la actualidad, la mayoría de los individuos, vivimos en dos realidades simultáneas, la realidad virtual y la realidad material. La primera de las mencionadas, aún tiene una regulación normativa endeble, plagada de carencias y demandante de nuevos

mecanismos jurídicos que permitan la salvaguarda eficaz de los derechos en general.

6. La Sociología Binaria, encuentra sustento teórico en la Sociología y en el Derecho Binario, teniendo como principal objetivo el estudio de la interacción entre los individuos y con su entorno social, mediante el uso de las nuevas tecnologías y la internet, pasando de un plano material a un plano virtual, pero en todo momento se debe dejar claro que la Sociología Binaria, es una rama de la sociología, la cual es un campo mas amplio que el Derecho mismo.

7. Los Delitos Binarios, son el resultado del perfeccionamiento de los mecanismos del delincuente para efectuar sus actos antijurídicos, antisociales, típicos, culpables y punibles, mediante el uso de las nuevas tecnologías y/o el internet, propiciando que el delincuente binario, tenga un grado de temibilidad mayor, una mayor dificultad en su persecución y por tanto merecedor de una mayor sanción.

CAPÍTULO 2
LOS DELITOS INFORMÁTICOS Y CIBERNÉTICOS A LA LUZ DEL DERECHO COMPARADO

En el presente capítulo, se tiene como principal objetivo, comparar las diversas legislaciones en materia penal, que imperan en otros países y el propio México, con el fin de establecer, la evolución que ha existido con respeto a los delitos cibernéticos, la manera en que se han tipificado y partiendo de esto, proyectar la relevancia de perfeccionar la legislación mexicana.

2.1. Argentina

En la legislación de Argentina, existen apuntamientos que permiten vislumbrar aunque no de manera formal, la existencia de los delitos informáticos, tal y como se advierte del código penal de la Nación Argentina, que en su capítulo VII, articulo 183, relativo a los daños, a la letra dice:

"…En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. (Párrafo incorporado por art. 10 de la Ley N° 26.388, B.O. 25/6/2008)"[14]

Si analizamos la descripción anterior, aunque el tipo penal descrito, refiere daños, no menos cierto es, que hace alusión a cuestiones informáticas, lo cual conlleva la posibilidad de tratar jurídicamente este tipo de delitos.

2.2. Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática, el 15 de mayo de 1986 se adoptó la Segunda Ley contra la Criminalidad Económica.

[14] Código Penal de la Nación Argentina, Capitulo VII, articulo 183, http://www.infoleg.gov.ar/infolegInternet/anexos/15000-19999/16546/texact.htm

Esta ley reforma el Código Penal (art. 148 del 22 de diciembre de 1987) para contemplar los siguientes delitos:

1. Espionaje de datos (202a).
2. Estafa informática (263a).
3. Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273).
4. Alteración de datos (303a) es ilícito cancelar, inutilizar o alterar datos e inclusive la tentativa es punible.
5. Sabotaje informático (303b).
6. Destrucción de datos de especial significado por medio de deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
7. Utilización abusiva de cheques o tarjetas de crédito (266b).
8. Por lo que se refiere a la estafa informática, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos o a través de una intervención ilícita. Esta solución fue también adoptada en los Países Escandinavos y en Austria.[15]

Aunado a lo anterior, el Código Penal Alemán, su artículo 202a refiere:

Piratería informática

(1) Quien sin autorización se procure para sí o para otro, datos que no estén destinados para él y que estén especialmente asegurados contra

[15] Legislación y Delitos Informáticos – Alemania, http://www.segu-info.com.ar/delitos/alemania.htm

su acceso no autorizado, será castigado con pena privativa de la libertad hasta tres años o con multa.

(2) Datos en el sentido del inciso 1, son solo aquellos que se almacenan o trasmiten en forma electrónica, magnética, o de otra manera en forma no inmediatamente perceptible.[16]

De lo referido con antelación, se puede advertir claramente, cómo Alemania, tiene una visión superior a la legislación mexicana con respecto a los delitos informáticos, cubriendo una mayor cantidad de supuestos jurídicos y por ende, procurando una mejor persecución de los delitos informáticos.

2.3. Austria

Según la Ley de reforma del Código Penal del 22 de diciembre de 1987, se contemplan los siguientes delitos:

Destrucción de datos (art. 126) no solo datos personales sino también los no personales y los programas.

Estafa informática (art. 148) se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.[17]

[16] Código Penal Alemán, López Díaz, Claudia, traductora, articulo 202a, http://www.unifr.ch/ddp1/derechopenal/obrasjuridicas/oj_20080609_13.pdf

[17] Legislación y Delitos Informáticos – Austria, http://www.segu-info.com.ar/delitos/austria.htm

En los tipos penales descritos por el código Penal de Austria, se aprecia claramente la inclusión de supuestos delictivos que involucran el ámbito de la informática, desde una perspectiva de daños.

2.4. Chile

Chile fue el primer país latinoamericano en sancionar una Ley contra Delitos Informáticos. La ley 19223 publicada en el Diario Oficial (equivalente del Boletín Oficial argentino) el 7 de junio de 1993 señala que la destrucción o inutilización de un sistema de tratamiento de información puede ser castigado con prisión de un año y medio a cinco.

Como no se estipula la condición de acceder a ese sistema, puede encuadrarse a los autores de virus. Si esa acción afectara los datos contenidos en el sistema, la prisión se establecería entre los tres y los cinco años.

El hacking, definido como el ingreso en un sistema o su interferencia con el ánimo de apoderarse, usar o conocer de manera indebida la información contenida en éste, también es pasible de condenas de hasta cinco años de cárcel; pero ingresar en ese mismo sistema sin permiso y sin intenciones de ver su contenido no constituye delito.

Dar a conocer la información almacenada en un sistema puede ser castigado con prisión de hasta tres años, pero si el que lo hace es el responsable de dicho sistema puede aumentar a cinco años. Esta ley es muy similar a la inglesa aunque agrega la protección a la información privada.[18]

Aunque de forma limitada, en la legislación chilena, se contempla la persecución de los delitos informáticos, nuevamente desde una

[18] Legislación y Delitos Informáticos – Chile, http://www.segu-info.com.ar/delitos/chile.htm

perspectiva de daños, aportando en su legislación el término de hacking, el cual es una modalidad de los delitos informáticos.

2.5. China

El Tribunal Supremo Chino castigará con la pena de muerte el espionaje desde Internet, según se anunció el 23 de enero de 2001.
Todas las personas "implicadas en actividades de espionaje", es decir que "roben, descubran, compren o divulguen secretos de Estado" desde la red podrán ser condenadas con penas que van de diez años de prisión hasta la muerte. ¿Castigo ejemplar?

La corte determina que hay tres tipos de actividades donde la vigilancia será extrema: secretos de alta seguridad, los secretos estatales y aquella información que dañe seriamente la seguridad estatal y sus intereses. Se consideran actividades ilegales la infiltración de documentos relacionados con el Estado, la defensa, las tecnologías de punta, o la difusión de virus informático.

El Tribunal ha hecho especial énfasis al apartado del espionaje desde la red. A los llamados "criminales", además de tener asegurada una severa condena (la muerte), también se les puede... ¡confiscar los bienes![19]

Sin duda, la actividad punitiva de la República de China, refleja castigos mortales para quienes hagan del espionaje su actividad delictiva, pero lo relevante, también resulta ser, el hecho de contemplar los actos ilícitos relacionados con la informática como un tipo penal propiamente dicho, lo que a todas luces, nos habla de un giro a los apartados que hemos venido analizando, ya que esta vez, se habla de una sanción que rebasa la pena privativa de la libertad y además no solo de daños sino de conspiración y perjuicios a los intereses de la nación.

[19] Legislación y Delitos Informáticos – China, http://www.segu-info.com.ar/delitos/china.htm

2.6. España

Este país quizás sea el que mayor experiencia ha obtenido en casos de delitos informáticos, en Europa.

Su actual Ley Orgánica de Protección de Datos de Carácter Personal (LOPDCP) aprobada el 15 de diciembre de 1999, la cual reemplaza una veintena de leyes anteriores de la misma índole, contempla la mayor cantidad de acciones lesivas sobre la información.

Se sanciona en forma detallada la obtención o violación de secretos, el espionaje, la divulgación de datos privados, las estafas electrónicas, el hacking maligno o militar, el phreacking, la introducción de virus, etc.; aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa o cuando el hecho es cometido por parte de funcionarios públicos.

Así mismo su nuevo Código Penal establece castigos de prisión y multas "a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos"[20].

Código Penal Español, Titulo X, Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, Capítulo I, Del descubrimiento y revelación de secretos, Artículo 197, párrafo 2 y 4

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en

[20] Legislación y Delitos Informáticos – España, http://www.segu-info.com.ar/delitos/espania.htm

cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

Código Penal Español, Titulo XIII, Delitos contra el patrimonio y contra el orden socioeconómico, Capitulo IX, De los daños, Artículo 263, Párrafo 2

2. La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Código Penal Español, Sección tercera, De los delitos relativos al mercado y a los consumidores, Artículo 278, párrafo 1 y 3

1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Código Penal Español, Sección tercera, De los delitos relativos al mercado y a los consumidores, Artículo 286, párrafo 1, Apartado 1

1. Será castigado con las penas de prisión de seis meses a dos años y multa de seis a 24 meses el que, sin consentimiento del prestador de servicios y con fines comerciales, facilite el acceso inteligible a un servicio de radiodifusión sonora o televisiva, a servicios interactivos prestados a distancia por vía electrónica, o suministre el acceso condicional a los mismos, considerado como servicio independiente, mediante:

1.1 La fabricación, importación, distribución, puesta a disposición por vía electrónica, venta, alquiler, o posesión de cualquier equipo o programa informático, no autorizado en otro Estado miembro de la Unión Europea, diseñado o adaptado para hacer posible dicho acceso.

1.2 La instalación, mantenimiento o sustitución de los equipos o programas informáticos mencionados en el párrafo 1.

2.7. Estados Unidos

El primer abuso de una computadora se registró en 1958 mientras que recién en 1966 se llevó adelante el primer proceso por la alteración de datos de un banco de Mineapolis. En la primera mitad de la década del 70, mientras los especialistas y criminólogos discutían si el delito informático era el resultado de una nueva tecnología o un tema específico, los ataques computacionales se hicieron más frecuentes. Para acelerar las comunicaciones, enlazar compañías, centros de investigación y transferir datos, las redes debían (y deben) ser accesibles, por eso el Pentágono, la OTAN, las universidades, la

NASA, los laboratorios industriales y militares se convirtieron en el blanco de los intrusos.

Pero en 1976 dos hechos marcaron un punto de inflexión en el tratamiento policial de los casos: el FBI dictó un curso de entrenamiento para sus agentes acerca de delitos informáticos y el Comité de Asuntos del Gobierno de la Cámara presentó dos informes que dieron lugar a la Ley Federal de Protección de Sistemas de 1985.

Esta ley fue la base para que Florida, Michigan, Colorado, Rhode Island y Arizona se constituyeran en los primeros estados con legislación específica, anticipándose un año al dictado de la Computer Fraud y Abuse Act de 1986.

Este se refiere en su mayor parte a delitos de abuso o fraude contra casas financieras, registros médicos, computadoras de instituciones financieras o involucradas en delitos interestatales. También especifica penas para el tráfico de claves con intención de cometer fraude y declara ilegal el uso de passwords ajenas o propias en forma inadecuada. Pero sólo es aplicable en casos en los que se verifiquen daños cuyo valor supere el mínimo de mil dólares.

En 1994 se adoptó el Acta Federal de Abuso Computacional (18 U.S.C. Sec 1030), modificando el Acta de 1986. Aquí se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a los comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos.

Modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito. Así, esta ley es un acercamiento real al problema,

alejado de argumentos técnicos para dar cabida a una nueva era de ataques tecnológicos.

El aumento en la cantidad de casos de hacking y la sensación de inseguridad permanente que generaron (fomentada por la difusión de los hechos en programas especiales de televisión y artículos de revistas especializadas), cambiaron la percepción de las autoridades con respecto a los hackers y sus ataques. Los casos que demostraron ese cambio fueron los del "Cóndor" Kevin Mitnicky y los de "ShadowHawk" Herbert Zinn hijo.

El FCIC (Federal Computers Investigation Commitee), es la organización más importante e influyente en lo referente a delitos computacionales: los investigadores estatales y locales, los agentes federales, abogados, auditores financieros, programadores de seguridad y policías de la calle trabajan allí comunitariamente. El FCIC es la entrenadora del resto de las fuerzas policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional.

Además existe la Asociación Internacional de Especialistas en Investigación Computacional (IACIS), quien investiga nuevas técnicas para dividir un sistema en sus partes sin destruir las evidencias. Sus integrantes son "forenses de las computadoras" y trabajan, además de los Estados Unidos, en el Canadá, Taiwán e Irlanda[21].

2.8. Francia

Aquí, la Ley 88/19 del 5 de enero de 1988 sobre el fraude informático contempla:

[21] Legislación y Delitos Informáticos – Estados Unidos, http://www.segu-info.com.ar/delitos/estadosunidos.htm

Acceso fraudulento a un sistema de elaboración de datos. Se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

Sabotaje Informático. Falsear el funcionamiento de un sistema de tratamiento automático de datos.

Destrucción de datos. Se sanciona a quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos, suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.

Falsificación de documentos informatizados. Se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro[22].

2.9. Holanda

Hasta el día 1 de marzo de 1993, día en que entró en vigencia la Ley de Delitos Informáticos, Holanda era un paraíso para los hackers. Esta ley contempla con artículos específicos sobre técnicas de Hacking y Phreacking.

El mero hecho de entrar en una computadora en la cual no se tiene acceso legal ya es delito y puede ser castigado hasta con seis meses de cárcel. Si se usó esa computadora hackeada para acceder a otra, la pena sube a cuatro años aunque el crimen, a simple vista, no parece ser peor que el anterior. Copiar archivos de la máquina hackeada o procesar datos en ella también conlleva un castigo de cuatro años en la

[22] Legislación y Delitos Informáticos – Estados Unidos, http://www.segu-info.com.ar/delitos/francia.htm

cárcel. Publicar la información obtenida es ilegal si son datos que debían permanecer en secreto, pero si son de interés público es legal.

El daño a la información o a un sistema de comunicaciones puede ser castigado con cárcel de seis meses a quince años, aunque el máximo está reservado para quienes causaron la muerte de alguien con su accionar. Cambiar, agregar o borrar datos puede ser penalizado hasta con dos años de prisión pero, si se hizo vía remota aumenta a cuatro.

Los virus están considerados de manera especial en la ley. Si se distribuyen con la intención de causar problemas, el castigo puede llegar hasta los cuatro años de cárcel; si simplemente se "escapó", la pena no superará el mes.

El usar el servicio telefónico mediante un truco técnico (Phreacking) o pasando señales falsas con el objetivo de no pagarlo puede recibir hasta tres años de prisión. La venta de elementos que permitan el Phreaking se castiga con un año de prisión como tope y si ese comercio es el modo de ganarse la vida del infractor, el máximo aumenta a tres. La ingeniería social también es castigada con hasta tres años de cárcel.

Recibir datos del aire es legal (transmisiones satelitales), siempre y cuando no haga falta un esfuerzo especial para conseguirlos; la declaración protege datos encriptados, como los de ciertos canales de televisión satelital. Falsificar tarjetas de crédito de banca electrónica y usarlas para obtener beneficios o como si fueran las originales está penado con hasta seis años. Aunque... hacerlas y no usarlas parece ser legal[23].

[23] Legislación y Delitos Informáticos – Estados Unidos, http://www.segu-info.com.ar/delitos/holanda.htm

2.10. Inglaterra

Luego de varios casos de hacking surgieron nuevas leyes sobre delitos informáticos. En agosto de 1990 comenzó a regir la Computer Misuse Act (Ley de Abusos Informáticos) por la cual cualquier intento, exitoso o no de alterar datos informáticos con intención criminal se castiga con hasta cinco años de cárcel o multas sin límite.

El acceso ilegal a una computadora contempla hasta seis meses de prisión o multa de hasta dos mil libras esterlinas.

El acta se puede considerar dividida en tres partes: hackear (ingresar sin permiso en una computadora), hacer algo con la computadora hackeada y realizar alguna modificación no autorizada.

El último apartado se refiere tanto al hacking (por ejemplo, la modificación de un programa para instalar un backdoor), la infección con virus o, yendo al extremo, a la destrucción de datos como la inhabilitación del funcionamiento de la computadora.

Bajo esta ley liberar un virus es delito y en enero de 1993 hubo un raid contra el grupo de creadores de virus. Se produjeron varios arrestos en la que fue considerada la primera prueba de la nueva ley en un entorno real[24].

2.11. Delitos informáticos y cibernéticos en México

En el presente apartado, es de suma importancia, exponer, la manera en que los diversos Estados y el Distrito Federal, que conforman nuestro país, contemplan la persecución de los delitos informáticos y cibernéticos, por lo que a continuación, se presenta una relación de los

[24] Legislación y Delitos Informáticos – Estados Unidos, http://www.segu-info.com.ar/delitos/inglaterra.htm

diversos ordenamientos punitivos de cada Estado y el Distrito Federal, a fin de conocer lo expresado en primeras líneas de este párrafo.

Aguas Calientes

El Código Penal de Aguas Calientes, en sus artículos 195 y 220 nos dice respectivamente:

La Revelación de Secretos consiste en el aprovechamiento de archivos informáticos personales o en la revelación de una comunicación reservada que se conozca o que se haya recibido por motivo de empleo, cargo o puesto, sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado. Al responsable de Revelación de Secretos se le aplicarán de 3 meses a 1 año de prisión y de 15 a 30 días multa[25].

La Defraudación Fiscal consiste en: XIII.- Llevar dos o más libros similares o sistemas informáticos con distintos asientos o datos para registrar sus operaciones contables, fiscales o sociales; XIV.- Destruir, ordenar o permitir la destrucción total o parcial de los libros de contabilidad o sistemas informáticos previstos en la fracción anterior; XV.- Utilizar pastas o encuadernaciones de los libros a que se refiere la fracción XIII, para sustituir o cambiar las páginas foliadas, o alterar los sistemas informáticos de contabilidad que correspondan; Titulo Vigésimo Primero Delitos Contra La Seguridad En Los Medios Informáticos y Magnéticos[26].

El Código Penal de Aguas Calientes, en su artículo 223 nos dice:

[25] Código Penal de Aguas Calientes, Titulo Decimo Primero, "Delitos en contra de la confidencialidad", Capitulo I, "Revelación de Secretos", Articulo 195

[26] Ibidem, Titulo Decimo Octavo, "Delitos contra el Fisco Estatal", Capitulo Único, "Defraudación Fiscal", Articulo 220

El acceso sin autorización consiste en interceptar, interferir, recibir, usar o ingresar por cualquier medio sin la autorización debida o excediendo la que se tenga a un sistema de red de computadoras, un soporte lógico de programas de software o base de datos. Al responsable de Acceso sin Autorización se le sancionará con penas de 1 a 5 años de prisión y de 100 a 400 días multa.

Cuando el acceso sin autorización, tengan por objeto causar daño u obtener beneficio, se sancionará al responsable con penas de 2 a 7 años de prisión y de 150 a 500 días de multa. También se aplicarán las sanciones a que se refiere el párrafo anterior cuando el responsable tenga el carácter de técnico, especialista o encargado del manejo, administración o mantenimiento de los bienes informáticos accesados sin autorización o excediendo la que se tenga[27].

Asimismo, el referido ordenamiento legal, en su artículo 224 nos dice:

El Daño Informático consiste en la indebida destrucción o deterioro parcial o total de programas, archivos, bases de datos o cualquier otro elemento intangible contenido en sistemas o redes de computadoras, soportes lógicos o cualquier medio magnético.

Al responsable de daño informático se le sancionará de 1 a 5 años de prisión y de 100 a 400 días de multa.
Se le aplicarán de 2 a 7 años de prisión y de 150 a 500 días multa, cuando el responsable tenga el carácter de técnico especialista o encargado del manejo, administración o mantenimiento de los bienes informáticos dañados[28].

[27] Código Penal para Aguas Calientes, Titulo Vigésimo Primero, "Delitos Contra la Seguridad en los Medios Informáticos y Magnéticos", Capitulo I, denominado "Acceso sin Autorización", Artículo 223
[28] Ibidem, Capitulo II, denominado "Daño Informático", Artículo 224

De igual forma en sus artículos 225 y 226, el Código Penal de Aguas Calientes, refiere:

Cuando el Acceso sin Autorización o el Daño Informático se cometan culposamente se sancionarán con penas de 1 mes a 3 años de prisión y de 50 a 250 días multa[29].

La Falsificación Informática consiste en la indebida modificación, alteración o imitación de los originales de cualquier dato, archivo o elemento intangible contenido en sistema de redes de computadoras, base de datos, soporte lógico o programas. Al responsable del delito de Falsificación Informática se le aplicarán de 1 a 5 años de prisión y de 100 a 400 días multa. Las mismas sanciones se aplicarán al que utilice o aproveche en cualquier forma bienes informáticos falsificados con conocimiento de esta circunstancia. Se aplicarán de 2 a 7 años de prisión y de 150 a 500 días multa, cuando el responsable tenga el carácter de técnico, especialista o encargado del manejo, administración o mantenimiento de los bienes informáticos falsificados[30].

Baja California Norte

Del Código Penal de Baja California Norte, en su artículo 175[31], nos dice:

[29] Ibidem, Artículo 225
[30] Ibidem, Artículo 226
[31] Fue reformado por Decreto No. 161, publicado en el Periódico Oficial No. 24, de fecha 12 de junio de 1998, Sección I, Tomo CV, expedido por la H. XV Legislatura, siendo Gobernador Constitucional del Estado, el C. Lic. Héctor Terán Terán, 1995-2001; fue reformado por Decreto No. 378, publicado en el Periódico Oficial No. 38, de fecha 14 de septiembre de 2007, Tomo CXIV, Sección IV, expedido por la H. XVIII Legislatura, siendo Gobernador Constitucional el C. Eugenio Elorduy Walther 2001-2007.

Tipo y punibilidad.- Al que sin consentimiento de quien tenga derecho a otorgarlo revele un secreto, de carácter científico, industrial o comercial, o lo obtenga a través de medios electrónicos o computacionales , se le haya confiado, conoce o ha recibido con motivo de su empleo o profesión y obtenga provecho propio o ajeno se le impondrá prisión de uno a tres años y hasta cincuenta días multa, y en su caso, suspensión de dos meses a un año en el ejercicio de su profesión; si de la revelación del secreto resulta algún perjuicio para alguien, la pena aumentará hasta una mitad más. Al receptor que se beneficie con la revelación del secreto se le impondrá de uno a tres años de prisión y hasta cien días multa. REVELACIÓN DEL SECRETO: Se entiende por revelación de secreto cualquier información propia de una fuente científica, industrial o comercial donde se generó, que sea transmitida a otra persona física o moral ajena a la fuente. QUERELLA: El delito de revelación de secreto se perseguirá por querella de la persona afectada o de su representante legal[32].

Acorde con el Código Penal de Baja California Norte, en su artículo 175 bis[33], nos dice:

A quien sin autorización o indebidamente, modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y multa equivalente de cien a trescientos días[34].

[32] Código Penal de Baja California Norte, Titulo Tercero "Delitos Contra la Inviolabilidad del Secreto", Capitulo I "Revelación del Secreto", Artículo 175

[33] Fue adicionado mediante Decreto No. 378, publicado en el Periódico Oficial No. 38, de fecha 14 de septiembre de 2007, Tomo CXIV, Sección IV, expedido por la H. XVIII Legislatura, siendo Gobernador Constitucional el C. Eugenio Elorduy Walther 2001-2007.

[34] Ibidem, Capitulo II "Acceso Ilícito a Sistemas y Equipos de informática", Artículo 175 bis

Asimismo, en sus artículos 175 ter[35] y 175 quater[36], refiere:

A quien sin autorización o indebidamente, copie o accese a información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y multa equivalente de cincuenta a ciento cincuenta días de salario mínimo vigente[37].

Agravación de la pena.- las penas previstas en los artículos anteriores se duplicaran cuando las conductas delictivas se ejecuten en contra de sistemas o equipos de informática del estado o municipios.

Sin perjuicio de la agravación de la pena, que se imponga conforme al párrafo anterior, la pena se aumentara hasta en una mitad más, cuando el delito se ejecute por un servidor público[38].

Asimismo, en el propio ordenamiento punitivo para el estado de Baja California Norte, en su artículo 262[39], nos dice:

Pornografía de personas menores de dieciocho años de edad o de quien no tiene la capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo. A quien procure, facilite, induzca, propicie, obligue o permita a una persona menor de

[35] Fue adicionado mediante Decreto No. 378, publicado en el Periódico Oficial No. 38, de fecha 14 de septiembre de 2007, Tomo CXIV, Sección IV, expedido por la H. XVIII Legislatura, siendo Gobernador Constitucional el C. Eugenio Elorduy Walther 2001-2007

[36] Fue adicionado mediante Decreto No. 378, publicado en el Periódico Oficial No. 38, de fecha 14 de septiembre de 2007, Tomo CXIV, Sección IV, expedido por la H. XVIII Legislatura, siendo Gobernador Constitucional el C. Eugenio Elorduy Walther 2001-2007

[37] Ibidem, Artículo 175 ter

[38] Ibidem, Artículo 175 quater

[39] Fue reformado por Decreto No. 330, publicado en el Periódico Oficial No. 20, de fecha 11 de mayo de 2007, Sección I, Tomo CXIV, expedido por la Honorable XVIII Legislatura, siendo Gobernador Constitucional el C. Lic. Eugenio Elorduy Walter 2001-2007.

dieciocho años de edad o quien no tiene la capacidad para comprender el significado del hecho o de quien que no tiene la capacidad para resistirlo, a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de filmarlos, grabarlos, audio grabarlos, video grabarlos, describirlos, fotografiarlos o exhibirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de computo, medios electrónicos o de cualquier otra naturaleza , se le aplicarán de siete a doce años de prisión y de mil a dos mil días multa. Se impondrá la misma pena a quien por cualquier medio elabore, reproduzca, compre, venda, arriende, exponga, ofrezca, almacene, importe, exporte, publicite, transmita, fije, grabe, video grabe, audio grabe, fotografíe, filme, imprima, distribuya anuncios, grabaciones, impresos, videos, películas o fotografías, en cuyo contenido aparezca una persona menor de dieciocho años de edad o que no tiene la capacidad para comprender el significado del hecho o de quien que no tiene capacidad para resistirlo, realizando actos de exhibicionismo corporal, o lascivos o sexuales, reales o simulados. La misma pena se impondrá a quien por sí o a través de terceros, dirija, patrocine, administre, financie o supervise cualquiera de las conductas previstas anteriormente. En todos los casos previstos en este artículo se decomisarán los objetos, instrumentos y productos de los delitos.[40]

Por otra parte, continuando con el ordenamiento punitivo de Baja Californiana Norte, podemos advertir en su artículo 335[41] lo siguiente:

[40] Ibidem, Titulo Cuarto, "Delitos Contra El Libre Desarrollo de la Personalidad", Capitulo II "Pornografía y turismo sexual de personas menores de dieciocho años de edad o de quienes no tienen la capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo" Articulo 262

[41] Fue reformado por Decreto No. 184, publicado en el Periódico Oficial No. 9, de fecha 24 de febrero de 2006, Tomo CXIII, expedido por la H. XVIII Legislatura siendo Gobernador Constitucional el C. Eugenio Elorduy Walther 2001-2007

Exclusión de pena en virtud del parentesco y otro vínculo.- No se impondrá pena al que oculte al responsable de un hecho calificado por la Ley como delito, o impida que se averigüe, siempre que se trate de: I.- Los ascendientes o descendientes consanguíneos o por adopción; II.- El cónyuge, concubinato o concubina y parientes colaterales por consanguinidad hasta el cuarto grado y por afinidad hasta el segundo; III.- Los que estén ligados al delincuente por amor, respeto, gratitud o estrecha amistad; o IV.- Los periodistas, reporteros o personal que preste sus servicios dentro de alguna empresa o medio de comunicación escrito o electrónico , respecto de los nombres o datos de identificación de las personas que con motivo del ejercicio de su actividad, les proporcionen como información de carácter reservada, en la cual sustenten cualquier publicación o comunicado. La excusa no favorecerá a quien obre por motivos reprochables o emplee medios delictuosos[42].

Baja California Sur

El Código Penal de Baja California Sur, también contempla los delitos informáticos, manifestando lo siguiente en sus artículos 333, 334 y 335 respectivamente:

Se aplicarán de seis meses a un año de prisión y multa hasta por cincuenta días de salario, a quien viole cualquier tipo de correspondencia que no circule por el servicio de correos, en alguna de las formas siguientes: I.- Abrir indebidamente una comunicación escrita que no esté dirigida a él; y II.- Interceptar indebidamente una comunicación escrita que no le esté dirigida, aunque no se imponga de su contenido.[43]

[42] Ibídem, Titulo Cuarto, "Delitos cometidos en la administración de justicia", Capitulo V, "Encubrimiento por favorecimiento", Articulo 335

[43] Código Penal de Baja California Sur, Capítulo IV "Violación de correspondencia y otras comunicaciones privadas" Artículo 333

No se impondrá sanción a los que, ejerciendo la patria potestad o la tutela, abran las comunicaciones dirigidas a sus hijos o pupilos o un cónyuge o concubino, cuando se trate de la correspondencia dirigida al otro. Cuando la violación de correspondencia se realice entre parientes consanguíneos, afinidad o por adopción, solo se perseguirá a petición de parte ofendida[44].

La interceptación de cualquier comunicación verbal, gestual, electrónica o de cualquier otro tipo, sin consentimiento de quien la emite o sin autorización del Juez federal, será castigada con pena de uno a cinco años de prisión y multa de cincuenta a doscientos días de salario[45].

Campeche

En el Código Penal de Campeche, se advierten las siguientes consideraciones con relación a los delitos informáticos, en los artículos 211 y 212 respectivamente:

Se impondrán de uno a ocho años de prisión y multa de cincuenta a cien días de salario mínimo: I.- Al que falsifique los sellos o marcas oficiales; II.- Al que falsifique el sello, marca o contraseña que alguna autoridad usare para identificar cualquier objeto o para asegurar el pago de algún crédito; III.- Al que falsifique los punzones, matrices, planchas o cualquier otro objeto que sirva para la fabricación de títulos y demás documentos a que se refiere el capítulo anterior[46]

Se impondrán prisión de tres meses a tres años y multa de diez a cincuenta días de salario mínimo: I.- Al que falsifique llaves, el sello de

[44] Ibidem, Articulo 334
[45] Ibidem, Articulo 335
[46] Código Penal de Campeche, Título Decimosexto, "Falsedad Falsificación de sellos, llaves, punzones y marcas" Artículo 211

un particular, un sello, marca, estampilla o contraseña de una casa de comercio, de un banco o de un establecimiento industrial: o un boleto o ficha de un espectáculo público; II.- Al que enajene un sello, punzón o marca falsos, ocultando este vicio; III.- Al que dolosamente borre o haga desaparecer alguno de los sellos, marcas o contraseñas de que trata este artículo y el anterior; IV.- Al que a sabiendas hiciere uso de los sellos o de alguno otro de los objetos falsos que se mencionan en este artículo y el anterior[47].

Por otra parte, del referido ordenamiento punitivo estatal, podemos advertir lo siguiente en el artículo 373:

Se impondrán de cinco a diez años de prisión y multa hasta de doscientos días de salario mínimo, a los que causen incendio, inundación o explosión con daño o peligro de: I.- Un edificio, vivienda o cuarto donde se encuentre alguna persona; II.- Ropas, muebles u objetos en tal forma que puedan causarse graves daños personales; III.- Archivos públicos o notariales; IV.- Bibliotecas, museos, templos, escuelas o edificios y monumentos públicos; V.- Montes, bosques, selvas, pastos, mieses o cultivos de cualquier género; VI.- Apiarios.[48]

Chiapas

En el Código Penal de Chiapas, en el artículo 261, se advierte:

Cuando el autor del delito de difamación o de calumnia haya sido condenado por sentencia irrevocable, el ofendido podrá solicitar la publicación de la sentencia en tres periódicos, a costa del condenado. Cuando el delito se haya cometido por conducto de algún medio de comunicación, los dueños, gerentes o directores de éste, hayan sido o no responsables del delito, estarán obligados a difundir la sentencia en

[47] Ibidem, Artículo 212
[48] Ibidem, Capítulo VI, "Daño en propiedad ajena", Artículo 373

los términos en que el juzgador lo disponga, en la misma sección en donde se publicó el hecho imputado al sujeto pasivo, y en el mismo horario y programa en caso de tratarse de un medio electrónico. Se impondrán diez días de multa por cada día que transcurra sin que se realice dicha publicación, contado a partir del momento en que se notifique la obligación.[49]

De igual forma, del referido ordenamiento legal, podemos advertir en el numeral 303 lo siguiente:

El delito de fraude se sancionará: XXIV.- Al que para obtener algún beneficio para sí o para un tercero, por cualquier medio acceda, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la institución.[50]

Igualmente, nos percatamos en el numeral 333, lo relativo a las cuestiones informáticas:

Comete el delito de pornografía infantil el que procure, facilite o induzca por cualquier medio a un menor, con o sin su consentimiento, a realizar actos de exhibicionismo corporal, lascivos o sexuales, con el objeto y finalidad de video grabarlo, fotografiarlo, o exhibirlo a través de medios impresos o electrónicos, o con anuncios de cualquier clase, con o sin el fin de obtener un lucro.[51]

[49] Código Penal de Chiapas, Título Octavo "Delitos Contra el Honor", Capítulo III, "Disposiciones Comunes Para los Delitos Comprendidos en este Título" Artículo 261

[50] Ibidem, Título Décimo "Delitos en Contra de las Personas en su Patrimonio" Capítulo V, "Fraude", Artículo 303

[51] Ibidem, Título Décimo Segundo, "Delitos contra la moral y la dignidad de las personas" Capítulo III, "Corrupción de Menores e Incapaces", Artículo 333

Continuando con el mismo orden de ideas, encontramos en el numeral 404, lo siguiente:

Se impondrá pena hasta de cinco años de prisión y multa hasta de un año del salario mínimo vigente al que: IV.- Altere los medios de identificación electrónicos de tarjetas, títulos o documentos para el pago de bienes y servicios Título Décimo Noveno Delitos de Revelación de Secretos y de Acceso Ilícito a Sistemas y Equipos de Informática Capítulo II Acceso Ilícito a Sistemas de Informática[52]

Por otra parte, y aún dentro de la Ley Punitiva del Estado que nos ocupa, en los artículos 435, 436, 437 y 438, se advierte:

Se aplicará sanción de dos a cuatro años y multa de veinte a cuarenta días de salario, al que, sin el consentimiento de quien pueda resultar perjudicado, revele un secreto o comunicación reservada, que haya conocido con motivo de su empleo, cargo o comisión, o se le haya confiado, causando un perjuicio a alguien o lo emplee en provecho propio o ajeno.[53]

Se sancionará con prisión de dos a ocho años, multa de veinte a cien días de salario y suspensión de profesión o inhabilitación en su caso, cuando la revelación a que se refiere el artículo anterior sea hecha por persona que presta servicios profesionales o técnicos o por servidores públicos, y el secreto revelado o publicado sea de carácter industrial o mercantil[54].

[52] Ibidem, Título Décimo Séptimo "Falsedad", Capítulo II, "Falsificación de Documentos en General", Artículo 404

[53] Código Penal de Chiapas, Libro Segundo, Parte Especial, Título Décimo Noveno "Delitos de Revelación de Secretos y de Acceso Ilícito a Sistemas y Equipos de Informática", Capítulo I "Revelación de Secretos", Artículo 435

[54] Ibidem, Artículo 436

A quien revele, divulgue o utilice ilícitamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, o en una investigación, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa[55].

Cuando el sujeto activo de los delitos contemplados en este capítulo sea un servidor público, además de las penas establecidas se le impondrá destitución e inhabilitación para ejercer otro cargo, empleo o comisión públicos de seis meses a tres años[56].

Asimismo, del mismo ordenamiento legal referido con antelación, en los artículos 439, 440, 441, 442, se puede advertir:

Al que sin autorización modifique, destruya, o provoque perdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo o sistema de seguridad o al que no tenga derecho a accesar, se le impondrá una sanción de uno a cuatro años de prisión y de cuarenta a doscientos días multa.

Al que, estando autorizado o tenga derecho de acceso a los sistemas o equipo de informática protegido por algún mecanismo o sistema de seguridad, innecesariamente o en perjuicio de otro destruya, modifique, o provoque perdida de información que contengan los mismos, la pena prevista en el párrafo anterior, se aumentara en una mitad.[57]

Al que, sin autorización accese, modifique, copie, destruya o provoque perdida de información contenida en sistema o equipo de informática de alguna dependencia publica protegida por algún sistema o

[55] Ibidem, Artículo 437
[56] Ibidem, Artículo 438
[57] Ibidem, Capítulo II "Acceso Ilícito a Sistemas de Informática", Artículo 439

mecanismo de seguridad se le impondrá una sanción de dos a seis años de prisión y de doscientos a seiscientos días de multa[58].

Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia publica, innecesariamente o en perjuicio de otro o del servicio público modifique, destruya o provoque perdida de información que contengan se impondrá prisión de tres a ocho años y de trescientos a ochocientos días multa[59].

Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia publica, sin autorización copie, transmita o imprima información que contengan se le impondrá de uno a cuatro años de prisión y de cien a trescientos días multa[60].

Chihuahua

El Código Penal de Chihuahua, contempla en su numeral 185:

Comete este delito: I. Quien produzca, fije, grabe, videograbe, fotografíe o filme de cualquier forma imágenes o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho, sea en forma directa, informática , audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas. II. Quien reproduzca, publique, publicite, distribuya, difunda, exponga, envíe, transmita, importe, exporte o comercialice de cualquier forma imágenes o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas,

[58] Ibidem, Artículo 440
[59] Ibidem, Artículo 441
[60] Ibidem, Artículo 442

explícitas o no, reales o simuladas. III. Quien ofrezca, posea o almacene intencionalmente para cualquier fin, imágenes o la voz de personas menores de edad o de personas que no tengan la capacidad de comprender el significado del hecho, sea en forma directa, informática , audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas. Al autor de los delitos previstos en este artículo se le impondrá prisión de seis meses a seis años y quinientos a dos mil días multa.[61]

En el mismo orden de ideas, atendemos a los dispuesto por el numeral 211 que a la letra dice:

Además de las sanciones que correspondan conforme a los artículos anteriores, se aplicará prisión de seis meses a tres años, cuando el robo: Vll. Recaiga en un expediente, documento o en cualquier información que se encuentre registrada o archivada en sistema o equipo de informática protegidos por algún mecanismo de seguridad, con afectación de alguna función pública[62].

Por su parte, en el artículo 238, se refiere:

Se aplicará prisión de seis meses a seis años al que deteriore o destruya expediente o documento, de oficina o archivos públicos. Las mismas penas se aplicarán al que destruya, altere o provoque pérdida de información contenida en sistema o equipo de informática de oficina o archivos públicos, protegidos por algún mecanismo de seguridad.[63]

[61] Código Penal de Chihuahua, Título Sexto, "Delitos contra la Evolución o Desarrollo de la Personalidad", Capítulo II, "Pornografía con Personas Menores de Edad o que no tienen la capacidad para Comprender el Significado del Hecho", Artículo 185

[62] Ibidem, Título Décimo Cuarto, "Delitos contra el patrimonio", Capítulo I "Robo", Artículo 211

[63] Ibidem, Capítulo X, "Daños", Artículo 238

Igualmente, nos percatamos de los delitos informáticos en el numeral 326, de la ley punitiva del Estado que nos ocupa:

A quien abra o intercepte una comunicación escrita que no esté dirigida a él, se le impondrá de treinta a noventa días multa. Los delitos previstos en este artículo se perseguirán por querella. La misma sanción se impondrá en los casos en que la comunicación se encuentre registrada o archivada en sistemas o equipos de informática protegidos por algún mecanismo de seguridad[64]

Así también, analizamos lo comprendido en el numeral 333, del ordenamiento jurídico que nos ocupa:

Se impondrán de uno a tres años de prisión y de cincuenta a mil días multa al que, para obtener un beneficio o causar un daño, indebidamente produzca o edite, por cualquier medio técnico , imágenes, textos o voces, total o parcialmente falsos o verdaderos[65]

Coahuila

En el Código Penal del Estado de Coahuila, en los artículos 371 y 372 respectivamente, podemos advertir lo siguiente:

SANCIONES Y FIGURAS TÍPICAS DE SECUESTRO. Se aplicará prisión de dieciséis a cuarenta años y multa, al que por cualquier medio prive de la libertad a otro, con alguno de los propósitos siguientes:

[64] Ibidem, Título Vigésimo Segundo, "Delitos contra la seguridad y el normal funcionamiento de las Vías de comunicación y de los medios de transporte", Capítulo II, "Violación de correspondencia", Artículo 326

[65] Ibidem, Título Vigésimo Tercero, "Delitos contra la fe pública", Capítulo III, "Falsificación o alteración y uso indebido de documentos", Artículo 333

I. Obtener rescate para sí o para un tercero, o cualquier otra ventaja indebida.
II. Causar daño o perjuicio al secuestrado o a otra persona relacionada con éste.
III. Detener en calidad de rehén a una persona y amenazarla con privarla de la vida o con causarle daño, para que la autoridad o un particular realice o deje de realizar un acto cualquiera.
IV. Obligarle a ejecutar, directa o indirectamente, operaciones o transacciones bancarias, mercantiles, civiles o cualquier otra que produzca retiro o liberación de sumas en efectivo, transmisión de derechos o extinción de obligaciones, o a que proporcione al agente los documentos, tarjetas bancarias, claves, números de identificación personal y demás datos indispensables para que éste las lleve a cabo.

En todos los casos se impondrá como sanción el decomiso de los instrumentos, objetos y productos del delito, considerándose, entre éstos, los vehículos, armas, muebles y demás bienes de que se sirvan los responsables para la perpetración del delito de secuestro.

Asimismo, se impondrá como sanción la prohibición de residir o de acudir a determinado lugar; particularmente el que habite, labore o frecuente el ofendido por el delito[66].

SANCIONES Y CIRCUNSTANCIAS CALIFICATIVAS DE SECUESTRO. El delito de secuestro a que se refiere el artículo anterior será calificado y se sancionará: De veinte a cuarenta y cinco años de prisión y multa, cuando concurra alguna o algunas de las circunstancias siguientes:

1) El ofendido sea servidor público, dirigente sindical, empresarial o religioso, candidato a un cargo de elección popular, periodista o comunicador.

[66] Código Penal del Estado de Coahuila, Capítulo Segundo, “Secuestro”, Artículo 371

2) El secuestro se realice en casa habitación, sitio de trabajo, centro educativo, ruta o lugar comúnmente frecuentados por el pasivo o en las inmediaciones de los mismos, en vías o caminos públicos, en despoblado o sitios solitarios o en áreas desprotegidas.

3) Los autores y partícipes obren en grupo de dos o más personas.

4) Se realice con engaño, violencia física o moral ejercida en contra del ofendido o algún tercero.

5) Se haga uso de armas en el inicio de la comisión del delito o en el transcurso de su ejecución.

6) El hecho se cometa utilizando orden de aprehensión o detención falsas, o simulando tenerlas.

7) El secuestrador obligue bajo amenazas, engaños o violencia a un tercero a participar en cualquier etapa del delito.

8) Afecte gravemente los bienes o la actividad profesional o económica del ofendido.
II. De veinticinco a cincuenta años de prisión y multa cuando se dé alguna o algunas de las situaciones siguientes:

El ofendido sea menor de dieciocho años o mayor de sesenta, se trate de un incapaz, de una mujer embarazada o de una persona enferma que requiera el suministro de medicamentos o tratamientos especiales, o que por cualquier otra circunstancia esté en situación de inferioridad respecto del secuestrador.

2) Se ejecute la conducta en un pariente hasta el cuarto grado de consaguinidad, segundo de afinidad o primero civil, sobre la cónyuge o el cónyuge, la concubina o el concubinario, o aprovechando la

confianza depositada por el ofendido en el autor o en alguno o algunos de los partícipes por razones de amistad, gratitud, relación laboral u otro motivo similar que produzca confianza.

3) Intervenga un servidor público o ex servidor público, un miembro o ex miembro de cualquier institución de seguridad pública, o se ostente como tal sin serlo. 4) Se utilicen insignias, uniformes, placas, instalaciones, frecuencias, claves o códigos oficiales, se empleen redes, sistemas informáticos o cualquier otro medio de alta tecnología, que facilite la consecución de los propósitos del secuestrador. 5) Se haga uso de narcóticos, o cualquier sustancia depresora que anule, disminuya o tienda a anular la resistencia del ofendido. 6) Se cometa simultánea o sucesivamente contra más de una persona, sin perjuicio de las reglas aplicables en materia de concurso. 7) Se presione la entrega o verificación de lo exigido con amenaza de lesión o muerte al secuestrado. 8) La privación de la libertad del secuestrado se prolongue por más de cinco días. Cuando se trate de los incisos 3 y 4, además de la pena señalada, se impondrá, en su caso, la destitución del empleo, cargo o comisión y la inhabilitación definitiva para obtener y desempeñar otro. III. De treinta a cincuenta y cinco años de prisión y multa, cuando se surta alguno o algunos de los supuestos siguientes: 1) Se someta al secuestrado a tortura física o moral, maltrato o vejaciones, o a violencia sexual durante el tiempo en que se mantenga el secuestro. 2) Se le infiera al ofendido alguna o algunas de las lesiones enunciadas en los artículos del 339 al 342 de este Código, sin perjuicio de las penas que a éstas correspondan. 3) Se cometa con la finalidad de extraer al pasivo algún órgano de su cuerpo para trasplante o comercialización, independientemente de los delitos que resulten. 4) Se cometa con fines terroristas. 5 Si el secuestrado fallece durante el tiempo en que se encuentre privado de su libertad o si después de ser liberado, muere dentro de los ciento ochenta días siguientes por causas relacionadas directamente con el secuestro. IV. De treinta y cinco a sesenta años de prisión y multa, si el secuestrado es privado de la vida

por su secuestrador. En todos estos supuestos, además de las sanciones previstas para cada una de las circunstancias calificativas de secuestro; se aplicarán las que correspondan por los delitos que resulten, conforme a las reglas de concurso[67]

En el Código Penal de Coahuila, en los artículos 281 bis al 281 bis 4, encontramos lo siguiente:

Sanciones y figuras típicas de los delitos contra la seguridad en los medios informáticos cometidos en perjuicio de particulares. Se aplicará prisión de tres meses a tres años y multa a quien:

I. Sin autorización para acceder a un sistema informático y con perjuicio de otro, conozca, copie, imprima, use, revele, transmita, o se apodere de datos o información reservados, contenidos en el mismo.

II. Con autorización para acceder a un sistema informático y con perjuicio de otro, obtenga, sustraiga, divulgue o se apropie de datos o información reservados en él contenidos.

Si la conducta que en uno u otro caso se realiza es con el ánimo de alterar, dañar, borrar, destruir o de cualquier otra manera provocar la pérdida de datos o información contenidos en el sistema, la sanción será de cuatro meses a cuatro años de prisión y multa[68].

Circunstancias agravantes de los delitos anteriores.

Las penas previstas en el artículo anterior, se incrementarán en una mitad más:

[67] Ibidem, Capítulo Segundo, "Secuestro", Artículo 372

[68] Código Penal de Coahuila, Libro Segundo, Parte Especial, Titulo Segundo, "Delitos Contra la Seguridad Pública", Capitulo Tercero, "Delitos Contra la Seguridad en los Medios Informáticos", Articulo 281 bis.

I. Si el agente actuó con fines de lucro.

II. Si el agente accedió al sistema informático valiéndose de información privilegiada que le fue confiada en razón de su empleo o cargo, o como responsable de su custodia, seguridad o mantenimiento[69].

Sanciones y figuras típicas de los delitos contra la seguridad en los medios informáticos cometidos en perjuicio de una entidad pública. Se aplicará prisión de seis meses a seis años y multa a quien:

I. Sin autorización, acceda, por cualquier medio a un sistema informático, de una entidad pública de las mencionadas en el párrafo segundo del artículo 194[70], para conocer, copiar, imprimir, usar, revelar, transmitir o apropiarse de sus datos o información propios o relacionados con la institución.

II. Con autorización para acceder al sistema informático de una entidad pública de las mencionadas en el párrafo segundo del artículo 194, indebidamente copie, transmita, imprima, obtenga, sustraiga, utilice divulgue o se apropie de datos o información propios o relacionados con la institución.

Si la conducta que en uno u otro caso se realiza, tiene la intención dolosa de alterar, dañar, borrar, destruir, o de cualquier otra forma

[69] Ibidem, Artículo 281 bis 1

[70] Código Penal de Coahuila, Artículo 194, Párrafo II "Para todos los efectos de este código, se entenderá como entidad pública a la administración pública estatal o municipal; al poder legislativo y al poder judicial; los organismos o empresas de cualquiera de los poderes del estado, o del municipio, sean desconcentrados o descentralizados; los organismos o empresas de participación mayoritaria o minoritaria estatal o municipal; las organizaciones y sociedades asimiladas a aquellos; los que manejen bienes o recursos económicos públicos estatales o municipales mediante fideicomisos u otras formas jurídicas."

provocar la pérdida de los datos o información contenidos en el sistema informático de la entidad pública, la sanción será de uno a ocho años de prisión y multa.

Si el sujeto activo del delito es servidor público, se le sancionará, además, con la destitución del empleo, cargo o comisión e inhabilitación para ejercer otro hasta por seis años[71].

Circunstancias agravantes en los delitos anteriores. Las penas previstas en el artículo anterior se incrementarán en una mitad más:

I. Si el agente obró valiéndose de alguna de las circunstancias agravantes previstas en el artículo 290 BIS 1.

II. Si el hecho constitutivo de delito fue cometido contra un dato o sistemas informáticos concernientes al régimen financiero de las entidades públicas que se mencionan en el artículo 194, o por funcionarios o empleados que estén a su servicio.

III. Si la conducta afectó un sistema o dato referente a la salud o seguridad pública o a la prestación de cualquier otro servicio público[72].

Norma complementaria en orden a la terminología propia de los delitos contra la seguridad de los medios informáticos.

A los fines del presente capítulo, se entiende por:

I. Sistema informático: todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos para generar, enviar, recibir, recuperar,

[71] Ibidem, Artículo 281 bis 2
[72] Ibidem, Artículo 281 bis 3

procesar o almacenar información de cualquier forma o por cualquier medio.

II. Dato informático o información: toda representación de hechos, manifestaciones o conceptos, contenidos en un formato que puede ser tratado por un sistema informático[73].

Colima

En el caso del Código Penal de Colima, se agregó el fraude informático, en virtud de que en mayo de 2009, el Congreso del Estado de colima, aprobó reformas a la referida ley punitiva, con el fin de agregar como delito el fraude informático.

La finalidad es sancionar a quien por algún medio informático, telemático o electrónico, "alcance un lucro indebido valiéndose de alguna manipulación informática, instrucciones de código, predicción, intercepción de datos de envío o reinyección de datos".

En el dictamen presentado por la Comisión de Estudios Legislativos y Puntos Constitucionales, aprobado por unanimidad en sesión ordinaria, también se tipifica como delito la utilización de la red o de redes para montar sitios espejo o de trampa, que capten información crucial para el empleo no autorizado de datos.

Asimismo, "la suplantación de identidades; la modificación indirecta, mediante programas automatizados, de imagen, correo o vulnerabilidad del sistema operativo.

"O cualquier archivo principal, secundario y terciario del sistema operativo que afecte la confiabilidad y variación de la navegación en la

[73] Ibidem, Artículo 281 bis 4

red, o use artificio semejante para obtener lucro indebido", señala el documento.

Menciona que las conductas antes señaladas fueron integradas al Código Penal en su capítulo relativo al Fraude, para lo cual la legislación penal establece de uno a nueve años de prisión y multa hasta por 100 unidades.

Además, se incrementa la sanción hasta cuatro años más, "si el delincuente tiene licenciatura, ingeniería o cualquier otro grado académico reconocido en el rubro de la informática, telemática o sus afines".

Al aprobar, los legisladores locales consideraron necesaria esta reforma legal, "pues algunas personas están valiéndose de los adelantos tecnológicos para realizar conductas ilícitas tales como robos y fraudes, sin que las instituciones bancarias sean responsables de cualquier malversación".

Por su parte, la diputada Brenda Gutiérrez Vega, autora de esta iniciativa, dijo que si bien internet es un medio de comunicación, no existe una regulación cuando se causa un perjuicio a través de él, en cuanto a captar o enviar información de una manera ilegal, por lo que calificó de positiva la reforma[74].

Por otra parte, podemos tomar en cuenta en lo relativo a los delitos informáticos lo siguiente de los numerales 10, 157 Bis y 244, respectivamente, del propio ordenamiento punitivo del estado que nos ocupa:

[74] Agregan fraude informático al Código Penal de Colima; http://www.eseguridad.gob.mx/wb2/eMex/eMex_2e98c_not969_agregan_fraud

Se califican como delitos graves, para todos los efectos legales, por afectar de manera importante valores fundamentales de la sociedad, los siguientes delitos previstos por este Código: Corrupción de menores, en su modalidad de EXPLOTACIÓN PORNOGRÁFICA, prevista por el artículo 157 Bis, segundo párrafo, tratándose de la realización de acto de exhibicionismo corporal lascivo o sexual, con el objeto de videograbarlo, fotografiarlo o exhibirlo mediante anuncio impreso o electrónico ; LENOCINIO....[75]

Al que explote a un menor o a quien no tenga capacidad para comprender el significado del hecho, con fines de lucro o para conseguir una satisfacción de cualquier naturaleza, se le impondrá de dos años seis meses a ocho años de prisión y multa hasta por quinientas unidades. Para los efectos de este artículo, se tipifica como explotación de menor o de quien no tenga capacidad para comprender el significado del hecho, el permitir, inducir u obligar al sujeto pasivo, a la práctica de la mendicidad, o a realizar acto de exhibicionismo corporal libidinoso o de naturaleza sexual, con el objeto de videograbarlo, o fotografiarlo, o exhibirlo mediante cualquier tipo de impreso o medio electrónico[76]

Se impondrá de tres a seis años de prisión y multa de 100 a 15 mil unidades, a quien ilícitamente: III. Altere equipo o programas de cómputo utilizados para la verificación de automotores [77]

[75] Código Penal de Colima, Libro Primero, Título Segundo, "Delito y Delincuente", Artículo 10

[76] Ibidem, Libro Segundo, Título Quinto, "Delitos contra la moral pública", Capítulo II, "Corrupción de menores", Artículo 157 Bis

[77] Ibidem, Libro Segundo, Sección Quinta, "Delitos contra el ambiente", Título Único, Capítulo Único, "Delitos ambientales", Artículo 244

Distrito Federal

El Código Penal para el Distrito Federal, contempla sui géneris, los delitos informáticos desde la perspectiva de daño patrimonial, al hablar en su artículo 231 de lo siguiente:

XIV. Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución[78]

Durango

El Código Penal de Durango, refiere respecto de los delitos informáticos, en sus numerales 235 y 236 respectivamente, lo siguiente:

Se impondrán de tres a nueve años de prisión y de cien a cinco mil días multa, al que, sin consentimiento de quien esté facultado para ello: I.- Produzca, imprima, enajene, distribuya, altere o falsifique tarjetas , títulos o documentos utilizados para el pago de bienes y servicios o para disposición de efectivo; II.- Adquiera, utilice, posea o detente tarjetas , títulos o documentos para el pago de bienes y servicios, a sabiendas de que son alterados o falsificados; III.- Adquiera, utilice, posea o detente, tarjetas , títulos o documentos auténticos para el pago de bienes y servicios, sin consentimiento de quien esté facultado para ello; IV.- Altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios; V.- Acceda a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para

[78] Código Penal para el Distrito Federal, Título Décimo Quinto, Delitos Contra el Patrimonio, Capitulo III "Fraude", Articulo 231, Fracción XIV

disposición de efectivo; VI.- Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como a quien posea o utilice la información sustraída, de esta forma; o VII.- A quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios, o de los titulares de dichos instrumentos o documentos[79]

Se impondrán de tres a seis años de prisión y de tres a trescientos cincuenta días multa: II.- Al que falsifique el sello, marca o contraseña que alguna autoridad usare para identificar cualquier objeto o para asegurar el pago de algún impuesto, derecho o aprovechamiento[80]

De igual forma advertimos la presencia de los delitos informáticos en los numerales 271, 381, 418, 426 y 456 de la Ley Punitiva del Estado que nos ocupa:

Se impondrá de tres meses a un año de prisión y de tres a treinta y cinco días multa, al empleado de un telégrafo, teléfono o estación inalámbrica que perteneciere al Estado, que conscientemente dejare de transmitir un mensaje que se le entregue con ese objeto, o de comunicar al destinatario, el que recibiere de otra oficina[81].

Se aplicará de uno a cinco años de prisión y de cien a trescientos días multa, a quien sin consentimiento de otro y para conocer algún secreto, intimidad personal o comunicación reservada: I.- Se apodere de

[79] Código Penal de Durango, Libro segundo, "De los delitos", Título Primero, "Delitos contra el Estado", Subtitulo Sexto, "Delitos contra la fe pública", Capítulo Primero, "Falsificación de títulos al portador y documentos de crédito público", Artículo 235

[80] Ibidem, Artículo 236

[81] Ibidem, Subtítulo Segundo, "Delitos contra la seguridad de las vías de comunicación y medios de transporte", Capítulo Tercero, "Violación de correspondencia", Artículo 271

documentos u objetos de cualquier clase; II.- Reproduzca dichos documentos u objetos; y III.- Utilice medios técnicos para escuchar, observar, transmitir, grabar o reproducir la imagen o el sonido[82]

Se equipara al robo y se castigará como tal: II.- El aprovechamiento de energía eléctrica, algún fluido, líneas de televisión por cable, y telefónicas, sin consentimiento de la persona que legalmente pueda disponer y autorizar aquéllas; V (sic).- El apoderamiento material de los documentos que contengan datos de computadoras, o el aprovechamiento o utilización de dichos datos, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos[83].

Quien para obtener algún lucro para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores en perjuicio de persona alguna, independientemente de que los recursos no salgan de la Institución[84]

Se impondrá de setenta a doscientos días multa y de tres a siete años de prisión, a quien por cualquier medio altere o participe en la alteración del Registro Estatal de Electores, de los listados nominales o en la expedición ilícita de credenciales para votar[85].

[82] Ibidem, Subtítulo Tercero, "Delitos contra la libertad y seguridad personal", Capitulo Décimo, "Violación a la intimidad personal o familiar", Artículo 381
[83] Ibidem, Título Cuarto, "Delitos contra el patrimonio", Capítulo Primero, Artículo 418
[84] Ibidem, Capítulo Cuarto, "Fraude y Exacción Fraudulenta", Artículo 426, Fracción XXIII
[85] Ibidem, Título Quinto, Capítulo Único, "Delitos Electorales", Artículo 456

Guerrero

En el Código Penal de Guerrero, los Delitos Informáticos, se advierten desde una perspectiva de atentado a la evolución o desarrollo de la personalidad, al referir lo siguiente en su numeral 217:

Quien produzca, fije, grabe, videograbe, fotografíe o filme de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o personas con capacidades diferentes o de una persona que no tenga la capacidad para comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas.

Quien reproduzca, publique, ofrezca, publicite, distribuya, difunda, exponga, envíe, transmita, importe, exporte o comercialice de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o personas con capacidades diferentes o de una persona que no tenga la capacidad para comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas.

Quien posea o almacene intencionalmente para cualquier fin, imágenes, sonidos o la voz de personas menores de edad o personas con capacidades diferentes o de personas que no tengan la capacidad de comprender el significando del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas[86].

[86] Código Penal de Guerrero, Titulo IV, "Delitos Contra la Evolución o Desarrollo de la Personalidad", Capitulo II, "Pornografía con utilización de imágenes y/o voz de personas

Guanajuato

No tiene

Hidalgo

No tiene

Jalisco

En el Código Penal de Jalisco, en el Artículo 194, refiere de cierta forma la persecución de delitos informáticos, desde una perspectiva de la salvaguarda de la libertad.

Al responsable de secuestro se le sancionará con una pena de veinticinco a cuarenta años de prisión y multa por el importe de mil a tres mil días de salario mínimo, y en su caso destitución, e inhabilitación del servidor público para desempeñar otro empleo, comisión o cargo público, cuando:

Para lograr sus propósitos, se valga de redes o sistemas informáticos internacionales o de otros medios de alta tecnología, que impliquen marcada ventaja en el logro de su fin[87]

menores de edad o de personas que no tienen la capacidad para comprender el significado del hecho", Artículo 217, Fracciones I, II y III

[87] Código Penal de Jalisco, Título Décimo Cuarto, "Delitos contra la paz, libertad y seguridad de las personas", Capítulo VII, "Secuestro", Artículo 194, Fracción I, Inciso K

México

En el Código Penal del Estado de México, advertimos los delitos informáticos en el artículo 206, puesto que son sancionables las siguientes conductas:

Produzca, fije, grabe, videograbe, fotografíe o filme e imprima de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho o de resistirlo, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas.

Reproduzca, publique, ofrezca, publicite, almacene, distribuya, difunda, exponga, envíe, transmita, importe, exporte o comercialice de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho o de resistirlo, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas.

Posea intencionalmente para cualquier fin, imágenes, sonidos o la voz de personas menores de edad o de personas que no tengan la capacidad de comprender el significado del hecho o de resistirlo, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas.[88]

[88] Código Penal del Estado de México, Titulo Segundo, "Delitos contra la colectividad", Subtitulo cuarto, "Delitos contra el pleno desarrollo y la dignidad de las personas", Capitulo II, "Utilización de imágenes y/o voz de personas menores de edad o personas que no tienen la capacidad para comprender el significado del hecho para la pornografía", Articulo 206, Fracciones I, II y III

Michoacán

No tiene

Morelos

En el Código Penal de Michoacán, se contemplan supuestos delictivos que se advierten como delitos informáticos, al expresar en su artículo 212, que se sancionará lo siguiente:

Comete el delito de utilización de imágenes y/o voz de personas menores de edad y de personas que no tengan la capacidad para comprender el significado del hecho para la pornografía:

Quien produzca, fije, grabe, videograbe, fotografíe o filme de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas, con o sin fines lucrativos;

Quien reproduzca, publique, ofrezca, publicite, distribuya, difunda, exponga, envíe, transmita, importe, exporte o comercialice de cualquier forma imágenes, sonidos o la voz de una persona menor de edad o de una persona que no tenga la capacidad para comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas;

Quien posea o almacene intencionalmente para cualquier fin, imágenes, sonidos o la voz de personas menores de edad o de personas que no tengan la capacidad de comprender el significado del hecho, sea en forma directa, informática, audiovisual, virtual o por

cualquier otro medio en las que se manifiesten actividades sexuales o eróticas, explícitas o no, reales o simuladas; y

Quien produzca, facilite, incite, financie, distribuya, publique o divulgue, por si o tercera persona, mediante sistemas informáticos y/o similares a los que se reproducen por vía de internet, imágenes pornográficas de personas menores de edad o de personas que no tienen la capacidad para comprender el significado del hecho, teniendo actividades sexuales explicitas, reales o simuladas o bien reproduzcan partes genitales de éstos con fines primordialmente sexuales[89].

Nayarit

El Código Penal de Nayarit, no tiene un capitulo especifico relacionado con éste tipo de delitos, sin embargo, hace alusión a algunos mecanismo electrónicos para la configuración de delitos tales como el fraude y contra la moral pública.

Nuevo León

Nuevo León en su ordenamiento Punitivo Local, involucra lo siguiente:

Se aumentará hasta la mitad de la pena a imponer por los delitos que resultaren, cuando se efectúen mediante la utilización de la televisión, radio, prensa escrita o internet[90].

Comete el delito de pornografía infantil, el que[91]: I. induzca, incite, propicie, facilite u obligue a persona menor de edad a realizar actos de

[89] Código Penal de Morelos, Título Décimo Primero, "Delitos contra el desarrollo y la dignidad de la persona", Capítulo I, "De las personas menores de edad y de quienes no tienen la capacidad para comprender el significado del hecho", Articulo 212, Fracciones I, II, III Y IV

[90] Código Penal de Nuevo León, artículo 352 bis, adicionado, p.o. 28 de julio de 2004

[91] Código Penal de Nuevo León, artículo 201 bis, adicionado con sus fracciones, p.o. 28 de abril de 2004

exhibicionismo corporal o de pornografía; II. Video grabe, audio grabe, fotografié o plasme en imágenes fijas o en movimiento, a persona menor de edad realizando actos de exhibicionismo corporal o de pornografía; III. Promueva, invite, facilite o gestione por cualquier medio, la realización de actividades en las que se ofrezca la posibilidad de observar actos de exhibicionismo corporal o de pornografía, que estén siendo llevadas a cabo por persona menor de edad; IV. siendo mayor de edad, participe como activo o pasivo en los actos de exhibicionismo corporal o de pornografía realizados por persona menor de edad. Se entiende por actos de exhibicionismo corporal, a toda representación del cuerpo humano, con fin lascivo sexual. se considera acto de pornografía a toda representación realizada por cualquier medio, de actividades lascivas sexuales explicitas, reales o simulada, las fotografías, videograbaciones, audio grabaciones o las imágenes fijas o en movimiento, impresas, plasmadas o que sean contenidas o reproducidas en medios magnéticos, electrónicos o de otro tipo y que constituyan recuerdos familiares; los programas preventivos, educativos o de cualquier índole que diseñen e impartan las instituciones públicas, privadas o sociales que tengan por objeto la educación sexual, educación sobre función reproductiva, la prevención de enfermedades de transmisión sexual, el embarazo de adolescentes, no constituyen pornografía infantil.

El fraude en éste Estado, también involucra medios electrónicos.

Oaxaca

En el caso del Estado en comento, se advierte el siguiente tipo penal, relacionado son los medios electrónicos:

Comete el delito de abuso sexual, quien sin consentimiento de una persona ejecute en ella o la haga ejecutar un acto sexual, que no sea la cópula, o la obligue a observar cualquier acto sexual aun a través de medios electrónicos. Al responsable de tal hecho, se le impondrá de

dos a cinco años de prisión y multa de cincuenta a doscientos días de salario mínimo. La pena prevista en esté delito, se aumentará en una mitad en su mínimo y en su máximo cuando: I.- El delito fuere cometido contra persona menor de doce años; II.- Cuando se realice en persona que no tenga la capacidad de comprender el significado del hecho o por cualquier causa no pueda resistirlo; III.- Sea cometido por dos o más personas; IV.- Se hiciera uso de violencia física o moral; y V.- Se hubiera administrado a la víctima alguna sustancia tóxica[92].

De igual forma, advertimos en el siguiente tipo penal la injerencia de los medios electrónicos: Comete el delito de secuestro exprés el que prive de la libertad a otra persona, con el objeto de obtener un lucro mediante el uso de cualquiera de los siguientes medios: Tarjetas de crédito, tarjetas de débito, título de crédito, medios electrónicos, informáticos, mecánicos, en especie o efectivo. Al que cometa el delito señalado en el párrafo anterior, se le impondrá la pena de diez a quince años de prisión y multa de quinientos a setecientos treinta días de salario. Si el tiempo de la privación de la libertad excediera de cinco horas se aplicará lo dispuesto en el artículo 348[93].

Puebla

En Puebla, también advertimos la presencia de los delitos cometidos con los medios digitales:

Al que ilegalmente fabricare, imprimiere, grabare, transportare, exhibiere, vendiere o hiciere circular por cualquier medio , imágenes, libros, revistas, escritos, fotografías, dibujos, carteles, videocintas,

[92] Código Penal del Estado de Oaxaca, Titulo Decimosegundo. Delitos contra la libertad, la seguridad y el normal desarrollo psicosexual. CAPITULO I. Abuso y hostigamiento sexual, estupro y violación, articulo 241

[93] Código Penal del Estado de Oaxaca, Titulo Décimo Octavo. Delitos contra la libertad y violación de otras garantías. CAPITULO II, Secuestro, artículo 348 Bis

mecanismos u objetos lascivos, con implicaciones sexuales, se le aplicará prisión de treinta días a tres años y multa de diez a cien días de salario[94].

Comete el delito de pornografía de menores e incapaces, quien con relación a una persona menor de dieciocho años de edad o de quien no tuviere capacidad de comprender el significado de los hechos o de quien por la razón que fuere no pudiere oponer resistencia, realice alguna de las siguientes conductas: I.- Produzca imágenes o representaciones de exhibicionismo sexual, mediante fotografías, filmes, videos, o cualquier otro medio impreso, electrónico o producido por el avance tecnológico ; II.- Realice materialmente la toma de filmes, videos o cualquier otro medio de obtención de las imágenes a que se refiere la fracción anterior; 2. III.- Emplee, dirija, administre, supervise o participe de algún modo en los actos a que se refiere este artículo a título de propietario, de director, empresario o cualquier otro que implique la participación en los actos mencionados en esta disposición, o IV.- El que a sabiendas de que se trata de las personas a que se refiere este artículo reproduzca, venda, compre, rente, exponga, publicite, difunda o envíe por cualquier medio las imágenes señaladas en esta disposición[95].

Asimismo, encontramos otros tipos penales dentro de la legislación punitiva de puebla, que traen aparejados medios digitales o electrónicos para delinquir.

[94] Código de Defensa Social para el Estado Libre y Soberano de Puebla, Libro Segundo, Delitos en Particular, Capitulo Séptimo, delitos contra la moral pública; contra derechos de menores, Incapaces o personas que no pudieren resistir y contra la dignidad de la persona, Sección Primera, Ultrajes a la moral pública, Artículo 215

[95] Código de Defensa Social para el Estado Libre y Soberano de Puebla, Sección segunda, corrupción y pornografía de menores e incapaces o personas que no pudieren resistir, Artículo 219

Querétaro

En Querétaro, se advierte la presencia de diversos tipos penales cuyos medios de comisión delictiva refieren un aspecto digital:

Se impondrá prisión de 3 meses a 3 años y de 15 a 90 días multa, al que para obtener un beneficio o para causar un daño: I.- Falsifique o altere un documento público o privado; II.- Inserte o haga insertar un documento Público o privado hechos falsos concernientes a circunstancias que el documento deba probar, altere uno verdadero o lo suprima, oculte o destruya; III.- Aproveche la firma o huella digital estampada en un documento en blanco, estableciendo una obligación o liberación o la estampe en otro documento que pueda, comprender bienes jurídicos ajenos, o IV.- Se atribuya, al extender un documento, o atribuya a un tercero un nombre, investidura, título, calidad o circunstancia que no tenga y que sea necesaria para la validez del acto. Igual pena se aplicará al tercero si se actúa en su representación o con su consentimiento[96].

De igual forma en el ámbito sexual, advertimos:

Al que por cualquier medio filme, grabe o imprima actos de exhibicionismo corporal, lascivos o sexuales de menores de dieciocho años de edad o de incapaces, con el fin de exhibirlos, difundirlos, o transmitirlos por cualquier medio impreso o electrónico, se le impondrá prisión de 2 a 10 años, de 20 a 600 días multa y se le inhabilitará para ser tutor o curador. La misma pena se impondrá a quién: I.- Elabore, reproduzca, venda, arriende, exponga, publique o transmita el material a que se refiere este tipo penal, además de decomiso de los objetos,

[96] Legislación Penal del Estado de Querétaro, Capitulo II, Falsificación y uso indebido de documentos, Articulo 231

instrumentos y productos del delito. II.- Procure o facilite la realización de las conductas ilícitas señaladas en el presente artículo[97].

Quintana Roo

En el Estado que nos ocupa, existe la previsión de la comisión de actos delictivos mediante medios digitales, en el ámbito sexual, y contra el patrimonio, citamos algunos ejemplos:

Se impondrá prisión de seis meses a tres años y de quince a noventa días multa, al que para obtener un beneficio o para causar un daño, falsifique o altere un documento público o privado. Las mismas penas se impondrá al que, a sabiendas y con los fines a que se refiere el párrafo anterior, haga uso de un documento falso o alterado, o haga uso indebido de un documento verdadero, expedido en favor de otro, como si hubiera sido expedido a su nombre. Artículo 189 Bis.- Se impondrá hasta una mitad más de las penas previstas en el artículo anterior al que: I.- Produzca, imprima, enajene aun gratuitamente, distribuya o altere tarjetas, títulos, documentos o instrumentos utilizados para el pago de bienes o servicios o para disposición en efectivo, sin consentimiento de quien esté facultado para ello. II.- Adquiera, posea o detente ilícitamente tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo a sabiendas de que son alterados o falsificados. III.- Copie o reproduzca, altere los medios de identificación electrónica, cintas o dispositivos magnéticos de documentos para el pago de bienes o servicios o para disposición en efectivo. IV.- Accese indebidamente los equipos y sistemas de cómputo o electromagnéticos de las instituciones emisoras de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo. Las mismas penas se impondrán a quien utilice indebidamente información

[97] Código Penal para el Estado de Querétaro, Capitulo IV, pornografía con menores o incapaces, Artículo 239 bis

confidencial o reservada de la institución o persona que legalmente esté facultada para emitir tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición de efectivo. Si el sujeto activo es empleado o dependiente del ofendido, las penas aumentarán hasta en una mitad más. En el caso de que se actualicen otros delitos con motivo de las conductas a que se refiere ese artículo se aplicarán las reglas del concurso[98].

Comete el delito de pornografía infantil quien, a persona menor de dieciocho años: I.- Induzca, incite, propicie, facilite u obligue a realizar actos de exhibicionismo corporal o de pornografía; II.- Video grabe, audio grabe, fotografíe o plasme en imágenes fijas o en movimiento, realizando actos de exhibicionismo corporal o de pornografía; III.- Promueva, invite, facilite o gestione por cualquier medio, la realización de actividades en las que se ofrezca la posibilidad de observar actos de exhibicionismo corporal o de pornografía, que estén siendo llevadas a cabo por persona menor de dieciocho años de edad. Comete también el delito de pornografía infantil el que siendo mayor de edad, participe como activo o pasivo en los actos de exhibicionismo corporal o de pornografía realizados por persona menor de edad. Se entiende por actos de exhibicionismo corporal a toda representación del cuerpo humano, con fin lascivo sexual. Se considera acto de pornografía a toda representación realizada por cualquier medio, de actividades lascivas sexuales explícitas, reales o simuladas. Las fotografías, video grabaciones, audio grabaciones o las imágenes fijas o en movimiento, impresas, plasmadas o que sean contenidas o reproducidas en medios magnéticos, electrónicos o de otro tipo y que constituyan recuerdos familiares; los programas preventivos, educativos o de cualquier índole que diseñen e impartan las instituciones públicas, privadas o sociales que tenga por objeto la educación sexual, educación sobre la función reproductiva, la prevención de enfermedades de transmisión sexual o

[98] Código Penal para el Estado Libre y Soberano de Quintana Roo, Capítulo II, Falsificación de Documentos y Uso de Documentos Falsos. Artículo 189

de embarazo de adolescentes, no constituyen pornografía infantil. La sanción por el delito de pornografía infantil será de siete a veinte años de prisión y de 400 a 500 días multa. En todos los casos se aplicará también como pena el decomiso de objetos, instrumentos y productos del delito, respetando los derechos de terceros[99].

San Luis Potosí

En el Estado que nos ocupa, también advertimos la presencia de los delitos que involucran las nuevas tecnologías:

Comete el delito de violación de correspondencia quien: Dolosamente abre o intercepta una comunicación escrita que no está dirigida a él, y II. Siendo empleado de cualquier servicio o empresa de comunicación, conscientemente deja de transmitir o entregar un mensaje que con ese objeto se le encomienda o de comunicar al destinatario el que recibe de otra oficina. Este delito se sancionará con una pena de tres a seis meses de prisión o sanción pecuniaria de cinco a diez días de salario mínimo[100].

Sinaloa

Comete 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; o 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

[99] Código Penal para el Estado Libre y Soberano de Quintana Roo, Pornografía infantil, Artículo 192-bis

[100] Código Penal para el Estado de San Luis Potosí, Capitulo III, Violación de correspondencia, Artículo 307

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[101].

Se impondrán de tres a nueve años de prisión y de cien a quinientos días multa, al que, sin consentimiento de quien esté facultado para ello: I. Produzca, imprima, enajene, aun gratuitamente, distribuya, altere o falsifique tarjetas, títulos o documentos utilizados para la adquisición de bienes y servicios o para disposición de efectivo, otorgados por empresas comerciales distintas de las bancarias; II. Adquiera con propósito de lucro indebido, utilice, posea o detente, sin causa legitima, los objetos a que se refiere la fracción anterior o auténticos, sin el consentimiento de quien este facultado para ello; III. Altere los medios de identificación electrónica, o cualquiera de los objetos a que se refiere la fracción I. IV. Acceda a los equipos electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo; V. Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como a quien posea o utilice la información sustraída, de esta forma; VI. Utilice indebidamente información confidencial o reservada de las instituciones o personas que legalmente esté facultada para emitir tarjetas, títulos o documentos utilizados para el pago de bienes y servicios, o de los titulares de dichos instrumentos o documentos; y, VII. Produzca, imprima, enajene, distribuya, altere, o falsifique vales utilizados para canjear bienes y servicios. En los casos de las fracciones VI y VII, si el sujeto activo es empleado o dependiente del ofendido, las penas se aumentarán hasta en una mitad[102].

[101] Código Penal del Estado de Sinaloa, Capítulo V, Delito Informático, Artículo 217
[102] Código Penal del Estado de Sinaloa, Capítulo V, Delito Informático, Artículo 271 bis

Sonora

En el estado en comento, no se advierte un apartado de delitos informáticos, cibernéticos ni electrónicos, pero en los rubros, electoral y del patrimonio, si se presentan los tipos penales conducentes, haciendo alusión a los medios digitales para la comisión de tales delitos.

Tabasco

En Tabasco, en tratándose de delitos contra el patrimonio, la intimidad y la comunicación, podemos constatar que se contempla en la comisión de los respectivos supuestos delictivos, la utilización de medios digitales:

Se impondrá prisión de seis meses a cinco años, a quien sin consentimiento de otro o sin autorización judicial, en su caso, y para conocer asuntos relacionados con la intimidad de aquél: I. Se apodere de documentos u objetos de cualquier clase; II. Reproduzca dichos documentos u objetos, III. Utilice medios técnicos para escuchar u observar, transmitir, grabar o reproducir la imagen o el sonido[103].

Se impondrán de tres a nueve años de prisión y de doscientos a quinientos días de multa al que: I. En forma y sin autorización de quien esté facultado para ello, adquiera, utilice, posea o detente, tarjetas utilizadas en el comercio para obtener bienes o servicio, títulos o documentos que permitan el uso de éstas o sus bandas magnéticas. La misma pena se aplicará si esas tarjetas, títulos, documentos o bandas magnéticas son falsos. Si el sujeto activo es empleado o dependiente del ofendido, las penas se aumentarán en una mitad más y II. Sin consentimiento de quien esté facultado para ello, produzca, imprima, enajene aun gratuitamente o distribuya, tarjetas utilizadas en el

[103] Código Penal para el Estado de Tabasco, Titulo séptimo, Delitos contra la intimidad personal, Capitulo Único, violación de la intimidad personal, Artículo 163

comercio para obtener bienes o servicios, títulos o documentos que permitan el uso de éstas o sus bandas magnéticas falsifique o altere esas tarjetas, bandas, títulos o documentos[104].

Tamaulipas

Como ya es común advertir, los delitos contra el patrimonio, se han reformado en el entendido de que se pueden cometer mediante el uso de las nuevas tecnologías y Tamaulipas lo prevé en sus ordenanzas penales de la siguiente forma:

Se sancionará con la pena del robo: IV.- El apoderamiento material de los documentos que contengan datos de computadoras o el aprovechamiento o utilización de dichos datos, sin consentimiento de la persona que legalmente pueda disponer de los mismos[105]

El delito de robo simple se sancionará en la forma siguiente: I.- Cuando el valor de lo robado no exceda de cien días de salario, se impondrá una sanción de dos meses a dos años de prisión y multa de cinco a cuarenta días salario; II.- Si excede de cien, pero no de doscientos días salario, la pena será de dos a seis años de prisión y multa de cuarenta a ochenta días salario; y III.- Cuando excediere de doscientos días salario, la sanción será de seis a doce años de prisión y multa de ochenta a ciento cuarenta días salario[106].

[104] Código Penal para el Estado de Tabasco, Titulo Decimo, Delitos contra el patrimonio Capítulo VI, Fraude, Artículo 191 bis
[105] Código Penal para el Estado de Tamaulipas, Titulo Decimonoveno, Delitos contra el patrimonio de las personas, Capítulo I, Robo, Artículo 400
[106] Ibídem, Artículo 402

Tlaxcala

En el estado que nos ocupa se presenta un apartado claro y específico para los delitos informáticos y electrónicos:

Se aplicará prisión de seis meses a dos años y multa hasta de veinte días de salario, al que procure o facilite la corrupción de un menor de dieciocho años, cualquiera que sea la naturaleza de la corrupción con excepción de las conductas siguientes: I.- Quien induzca, procure, facilite o permita por cualquier medio, la realización de actos eróticos o de exhibicionismo corporal, reales o simulados con el fin de grabarlos, videograbarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, sistemas de cómputo, medios electrónicos o de cualquier otra naturaleza; II.- Quien fije, grabe, videograbe, fotografíe, filme o describa actos de carácter erótico o de exhibicionismo corporal en los que participe persona menor de dieciocho años o persona que no tiene capacidad para comprender el significado del hecho; III.- Quien reproduzca, ofrezca, almacene, distribuya, venda, compre, rente, exponga, publique, publicite, transmita, importe o exporte por cualquier medio las grabaciones, videograbaciones, fotografías o filmes a que se refieren las conductas descritas en la fracción II de este artículo, y IV.- Quien financie cualquiera de las actividades descritas en las fracciones anteriores. Se impondrá pena de siete a once años de prisión y multa de mil a dos mil días de salario mínimo general vigente, al autor de los delitos previstos en las fracciones I y II. Se impondrá pena de seis a diez años de prisión y multa de mil a dos mil días de salario mínimo general vigente, al autor de los delitos previstos en las fracciones III y IV. En todos los casos se decomisarán los instrumentos del delito[107].

[107] Código Penal del Estado de Tlaxcala, Delitos cometidos por medios electrónicos e informáticos, Artículo 166

Veracruz

En éste Estado, al igual que en el caso anterior, podemos advertir un apartado específico de los delitos informáticos:

Comete delito informático quien: Si derecho, y con perjuicio de tercero: I.- ingrese a una base de datos, sistema o red computadoras, para obtener, conocer, utilizar, alterar, o reproducir, la información, en ellos contenida; o II.- Intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático, o la información contenida en el mismo o en la base sistema o red. Al responsable de este Delito, se le impondrán, de seis meses a dos años de prisión, y multa, hasta de 300 días de salario, si se comete con fines de lucro las penas se aumentaran en una mitad. Esto es todo lo que en la legislación del estado de Veracruz se encuentra vigente[108].

Yucatán

En Yucatán, no encontramos, tal y como en casos anteriores, un apartado como tal de delitos informáticos, pero nuevamente aludimos al uso de los medios digitales para la comisión de otros delitos ya previstos por las ordenanzas punitivas estatales:

Al que procure o facilite por cualquier medio que uno o más menores de dieciséis años, con o sin su consentimiento, los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, con objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, se le impondrán de cinco a diez años de prisión y de cuatrocientos a quinientos días-multa. Al que fije, grabe o imprima actos de exhibicionismo corporal, lascivos o sexuales en que participen uno o más menores de dieciséis años, se le impondrá la pena de diez a

[108] Código Penal del Estado de Veracruz, Capitulo III, Delitos Informáticos, Articulo 181

catorce años de prisión y de cuatrocientos a quinientos días - multa. La misma pena se impondrá a quien con fines de lucro o sin él, elabore, reproduzca, venda, arriende, exponga, publicite o transmita el material a que se refieren las acciones anteriores. Se impondrá prisión de ocho a dieciséis años y de cuatrocientos cincuenta a quinientos días-multa, así como el decomiso de los objetos, instrumentos y productos del delito, a quien por sí o a través de terceros, dirija, administre o supervise cualquier tipo de asociación delictuosa con el propósito de que se realicen las conductas previstas en los dos párrafos anteriores con menores de dieciséis años. Para los efectos de este artículo se entiende por pornografía infantil, la representación sexualmente explícita de imágenes de menores de dieciséis años[109].

Zacatecas

En zacatecas existen en la ley punitiva estatal, contemplación de los delitos informáticos y alusión a medios electrónicos para la comisión de delitos en el ámbito electoral, veamos algunos ejemplos:

A quien por cualquier medio, procure, induzca o facilite a una persona menor de edad o quien no tenga la capacidad para comprender el significado del hecho, al consumo de estupefacientes, substancias psicotrópicas u otras susceptibles de producir dependencia o bebidas embriagantes, para que adquiera los hábitos de la fármacodependencia o el alcoholismo, o a formar parte de una asociación delictuosa o de la delincuencia organizada, se le impondrá pena de seis meses a tres años de prisión y multa de veinte a cincuenta cuotas. Cuando de la práctica reiterada del activo, el pasivo del delito adquiera los hábitos de la farmacodependencia o del alcoholismo, o forme parte de una asociación delictuosa o de la delincuencia organizada, las penalidades podrán aumentarse hasta en un tanto más. A quien emplee, aun

[109] Código Penal del Estado de Yucatán, Capítulo II, Corrupción de menores e incapaces, trata de menores y pornografía infantil, Artículo 211

gratuitamente, a personas menores de dieciocho años o que no tengan la capacidad de comprender el significado del hecho, utilizando sus servicios en lugares o establecimientos donde preponderantemente se expendan bebidas alcohólicas para su consumo inmediato o se presenten al público espectáculos sexuales, se le aplicará prisión de seis meses a un año y multa de cinco a veinte cuotas así como el cierre definitivo del establecimiento[110].

A quien permita directa o indirectamente el acceso de una persona menor de edad a escenas, espectáculos, obras gráficas o audiovisuales de carácter pornográfico, se le impondrá prisión de uno a tres años y multa de veinte a cincuenta cuotas. Las mismas penas se impondrán al que ejecutare o hiciere ejecutar a otra persona actos de exhibición sexual ante personas menores de edad o que no tengan la capacidad para comprender el significado del hecho. El que, por cualquier medio directo, vendiere, difundiere o exhibiere material pornográfico entre personas menores de edad o personas que no tengan la capacidad para comprender el significado del hecho, será castigado con la pena de prisión de seis meses a un año y multa de cinco a veinte cuotas[111].

2.12. Conclusiones de éste capítulo

En el presente apartado, se demostró que países tales como Austria, Chile, China, España, Estados Unidos, Francia, Holanda e Inglaterra, incluyen dentro de sus ordenamientos punitivos el reconocimiento los delitos informáticos y cibernéticos.

Asimismo, en tratándose de México, se demostró que todos los Códigos Penales del país, incluyen dentro de sus tipos penales la comisión de delitos mediante las nuevas tecnologías y la internet, por

[110] Código Penal del Estado de Zacatecas, Delitos Informáticos, Articulo 181
[111] Ibídem, Artículo 181 Bis

tanto, se puede afirmar que en México, hay un reconocimiento claro de los delitos cibernéticos de facto y en algunos casos como en el Estado de Veracruz existen capítulos especiales de delitos informáticos, pero que también reconocen los delitos cibernéticos de facto.

CAPÍTULO 3
LA PERSECUCIÓN DE LOS DELITOS CIBERNÉTICOS

3.1. Generalidades

Actualmente, el derecho a una administración de justicia pronta y expedita, se encuentra contemplado como un derecho humano[112], dentro de nuestra Carta Magna, en su numeral 17, lo cual permite que los ciudadanos podamos acudir ante las autoridades encargadas de tal función para poner de su conocimiento hechos que consideramos pueden ser constitutivos de un delito en agravio de nuestra persona o de persona distinta según sea el caso y esperar que mediante las Procuradurías, ya sean, la General de la República para delitos federales, o las Generales de Justicia de los Estados para delitos del fuero común, sean resueltos dichos delitos o de ser posible, se llegue a la verdad histórica de los hechos, sin embargo, a lo largo de la presente obra, se verá que estos postulados de prontitud y expedites, se encuentran muy bien plasmados en el papel, pero desafortunadamente no tienen una eficacia real, es decir, no resuelven los problemas en la administración de justicia, la cual se encuentra dotada de una notoria lentitud para determinar y fuertes rezagos en el desarrollo de las indagatorias.

Por otra parte, la era digital que actualmente nos toca vivir, revestida de avances tecnológicos y desarrollo, ha permeado un territorio distinto con nuevas y mejores formas para delinquir de los que actualmente son denominados, como los Ciber-delincuentes, es decir, aquellos individuos que cometen una conducta antisocial, antijurídica y típica, culpable y punible, valiéndose de las nuevas tecnologías y el internet y se valen también de un cierto grado de conocimiento en ese rubro para

[112] El reconocimiento formal de los Derechos Humanos en la Constitución Política de los Estados Unidos Mexicanos, se dio a conocer mediante lo publicado en el Diario Oficial de la Federación el 10 de junio de 2011, en el siguiente: DECRETO por el que se modifica la denominación del Capítulo I del Título Primero y reforma diversos artículos de la Constitución Política de los Estados Unidos Mexicanos; "TÍTULO PRIMERO, CAPÍTULO I, De los Derechos Humanos y sus Garantías"

delinquir, lo cual genera que en tratándose de delitos informáticos y cibernéticos, que dicho sea de paso son conceptos distintos, la ya de por si ineficaz administración de justicia, sea aún menos eficaz para resolver este tipo de delitos de la cuarta y quinta generación, lo anterior, sin dejar de lado que la globalización juega un papel preponderante en las consideraciones del combate a la ciber-delincuencia, puesto que dicho fenómeno, también conocido como mundialización, permite que se transciendan las barreras económicas, políticas, sociales, culturales, entre otras y finalmente, ahora los delincuentes también han globalizado los delitos, que en tratándose de los de carácter cibernético, operan en un país y repercuten en consecuencias para otro y por ende se debe globalizar también la justicia, para la persecución de estos delitos, pero desafortunadamente, este aspecto actualmente solo está disponible para delitos de otra índole que no sean los de tipo cibernético, pues la coadyuvancia con autoridades de tipo internacional, no atiende a este tipo de asuntos o lo hace dándole mucha menor importancia.

3.1.1. Derechos Fundamentales

Resulta importante destacar, que uno de los derechos fundamentales (ahora con carácter de derecho humano), que consagra la Constitución Política de los Estados Unidos Mexicanos, es el de una administración de justicia pronta y expedita, lo cual, se advierte a través del numeral 17 del referido ordenamiento legal supremo.

No se hará énfasis en la distinción doctrinal entre derechos humanos, garantías individuales o derechos fundamentales, por no ser el objeto de la presente investigación discernir sobre las diferencias, sin embargo, *grosso modo* es factible referirse en éste punto a derechos fundamentales, porque al hablar de garantías individuales, entendemos que el concepto de garantía no es equivalente al concepto de derecho, es decir, al hablar de garantía se entiende únicamente como un medio que permite alcanzar un derecho y no el derecho *per se*. Cabe señalar,

que actualmente ya ha sido suprimido el término de garantías individuales de la Carta Magna.

Por otra parte, en lo referente al concepto de derechos humanos, actualmente reconocidos en el capítulo primero de la Carta Magna, implica una connotación más amplia, intrínsecamente valida, mas allá del derecho positivo, siendo el objeto de tutela más importante en nuestros días.

Sin embargo, se considera factible que para los fines del presente trabajo, se entienda a la administración de justicia pronta y expedita como un derecho fundamental, salvaguardado por la Carta Magna, entendiendo por derechos fundamentales, aquellos que están previstos en el texto constitucional y en los tratados internacionales.

3.1.2. Administración de Justicia

Es así, que después de las consideraciones anteriores, se puede continuar analizando, lo que es la administración de justicia en el ámbito penal. Pues bien, debemos tener presente que en el orden criminal, que es al que se hará referencia en todo momento por tratarse de ciber-delincuencia, está en manos de la Procuraduría General de la República a través de sus respectivas Agencias del Ministerio Público Federal, Sub-procuradurías y fiscalías especializadas, teniendo a su cargo a la Policía Ministerial Federal, lo anterior, en los delitos federales, pero en aquellos del fuero común, atienden las Procuradurías Generales de Justicia de los Estados, a través de sus Agencias del Ministerio Público del fuero común, Sub-procuradurías, Agencias y Fiscalías Especializadas, tendiendo a su cargo, a las diversas Policías Ministeriales de los Estados y en el caso de Veracruz a la Agencia Veracruzana de Investigación. A todo lo anterior, se le conoce como la Procuración de Justicia, que tiene lugar mediante el procedimiento denominado Averiguación Previa, que es la primera

etapa del Juicio Penal Federal, pero en el caso del fuero común y muy particularmente en el Estado de Veracruz, la primera etapa del procedimiento penal es denominada Investigación Ministerial la cual está a cargo de la Procuración de Justicia Estatal. Es así que la Procuración de Justicia tanto en el fuero común como en el Federal, constituyen lo que se denomina Administración de Justicia, por ser las Procuradurías tanto las locales como la Federal, integrantes del Poder Ejecutivo, es decir, forman parte de la Administración Publica; Y en cierto modo, el Poder Ejecutivo, de manera formal, realiza una actividad administrativa, pero de manera material realiza una actividad jurisdiccional.

3.1.3. Justicia Pronta Y Expedita

Cuando escuchamos hablar de una justicia pronta y expedita, para algunos, lo que probablemente, se vendría a la mente, es un derecho fundamental, consagrado en el numeral 17 de la Constitución Política de los Estados Unidos Mexicanos, al referirse a una Administración de Justicia en tales términos; Pero para muchos otros, se viene a la mente una falacia. ¿Por qué un juicio tan temerario como éste?, la respuesta puede deberse al análisis concreto de la aplicación de los términos "pronta" y "expedita" teniendo estos preceptos la intención de promulgar una persecución de los delitos de manera rápida, eficaz libre de cualquier atadura que le impida el curso a las investigaciones ministeriales o averiguaciones previas, según sea el caso; pero ¿cuál es la realidad? Recordemos que desde una visión tridimensional del derecho, la ley puede estar revestida de un contenido justo y moral (iusnaturalismo), emitida por un órgano formalmente válido (iuspositivismo) y dedicada a resolver problemas sociales con eficacia (realismo sociológico); Pues de estas tres corrientes del Derecho, que conciben a la norma, con finalidades distintas, nosotros tendemos a la postura de que la norma, independientemente de que debe estar dotada de un contenido justo y moral y de que debe estar expedida por un órgano formalmente valido, tiene que resolver problemas sociales

de manera eficaz, lo cual no se logra con preceptos constitucionales plasmados solo en papel pero que en la realidad, nada tienen de aplicación, tales como la administración de justicia “pronta” y “expedita”. Si se analiza por un momento el curso de las indagatorias que se efectúan con motivo de las investigaciones ministeriales o averiguaciones previas según sea la esfera de competencia, entenderemos, que los procedimientos, están plagados de una gama de trámites burocráticos que no solo retrasan las indagatorias, sino que muchas veces son el impedimento principal para el desarrollo de las misma y para ello, es pertinente narrar a modo de ejemplo, lo que acontece generalmente cuando un hecho que presuntamente es constitutivo del delito de despojo, es puesto en conocimiento de la autoridad en el fuero común: Una persona que se dice agraviada por otra que presuntamente cometió un hecho delictivo que posiblemente constituye el despojo, acude a la Agencia del Ministerio Público del Fuero Común en turno, a poner en conocimiento de la autoridad tales circunstancias, a lo que tiene dos opciones, rendir su declaración ministerial por comparecencia a lo que seguramente el oficial de mesa que le tome la declaración, podrá darle fecha para que se presente dentro de una semana, por tratarse de un delito que se persigue por querella de parte, en tratándose de familiares, o bien, el agraviado, podrá conseguir un abogado, que le haga la declaración por escrito, con todas los requisitos de rigor que marca la ley entre los cuales destacan las probanzas que típicamente son los testigos, la inspección ocular y quizás una pericial si se descubre durante la indagatoria que el bien inmueble despojado ha sufrido daños que deban repararse.

Acto seguido y después de esas consideraciones, se acude nuevamente con el oficial de mesa que lleva la investigación ministerial, para que le dé curso a la querella, a lo que una vez que la recibe por escrito y que la consulta con el Agente del Ministerio Público, para analizar si no hay oscuridad en la misma, le da nuevamente fecha al que la viene a interponer, para que acuda a la ratificación de la misma

una semana después quizás. Hecho lo anterior, y una vez ratificada la denuncia, comienza propiamente la indagatoria, y dan fecha para que se presenten los testigos a declarar, lo cual es con intervalos de tiempo de alrededor de una semana para que reciban y les tomen su declaración a los testigos previo interrogatorio directo. Una vez recibidos los testigos, viene la inspección ocular, la cual es programada por el oficial de mesa, dentro de otras dos semanas quizás, posteriores a la toma de la declaración de los testigos.

Una vez apersonado en el lugar de los presuntos hechos delictivos, el oficial de mesa, sienta su razonamiento y pregunta al presunto agraviado, que si considera que haya daños, en la propiedad que dice que es suya, y de la cual previamente acreditó la propiedad, si el presunto agraviado considera que si hay daños, éstos deberán ser valorados por un perito experto, el cual tiene que ser dependiente del departamento de servicios periciales adscrito a la Procuraduría General de Justicia en cuestión, a lo que el oficial de mesa le dice al presunto agraviado, que vaya dentro de una semana para ver si ya giró el oficio a servicios periciales para que instruyan a un perito para que haga la valoración en el inmueble referido. Ese trámite se lleva alrededor de un mes, en lo que mandan dicho oficio a servicios periciales, lo regresan acusado de recibido, le forman otro folio en servicios periciales, turnan el asunto con el perito de guardia, éste agenda según sus ocupaciones la visita al inmueble para valorar los daños y finalmente acude en compañía del presunto agraviado al inmueble que se presume fue dañado y hace su peritaje y rinde su informe y lo turna de regreso a la Agencia del Ministerio Público que inicialmente conoció y con el oficial de mesa encargado de la indagatoria, esto después de haber trascurrido al menos cuatro meses de presentada la querella. Una vez hecho lo anterior, se puede mandar a llamar a declarar al presunto responsable, es decir, al inculpado, en el domicilio que previamente fue fijado para tales efectos, a lo que se gira un oficio en donde se le hace de su conocimiento al inculpado que existe una investigación ministerial en su contra, que debe rendir su declaración al respecto de las

acusaciones que se le imputan, y el oficio donde se le hace saber esto, dice al calce, cita primera.

Si el presunto responsable, no acude, después de otras dos semanas, se le gira una segunda cita e inclusive una tercera cita ya con carácter de urgente, a lo que después de un mes tratando de que declare el presunto responsable, este acude ante el oficial de mesa y se apega al 20 constitucional y pide rendir su declaración por escrito posteriormente y se le otorga una semana más para que se apersone con su abogado. Hecho esto, se presenta con el abogado el presunto responsable y en su declaración por escrito, niega los hechos, aporta testigos, aporta un peritaje, en ese mismo acto de la declaración, a su vez, denuncia por el delito de falsas deducías y simulación de pruebas, se desahogan todas las probanzas, y después de alrededor de año y medio, se tiene todo listo y se destina la indagatoria para determinar, pero esa determinación puede tardar alrededor de seis meses o más dependiendo de las ocupaciones de los Agentes u oficiales de mesa, esto sin importar que el término de ley sean 180 días para determinar. Y entonces estamos hablando que de un asunto que se persigue por querella de parte y que aparentemente no tiene mayores complicaciones, la justicia es pronta y expedita en alrededor de dos años para desahogar la primera etapa del procedimiento penal.

Es en estos casos, que dicho sea de paso, abundan en las Agencias, donde nuestro derecho a una administración de justicia pronta y expedita, se traduce como una simple falacia, pues después de dos largos años, se determina con el riesgo de que no haya lugar al ejercicio de la acción penal y reparadora del daño y entre el recurso de queja en el caso del Estado de Veracruz o el amparo indirecto, el tiempo es más largo sólo para trascender de la investigación ministerial a la etapa de instrucción previa ya ante el Juzgado competente y en el cual de estimarse necesario se girará la correspondiente orden de aprehensión después de alrededor de dos meses de llegada la

indagatoria al citado Juzgado y con la posibilidad de que como se trata de delito que no es grave, se pague una fianza y con eso se acaban dos años de indagatoria y se vislumbran otros dos más por lo menos, para las etapas restantes del procedimiento penal.

Con este relato extraído de la realidad, podemos advertir, como la administración de justicia, difícilmente es pronta y expedita, y si esto ocurre con delitos que se persiguen por querella de parte, ¿qué ocurre con indagatorias más complejas en donde se involucran delitos graves y se vulneran bienes jurídicamente tutelados más importantes como la vida?, ahora se verá como estos procedimientos, también se tornan complejos e ineficientes en tratándose de delitos cibernéticos.

3.2. El Combate a la Ciber-delincuencia

Como consecuencia de la revolución tecnológica-informática, surge la regulación de los delitos informáticos, tanto en el ámbito federal, como en las esferas locales, a través de los ordenamientos punitivos respectivos. De lo anterior, es importante destacar, que la necesidad de enfrentar a la nueva era de ciber-delincuentes, originó las reformas en las leyes punitivas estatales y en la federal, que tratan de enfrentar estos delitos de la cuarta y quinta generación. Pero nos queda la duda aún de ¿Qué son los ciber-delincuentes? y para lo cual, se intenta explicar.

Resultaría difícil comprender que al igual que en la medicina se habla de que no hay enfermedades, si no enfermos, en el mismo orden de ideas, pero traslapado al ámbito jurídico, se puede expresar que no es necesario el análisis de delitos si no es en fusión del análisis del actuar de los delincuentes, así pues, con la llegada de la era digital, el cambio social que sobrevino, las nuevas tecnologías, que abrieron un mundo de posibilidades para el hombre, también abrieron un mundo de posibilidades para delinquir, esto es, un territorio nuevo para cometer delitos, es por ello, que en este apartado, se hace referencia a la gran

diferencia entre lo que actualmente se conoce como delincuente y lo que se denomina como ciber-delincuente, el cual, aparte de cometer una conducta antisocial, antijurídica, y típica, culpable y punible, también posee otro atributo que lo hace diferente del delincuente tradicional, y esto es, un conocimiento de las nuevas tecnologías, de la computación y de lenguaje de la informática, lo cual, lo vuelve todavía más peligroso que al delincuente tradicional, ya que si hacemos una reflexión profunda al respecto, el delincuente, es aquel que comete un delito, que actualice el tipo penal, y que, realiza una conducta antijurídica, antisocial y típica, culpable y punible y en virtud de ello, es que prácticamente todos los ciudadanos, somos delincuentes en potencia, no porque tengamos la intención de cometer un delito, sino porque el libre albedrío del que gozamos, nos permite hasta cierto punto cometer un delito, el cual posteriormente sería castigado conforme a la ley, sin embargo, se debe tener muy presente, que la ley es de carácter prohibitiva y punitiva, lo que trae como consecuencia, que haya un alineamiento al orden jurídico, sin embargo esto no quiere decir que en cualquier momento no se pueda cometer un delito, es decir, todos los individuos son delincuentes en potencia, pues aunque no se tenga la intención de hacerlo, existe la posibilidad y la libertad de cometer un delito.

Sin embargo, en tratándose de delitos informáticos y cibernéticos, no todos los ciudadanos son delincuentes en potencia, pues no todos los individuos, conocen de informática, saben utilizar un ordenador, saben navegar en el ciberespacio, o simplemente no todos tienen conocimiento de computación, lo que orilla a comprender, que no todos los ciudadanos son ciber-delincuentes en potencia, ya que como se ha mencionado antes, estos ciber-delincuentes, requieren de un mayor grado de conocimiento, y por ende tienen mayor temibilidad, eso hace que el grupo de ciber-delincuentes en potencia, sea más reducido, que el grupo de delincuentes tradicionales, y por ende esto permite que el nivel de delitos informáticos, sea menor que el nivel de delitos

tradicionales, pero a la vez, la procuración de justicia en tratándose de delitos informáticos debe poseer un conocimiento mayor, una preparación más firme, tecnología más avanzada y capacitación constante en el rubro de la informática, ya que si nos remontamos a los delitos cometidos por los delincuentes tradicionales, tales como son el robo a mano armada, violación, lesiones, despojo, etc. es decir delitos que no requieren mayor conocimiento para su comisión, estos suelen combatirse con armas de fuego, con individuos capacitados en defensa personal, y hasta con un departamento de servicios periciales, a la altura de los delitos, sin embargo, en tratándose de Ciber-delincuentes, éstos poseen mayor conocimiento, saben navegar en el ciberespacio, conocen de redes, conocen virus digitales, saben infiltrarse a los ordenadores y destruirlos, pero también saben escabullirse y esto los convierte en seres más peligrosos, ya que desde una simple computadora, pueden cometer delitos graves, y es por ello, que la procuración de justicia, debe ser más preparada, con conocimientos de informática, con un departamento de servicios periciales robustecido con científicos encargados de dirimir controversias relacionadas con delitos informáticos a fin de llegar a la verdad histórica de los hechos que plantea un agraviado.

Por otra parte, se debe hacer una consideración que es medular, para el entendimiento de la temibilidad de los ciber-delincuentes, y es que actualmente los ordenamientos punitivos tanto estatales como federales, hablan de delitos informáticos, reduciéndose éstos, simplemente a la invasión no autorizada de ordenadores o bien, a la destrucción de sistemas lógicos a los que no se estaba autorizado ingresar, pero dicho tipo penal de delitos informáticos, independientemente de su esfera de competencia, no contempla la comisión de los delitos que se cometen haciendo uso de las nuevas tecnologías y es aquí donde hace falta que se contemple la concepción de los delitos cibernéticos, los cuales involucran a los delitos informáticos, pero además, aquellos que se cometen haciendo uso de las nuevas tecnologías, es decir, un fraude cometido por Internet no

puede recibir el mismo tratamiento que un fraude tradicional, y por ende es un ciber-delito, mas no un delito informático.

Es por lo anterior, que debe quedar muy claro, que los ciber-delincuentes, no son solo aquellos que cometen delitos informáticos, sino más aún, los ciber-delincuentes, son aquellos que cometen una conducta antijurídica, antisocial, típica, culpable y punible, valiéndose de las nuevas tecnologías mediante cierto grado de conocimiento de la informática. Esta definición nos deja ver claramente, que existen dos tipos de delincuentes los tradicionales y los ciber-delincuentes, siendo estos últimos más peligrosos, pues son más difíciles de perseguir, y los encargados para ello, como son los integrantes de la Procuraduría de Justicia, deben estar más capacitados para atender este tipo de delincuentes.

Para dejar claro lo anterior, es prudente ejemplificar la diferencia entre un delito cometido por un delincuente tradicional y un delito cometido por un Ciber-delincuente.

Antes de pasar al ejemplo, se debe hacer la precisión que si bien es cierto, se reconocen los delitos cibernéticos en la presente investigación, no se está de acuerdo con el concepto, el cual previa argumentación jurídica, se tenderá a perfeccionar con otro que permita una mejor comprensión.

Un individuo, que se anuncia en la Internet, a través de una página de venta, valiéndose de ciertas modificaciones en la web, para aparentar que es un excelente vendedor, de prestigio, y de categoría, pues se encuentra situado en los lugares de mayor prestigio de una página de venta por Internet, dicho individuo, ofrece la venta de una computadora portátil, por un costo de $10,000.00, otra persona, accede a comprar dicha computadora, teniendo que hacer un depósito de la cantidad convenida a una cuenta que previamente el vendedor le ha otorgado,

sin embargo, pasado un tiempo después de haber realizado dicho depósito, el comprador no recibe su producto y finalmente, se advierte que fue víctima de un delito. De este ejemplo, si se quisiera saber, de qué tipo de delito fue víctima este individuo, quizás algunos pudieran pensar que de un delito informático, lo cual estaría totalmente errado, si atendemos al tipo penal, nos encontramos en presencia del delito de fraude, sin embargo el delincuente que formuló dicho delito, no es un delincuente tradicional, ya que se ha valido de un conocimiento que tiene sobre las nuevas tecnologías y al mismo tiempo se ha valido de la informática, para cometer sus delitos, en consecuencia, se está en presencia de un ciber-delincuente y por ende de la comisión de un delito cibernético. Los ciberdelincuentes, cuentan con grado de temibilidad mucho mayor, mayor ventaja para delinquir, y menos posibilidades de ser atrapados.

Por otra parte, vale la pena mencionar, qué es lo que ocurre, cuando es cometido un delito cibernético, y qué pasa cuando la autoridad se confunde en su persecución y es incapaz de discernir la diferencia entre delitos informáticos y delitos cibernéticos y más aún cuando echan mano del actual organismo dependiente de la policía federal preventiva denominado la policía cibernética.

Pues bien, como ya se ha visto antes, los delitos informáticos y los delitos cibernéticos, son distintos, siendo estos últimos, aun no definidos por los ordenamientos punitivos estatales ni federales; asimismo, existe otro problema y es cuando se pone un hecho delictivo de esta naturaleza bajo la tutela de una Agencia del Ministerio Publico, el primer conflicto, es la esfera de competencia, la cual es difícil concretar por parte de la autoridad, ya que el ciberespacio no tiene jurisdicción.

Los delitos cibernéticos son de competencia del fuero común, ya que las situaciones se dan entre particulares, la federación no actúa como sujeto pasivo. Pero el otro razonamiento revestido de mayor

credibilidad y fundamento, es que en el momento en que se utilizan las vías de la comunicación como medio para delinquir se vuelve competencia del fuero federal. Particularmente este segundo razonamiento, es el adecuado para la persecución de la mayoría de los ciber-delitos, asimismo el código penal dice que los delitos cometidos en el extranjero con repercusión en nuestro país, son de competencia federal, lo cual podría configurarse si alguien nos defrauda de otro país como España por ejemplo.

Finalmente, se puede pensar, que tal y como se advirtió en apartados anteriores, la justicia nada tiene de pronta y expedita en tratándose de delitos comunes, y entonces, mucho menos podrá ser así, en tratándose de delitos informáticos y cibernéticos, y por ende se ratifica el hecho de que el derecho fundamental a una administración de justicia pronta y expedita, continúa siendo una expectativa.

3.3. Implicaciones en el Mundo Globalizado

¿Qué tiene que ver la globalización en todo esto? la respuesta es muy sencilla, sólo basta con entender un poco a este concepto que dicho sea de paso, ha sido concebido por otros autores también como mundialización, y en ambos casos se refiere al esparcimiento generalizado de los criterios tanto culturales, como económicos, sociales, religiosos, y de otras índoles por todo el mundo, rompiendo con las barreras que existen y que encierran a los países teniendo como consecuencia por ejemplo, que en China se utilice la mezclilla o que en México celebremos el halloween, o que utilicemos y consumamos marcas que son de otros países; la globalización no es solo traspasar las barreras económicas de los países, sino que se traspasan las barreras culturales, religiosas, científicas, y de prácticamente todos los rubros, dando lugar a la homogenización de criterios y a un aparente hibrido de lo que originalmente tenía un país. Pero después de esta concepción de globalización, seguramente nos

seguimos preguntando, ¿Qué tiene que ver con el asunto de la administración de justicia, los derechos fundamentales y el combate a la ciber-delincuencia? Nuevamente la respuesta esta ante nosotros, partiendo de la concepción anterior de globalización, y es que la Internet, como instrumento típico para cometer delitos cibernéticos, es una de las formas más comunes para entender la globalización, ya que con esta red internacional, podemos interactuar con todos los países del mundo, conocer sus culturas, aceptarlas, adoptarlas e inclusive intercambiar aportaciones propias por las ajenas y con ello, invariablemente, se hace presente la ciber-delincuencia y más aún, los problemas para combatirla, ya que de primera instancia y tal y como se veía en casos anteriores, cuando un ciber-delito, es perpetrado en otro país y tiene incidencia en el nuestro, se convierte en delito federal, pero además, se debe tener en consideración, que actualmente, con el uso de las nuevas tecnologías, surge lo que podríamos denominar la globalización de los delitos, es decir ahora es posible que una persona pueda perpetrar un delito en un país, ejecutarlo en otro y finalmente que las consecuencias repercutan en otro más, y con ello, debe por ende, existir una globalización de la justicia, la cual tiene sustento en los tratados internacionales, que permiten la coadyuvancia de organizaciones internacionales que combaten el crimen, de tal suerte que un delincuente que ejecuta su delito en el extranjero y cuyas consecuencias tienen repercusión en nuestro país, puede ser perseguido desde México, y rastreado, a fin de solicitar el apoyo de las organizaciones internacionales como la INTERPOL por citar un ejemplo y tener a fin, detener y castigar ciber-delincuente. Es así, que se puede advertir con mayor claridad, la relación que tiene el fenómeno de la globalización con el combate a la ciber- delincuencia, y por ende con la administración de justicia y con la preservación del derecho fundamental de la prontitud y expedites para su cumplimiento, que dicho sea de paso, esto último, parece ser aún más difícil con la globalización de los delitos. Es decir, si en apartados anteriores, ya se había comentado que la justicia no es pronta ni expedita en tratándose de delitos no graves y en consecuencia al tratarse de delitos de mayor

complejidad para su resolución, era lógico entender que mucho menos habría estos principios, esto orilla a comprender, que al intentar hablar de prontitud y expedites, en tratándose de la persecución de delitos informáticos y cibernéticos, los referidos preceptos, son menos aplicables a la realidad todavía y por ende, nos queda arribar a la idea de que si esto ocurre en el ámbito nacional, qué se puede esperar al hablar de delitos que han trascendido las fronteras de nuestro país es decir de la globalización de los delitos, pues simplemente resulta difícil concebir la idea de que habrá prontitud y expedites en la persecución de los delitos y más aún, es probable, que dichos delitos, nunca toquen las puertas de instancias internacionales y mucho menos que se llegue a resolver o a conocer la verdad histórica de los hechos que se persiguen.

3.4. Consideraciones finales de éste capítulo

Una vez advertidos los apartados anteriores, es necesario hacer algunas consideraciones finales, que servirán para concretizar la idea central del presente capítulo.

En México, sabido es, que la Procuración de Justicia, presenta diversos problemas para la persecución de los delitos tal y como lo hemos visto en líneas que anteceden, y que si de suyo, ya es difícil demostrar la culpabilidad de un presunto delincuente con quien se tuvo contacto cara a cara y de quien se conoce su domicilio y al cual quizás también se le ve a diario, imaginémonos por unos momentos, la dificultad de hacer pronta y expedita la persecución de un presunto delito, cuando es de mayor complejidad, como lo es un delito cibernético o un delito informático y si a esto le agregamos que pudo haber sido perpetrado en el extranjero y con repercusiones en nuestro país, la idea de una determinación favorable, es casi impensable.

Pero ¿qué se puede reflexionar de todo esto?, ¿qué se puede hacer para que esta situación mejore?, para que los principios de prontitud y expedites, realmente sean eficaces y no solo se adviertan como una falacia o ¿es que acaso la justicia tal y como se viene administrando hoy en día, ya es pronta y expedita? Porque si es así, habría que valorar detenidamente cuál es la percepción generalizada que se tiene de prontitud y expedites. Es cierto, se debe mencionar, que muchos actos delictivos, por su naturaleza, complejidad y dificultad para su esclarecimiento, no pueden ser resueltos tan rápido como se quisiera, e inclusive es justificada la idea del no esclarecimiento de ciertos crímenes, por ser de imposible indagación, en virtud de las circunstancias, y en ese sentido, no podemos hacer observaciones criticas fundadas; Pero qué pasa, cuando son delitos, en los que se aportan los medios probatorios suficientes, donde los presuntos delincuentes, están al alcance para ser aprehendidos y donde los hechos son tan claros que hasta la idea de una justicia por propia mano se hace concebible, entonces, ya resulta difícil entender que las indagatorias aun así, sigan tardándose años por meros trámites administrativos y rezagos en el cumplimiento de la obligación de la autoridad competente. Entonces volvemos al mismo punto, ¿Qué hace falta para que el Derecho Fundamental de una administración de justicia pronta y expedita, deje de ser letra muerta y se haga eficaz en tratándose del combate a la ciber-delincuencia?

La respuesta no es simple y si se analiza, tampoco sería posible por el momento aportarla, sin embargo, si existen las condiciones de hacer algunas aproximaciones a una posible solución, pero para ello, se debe atender a otra situación que a continuación se plantea.

Es indudable, que los órganos de Procuración de Justicia, deben contar con el auxilio de otras instituciones que permitan alcanzar los fines de la indagatoria que *grosso modo* es esclarecer la verdad histórica de los hechos, y para lo cual, en el caso de los delitos informáticos y los delitos cibernéticos, existe un organismo dependiente de la Policía

Federal Preventiva, denominado Policía Cibernética, desafortunadamente, solo existe la dependencia en la ciudad de México, su auxilio, en teoría se hace presente previa denuncia y/o querella presentada ante la agencia competente y finalmente la labor de esta Policía Cibernética, sólo es de aplicaciones formales pero no materiales.

Los particulares son los que se han adjudicado en virtud de la necesidad de la población cibernauta, la tarea de desarrollar softwares para el combate a la ciber-delincuencia, es decir, empresas tales como Panda Antivirus, Kaspersky, Norton, Macafee, Microsoft, entre otras, que desarrollan antivirus y sistemas tales como el Firewall, el Antispyware, el Antiadware, que impiden que los ciber-delincuentes, se infiltren a nuestros ordenadores caseros, para efectos de que no vulneren nuestra seguridad informática, desafortunadamente, estos intentos de las diversas empresas mencionadas, y dicho sea de paso que se venden a los usuarios pagando un costo considerable, no son suficientes, ya que actualmente los ciber-delincuentes, superan en número y conocimiento a los expertos que los combaten y más aún todavía, combaten entre sí, para erradicar un virus de otro ciber-delincuente, situado en un ordenador al que piensan invadir, para efectos de ser ellos los manipuladores de ese nuevo territorio… es decir, tal y como en las películas de los gangsters, en donde la policía parecía ser totalmente ignorada y eran las pandillas las que se peleaban entre sí para adueñarse del territorio, de igual forma ocurre en el ciberespacio, pero la disputa es entre mejores virus y programas para invadir los ordenadores y la lucha consiste en dejar inservible el software de otro ciber-delincuente que es la competencia. La tarea de garantizar la seguridad de los ordenadores de los cibernautas, debería corresponder al estado y este a su vez, garantizar a la ciudadanía con organismos especializados, que ante la comisión de delitos de esta naturaleza, se podrá hacer una indagatoria eficaz y no una que duerma el sueño de los justos.

Es así, que para hacer una aproximación de solución al problema de la falta de eficacia en la aplicación del derecho fundamental que plasma el 17 Constitucional Federal, que nos habla de una administración de justicia pronta y expedita, y en tratándose particularmente en el combate a la ciber-delincuencia en aras de un mundo globalizado, podemos decir, que lo que falta es una adecuada instauración de instituciones que estén verdaderamente capacitadas, para coadyuvar con la procuración de justicia, y que el Estado provea los medios necesarios para que en los casos de delincuencia cibernética o informática, de índole internacional se pueda contar con la cooperación eficaz de otros organismos internacionales tales como la INTERPOL (Organización Internacional de la Policía Criminal), para esclarecer los hechos delictivos.

Ahora bien, si se revisan los registros del INEGI (Instituto Nacional de Estadística, Geografía e Informática), por citar una fuente oficial, se puede advertir, que los índices de delitos informáticos cometidos en todo el país, son muy bajos, claro, que se debe tomar en cuenta, que no se registran los delitos cibernéticos, los cuales como hemos visto anteriormente, no están aún reconocidos formalmente por los ordenamientos punitivos tanto estatales como el federal, pero sí están reconocidos de manera tácita, al crear una Policía Cibernética, la cual conoce no solo de delitos informáticos, si no de cuestiones tales como la pornografía infantil por Internet, los fraudes cibernéticos entre otros delitos que no encuadran con el tipo penal de delitos informáticos, lo cual deja entrever que el propio estado, reconoce que hay delitos cibernéticos que abarcan a los propios delitos informáticos, pero que no está contemplado por las leyes punitivas en las distintas esferas.

Por lo que habría que valorar que tantos delitos cibernéticos, están integrados en las estadísticas de fraudes, invasión a la intimidad, extorsión, delitos contra el honor, y muchos otros que se cometen con

el uso de las nuevas tecnologías pero que no están contemplados como delitos cibernéticos.

Sin embargo, partiendo de un supuesto hipotético, donde los índices tanto de delitos cibernéticos como los informáticos, fueran bajos en su comisión en todo el país, ¿eso sería una justificación para dejar de lado la capacitación y mejoramiento en la persecución de este tipo de delitos? Y más aún, reflexionemos un poco, cuantos de nosotros verdaderamente denunciaríamos un fraude por Internet cometido en agravio de nuestro patrimonio, o amenazas de otro particular por correo electrónico o intrusiones no autorizadas a nuestro correo electrónico o la publicación en una página web de fotos personales, ¿Cuántos?... Seguramente, se infiere la respuesta, muy pocos y la razón es, porque muy en el fondo se tiene el presentimiento, que sólo se gastaría tiempo, dinero, esfuerzo y no se llegaría a ningún resultado o la autoridad no hará nada para resolver esos presuntos hechos delictivos. Por lo que otro aspecto que ayudaría a la aproximación de la solución que se viene planteando es la cultura de la denuncia en este tipo de delitos tanto informáticos como cibernéticos, para generar en la autoridad interés por mejorar y capacitar a las autoridades perseguidoras de tales ilícitos.

Puntos concluyentes

Finalmente, se puede arribar a ciertos puntos concluyentes que se desprenden de todo lo anteriormente expuesto:

- Existe una diferencia doctrinal entre los términos Derechos Fundamentales, Garantías Individuales (actualmente suprimido de la Carta Magna en México) y Derechos Humanos, por lo que resultaría incorrecto utilizar dichos términos indistintamente o cual si fuesen sinónimos, teniendo a bien, haber optado para los fines de la presente investigación, por el término Derechos

Fundamentales, siendo estos últimos, los que se encuentran suscritos en nuestro ordenamiento legal supremo y en los tratados internacionales.

- La Impartición de Justicia, es una labor propia y exclusiva del Poder Judicial, sin embargo, en virtud de la teoría de los actos formales y materiales, sabemos que el Poder Ejecutivo, a través de la Procuraduría General de la República (materia federal) o de las Procuradurías Generales de Justicia de los Estados (fuero común), puede realizar formalmente la labor de administración de justicia, pero materialmente realiza una actividad jurisdiccional que es lo que se conoce como Procuración de Justicia.

- Uno de los derechos fundamentales que se encuentra plasmado en nuestra Constitución Política Federal, es el que se advierte del numeral 17, que plasma el derecho a una administración de justicia pronta y expedita, es decir, que las indagatorias llevadas a cabo por las procuradurías ya sean las locales o la federal, tengan un desarrollo eficaz, rápido, claro y sin rezagos de ninguna especie, sin embargo, sabido es que este derecho, únicamente se encuentra plasmado en papel, pero no está revestido de una eficacia real, por lo que resultaría factible decir que el Derecho Fundamental a una prontitud y expedites en la administración de justicia, es cuestionable.

- Al estar inmersos en una era digital, existen nuevos avances, nuevos retos y también la generación de delitos denominados, los delitos informáticos y los aún no reconocidos pero si existentes delitos cibernéticos, que son aquellos que se cometen haciendo uso de las nuevas tecnologías y por ende surgen lo que denominamos ciber-delincuentes que son aquellos que comenten (comisión por acción o comisión por omisión) una

conducta antisocial, antijurídica y típica, culpable y punible, valiéndose del uso de las nuevas tecnologías y de cierto grado de conocimiento en ese rubro para delinquir.

- Con el fenómeno de la globalización, vienen también implicaciones de tipo internacional que se ligan a la comisión de los delitos, esto es, la expansión de criterios tecnológicos, científicos, sociales, políticos, económicos y de muchos otros rubros, no deja de lado la globalización de los delitos, teniendo esto como consecuencia que se puedan perpetrar los delitos desde un país, accionarlos en otro y tener las repercusiones en otro más, lo que se presenta como una problemática para la administración de justicia que si de suyo, ya era lenta y con diversos rezagos en sus indagatorias, con la globalización de los delitos, ahora ya no se vislumbra la pronta y expedita resolución de los delitos cibernéticos e informáticos, pues se globalizan los delitos, pero no la justicia.

- La cultura de la denuncia en tratándose de delitos cibernéticos e informáticos, permitirá que haya mayor interés por parte del Estado, en mejorar y capacitar más y mejor a las instituciones de Procuración de Justicia, para lograr un combate contra la ciber-delincuencia más eficaz.

- Para perseguir a los ciber-delincuentes, lo que falta es una adecuada instauración de instituciones capacitadas, para colaborar con las Agencias Investigadoras, y que el Estado provea los medios necesarios para que en los casos de delincuencia cibernética o informática, de índole internacional se pueda contar con la cooperación de organismos internacionales para castigar a los responsables.

CAPÍTULO 4
ANÁLISIS DE LA INVESTIGACIÓN DE CAMPO RELACIONADA CON LA PERSECUCIÓN DE LOS DELITOS CIBERNÉTICOS

4.1. Validación de la muestra y el instrumento de recolección de datos

Es indudable, que en toda investigación, se debe siempre acudir a la verificación científica de los postulados que se pretende aportar y de las afirmaciones que se proyectan como ciertas, para lo cual, se tuvo a bien, encuestar a los integrantes de las diversas subprocuradurías que integran las tres zonas del Estado de Veracruz (norte, centro y sur), con el fin de acreditar lo que originalmente es necesario demostrar en la presente investigación, pero antes de ir a los referidos resultados, primero se debe validar tanto el instrumento de recolección de datos, que en este caso es mixto (cualitativo y cuantitativo) como la muestra de la que se obtuvieron los mismos.

Veracruz, descansa la administración de justicia en la Procuraduría General de Justicia del Estado de Veracruz, la cual a su vez, tiene a su cargo a siete subprocuradurías que cubren tres zonas, la zona Norte, la Centro y la Sur, las cuales tienen a sus cargos las 300 agencias del ministerio público que se encargan junto con otras dependencias de la propia procuraduría, de perseguir y consignar a los delincuentes. Esto se referirá mejor en el siguiente organigrama:

CUADRO 3

Fuente: Página del Gobierno del Estado de Veracruz, Procuraduría General de Justicia

Pues bien, a continuación se presentan las subprocuradurías que persiguen y consignan a los delincuentes:

- Subprocuraduría Regional Zona Norte Tantoyuca – Distritos primero a quinto – 28 municipios
- Subprocuraduría Regional Zona Norte Tuxpan – Distritos sexto a octavo – 21 municipios
- Subprocuraduría Regional Zona Centro Xalapa – Distritos noveno a duodécimo – 44 municipios
- Subprocuraduría Regional Zona Centro Veracruz – Distrito decimoséptimo – 14 municipios
- Subprocuraduría Regional Zona Centro Córdoba – Distritos decimotercero a decimosexto – 60 municipios
- Subprocuraduría Regional Zona Centro Cosamaloapan – Distritos decimoctavo a decimonoveno – 23 municipios
- Subprocuraduría Regional Zona Sur Coatzacoalcos – Distritos vigésimo y vigesimoprimero – 25 municipios

Con base en las siete subprocuradurías mencionadas con antelación, se escogieron mediante un muestreo probabilístico, la muestra que es fundamento de la presente investigación, entendiendo por muestreo probabilístico “aquellos que se basan en el principio de equiprobabilidad. Es decir, aquellos en los que todos los individuos tienen la misma probabilidad de ser elegidos para formar parte de una muestra y, consiguientemente, todas las posibles muestras de tamaño

"n" tienen la misma probabilidad de ser elegidas. Sólo estos métodos de muestreo probabilísticos nos aseguran la representatividad de la muestra extraída y son, por tanto, los más recomendables"[113].

Pero también dentro de los muestreos probabilísticos, encontramos una subdivisión que se denomina "Muestreo aleatorio estratificado", el cual "suele reducir el error muestral para un tamaño dado de la muestra. Consiste en considerar categorías típicas diferentes entre sí (estratos) que poseen gran homogeneidad respecto a alguna característica (se puede estratificar, por ejemplo, según la profesión, el municipio de residencia, el sexo, el estado civil, etc). Lo que se pretende con este tipo de muestreo es asegurarse de que todos los estratos de interés estarán representados adecuadamente en la muestra. Cada estrato funciona independientemente, pudiendo aplicarse dentro de ellos el muestreo aleatorio simple o el estratificado para elegir los elementos concretos que formarán parte de la muestra"[114]

Atendiendo a lo anterior, se escogió una muestra de 4 de 7 subprocuradurías que representan al Estado de Veracruz, dos de la zona centro, una de la zona sur y una de la zona norte, para que con base en el tipo de muestreo mencionado con antelación el margen de error se reduzca considerablemente y los resultados aportados sean más fidedignos.

Es así que, se escogieron 4 subprocuradurías que de la población total que son 7, representan el 57.14% de dicha población.

Las subprocuradurías en cuestión son:

- Subprocuraduría Regional Zona Norte Tantoyuca – Distritos primero a quinto – 28 municipios

[113] http://www.psico.uniovi.es/Dpto_Psicologia/metodos/tutor.7/p2.html
[114] Ibídem

- Subprocuraduría Regional Zona Centro Veracruz – Distrito decimoséptimo – 14 municipios

- Subprocuraduría Regional Zona Centro Córdoba – Distritos decimotercero a decimosexto – 60 municipios

- Subprocuraduría Regional Zona Sur Coatzacoalcos – Distritos vigésimo y vigesimoprimero – 25 municipios

De igual forma, con base en las 300 agencias del ministerio público que existen en Veracruz, que se encuentran representadas por las siete subprocuradurías mencionadas en primeras líneas de este apartado, se escogió una muestra aleatoria de 56 agencias y dependencias, que representan el 18.67% de la población total.
De la muestra de 56 agencias, ésta necesariamente para ser una muestra representativa, debía pertenecer a las subprocuradurías de las tres zonas en cuestión que se han tomado también como muestra, quedando de la siguiente manera:

- 18 agencias sub Tantoyuca (Norte)
- 16 agencias sub Veracruz (Centro)
- 12 agencias sub Córdoba (Centro)
- 10 agencias sub Coatzacoalcos (Sur)

Es decir, a modo de resumen, de 7 subprocuradurías, se tomaron 4 como muestra, de las tres zonas que constituyen el Estado de Veracruz (Norte, Centro y Sur), asimismo, las 7 subprocuradurías que son la población total, albergan a su cargo 300 agencias, de las cuales se tomaron como muestra 56, que están al cargo de las 4 subprocuradurías de nuestra muestra.

Cabe destacar, que de las 56 agencias mencionadas como muestra, se entrevistaron a sus respectivos funcionaros adscritos a las mismas, es decir, un representante por agencia, lo que nos da un total de 56 personas entrevistadas, entre las que se incluyeron oficiales de mesa, agentes del ministerio público y agentes de la agencia veracruzana de investigación, lo cual los convierte en las personas ideales para contestar las preguntas que mas adelante se advertirán, toda vez que son los responsables de la persecución de los delitos al interior de las referidas agencias del ministerio público.

Pero ¿Por qué es válida la muestra que presentamos de 56 agencias?, es decir, la muestra en una investigación es de suma relevancia para validar los resultados obtenidos ya que si tomamos un vaso y recogemos agua del mar y en este vaso, no encontramos peces, no asumimos que no hay peces en el mar, simplemente la muestra fue insuficiente, por tanto ¿cómo sabemos que 56 agencias y dependencias de la procuración de justicia son suficientes para aportarnos resultados fidedignos? La respuesta a continuación:

Una fórmula muy extendida que orienta sobre el cálculo del tamaño de la muestra para datos globales es la siguiente:

$$n = \frac{k^2 * p * q * N}{(e^2 * (N-1)) + k^2 * p * q}$$

N: es el tamaño de la población o universo (número total de posibles encuestados).

k: es una constante que depende del nivel de confianza que asignemos. El nivel de confianza indica la probabilidad de que los resultados de la presente investigación sean ciertos: un 95,5 % de confianza es lo mismo que decir que nos podemos equivocar con una probabilidad del 4,5%.

Los valores k más utilizados y sus niveles de confianza son:
k 1,15 1,28 1,44 1,65 1,96 2 2,58

Nivel de confianza 75% 80% 85% 90% 95% 95,5% 99%

e: es el error muestral deseado. El error muestral es la diferencia que puede haber entre el resultado que obtenemos preguntando a una muestra de la población y el que obtendríamos si preguntáramos al total de ella. Ejemplos:

Ejemplo 1: si los resultados de una encuesta dicen que 100 personas comprarían un producto y tenemos un error muestral del 5% comprarán entre 95 y 105 personas.

Ejemplo 2: si hacemos una encuesta de satisfacción a los empleados con un error muestral del 3% y el 60% de los encuestados se muestran satisfechos significa que entre el 57% y el 63% (60% +/- 3%) del total de los empleados de la empresa lo estarán.
Ejemplo 3: si los resultados de una encuesta electoral indicaran que un partido iba a obtener el 55% de los votos y el error estimado fuera del 3%, se estima que el porcentaje real de votos estará en el intervalo 52-58% (55% +/- 3%).

p: es la proporción de individuos que poseen en la población la característica de estudio. Este dato es generalmente desconocido y se suele suponer que p=q=0.5 que es la opción más segura.

q: es la proporción de individuos que no poseen esa característica, es decir, es 1-p.

n: es el tamaño de la muestra (número de encuestas que vamos a hacer)[115].

Pues bien, con base en la fórmula de obtención de muestra anterior, nos permitimos asignar los datos de la presente investigación:

N= 300 Agencias del Ministerio Público (Tamaño de la población)
K= 1.65 - 90% - (Nivel de confianza)
e= 10% (Error muestral)
p= 0.5 (parte de la población que posee las característica del estudio)
q= 0.5 (parte de la población que no posee las característica del estudio)
n= Tamaño de la Muestra = 56

En el caso de que sí se conozca el tamaño de la población, se usa la fórmula anterior

Por tanto, a la luz de los razonamientos anteriores y con base en la muestra obtenida, se tendra un margen de error de 10%, por tanto si un 85% de los encuestados manifiestan desconocer los delitos cibernéticos, esto querrá decir que entre 75% y 95% de la población que procura la justicia en el Estado de Veracruz, no conoce los delitos cibernéticos.

El instrumento de recolección de datos mixto (cualitativo/cuantitativo), que se aplicó a los encuestados, que constituyen autoridades procuradoras de justicia en el estado de Veracruz en las tres zonas que lo constituyen (Norte, Centro y Sur), se encuentra conformado por las siguientes preguntas (Para ver el instrumento que se aplicó, así como

[115] http://www.feedbacknetworks.com/cas/experiencia/sol-preguntar-calcular.htm

las respuestas expresadas, pasar al apartado de anexos de la presente investigación):

PREGUNTAS CUANTITATIVAS

¿Conoce usted los Delitos Cibernéticos?
Si / No

¿Existen denuncias relativas a la comisión de delitos cibernéticos presentadas ante esta agencia entre los años 2006 y 2009? Si su respuesta es no pase a la pregunta 6.
Si / No

¿Los delitos cibernéticos están contemplados por los ordenamientos punitivos de Veracruz y Federal respectivamente?
Si / No

¿Sabe usted cual es la policía cibernética?
Si / No

¿Ha usted hecho uso del apoyo de la policía cibernética para la resolución de alguna investigación ministerial?
Si / No

¿Sabe usted cual es la diferencia entre los delitos informáticos y los delitos cibernéticos?
Si / No

¿Considera usted que la autoridad Procuradora de Justicia, reconoce “de hecho” los delitos cibernéticos?
Si / No

¿Estaría usted de acuerdo en que la autoridad procuradora de justicia, reconoce los delitos cibernéticos “de hecho” más no “de derecho”?
Si / No

¿Considera que actualmente ante la falta de inclusión de los delitos cibernéticos en los códigos penales, la autoridad procuradora de justicia, le da tratamiento en sus indagatorias a los delitos cibernéticos como si fueran delitos de los ya previstos por los códigos?
Si / No

¿Considera que los tipos penales que actualmente están vigentes, son insuficientes para la persecución de los delitos cibernéticos?
Si / No

¿Cree usted que los delitos cibernéticos merecen un tratamiento en la indagatoria diferente al que típicamente se da a los demás delitos contemplados por las leyes punitivas tanto del Estado como Federal?
Si su respuesta es no pase a la pregunta 18.
Si / No

¿Tiene usted conocimiento sobre si a la fecha, existe en la Dirección General de Servicios Periciales correspondiente, un experto en informática forense?
Si / No

¿Considera que para la persecución de los delitos cibernéticos debe existir un experto en informática forense en la Dirección General de Servicios Periciales correspondiente?
Si / No

¿Considera usted que existe dificultad para validar el alcance y valor probatorio de los medios de prueba digitales en las investigaciones ministeriales de cualquier índole?
Si / No

¿Existe una diferencia entre los delitos informáticos y los delitos cibernéticos? Si su respuesta es no pase a la pregunta 26.
Si / No

¿Considera que con la descripción del tipo penal de delitos informáticos, es posible la persecución de los delitos cibernéticos?
Si / No

¿Sabe usted cual es la distinción entre el delincuente cibernético y el delincuente tradicional?
Si / No

¿Considera que el delincuente cibernético tiene un grado mayor de temibilidad que el delincuente tradicional?
Si / No

¿Considera que las investigaciones ministeriales relacionadas con el delincuente cibernético, necesitan un tratamiento diferente que las que involucran al delincuente tradicional?
Si / No

¿Considera que el tratamiento que le da la autoridad procuradora de justicia a los delitos cibernéticos en las indagatorias correspondientes, a través de las agencias de ministerio público, debería ser especializado?
Si / No

¿Considera que los delitos informáticos son un tipo penal que podría incluirse dentro de los delitos cibernéticos de estar estos últimos tipificados?
Si / No

¿Existen denuncias relativas a la comisión de delitos informáticos presentadas ante esta agencia? Si su respuesta es no pase a la pregunta número 39.
Si / No

¿Considera que de tipificarse el tipo penal de delitos cibernéticos, deberían preservarse aún los delitos informáticos?
Si / No

PREGUNTAS CUALITATIVAS

¿Cómo podría usted definir a los delitos cibernéticos?

¿Con qué frecuencia se presentan denuncias relativas a la comisión de delitos cibernéticos?

¿Con qué frecuencia son consignados los presuntos responsables por la comisión de delitos cibernéticos?

¿Por qué la legislación punitiva del Estado de Veracruz y la Federal, no contemplan dentro de sus tipos penales a los delitos cibernéticos?

De los que saben la diferencia entre los delitos informáticos y los delitos cibernéticos, expresaron que:

¿Cómo considera que debe ser el tratamiento en la indagatoria para la persecución de los delitos cibernéticos?

¿Quién es el encargado de validar el alcance y valor probatorio de los medios de prueba digitales en las investigaciones ministeriales?

¿Quién es el perito experto de la correspondiente Dirección General de Servicios Periciales que valida el alcance y valor probatorio de los

medios digitales en tratándose de la comisión de los delitos cibernéticos?

¿Quién es el perito experto de la correspondiente Dirección General de Servicios Periciales que valida los daños a los medios digitales, electrónicos y de nuevas tecnologías, en tratándose de la comisión de los delitos cibernéticos?

¿Cuándo usted dirige un oficio a la Dirección General de Servicios Periciales, para efectos de solicitar el apoyo de un perito experto en tratándose de una indagatoria relativa a la comisión de delitos cibernéticos, ¿De qué perito específicamente requiere el apoyo?

¿Cuál considera que es la diferencia entre los delitos informáticos y los delitos cibernéticos?

¿Qué es para usted el delincuente cibernético?

¿Por qué, muy a pesar de que el Estado reconoce los delitos cibernéticos “de hecho”, no los incluye dentro de la legislación penal correspondiente, para entonces reconocerlos también “de derecho”?

¿Por qué el estado ha creado una policía cibernética para coadyuvar con la persecución de los delitos de esta índole, pero no se reconocen en los ordenamientos punitivos Estatales y Federal respectivamente?

¿Cuál es el tratamiento que la autoridad procuradora de justicia le da a los delitos cibernéticos en las indagatorias correspondientes, a través de las agencias de ministerio público?
¿Con qué frecuencia se presentan denuncias relativas a la comisión de delitos informáticos?

¿Con qué frecuencia son consignados los presuntos responsables por la comisión de delitos informáticos?

Finalmente, se debe mencionar que el fundamento de la muestra que se utilizó en el instrumento aplicado es el siguiente:

De conformidad con lo dispuesto en el art. 115 de la ley orgánica del poder judicial del estado

Artículo 115. El territorio del Estado se divide en los siguientes Distritos Judiciales:

I. Primer Distrito: Pánuco.

Pánuco
Pueblo Viejo
Tampico Alto
El Higo.

II. Segundo Distrito: Ozuluama.

Ozuluama
Naranjos
Amatlán
Citlaltépetl
Chinampa de Gorostiza
Tamalín
Tantima
Tancoco.

III. Tercer Distrito: Tantoyuca.

Tantoyuca
Chiconamel

Chalma
Chontla
Ixcatepec
Platón Sánchez
Tempoal.

IV. Cuarto Distrito: Huayacocotla.

Huayacocotla
Zacualpan
Ilamatlán
Texcatepec.

V. Quinto Distrito: Chicontepec.

Chicontepec
lxhuatlán de Madero
Benito Juárez
Tlachichilco
Zontecomatlán.

VI. Sexto Distrito: Tuxpan.

Tuxpan
Cerro Azul
Tamiahua
Álamo Temapache
Tepetzintla.

VII. Séptimo Distrito: Poza Rica.

Poza Rica de Hidalgo
Cazones de Herrera

Castillo de Teayo
Tihuatlán
Coatzintla

VIII. Octavo Distrito: Papantla.

Papantla
Coahuitlán
Coxquihui
Coyutla
Chumatlán
Espinal
Filomeno Mata
Gutiérrez Zamora
Mecatlán
Tecolutla
Zozocolco de Hidalgo

IX. Noveno Distrito: Misantla.

Colipa,
Juchique de Ferrer
Martínez de la Torre
Nautla
San Rafael
Tenochtitlán
Vega de Alatorre
Yecuatla.

X. Décimo Distrito: Jalacingo.

Jalacingo
Atzalan
Altotonga

Las Minas
Perote
Tlapacoyan
Villa Aldama

XI. Decimoprimer Distrito: Xalapa.

Xalapa
Pacho Viejo del Municipio de Coatepec
Acajete
Acatlán
Actopan
Alto Lucero
Banderilla
Coacoatzintla
Chiconquiaco
Emiliano Zapata
Jilotepec
Landero y Coss
Las Vigas de Ramírez
Naolinco
Miahuatlán
Rafael Lucio
Tatatila
Tepetlán
Tlacolulan
Tlalnelhuayocan
Tonayán.

XII. Decimosegundo Distrito: Coatepec.

Coatepec
Apazapan

Ayahualulco
Cosautlán de Carvajal
lxhuacán de los Reyes
Jalcomulco
Teocelo
Xico.

XIII. Decimotercer Distrito. Huatusco.

Huatusco
Alpatláhuac
Calcahualco
Comapa
Coscomatepec
lxhuatlán del Café
Sochiapa
Tenampa
Tepatlaxco
Tlacotepec de Mejía
Tlaltetela
Totutla
Zentla.

XIV. Decimocuarto Distrito: Córdoba.

Córdoba
Amatlán de los Reyes
Atoyac
Ayojapa, del Municipio de Zongolica
Camarón de Tejeda
Carrillo Puerto
Coetzala
Cuichapa
Cuitláhuac

Chocamán
Fortín
Naranjal
Omealca
Paso del Macho
Tezonapa
Tomatlán
Yanga
Ayojapa del Municipio de Zongolica.

XV. Decimoquinto Distrito: Orizaba.

Orizaba
Acultzingo
Aquila
Atzacan
Camerino Z
Mendoza
San Andrés Tenejapa
Huiloapan de Cuauhtémoc
Lxhuatlancillo
Ixtaczoquitlán
La Perla
Maltrata
Mariano Escobedo
Nogales
Rafael Delgado
Río Blanco
Soledad Alzompa
Tlilapan.

XVI. Decimosexto Distrito: Zongolica.

Zongolica
Atlahuilco
Astacinya
Los Reyes
Magdalena
Mixtla de Altamirano
Tehuipango
Tequila
Texhuacán
Tlaquilpa
Xoxocotla.

XVII. Decimoséptimo Distrito: Veracruz

Veracruz
Alvarado
La Antigua
Boca del Río
Cotaxtla
Medellín
Paso de Ovejas
Puente Nacional
Soledad de Doblado
Ignacio de la Llave
Tlalixcoyan
Jamapa
Manlio Fabio Altamirano
Úrsulo Galván.

XVIII. Decimoctavo Distrito: Cosamaloapan.

Cosamaloapan
Carlos A. Carrillo
Acula

Amatitlán
Chacaltianguis
Ixmatlahuacan
Otatitlán
José Azueta
Santiago Sochiapan
Tierra Blanca
Tlacotalpan
Tlacojalpan
Tres Valles
Tuxtilla
Playa Vicente.

XIX. Decimonoveno Distrito: San Andrés Tuxtla.

San Andrés Tuxtla
Ángel R. Cabada
Catemaco
Hueyapan de Ocampo
Juan Rodríguez Clara
Lerdo de Tejada
Saltabarranca
Santiago Tuxtla e Isla

XX. Vigésimo Distrito: Acayucan.

Acayucan
Mecayapan
Oluta
San Juan Evangelista
Sayula de Alemán
Soconusco
Soteapan

Texistepec
Jáltipan
Jesús Carranza.

XXI. Vigésimo Primer Distrito: Coatzacoalcos.

Coatzacoalcos
Tatahuicapan de Juárez
Uxpanapa
Agua Dulce
Cosoleacaque
Chinameca
Las Choapas
Hidalgotitlán
lxhuatlán del Sureste
Minatitlán
Moloacán
Nanchital de Lázaro Cárdenas del Río
Oteapan
Pajapan
Zaragoza.

Asimismo, en relación a las subprocuradurías, se tiene como fundamento:

La Ley Orgánica de la Procuraduría General de Justicia del Estado de Veracruz de Ignacio de la Llave (G.O. 30 de Abril de 2008)

PRIMERO.-El presente Decreto entrará en vigor al día siguiente de su publicación en la Gaceta Oficial, órgano del Gobierno del Estado.

SEGUNDO.- Las Siete Subprocuradurías Regionales tendrán las denominaciones y competencia territorial siguientes: La Subprocuraduría Regional de Justicia Zona Norte- Tantoyuca ejercerá

su función en el Primero, Segundo, Tercero, Cuarto y Quinto Distritos Judiciales; la Subprocuraduría Regional de Justicia Zona Norte-Poza Rica en el Sexto, Séptimo y Octavo Distritos Judiciales; La Sucbprocuraduría Judicial Zona Centro-Xalapa en el Noveno, Décimo, Undécimo y Duodécimo Distritos Judiciales; La Subprocuraduría Regional Zona Centro-Córdoba en el Décimo Tercero, Décimo Cuarto, Décimo Quinto y Décimo Sexto Distritos Judiciales; La Subprocuraduría Regional de Justicia Zona Centro- Veracruz en el Décimo Séptimo Distrito Judicial; La Subprocuraduría Regional Zona Centro-Cosamaloapan en el Décimo Octavo y Décimo Noveno Distritos Judiciales; y la Subprocuraduría Regional de Justicia Zona Sur-Coatzacoalcos en el Vigésimo y Vigésimo Primer Distritos Judiciales.

TERCERO.- Las Subprocuradurias Regionales que actualmente tramiten investigaciones ministeriales o asuntos relacionados con Agencias del Ministerio Público pertenecientes a Distritos Judiciales que se reubican a la creación de las nuevas suprocuraduría deberán de remitir de inmediato los expedientes correspondientes, previas anotaciones en los libros de control, así como todos los asuntos relacionados en estudio y los accesorios relativos.

CUARTO.- La Dirección General de Administración de la Procuraduría General de Justicia, gestionará la asignación de los recursos humanos y materiales que correspondan, ante la instancia competente, para la implementación y puesta en marcha inmediata de las nuevas subprocuradurías regionales creadas.

QUINTO.- Se derogan todas las demás disposiciones que se opongan al presente Decreto.

De igual forma, jurídicamente se funda la muestra con lo siguiente:

Ley Orgánica de la Procuraduría General de Justicia del Estado de Veracruz de Ignacio de la Llave

Capítulo II
De su Organización

Artículo 17. La Procuraduría General de Justicia del Estado estará a cargo de un Procurador General, quien será el titular de la institución del Ministerio Público y superior jerárquico de todo el personal de la misma.
Artículo 18. Para el ejercicio de las funciones y despacho de los asuntos de su competencia, la Procuraduría General de Justicia contará con los servidores públicos de confianza siguientes:

I. Un Procurador General de Justicia;
(REFORMADA, G.O. 30 DE ABRIL DE 2008)
II. Siete Subprocuradores Regionales: dos en la Región Norte, con residencia en Tantoyuca y Poza Rica respectivamente; cuatro en la Región Centro con residencia en Xalapa-Enríquez, Córdoba, Veracruz y Cosamaloapan; y, uno en la región sur, con residencia en Coatzacoalcos;
III. Un Subprocurador Especializado en asuntos Indígenas;
IV. Un Subprocurador de Supervisión y Control;
V. Un Director General de Investigaciones Ministeriales;
VI. Un Director General de Control de Procesos;
VII. Un Director General Jurídico;
VIII. Un Director General de la Policía Ministerial;
IX. Un Director de los Servicios Periciales;
X. Un Director del Instituto de Formación Profesional;
XI. Un Director del Centro de Atención a las Víctimas del Delito;
XII. Un Director del Centro de Información;
XIII. Un Director General de Administración;
XIV. Un Subdirector de Recursos Financieros;

XV. Un Subdirector de Recursos Materiales;
XVI. Un Subdirector de Recursos Humanos;
XVII. Agentes del Ministerio Público Auxiliares del Procurador;
XVIII. Agentes del Ministerio Público Investigadores y Adscritos a los Juzgados de Primera Instancia y Menores;
XIX. Agentes del Ministerio Público Municipales, en las cabeceras municipales en donde no haya agentes designados, fungirá como investigador y adscrito el Síndico del Ayuntamiento;
XX. Agentes del Ministerio Público Especializados en Delitos cometidos por Servidores
Públicos;
XXI. Agentes del Ministerio Público Especializados en Delitos Electorales;
XXII. Agentes del Ministerio Público Visitadores;
XXIII. Agentes de la Policía Ministerial;
XXIV. Peritos;
XXV. Oficiales Secretarios; y
XXVI. Contralor Interno.

Es así como se funda jurídica y científicamente la muestra que fue base de aplicación del instrumento de recolección de datos mixto (cualitativo y cuantitativo)

4.2. Resultados obtenidos de la aplicación del instrumento de recolección de datos mixto

Decodificación de las encuestas realizadas con base en la muestra estadística, a las Subprocuradurías Generales de Justicia del Estado de Veracruz de las diferentes zonas, para la obtención de los datos que fundamentan la presente investigación (se puede ver el instrumento aplicado en el anexo de la presente investigación)

TABLA 2

PARTE CUANTITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA			
SUBPROCURADURÍA	**PREGUNTA**	**SI**	**NO**
SUBPROCURADURÍA VERACRUZ 16 PERSONAS ENCUESTADAS, ADSCRITAS EN AGENCIA DEL MINISTERIO PÚBLICO	¿Conoce usted los Delitos Cibernéticos?	14	2
	¿Existen denuncias relativas a la comisión de delitos cibernéticos presentadas ante esta agencia entre los años 2006 y 2009?	7	9
	¿Los delitos cibernéticos están contemplados por los ordenamientos punitivos de Veracruz y Federal respectivamente?	14	2
	¿Sabe usted cual es la policía cibernética?	6	10
	¿Ha usted hecho uso del apoyo de la policía cibernética para la resolución de alguna investigación ministerial?	4	12
	¿Sabe usted cual es la diferencia entre los delitos informáticos y los delitos cibernéticos?	7	9
	¿Considera usted que la autoridad Procuradora de Justicia, reconoce “de hecho” los delitos cibernéticos?	14	2
	¿Estaría usted de acuerdo en que la autoridad procuradora de justicia, reconoce los delitos cibernéticos “de hecho” más no “de derecho”?	6	10
	¿Considera que actualmente ante la falta de inclusión de los delitos cibernéticos en los códigos penales, la autoridad procuradora de justicia, le da tratamiento	7	9

PARTE CUANTITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA			
SUBPROCURADURÍA	**PREGUNTA**	**SI**	**NO**
	en sus indagatorias a los delitos cibernéticos como si fueran delitos de los ya previstos por los códigos?		
	¿Considera que los tipos penales que actualmente están vigentes, son insuficientes para la persecución de los delitos cibernéticos?	15	1
	¿Cree usted que los delitos cibernéticos merecen un tratamiento en la indagatoria diferente al que típicamente se da a los demás delitos contemplados por las leyes punitivas tanto del Estado como Federal?	12	4
	¿Tiene usted conocimiento sobre si a la fecha, existe en la Dirección General de Servicios Periciales correspondiente, un experto en informática forense?	5	11
	¿Considera que para la persecución de los delitos cibernéticos debe existir un experto en informática forense en la Dirección General de Servicios Periciales correspondiente?	16	0
	¿Considera usted que existe dificultad para validar el alcance y valor probatorio de los medios de prueba digitales en las investigaciones ministeriales de cualquier índole?	15	1
	¿Existe una diferencia entre los delitos informáticos y los delitos cibernéticos?	7	9

PARTE CUANTITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA			
SUBPROCURADURÍA	**PREGUNTA**	**SI**	**NO**
	¿Considera que con la descripción del tipo penal de delitos informáticos, es posible la persecución de los delitos cibernéticos?	11	5
	¿Sabe usted cual es la distinción entre el delincuente cibernético y el delincuente tradicional?	13	3
	¿Considera que el delincuente cibernético tiene un grado mayor de temibilidad que el delincuente tradicional?	12	4
	¿Considera que las investigaciones ministeriales relacionadas con el delincuente cibernético, necesitan un tratamiento diferente que las que involucran al delincuente tradicional?	14	2
	¿Considera que el tratamiento que le da la autoridad procuradora de justicia a los delitos cibernéticos en las indagatorias correspondientes, a través de las agencias de ministerio público, debería ser especializado?	14	2
	¿Considera que los delitos informáticos son un tipo penal que podría incluirse dentro de los delitos cibernéticos de estar estos últimos tipificados?	13	3
	¿Existen denuncias relativas a la comisión de delitos informáticos presentadas ante esta agencia?	7	9
	¿Considera que de tipificarse el tipo penal	16	0

PARTE CUANTITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA			
SUBPROCURADURÍA	**PREGUNTA**	**SI**	**NO**
	de delitos cibernéticos, deberían preservarse aún los delitos informáticos?		
SUBPROCURADURÍA COATZACOALCOS 10 PERSONAS ENCUESTADAS, ADSCRITAS EN AGENCIA DEL MINISTERIO PÚBLICO	¿Conoce usted los Delitos Cibernéticos?	4	6
	¿Existen denuncias relativas a la comisión de delitos cibernéticos presentadas ante esta agencia entre los años 2006 y 2009?	0	10
	¿Los delitos cibernéticos están contemplados por los ordenamientos punitivos de Veracruz y Federal respectivamente?	3	7
	¿Sabe usted cual es la policía cibernética?	2	8
	¿Ha usted hecho uso del apoyo de la policía cibernética para la resolución de alguna investigación ministerial?	0	10
	¿Sabe usted cual es la diferencia entre los delitos informáticos y los delitos cibernéticos?	2	8
	¿Considera usted que la autoridad Procuradora de Justicia, reconoce “de hecho” los delitos cibernéticos?	4	6
	¿Estaría usted de acuerdo en que la autoridad procuradora de justicia, reconoce los delitos cibernéticos “de hecho” más no “de derecho”?	5	5
	¿Considera que actualmente ante la falta de inclusión de los delitos cibernéticos en los códigos penales, la autoridad procuradora de justicia, le da tratamiento	4	6

PARTE CUANTITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA			
SUBPROCURADURÍA	**PREGUNTA**	**SI**	**NO**
	en sus indagatorias a los delitos cibernéticos como si fueran delitos de los ya previstos por los códigos?		
	¿Considera que los tipos penales que actualmente están vigentes, son insuficientes para la persecución de los delitos cibernéticos?	5	5
	¿Cree usted que los delitos cibernéticos merecen un tratamiento en la indagatoria diferente al que típicamente se da a los demás delitos contemplados por las leyes punitivas tanto del Estado como Federal?	2	8
	¿Tiene usted conocimiento sobre si a la fecha, existe en la Dirección General de Servicios Periciales correspondiente, un experto en informática forense?	0	10
	¿Considera que para la persecución de los delitos cibernéticos debe existir un experto en informática forense en la Dirección General de Servicios Periciales correspondiente?	7	3
	¿Considera usted que existe dificultad para validar el alcance y valor probatorio de los medios de prueba digitales en las investigaciones ministeriales de cualquier índole?	3	7
	¿Existe una diferencia entre los delitos informáticos y los delitos cibernéticos?	3	7

PARTE CUANTITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA			
SUBPROCURADURÍA	**PREGUNTA**	**SI**	**NO**
	¿Considera que con la descripción del tipo penal de delitos informáticos, es posible la persecución de los delitos cibernéticos?	1	9
	¿Sabe usted cual es la distinción entre el delincuente cibernético y el delincuente tradicional?	5	5
	¿Considera que el delincuente cibernético tiene un grado mayor de temibilidad que el delincuente tradicional?	2	8
	¿Considera que las investigaciones ministeriales relacionadas con el delincuente cibernético, necesitan un tratamiento diferente que las que involucran al delincuente tradicional?	4	6
	¿Considera que el tratamiento que le da la autoridad procuradora de justicia a los delitos cibernéticos en las indagatorias correspondientes, a través de las agencias de ministerio público, debería ser especializado?	7	3
	¿Considera que los delitos informáticos son un tipo penal que podría incluirse dentro de los delitos cibernéticos de estar estos últimos tipificados?	5	5
	¿Existen denuncias relativas a la comisión de delitos informáticos presentadas ante esta agencia?	0	10
	¿Considera que de tipificarse el tipo penal	6	4

PARTE CUANTITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA			
SUBPROCURADURÍA	**PREGUNTA**	**SI**	**NO**
	de delitos cibernéticos, deberían preservarse aún los delitos informáticos?		
SUBPROCURADURÍA CÓRDOBA 12 PERSONAS ENCUESTADAS, ADSCRITAS EN AGENCIA DEL MINISTERIO PÚBLICO	¿Conoce usted los Delitos Cibernéticos?	4	8
	¿Existen denuncias relativas a la comisión de delitos cibernéticos presentadas ante esta agencia entre los años 2006 y 2009?	0	12
	¿Los delitos cibernéticos están contemplados por los ordenamientos punitivos de Veracruz y Federal respectivamente?	2	10
	¿Sabe usted cual es la policía cibernética?	3	9
	¿Ha usted hecho uso del apoyo de la policía cibernética para la resolución de alguna investigación ministerial?	0	12
	¿Sabe usted cual es la diferencia entre los delitos informáticos y los delitos cibernéticos?	3	9
	¿Considera usted que la autoridad Procuradora de Justicia, reconoce “de hecho” los delitos cibernéticos?	3	9
	¿Estaría usted de acuerdo en que la autoridad procuradora de justicia, reconoce los delitos cibernéticos “de hecho” más no “de derecho”?	8	4
	¿Considera que actualmente ante la falta de inclusión de los delitos cibernéticos en los códigos penales, la autoridad procuradora de justicia, le da tratamiento	10	2

PARTE CUANTITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA			
SUBPROCURADURÍA	**PREGUNTA**	**SI**	**NO**
	en sus indagatorias a los delitos cibernéticos como si fueran delitos de los ya previstos por los códigos?		
	¿Considera que los tipos penales que actualmente están vigentes, son insuficientes para la persecución de los delitos cibernéticos?	7	5
	¿Cree usted que los delitos cibernéticos merecen un tratamiento en la indagatoria diferente al que típicamente se da a los demás delitos contemplados por las leyes punitivas tanto del Estado como Federal?	6	6
	¿Tiene usted conocimiento sobre si a la fecha, existe en la Dirección General de Servicios Periciales correspondiente, un experto en informática forense?	3	9
	¿Considera que para la persecución de los delitos cibernéticos debe existir un experto en informática forense en la Dirección General de Servicios Periciales correspondiente?	11	1
	¿Considera usted que existe dificultad para validar el alcance y valor probatorio de los medios de prueba digitales en las investigaciones ministeriales de cualquier índole?	10	2
	¿Existe una diferencia entre los delitos informáticos y los delitos cibernéticos?	4	8

PARTE CUANTITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA			
SUBPROCURADURÍA	**PREGUNTA**	**SI**	**NO**
	¿Considera que con la descripción del tipo penal de delitos informáticos, es posible la persecución de los delitos cibernéticos?	8	4
	¿Sabe usted cual es la distinción entre el delincuente cibernético y el delincuente tradicional?	5	7
	¿Considera que el delincuente cibernético tiene un grado mayor de temibilidad que el delincuente tradicional?	2	10
	¿Considera que las investigaciones ministeriales relacionadas con el delincuente cibernético, necesitan un tratamiento diferente que las que involucran al delincuente tradicional?	6	6
	¿Considera que el tratamiento que le da la autoridad procuradora de justicia a los delitos cibernéticos en las indagatorias correspondientes, a través de las agencias de ministerio público, debería ser especializado?	10	2
	¿Considera que los delitos informáticos son un tipo penal que podría incluirse dentro de los delitos cibernéticos de estar estos últimos tipificados?	8	4
	¿Existen denuncias relativas a la comisión de delitos informáticos presentadas ante esta agencia?	1	11

PARTE CUANTITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA			
SUBPROCURADURÍA	**PREGUNTA**	**SI**	**NO**
	¿Considera que de tipificarse el tipo penal de delitos cibernéticos, deberían preservarse aún los delitos informáticos?	5	7
SUBPROCURADURÍA TANTOYÚCA 18 PERSONAS ENCUESTADAS, ADSCRITAS EN AGENCIA DEL MINISTERIO PÚBLICO	¿Conoce usted los Delitos Cibernéticos?	14	4
	¿Existen denuncias relativas a la comisión de delitos cibernéticos presentadas ante esta agencia entre los años 2006 y 2009?	6	12
	¿Los delitos cibernéticos están contemplados por los ordenamientos punitivos de Veracruz y Federal respectivamente?	10	8
	¿Sabe usted cual es la policía cibernética?	8	10
	¿Ha usted hecho uso del apoyo de la policía cibernética para la resolución de alguna investigación ministerial?	2	16
	¿Sabe usted cual es la diferencia entre los delitos informáticos y los delitos cibernéticos?	3	15
	¿Considera usted que la autoridad Procuradora de Justicia, reconoce “de hecho” los delitos cibernéticos?	10	8
	¿Estaría usted de acuerdo en que la autoridad procuradora de justicia, reconoce los delitos cibernéticos “de hecho” más no “de derecho”?	11	7
	¿Considera que actualmente ante la falta de inclusión de los delitos cibernéticos en los códigos penales, la autoridad	10	8

PARTE CUANTITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA			
SUBPROCURADURÍA	**PREGUNTA**	**SI**	**NO**
	procuradora de justicia, le da tratamiento en sus indagatorias a los delitos cibernéticos como si fueran delitos de los ya previstos por los códigos?		
	¿Considera que los tipos penales que actualmente están vigentes, son insuficientes para la persecución de los delitos cibernéticos?	13	5
	¿Cree usted que los delitos cibernéticos merecen un tratamiento en la indagatoria diferente al que típicamente se da a los demás delitos contemplados por las leyes punitivas tanto del Estado como Federal?	11	7
	¿Tiene usted conocimiento sobre si a la fecha, existe en la Dirección General de Servicios Periciales correspondiente, un experto en informática forense?	1	17
	¿Considera que para la persecución de los delitos cibernéticos debe existir un experto en informática forense en la Dirección General de Servicios Periciales correspondiente?	16	2
	¿Considera usted que existe dificultad para validar el alcance y valor probatorio de los medios de prueba digitales en las investigaciones ministeriales de cualquier índole?	16	2
	¿Existe una diferencia entre los delitos informáticos y los delitos cibernéticos?	11	7

PARTE CUANTITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA			
SUBPROCURADURÍA	**PREGUNTA**	**SI**	**NO**
	¿Considera que con la descripción del tipo penal de delitos informáticos, es posible la persecución de los delitos cibernéticos?	6	12
	¿Sabe usted cual es la distinción entre el delincuente cibernético y el delincuente tradicional?	7	11
	¿Considera que el delincuente cibernético tiene un grado mayor de temibilidad que el delincuente tradicional?	6	12
	¿Considera que las investigaciones ministeriales relacionadas con el delincuente cibernético, necesitan un tratamiento diferente que las que involucran al delincuente tradicional?	10	8
	¿Considera que el tratamiento que le da la autoridad procuradora de justicia a los delitos cibernéticos en las indagatorias correspondientes, a través de las agencias de ministerio público, debería ser especializado?	8	10
	¿Considera que los delitos informáticos son un tipo penal que podría incluirse dentro de los delitos cibernéticos de estar estos últimos tipificados?	5	13
	¿Existen denuncias relativas a la comisión de delitos informáticos presentadas ante esta agencia?	1	17

PARTE CUANTITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA			
SUBPROCURADURÍA	**PREGUNTA**	**SI**	**NO**
	¿Considera que de tipificarse el tipo penal de delitos cibernéticos, deberían preservarse aún los delitos informáticos?	5	13

TABLA 3

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
SUBPROCURADURÍA VERACRUZ 16 PERSONAS ENCUESTADAS, ADSCRITAS EN AGENCIA DEL MINISTERIO PÚBLICO	¿Cómo podría usted definir a los delitos cibernéticos?	Delitos relacionados con las tarjetas de crédito, internet y medios informáticos, medios electrónicos, uso de las computadoras, tecnología, de cuello blanco, hacker de cuentas
	¿Con qué frecuencia se presentan denuncias relativas a la comisión de delitos cibernéticos?	4%, ninguno, poca frecuencia, excepcionalmente
	¿Con qué frecuencia son consignados los presuntos responsables por la comisión de delitos	Poca frecuencia

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	cibernéticos?	
	¿Por qué la legislación punitiva del Estado de Veracruz y la Federal, no contemplan dentro de sus tipos penales a los delitos cibernéticos?	Si los contempla
	De los que saben la diferencia entre los delitos informáticos y los delitos cibernéticos, expresaron que:	Son lo mismo
	¿Cómo considera que debe ser el tratamiento en la indagatoria para la persecución de los delitos cibernéticos?	Especializado
	¿Quién es el encargado de validar el alcance	El perito encargado de servicios periciales experto en informática forense

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	y valor probatorio de los medios de prueba digitales en las investigaciones ministeriales?	
	¿Quién es el perito experto de la correspondiente Dirección General de Servicios Periciales que valida el alcance y valor probatorio de los medios digitales en tratándose de la comisión de los delitos cibernéticos?	El perito encargado en informática forense
	¿Quién es el perito experto de la correspondiente Dirección General de Servicios Periciales que valida los daños a	El que designa servicios periciales, el de informática forense.

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	los medios digitales, electrónicos y de nuevas tecnologías, en tratándose de la comisión de los delitos cibernéticos?	
	¿Cuándo usted dirige un oficio a la Dirección General de Servicios Periciales, para efectos de solicitar el apoyo de un perito experto en tratándose de una indagatoria relativa a la comisión de delitos cibernéticos, ¿De qué perito específicamente requiere el apoyo?	Informática forense

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	¿Cuál considera que es la diferencia entre los delitos informáticos y los delitos cibernéticos?	Ninguna
	¿Qué es para usted el delincuente cibernético?	El que utiliza los medios electrónicos para delinquir
	¿Por qué, muy a pesar de que el Estado reconoce los delitos cibernéticos “de hecho”, no los incluye dentro de la legislación penal correspondiente, para entonces reconocerlos también “de derecho”?	Porque los legisladores no tienen conocimientos claros sobre la distinción
	¿Por qué el estado ha creado una policía cibernética para	Si los reconoce de manera informal

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	coadyuvar con la persecución de los delitos de esta índole, pero no se reconocen en los ordenamientos punitivos Estatales y Federal respectivamente?	
	¿Cuál es el tratamiento que la autoridad procuradora de justicia le da a los delitos cibernéticos en las indagatorias correspondientes, a través de las agencias de ministerio público?	El tratamiento tradicional
	¿Con qué frecuencia se presentan denuncias relativas a la comisión de	Poca frecuencia

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	delitos informáticos?	
	¿Con que frecuencia son consignados los presuntos responsables por la comisión de delitos informáticos?	Poca frecuencia
SUBPROCURADURÍA COATZACOALCOS 10 PERSONAS ENCUESTADAS, ADSCRITAS EN AGENCIA DEL MINISTERIO PÚBLICO	¿Cómo podría usted definir a los delitos cibernéticos?	Robo de datos y uso de internet
	¿Con qué frecuencia se presentan denuncias relativas a la comisión de delitos cibernéticos?	Se desconoce y ninguna
	¿Con qué frecuencia son consignados los presuntos responsables por la comisión de delitos	Se desconoce y ninguna

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	cibernéticos?	
	¿Por qué la legislación punitiva del Estado de Veracruz y la Federal, no contemplan dentro de sus tipos penales a los delitos cibernéticos?	Se desconoce
	De los que saben la diferencia entre los delitos informáticos y los delitos cibernéticos, expresaron que:	No expresaron nada
	¿Cómo considera que debe ser el tratamiento en la indagatoria para la persecución de los delitos cibernéticos?	Se desconoce
	¿Quién es el encargado de validar el alcance	Perito experto y se desconoce

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	y valor probatorio de los medios de prueba digitales en las investigaciones ministeriales?	
	¿Quién es el perito experto de la correspondiente Dirección General de Servicios Periciales que valida el alcance y valor probatorio de los medios digitales en tratándose de la comisión de los delitos cibernéticos?	Perito experto y se desconoce
	¿Quién es el perito experto de la correspondiente Dirección General de Servicios Periciales que valida los daños a	Perito experto y se desconoce

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	los medios digitales, electrónicos y de nuevas tecnologías, en tratándose de la comisión de los delitos cibernéticos?	
	¿Cuándo usted dirige un oficio a la Dirección General de Servicios Periciales, para efectos de solicitar el apoyo de un perito experto en tratándose de una indagatoria relativa a la comisión de delitos cibernéticos, ¿De qué perito específicamente	El perito en turno encargado

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	requiere el apoyo?	
	¿Cuál considera que es la diferencia entre los delitos informáticos y los delitos cibernéticos?	Informáticos, información, cibernéticos, internet
	¿Qué es para usted el delincuente cibernético?	Se desconoce y los que hacen mal uso de la internet
	¿Por qué, muy a pesar de que el Estado reconoce los delitos cibernéticos “de hecho”, no los incluye dentro de la legislación penal correspondiente, para entonces reconocerlos también “de derecho”?	Se desconoce
	¿Por qué el estado ha creado	Se desconoce

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	una policía cibernética para coadyuvar con la persecución de los delitos de esta índole, pero no se reconocen en los ordenamientos punitivos Estatales y Federal respectivamente?	
	¿Cuál es el tratamiento que la autoridad procuradora de justicia le da a los delitos cibernéticos en las indagatorias correspondientes, a través de las agencias de ministerio público?	Se desconoce
	¿Con qué frecuencia se presentan denuncias	Ninguna

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	relativas a la comisión de delitos informáticos?	
	¿Con que frecuencia son consignados los presuntos responsables por la comisión de delitos informáticos?	Ninguna
SUBPROCURADURÍA CÓRDOBA 12 PERSONAS ENCUESTADAS, ADSCRITAS EN AGENCIA DEL MINISTERIO PÚBLICO	¿Cómo podría usted definir a los delitos cibernéticos?	Tecnología, ciberespacio, medios electrónicos
	¿Con qué frecuencia se presentan denuncias relativas a la comisión de delitos cibernéticos?	Ninguna
	¿Con qué frecuencia son consignados los presuntos responsables por	Ninguna

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	la comisión de delitos cibernéticos?	
	¿Por qué la legislación punitiva del Estado de Veracruz y la Federal, no contemplan dentro de sus tipos penales a los delitos cibernéticos?	Poca frecuencia y falta de conocimiento
	De los que saben la diferencia entre los delitos informáticos y los delitos cibernéticos, expresaron que:	Los informáticos atienden al uso de información y los cibernéticos a las tecnologías
	¿Cómo considera que debe ser el tratamiento en la indagatoria para la persecución de los delitos cibernéticos?	Debe ser especializado

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	¿Quién es el encargado de validar el alcance y valor probatorio de los medios de prueba digitales en las investigaciones ministeriales?	El perito experto
	¿Quién es el perito experto de la correspondiente Dirección General de Servicios Periciales que valida el alcance y valor probatorio de los medios digitales en tratándose de la comisión de los delitos cibernéticos?	Perito en informática forense
	¿Quién es el perito experto de la correspondiente Dirección General	Perito experto en Informática forense

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	de Servicios Periciales que valida los daños a los medios digitales, electrónicos y de nuevas tecnologías, en tratándose de la comisión de los delitos cibernéticos?	
	¿Cuándo usted dirige un oficio a la Dirección General de Servicios Periciales, para efectos de solicitar el apoyo de un perito experto en tratándose de una indagatoria relativa a la comisión de delitos cibernéticos, ¿De qué perito	El perito experto en informática forense

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	específicamente requiere el apoyo?	
	¿Cuál considera que es la diferencia entre los delitos informáticos y los delitos cibernéticos?	Los informáticos es a información y los cibernéticos a internet
	¿Qué es para usted el delincuente cibernético?	Quien roba información de otros, no saben
	¿Por qué, muy a pesar de que el Estado reconoce los delitos cibernéticos “de hecho”, no los incluye dentro de la legislación penal correspondiente, para entonces reconocerlos	Se desconoce la razón

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	también “de derecho”?	
	¿Por qué el estado ha creado una policía cibernética para coadyuvar con la persecución de los delitos de esta índole, pero no se reconocen en los ordenamientos punitivos Estatales y Federal respectivamente?	Se desconoce
	¿Cuál es el tratamiento que la autoridad procuradora de justicia le da a los delitos cibernéticos en las indagatorias correspondientes, a través de las agencias de ministerio público?	Se desconoce

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	¿Con qué frecuencia se presentan denuncias relativas a la comisión de delitos informáticos?	Poca frecuencia
	¿Con que frecuencia son consignados los presuntos responsables por la comisión de delitos informáticos?	Poca frecuencia
SUBPROCURADURÍA TANTOYUCA 18 PERSONAS ENCUESTADAS, ADSCRITAS EN AGENCIA DEL MINISTERIO PÚBLICO	¿Cómo podría usted definir a los delitos cibernéticos?	Plagio de información, hackers, fraudes, tecnología
	¿Con qué frecuencia se presentan denuncias relativas a la comisión de delitos cibernéticos?	No hay
	¿Con qué	No hay

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	frecuencia son consignados los presuntos responsables por la comisión de delitos cibernéticos?	
	¿Por qué la legislación punitiva del Estado de Veracruz y la Federal, no contemplan dentro de sus tipos penales a los delitos cibernéticos?	Faltan iniciativas, los legisladores desconocen
	De los que saben la diferencia entre los delitos informáticos y los delitos cibernéticos, expresaron que:	La naturaleza del delito
	¿Cómo considera que debe ser el tratamiento en la indagatoria para	Especializado y capacitar al personal

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	la persecución de los delitos cibernéticos?	
	¿Quién es el encargado de validar el alcance y valor probatorio de los medios de prueba digitales en las investigaciones ministeriales?	Perito experto
	¿Quién es el perito experto de la correspondiente Dirección General de Servicios Periciales que valida el alcance y valor probatorio de los medios digitales en tratándose de la comisión de los delitos cibernéticos?	Informática forense
	¿Quién es el	El especializado en informática

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	perito experto de la correspondiente Dirección General de Servicios Periciales que valida los daños a los medios digitales, electrónicos y de nuevas tecnologías, en tratándose de la comisión de los delitos cibernéticos?	forense
	¿Cuándo usted dirige un oficio a la Dirección General de Servicios Periciales, para efectos de solicitar el apoyo de un perito experto en tratándose de una indagatoria relativa a la	Informática forense

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	comisión de delitos cibernéticos, ¿De qué perito específicamente requiere el apoyo?	
	¿Cuál considera que es la diferencia entre los delitos informáticos y los delitos cibernéticos?	No se sabe, es poca la diferencia
	¿Qué es para usted el delincuente cibernético?	Delitos cometidos mediante las computadoras y la internet
	¿Por qué, muy a pesar de que el Estado reconoce los delitos cibernéticos “de hecho”, no los incluye dentro de la legislación penal correspondiente, para entonces	Desconocimiento, son delitos nuevos

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	reconocerlos también “de derecho”?	
	¿Por qué el estado ha creado una policía cibernética para coadyuvar con la persecución de los delitos de esta índole, pero no se reconocen en los ordenamientos punitivos Estatales y Federal respectivamente?	Por ser un delito derivado de las computadoras
	¿Cuál es el tratamiento que la autoridad procuradora de justicia le da a los delitos cibernéticos en las indagatorias correspondientes,	Se desconoce

PARTE CUALITATIVA DEL INSTRUMENTO POR SUBPROCURADURÍA		
SUBPROCURADURÍA	**PREGUNTA**	**Respuesta**
	a través de las agencias de ministerio público?	
	¿Con qué frecuencia se presentan denuncias relativas a la comisión de delitos informáticos?	No hay
	¿Con que frecuencia son consignados los presuntos responsables por la comisión de delitos informáticos?	No hay

Del anterior vaciado, cabe señalar, que se expusieron las respuestas de mayor frecuencia en la contestación, pues evidentemente no todos contestaron lo mismo, pero si de forma similar, por lo que se unificó el contenido de las respuestas de la misma naturaleza y se presentó la de mayor frecuencia, pero es destacable también manifestar, que no se dejó fuera ningún tipo de respuesta, pues en todos los casos, eran similares o prácticamente las misma.

ANÁLISIS GENERAL DE LOS DATOS OBTENIDOS EN LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS MIXTOS

TABLA 4

PROCURACIÓN DE JUSTICIA EN VERACRUZ EN TRATÁNDOSE DE DELITOS CIBERNÉTICOS; PARTE CUANTITATIVA DEL INSTRUMENTO (56 PERSONAS ENCUESTADAS ADSCRITAS A LAS AGENCIAS)		
PREGUNTA	**SI**	**NO**
¿Conoce usted los Delitos Cibernéticos?	36	20
¿Existen denuncias relativas a la comisión de delitos cibernéticos presentadas ante esta agencia entre los años 2006 y 2009?	13	43
¿Los delitos cibernéticos están contemplados por los ordenamientos punitivos de Veracruz y Federal respectivamente?	29	27
¿Sabe usted cual es la policía cibernética?	19	37
¿Ha usted hecho uso del apoyo de la policía cibernética para la resolución de alguna investigación ministerial?	6	50
¿Sabe usted cual es la diferencia entre los delitos informáticos y los delitos cibernéticos?	15	41
¿Considera usted que la autoridad Procuradora de Justicia, reconoce “de hecho” los delitos cibernéticos?	31	25
¿Estaría usted de acuerdo en que la autoridad procuradora de justicia, reconoce los delitos cibernéticos “de hecho” más no “de derecho”?	30	26
¿Considera que actualmente ante la falta de inclusión de los delitos cibernéticos en los códigos penales, la autoridad procuradora de justicia, le da tratamiento en sus indagatorias a los delitos cibernéticos como si fueran delitos de los ya previstos por los códigos?	31	25

PROCURACIÓN DE JUSTICIA EN VERACRUZ EN TRATÁNDOSE DE DELITOS CIBERNÉTICOS; PARTE CUANTITATIVA DEL INSTRUMENTO (56 PERSONAS ENCUESTADAS ADSCRITAS A LAS AGENCIAS)		
PREGUNTA	**SI**	**NO**
¿Considera que los tipos penales que actualmente están vigentes, son insuficientes para la persecución de los delitos cibernéticos?	40	16
¿Cree usted que los delitos cibernéticos merecen un tratamiento en la indagatoria diferente al que típicamente se da a los demás delitos contemplados por las leyes punitivas tanto del Estado como Federal?	31	25
¿Tiene usted conocimiento sobre si a la fecha, existe en la Dirección General de Servicios Periciales correspondiente, un experto en informática forense?	9	47
¿Considera que para la persecución de los delitos cibernéticos debe existir un experto en informática forense en la Dirección General de Servicios Periciales correspondiente?	50	6
¿Considera usted que existe dificultad para validar el alcance y valor probatorio de los medios de prueba digitales en las investigaciones ministeriales de cualquier índole?	44	12
¿Existe una diferencia entre los delitos informáticos y los delitos cibernéticos?	25	31
¿Considera que con la descripción del tipo penal de delitos informáticos, es posible la persecución de los delitos cibernéticos?	26	30
¿Sabe usted cual es la distinción entre el delincuente cibernético y el delincuente tradicional?	30	26
¿Considera que el delincuente cibernético tiene un grado mayor de temibilidad que el delincuente tradicional?	22	34

PROCURACIÓN DE JUSTICIA EN VERACRUZ EN TRATÁNDOSE DE DELITOS CIBERNÉTICOS; PARTE CUANTITATIVA DEL INSTRUMENTO (56 PERSONAS ENCUESTADAS ADSCRITAS A LAS AGENCIAS)		
PREGUNTA	**SI**	**NO**
¿Considera que las investigaciones ministeriales relacionadas con el delincuente cibernético, necesitan un tratamiento diferente que las que involucran al delincuente tradicional?	34	22
¿Considera que el tratamiento que le da la autoridad procuradora de justicia a los delitos cibernéticos en las indagatorias correspondientes, a través de las agencias de ministerio público, debería ser especializado?	39	17
¿Considera que los delitos informáticos son un tipo penal que podría incluirse dentro de los delitos cibernéticos de estar estos últimos tipificados?	31	25
¿Existen denuncias relativas a la comisión de delitos informáticos presentadas ante esta agencia?	9	47
¿Considera que de tipificarse el tipo penal de delitos cibernéticos, deberían preservarse aún los delitos informáticos?	32	24

TABLA 5

PROCURACIÓN DE JUSTICIA EN VERACRUZ EN TRATÁNDOSE DE DELITOS CIBERNÉTICOS; PARTE CUALITATIVA DEL INSTRUMENTO (56 PERSONAS ENCUESTADAS ADSCRITAS A LAS AGENCIAS)	
PREGUNTA	**Respuesta**
¿Cómo podría usted definir a los delitos cibernéticos?	Delitos relacionados con las tarjetas de crédito, internet y medios informáticos, medios electrónicos, uso de las computadoras, tecnología, de cuello blanco, hacker de cuentas, Robo de datos y uso de internet, aquellos que

PROCURACIÓN DE JUSTICIA EN VERACRUZ EN TRATÁNDOSE DE DELITOS CIBERNÉTICOS; PARTE CUALITATIVA DEL INSTRUMENTO (56 PERSONAS ENCUESTADAS ADSCRITAS A LAS AGENCIAS)	
PREGUNTA	**Respuesta**
	involucran la tecnología, ciberespacio, medios electrónicos, y los relativos al plagio de información, hackers, fraudes, tecnología
¿Con qué frecuencia se presentan denuncias relativas a la comisión de delitos cibernéticos?	4%, ninguno, poca frecuencia, excepcionalmente, se desconoce, ninguna, No hay
¿Con qué frecuencia son consignados los presuntos responsables por la comisión de delitos cibernéticos?	Poca frecuencia , se desconoce, ninguna, no hay
¿Por qué la legislación punitiva del Estado de Veracruz y la Federal, no contemplan dentro de sus tipos penales a los	Si los contempla, Se desconoce, Poca frecuencia y falta de conocimiento, Faltan iniciativas, los legisladores desconocen

PROCURACIÓN DE JUSTICIA EN VERACRUZ EN TRATÁNDOSE DE DELITOS CIBERNÉTICOS; PARTE CUALITATIVA DEL INSTRUMENTO (56 PERSONAS ENCUESTADAS ADSCRITAS A LAS AGENCIAS)	
PREGUNTA	**Respuesta**
delitos cibernéticos?	
De los que saben la diferencia entre los delitos informáticos y los delitos cibernéticos, expresaron que:	Son lo mismo, No expresaron nada, Los informáticos atienden al uso de información y los cibernéticos a las tecnologías La naturaleza del delito
¿Cómo considera que debe ser el tratamiento en la indagatoria para la persecución de los delitos cibernéticos?	Especializado, Se desconoce, Debe ser especializado, Especializado y capacitar al personal
¿Quién es el encargado de validar el alcance y valor probatorio de los medios de	El perito encargado de servicios periciales experto en informática forense, Perito experto y se desconoce, El perito experto, Perito experto

PROCURACIÓN DE JUSTICIA EN VERACRUZ EN TRATÁNDOSE DE DELITOS CIBERNÉTICOS; PARTE CUALITATIVA DEL INSTRUMENTO (56 PERSONAS ENCUESTADAS ADSCRITAS A LAS AGENCIAS)	
PREGUNTA	**Respuesta**
prueba digitales en las investigaciones ministeriales?	
¿Quién es el perito experto de la correspondiente Dirección General de Servicios Periciales que valida el alcance y valor probatorio de los medios digitales en tratándose de la comisión de los delitos cibernéticos?	El perito encargado en informática forense, Perito experto y se desconoce, Perito en informática forense, Informática forense
¿Quién es el perito experto de la correspondiente Dirección General de Servicios Periciales que valida los daños a los medios digitales,	El que designa servicios periciales, el de informática forense, Perito experto, Se desconoce, Perito experto en Informática forense, El especializado en informática forense

PROCURACIÓN DE JUSTICIA EN VERACRUZ EN TRATÁNDOSE DE DELITOS CIBERNÉTICOS; PARTE CUALITATIVA DEL INSTRUMENTO (56 PERSONAS ENCUESTADAS ADSCRITAS A LAS AGENCIAS)	
PREGUNTA	**Respuesta**
electrónicos y de nuevas tecnologías, en tratándose de la comisión de los delitos cibernéticos?	
¿Cuándo usted dirige un oficio a la Dirección General de Servicios Periciales, para efectos de solicitar el apoyo de un perito experto en tratándose de una indagatoria relativa a la comisión de delitos cibernéticos, ¿De qué perito específicamente requiere el apoyo?	Informática forense, El perito en turno encargado, El perito experto en informática forense, Informática forense

PROCURACIÓN DE JUSTICIA EN VERACRUZ EN TRATÁNDOSE DE DELITOS CIBERNÉTICOS; PARTE CUALITATIVA DEL INSTRUMENTO (56 PERSONAS ENCUESTADAS ADSCRITAS A LAS AGENCIAS)	
PREGUNTA	**Respuesta**
¿Cuál considera que es la diferencia entre los delitos informáticos y los delitos cibernéticos?	Ninguna, Informáticos, información, cibernéticos, internet, Los informáticos es a información y los cibernéticos a internet, No se sabe, es poca la diferencia
¿Qué es para usted el delincuente cibernético?	El que utiliza los medios electrónicos para delinquir, Se desconoce, los que hacen mal uso de la internet, Quien roba información de otros, No saben, Delitos cometidos mediante las computadoras y la internet
¿Por qué, muy a pesar de que el Estado reconoce los delitos cibernéticos "de hecho", no los incluye dentro de la legislación penal correspondiente, para entonces reconocerlos también "de derecho"?	Porque los legisladores no tienen conocimientos claros sobre la distinción, Se desconoce, Se desconoce la razón, Desconocimiento, son delitos nuevos
¿Por qué el estado ha creado una	Si los reconoce de manera informal, Se desconoce, Se desconoce, Por ser un delito derivado de las

PROCURACIÓN DE JUSTICIA EN VERACRUZ EN TRATÁNDOSE DE DELITOS CIBERNÉTICOS; PARTE CUALITATIVA DEL INSTRUMENTO (56 PERSONAS ENCUESTADAS ADSCRITAS A LAS AGENCIAS)	
PREGUNTA	**Respuesta**
policía cibernética para coadyuvar con la persecución de los delitos de esta índole, pero no se reconocen en los ordenamientos punitivos Estatales y Federal respectivamente?	computadoras
¿Cuál es el tratamiento que la autoridad procuradora de justicia le da a los delitos cibernéticos en las indagatorias correspondientes, a través de las agencias de ministerio público?	El tratamiento tradicional, Se desconoce, Se desconoce, Se desconoce

PROCURACIÓN DE JUSTICIA EN VERACRUZ EN TRATÁNDOSE DE DELITOS CIBERNÉTICOS; PARTE CUALITATIVA DEL INSTRUMENTO (56 PERSONAS ENCUESTADAS ADSCRITAS A LAS AGENCIAS)	
PREGUNTA	**Respuesta**
¿Con qué frecuencia se presentan denuncias relativas a la comisión de delitos informáticos?	Poca frecuencia, Ninguna , Poca frecuencia, No hay
¿Con que frecuencia son consignados los presuntos responsables por la comisión de delitos informáticos?	Poca frecuencia, Ninguna, Poca frecuencia, No hay

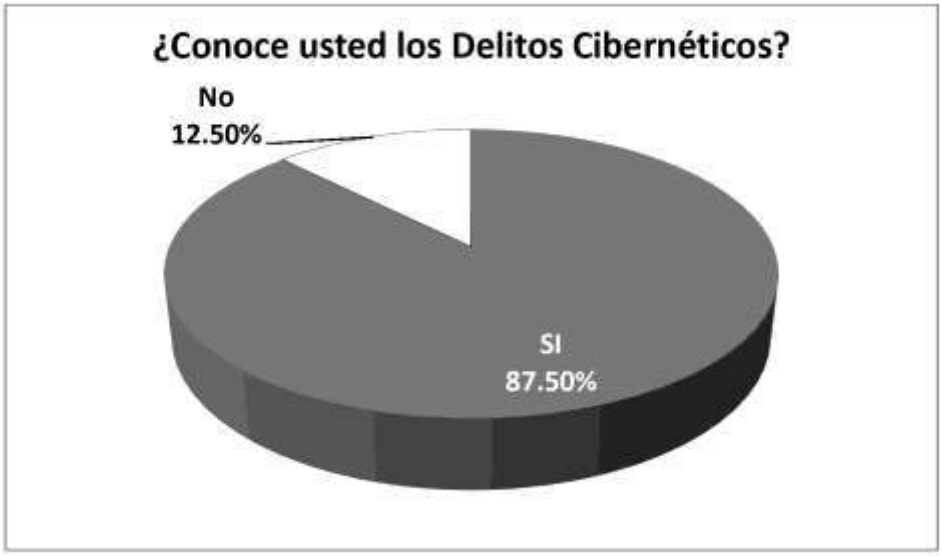
En la tabla anterior, se utilizó el mismo razonamiento que en la cualitativa anterior, es decir, se unificaron los criterios vertidos en las respuestas a fin de establecer una respuesta global, pero en el caso que ocupa esta investigación, las respuestas en general fueron muy similares y en el mismo sentido, lo que facilitó la unificación.

4.3. Sistematización gráfica de los resultados obtenidos

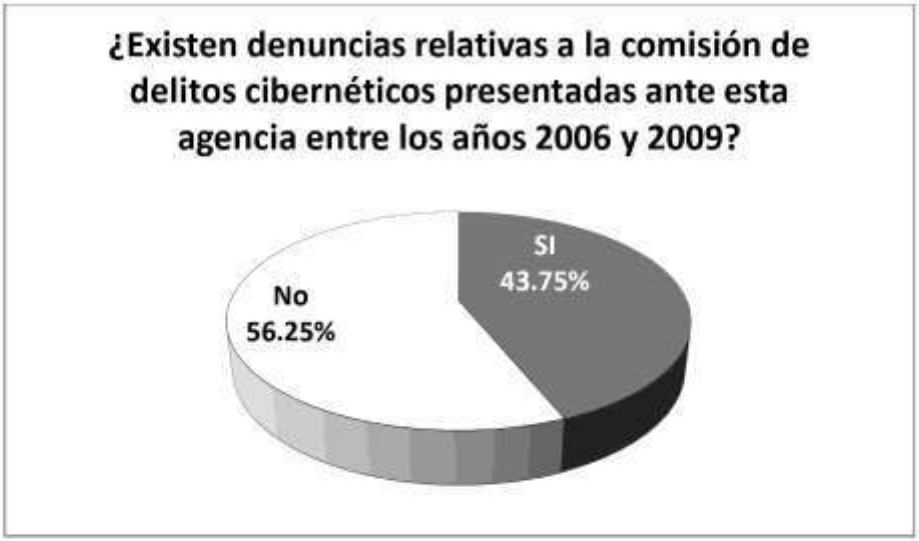
En el presente apartado, se presentan los resultados obtenidos, graficados para efectos de tener un mejor entendimiento sobre la demostración de la problemática y la acreditación de la hipótesis, todo esto encausado a la presentación de una propuesta de solución viable.

En relación a las encuestas realizadas a las agencias y dependencias procuradoras de justicia dependientes de la Subprocuraduría Regional Zona Centro Veracruz, se obtuvieron los siguientes resultados:

Gráfica 1

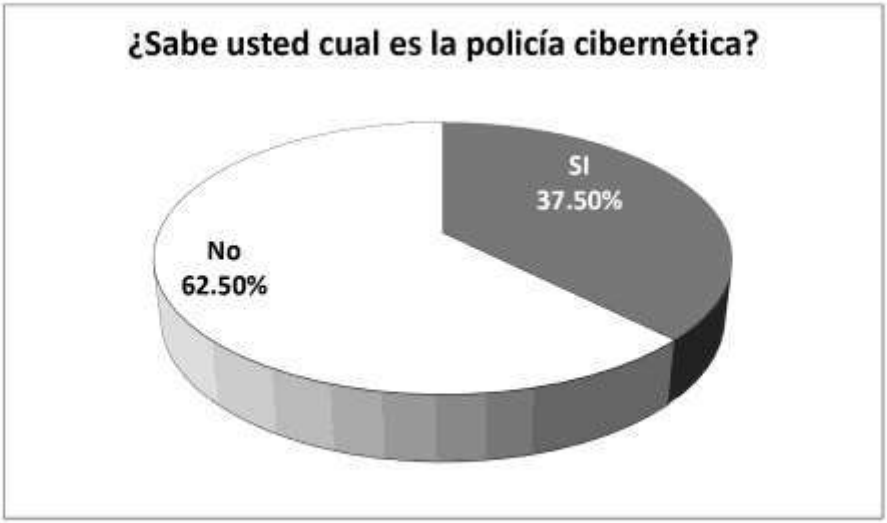


Gráfica 2

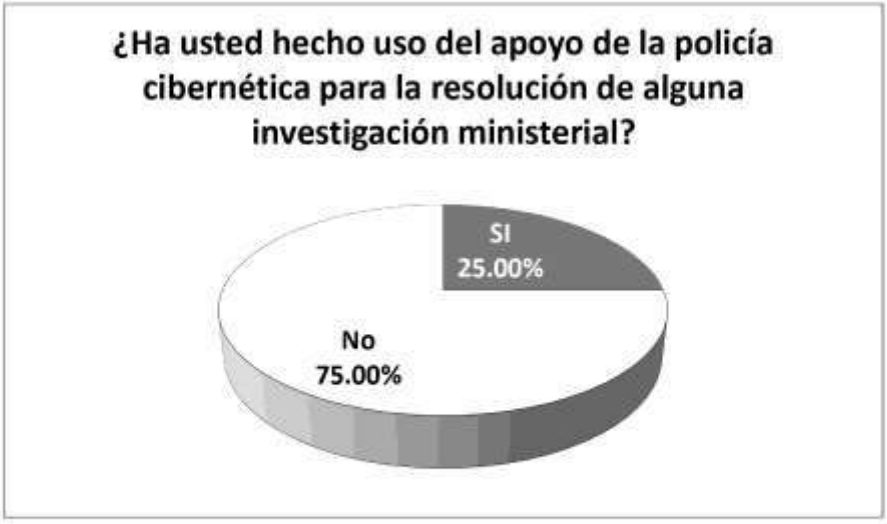


Gráfica 3

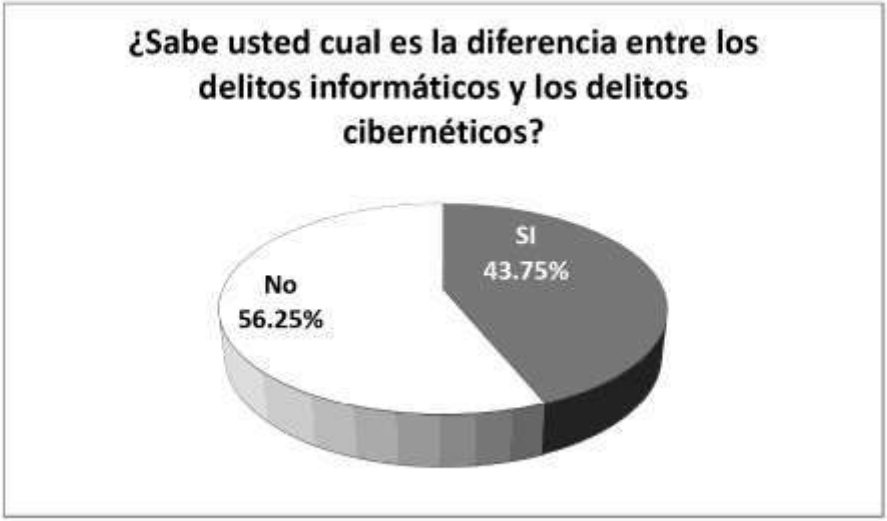
Gráfica 4



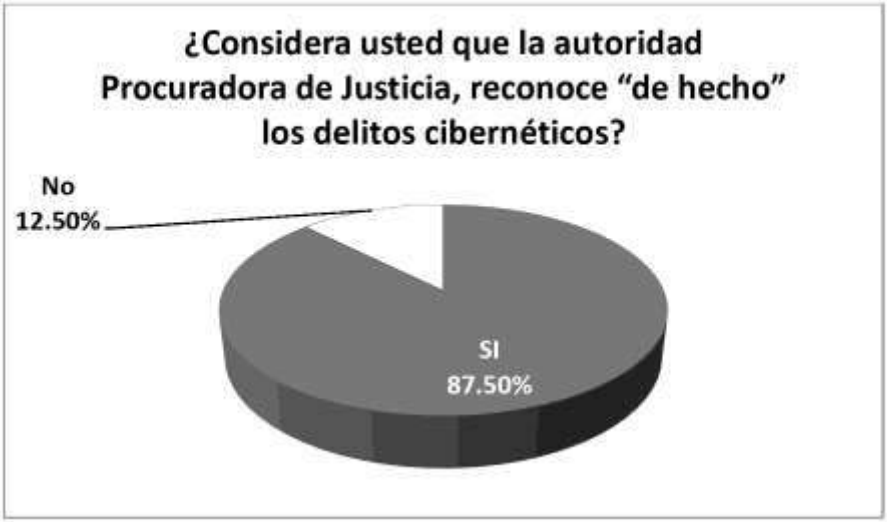
Gráfica 5



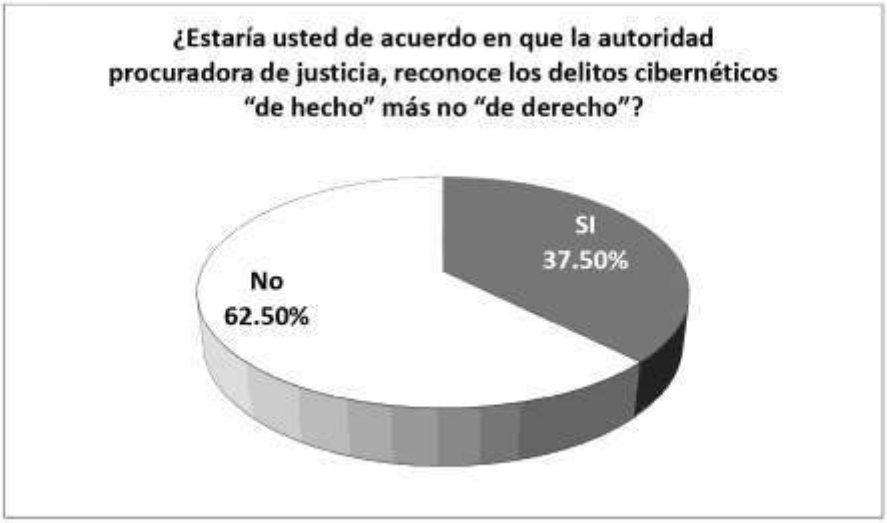
Gráfica 6



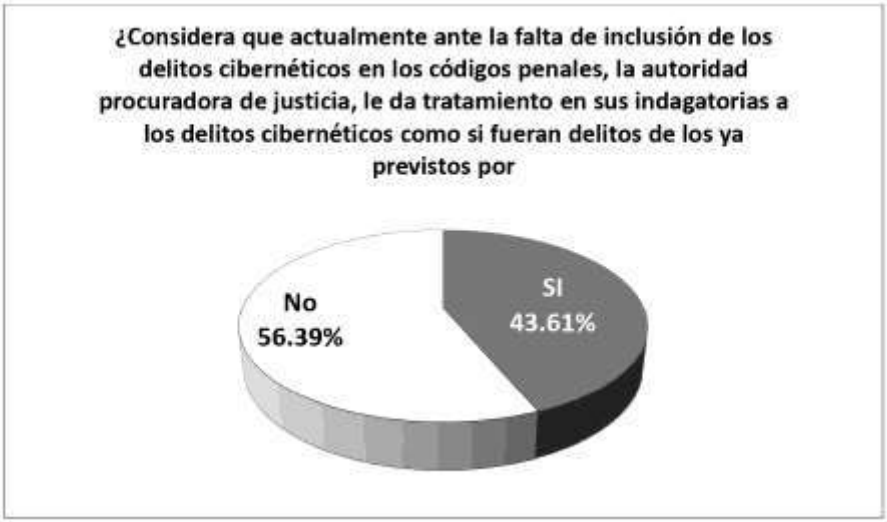
Gráfica 7



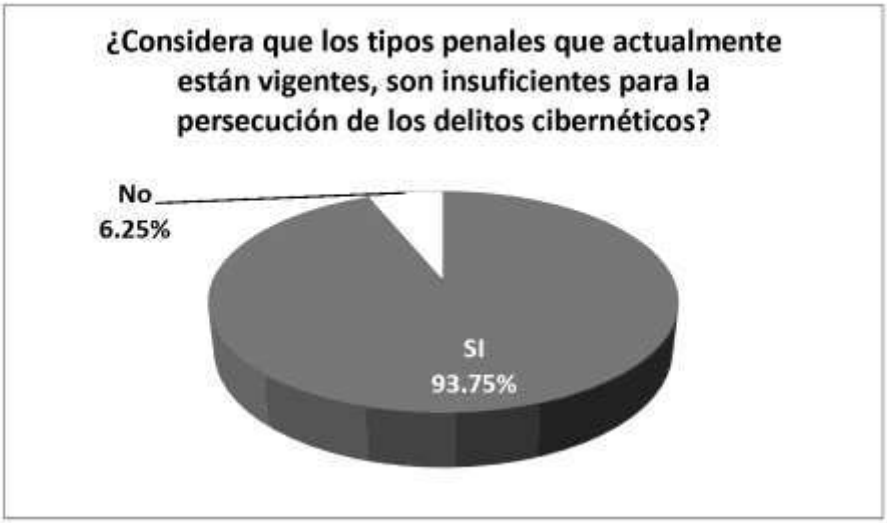
Gráfica 8



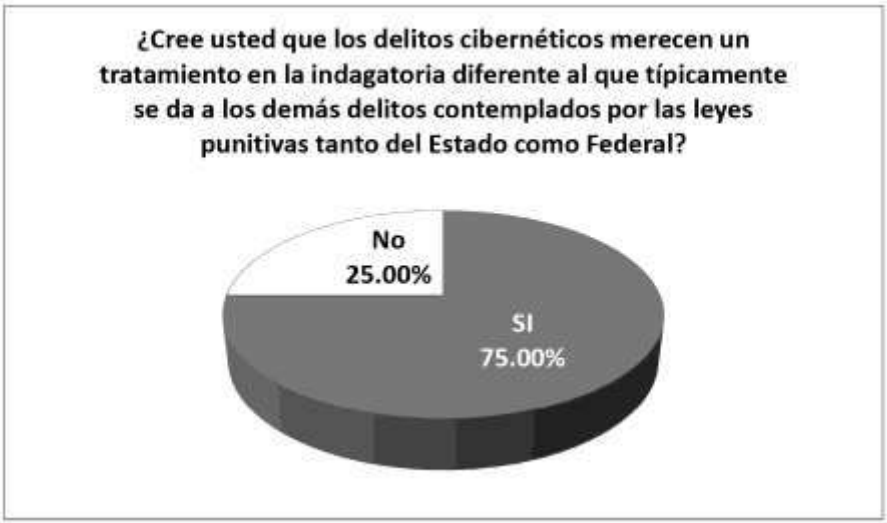
Gráfica 9



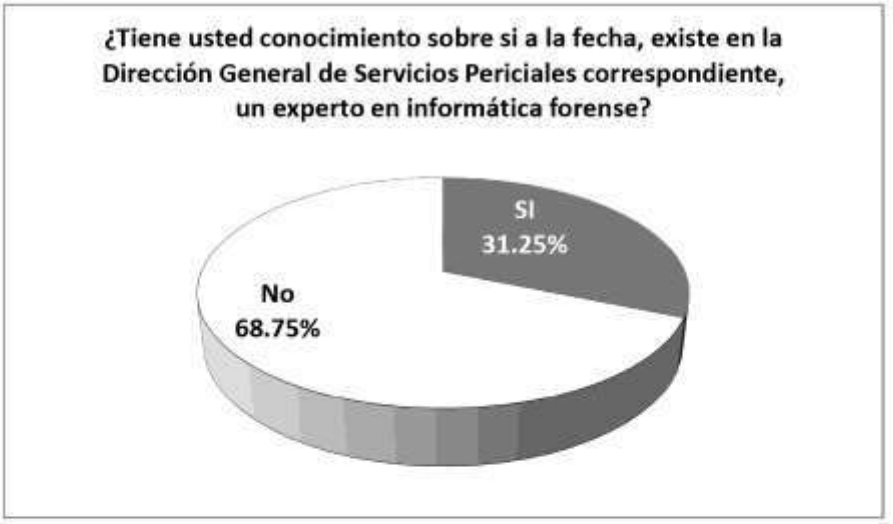
Gráfica 10



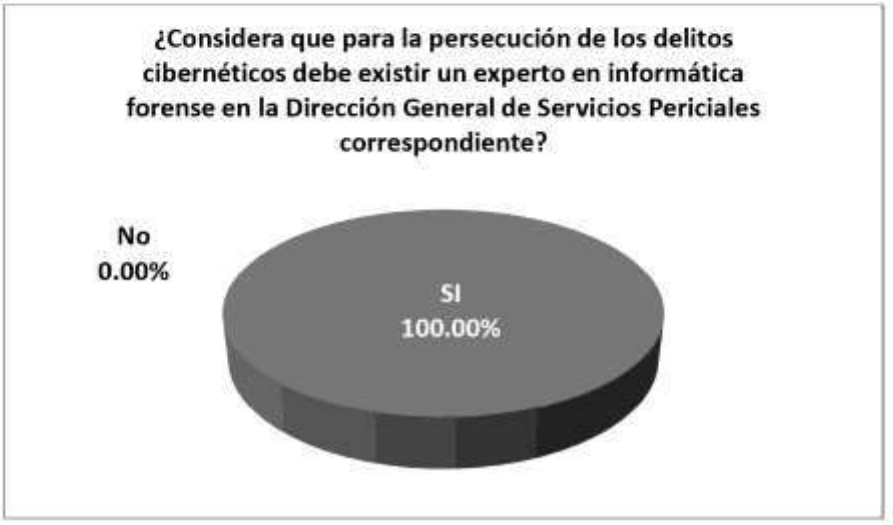
Gráfica 11



Gráfica 12

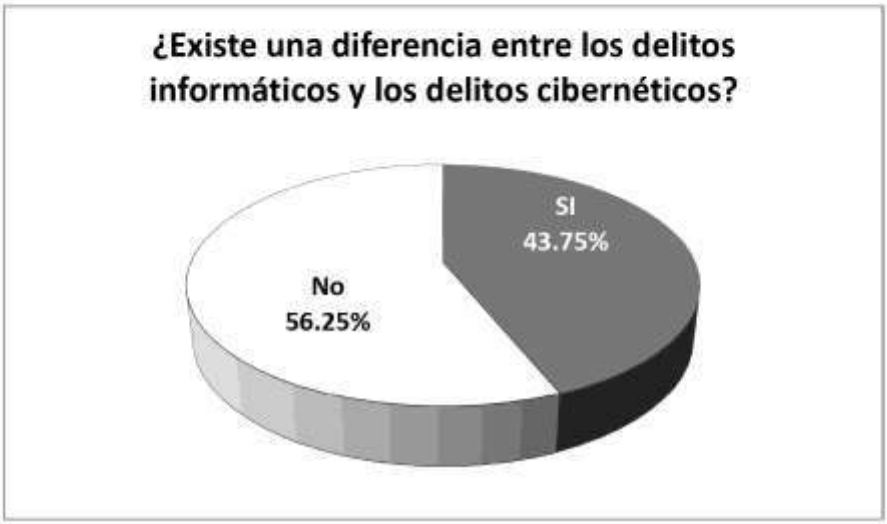


Gráfica 13



Gráfica 14

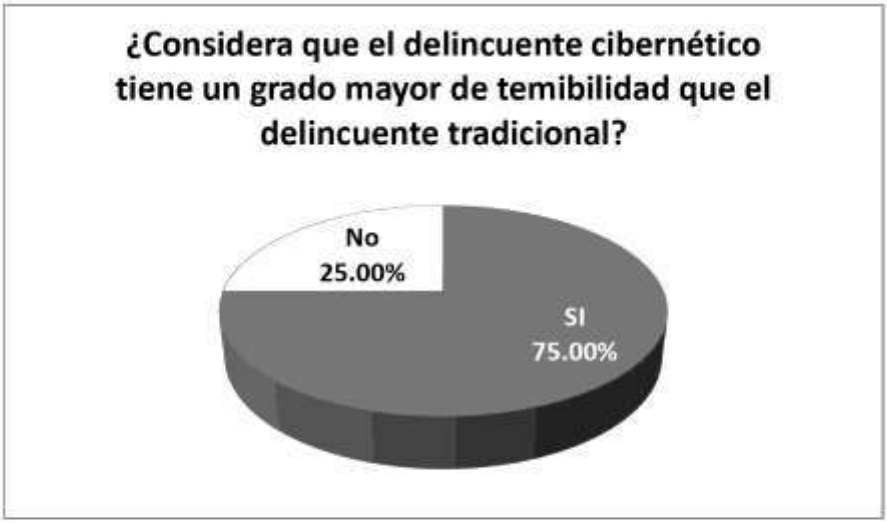
Gráfica 15



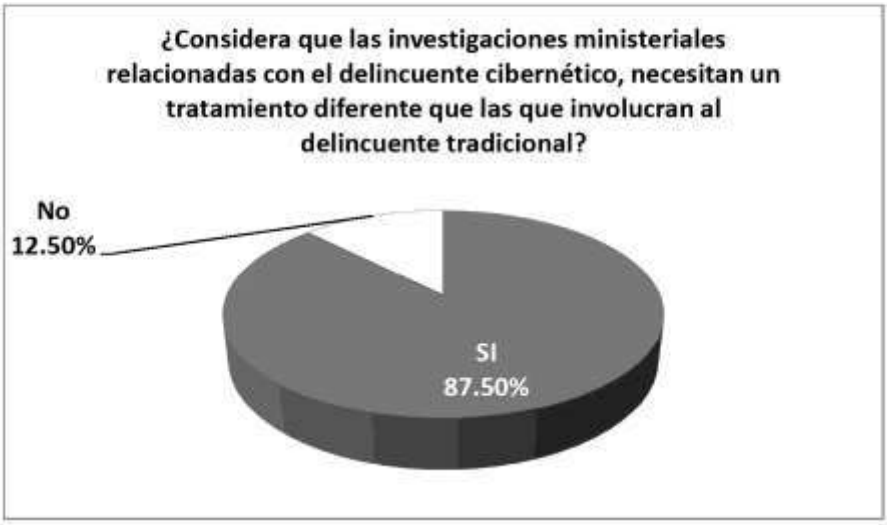
Gráfica 16

Gráfica 17

Gráfica 18

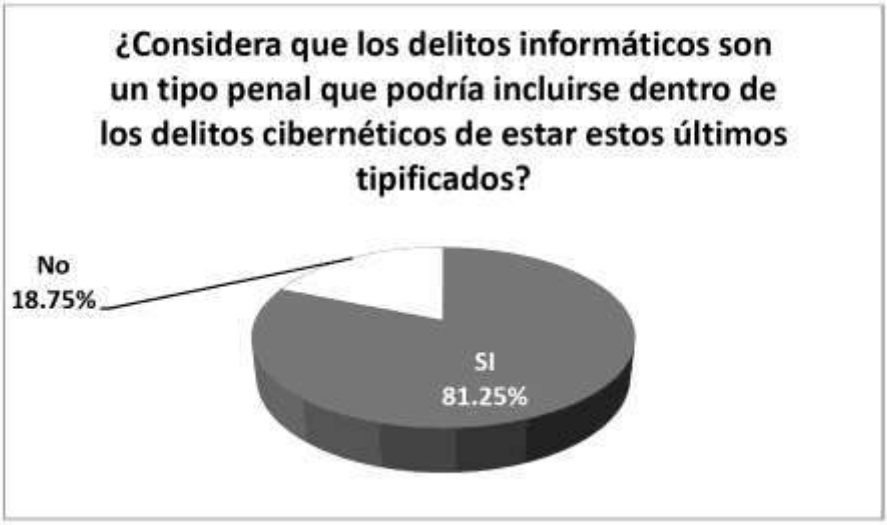


Gráfica 19

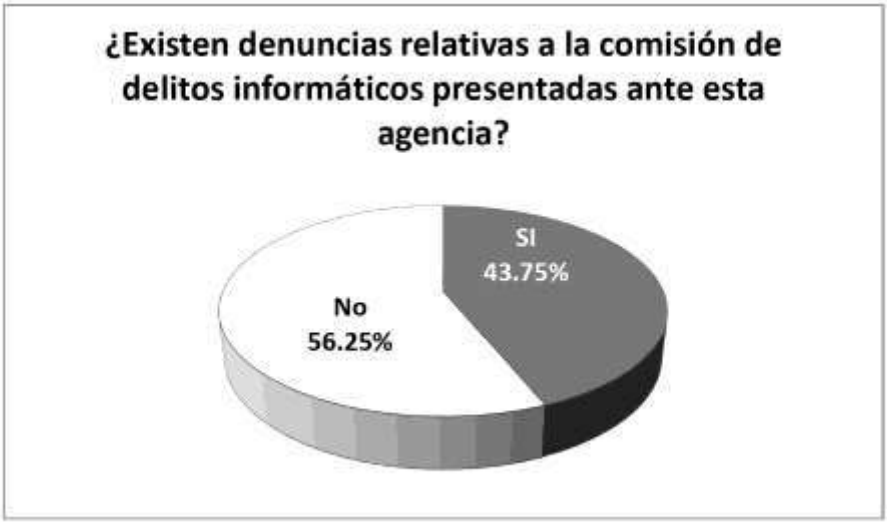


Gráfica 20

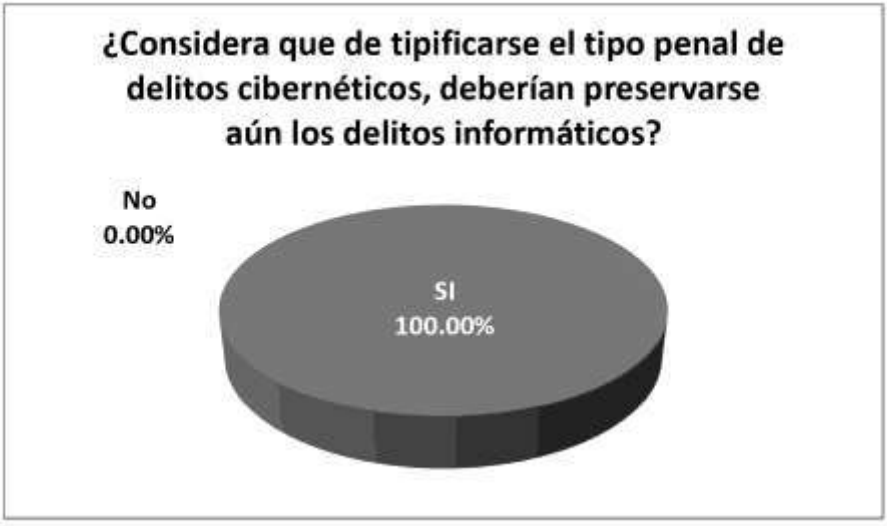
Gráfica 21



Gráfica 22

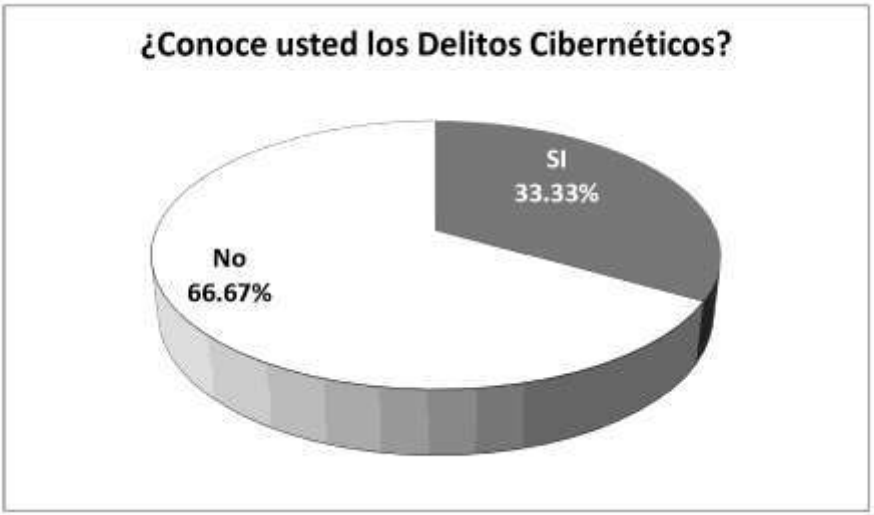


Gráfica 23

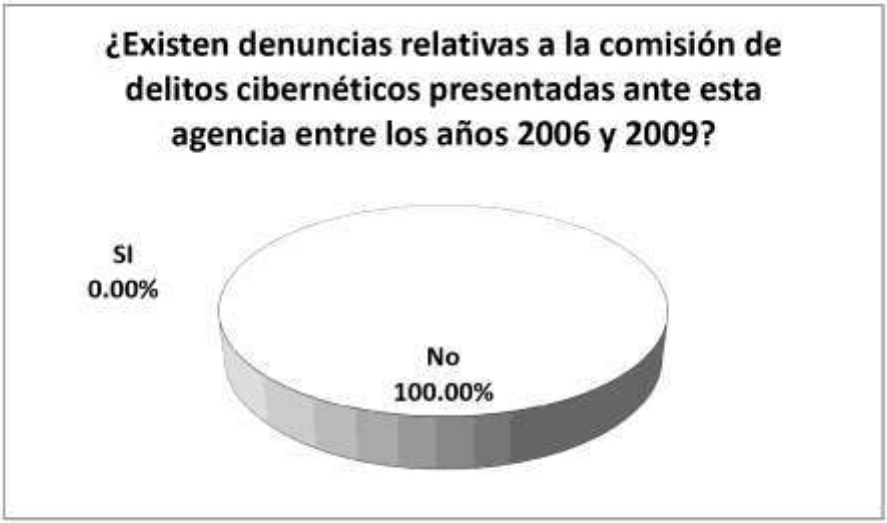


En relación a las encuestas realizadas a las agencias y dependencias procuradoras de justicia dependientes de la SUBPROCURADURÍA REGIONAL ZONA CENTRO CÓRDOBA, se obtuvieron los siguientes resultados:

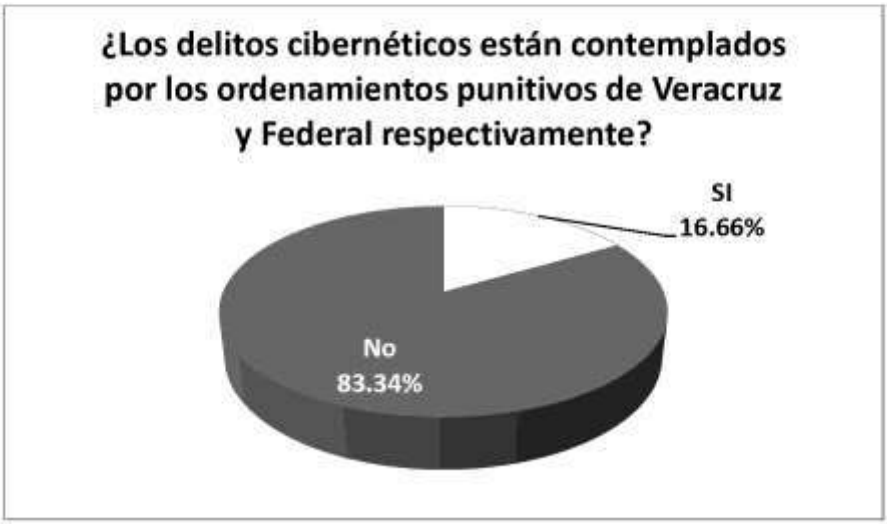
Gráfica 24



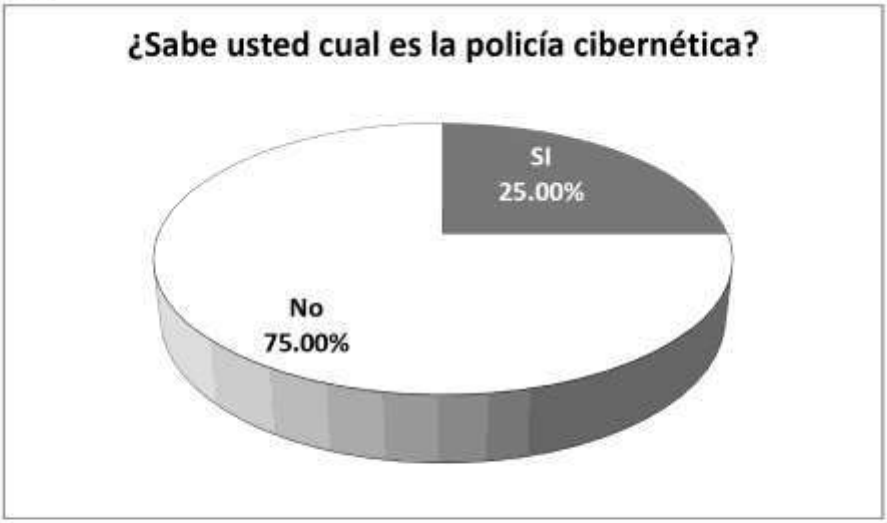
Gráfica 25



Gráfica 26

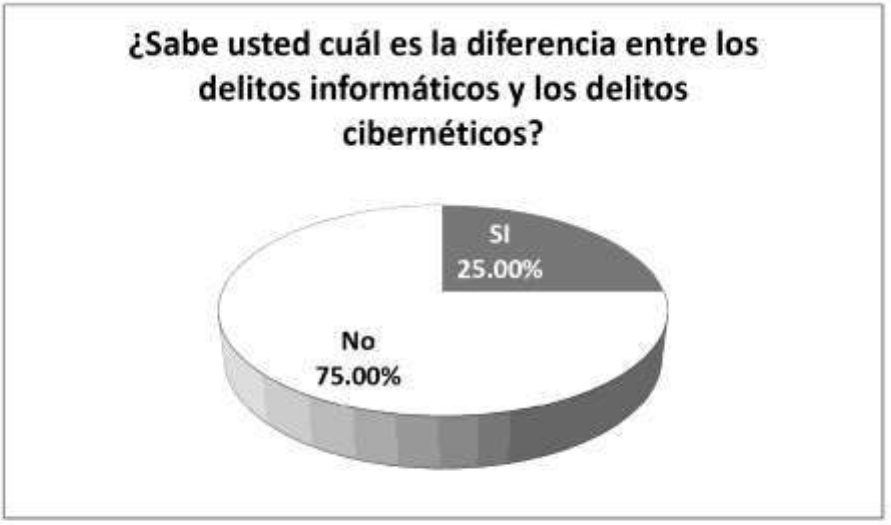


Gráfica 27

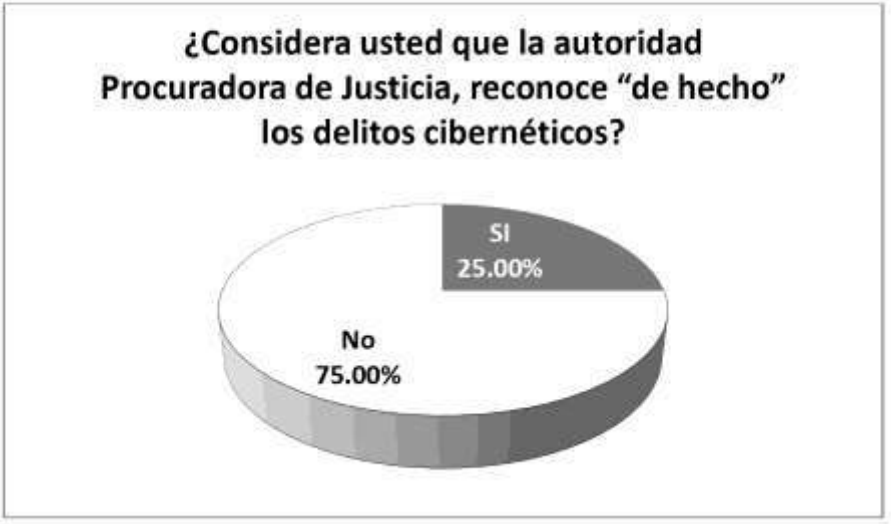


Gráfica 28

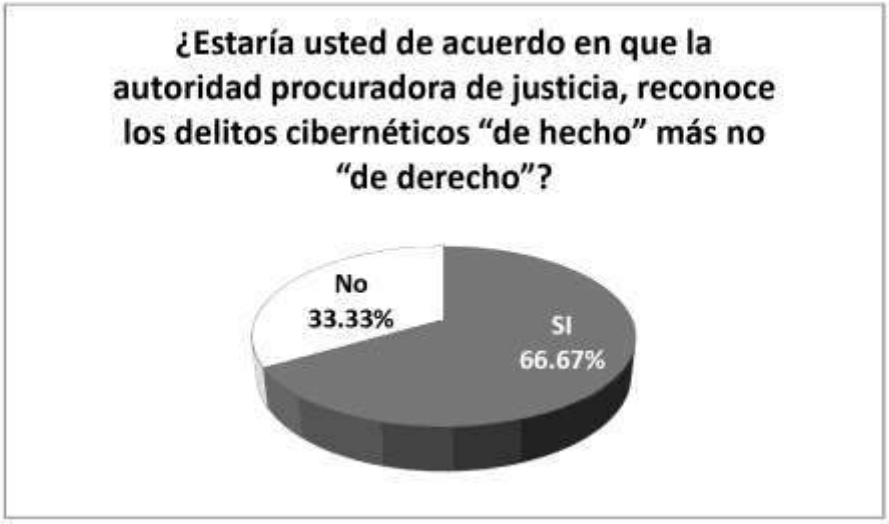
Gráfica 29



Gráfica 30

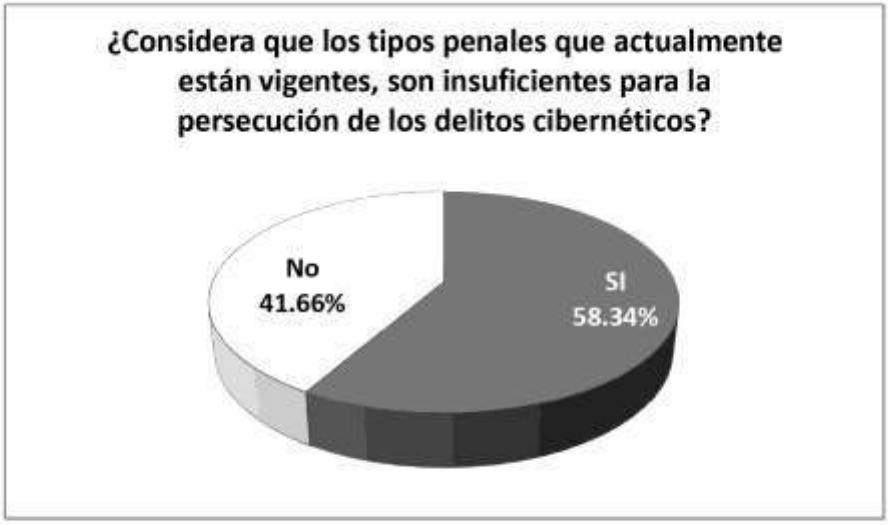


Gráfica 31



Gráfica 32

Gráfica 33



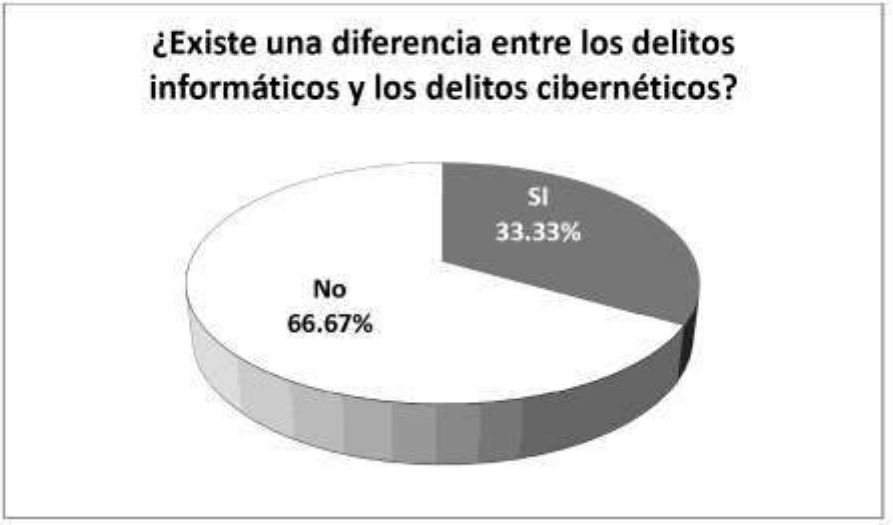
Gráfica 34

Gráfica 35

Gráfica 36

Gráfica 37

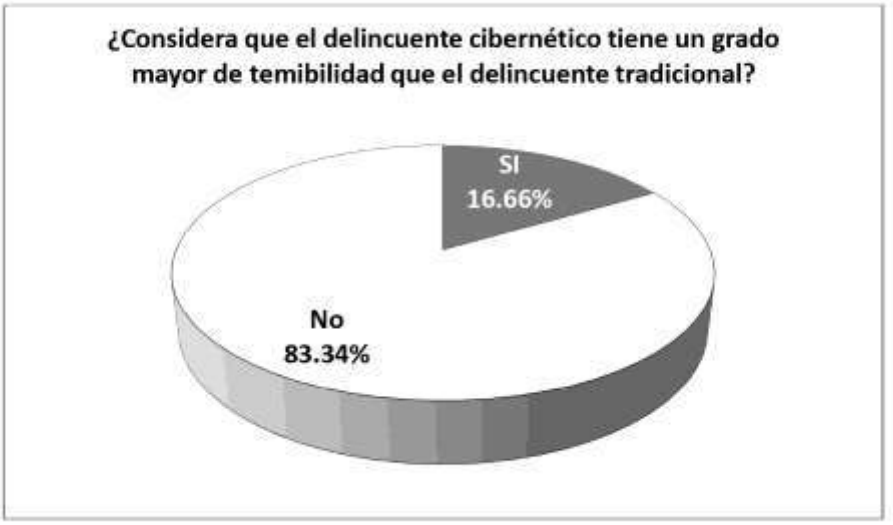
Gráfica 38



Gráfica 39

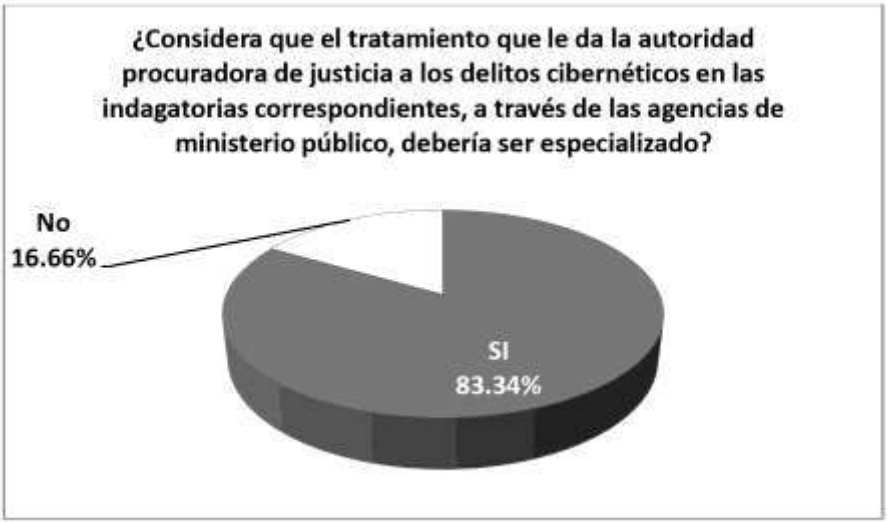
Gráfica 40

Gráfica 41



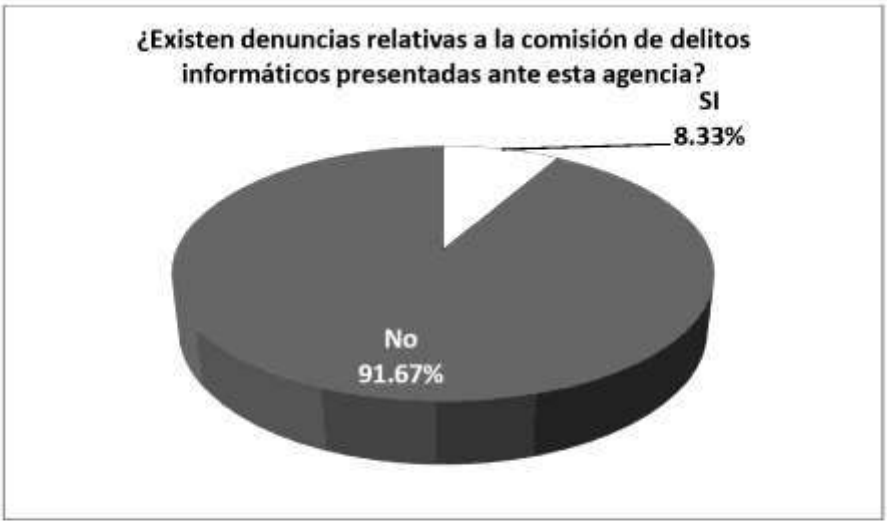
Gráfica 42

Gráfica 43



Gráfica 44

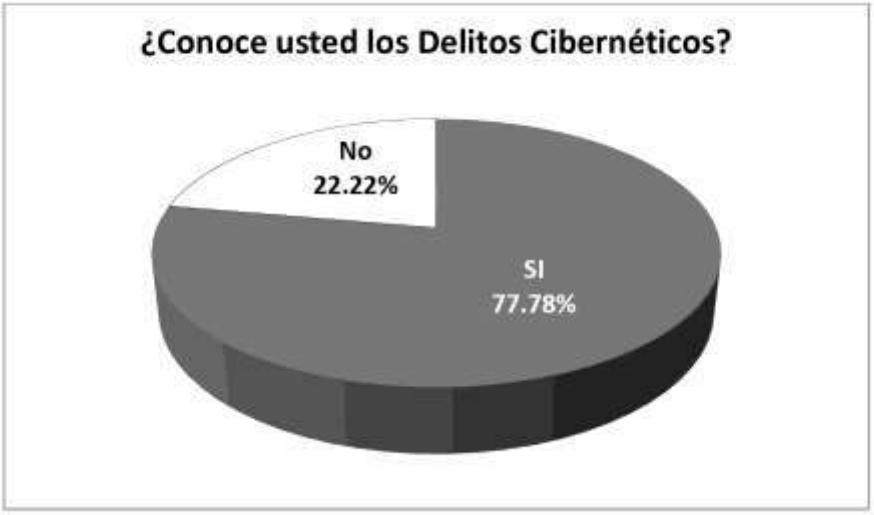
Gráfica 45



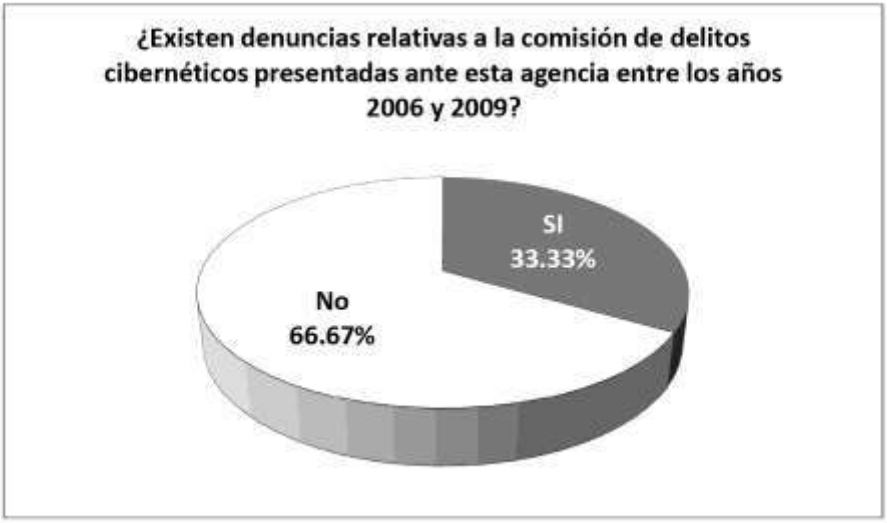
Gráfica 46

En relación a las encuestas realizadas a las agencias y dependencias procuradoras de justicia dependientes de la SUBPROCURADURÍA REGIONAL ZONA NORTE TANTOYUCA, se obtuvieron los siguientes resultados:

Gráfica 47

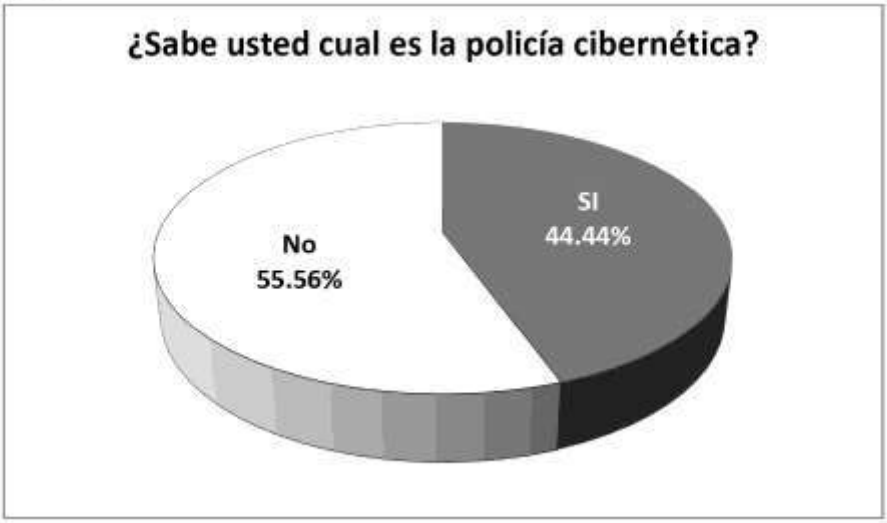


Gráfica 48

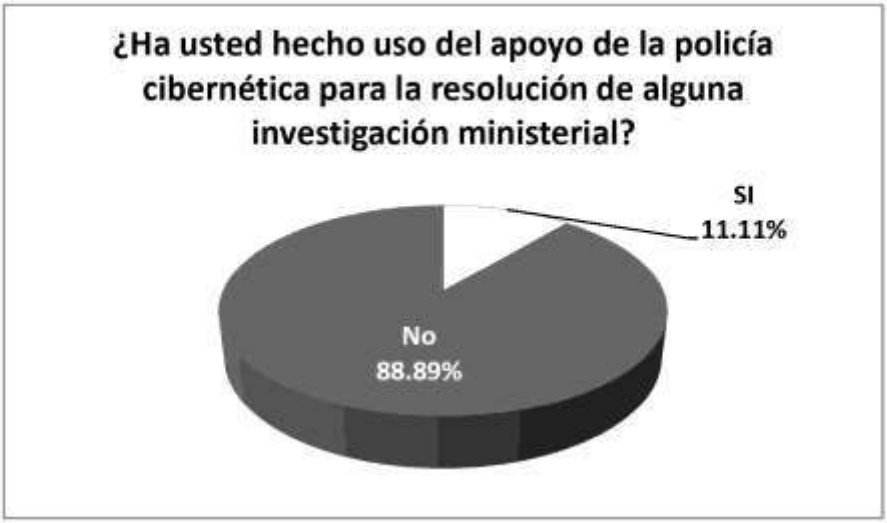


Gráfica 49

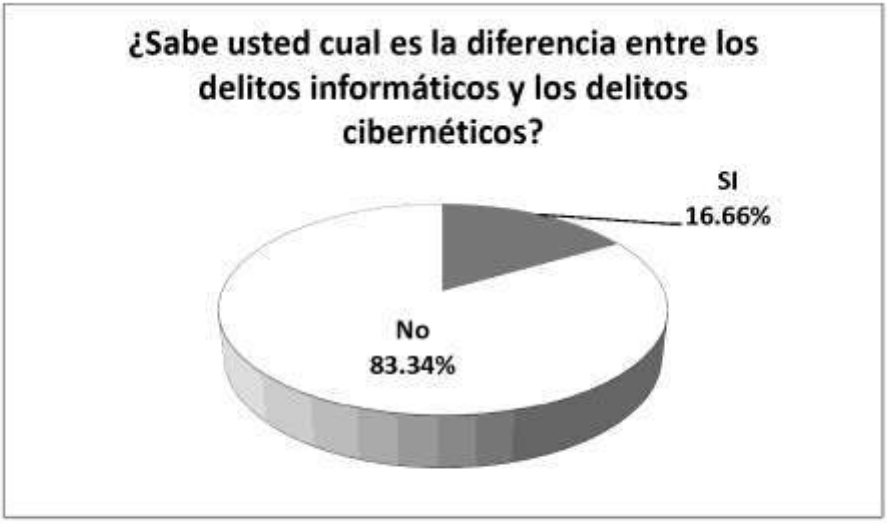
Gráfica 50



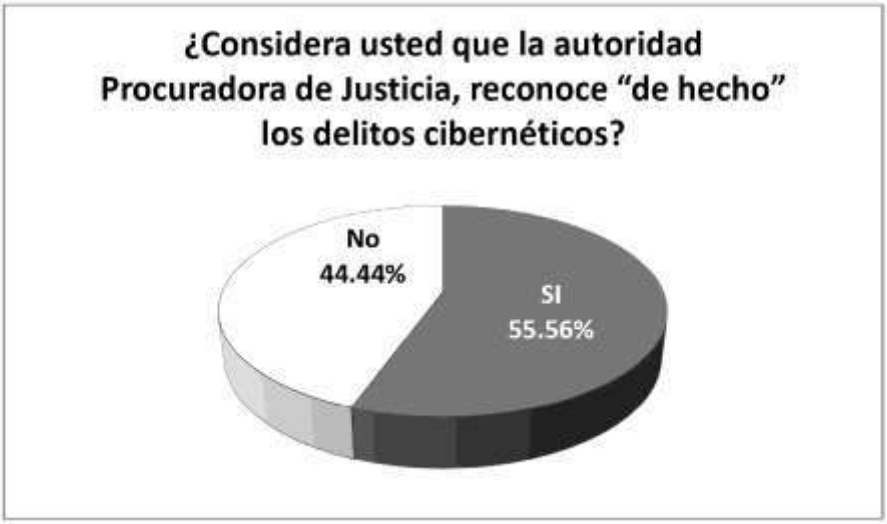
Gráfica 51



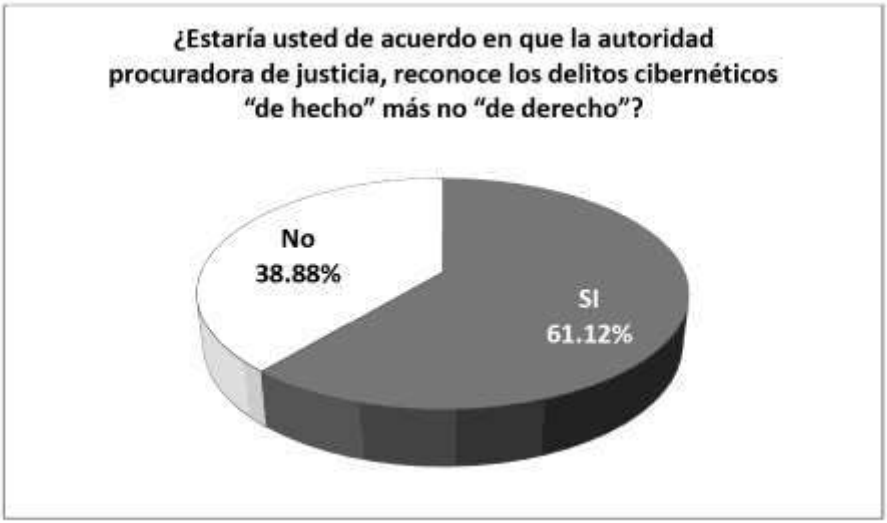
Gráfica 52



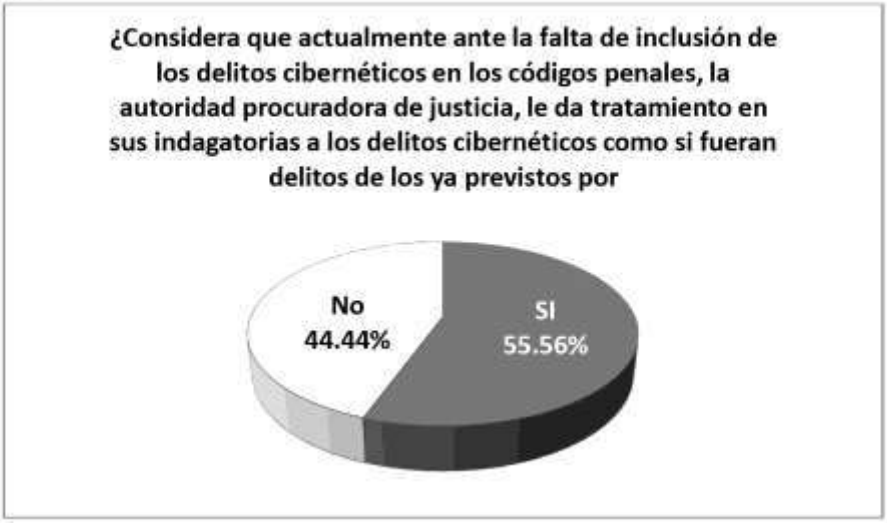
Gráfica 53



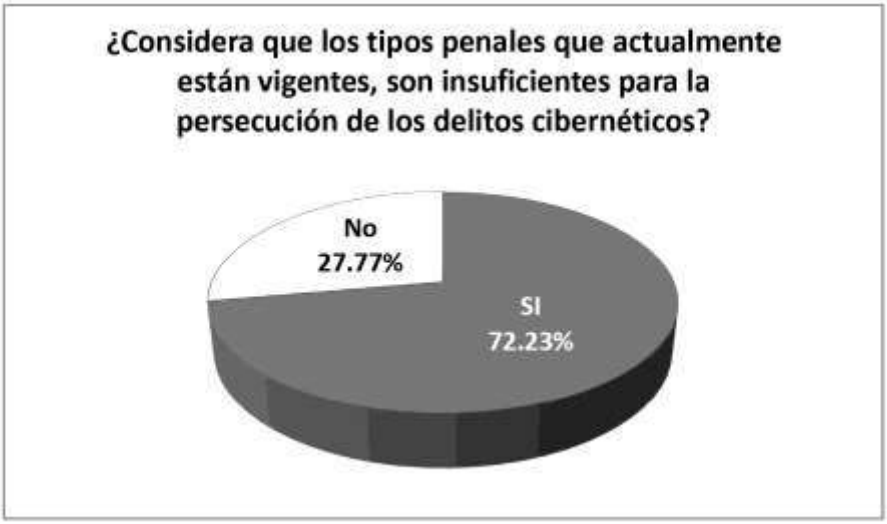
Gráfica 54



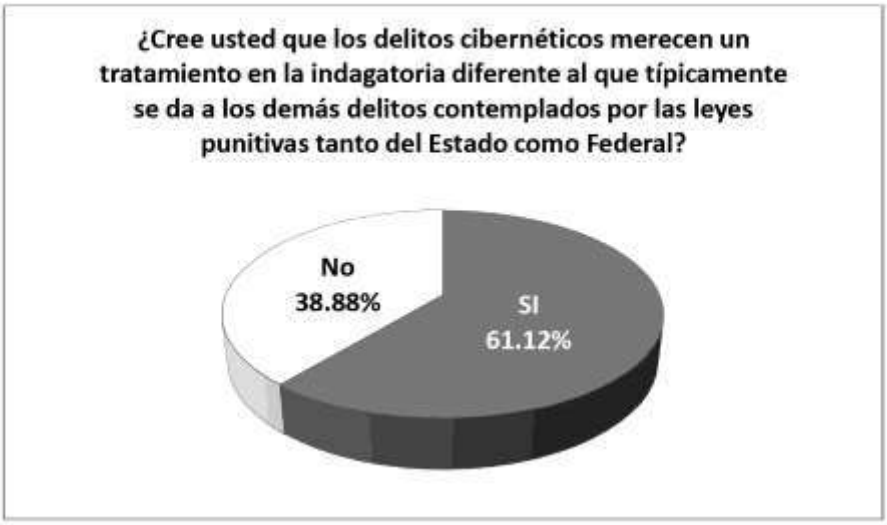
Gráfica 55



Gráfica 56



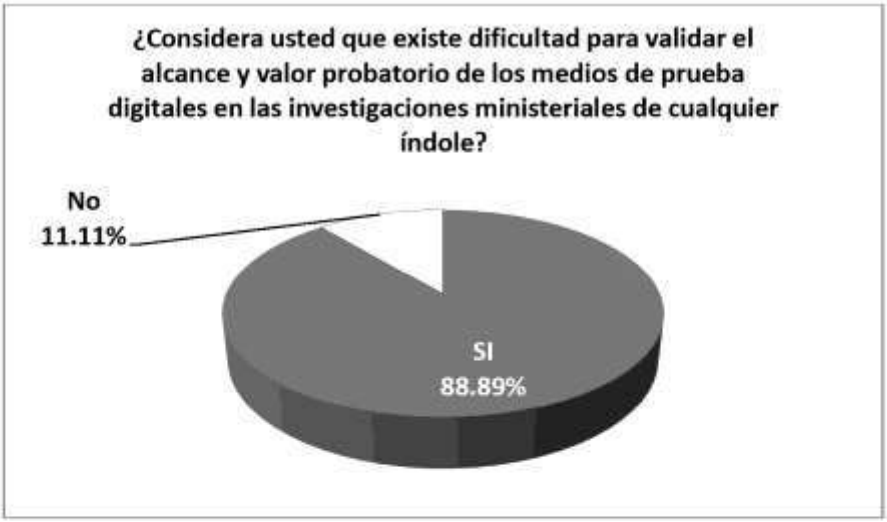
Gráfica 57



Gráfica 58

Gráfica 59

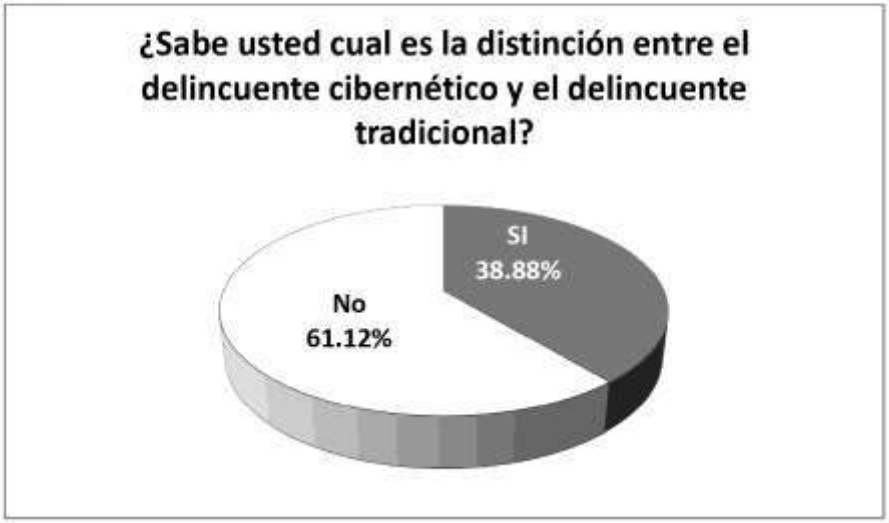
Gráfica 60



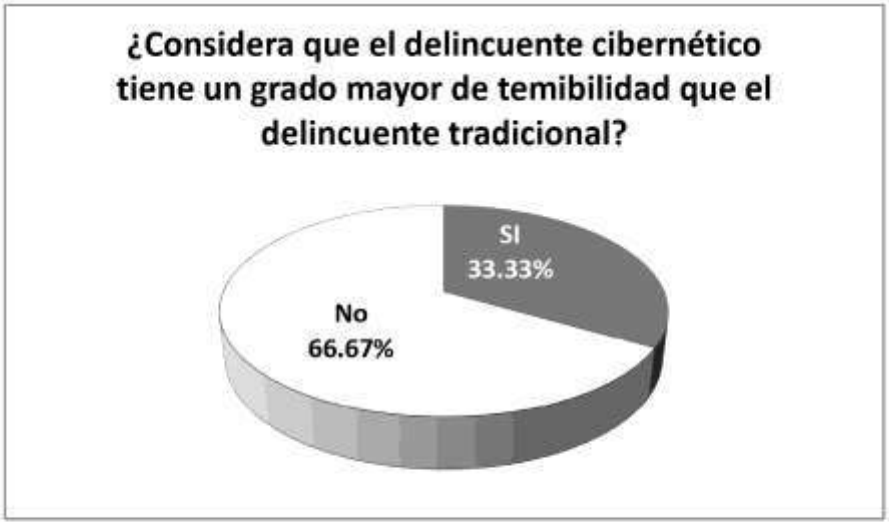
Gráfica 61

Gráfica 62

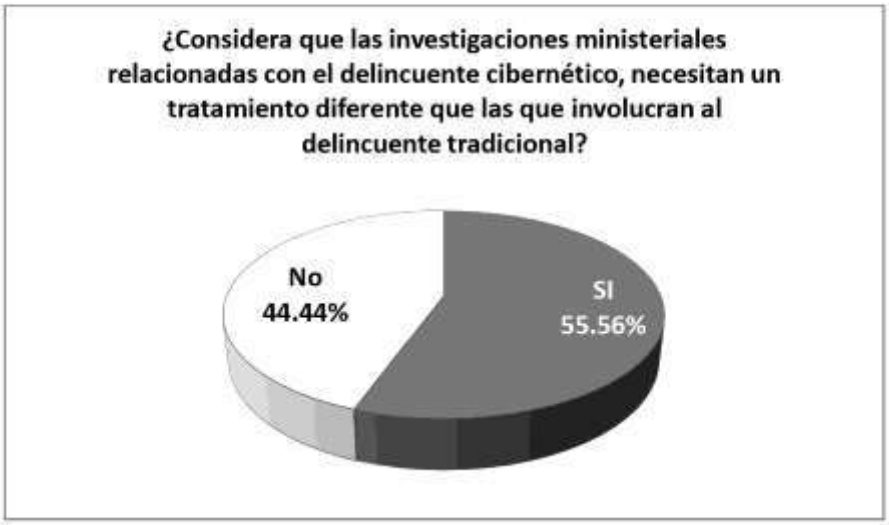
Gráfica 63



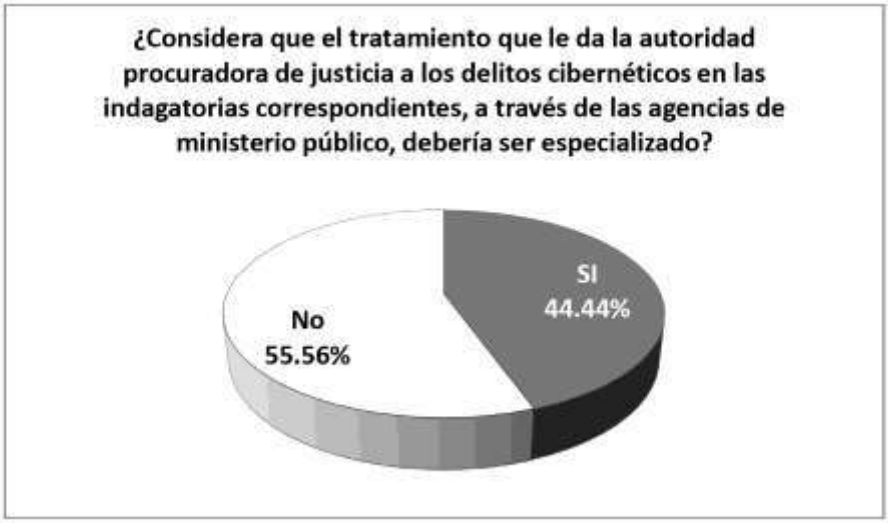
Gráfica 64



Gráfica 65



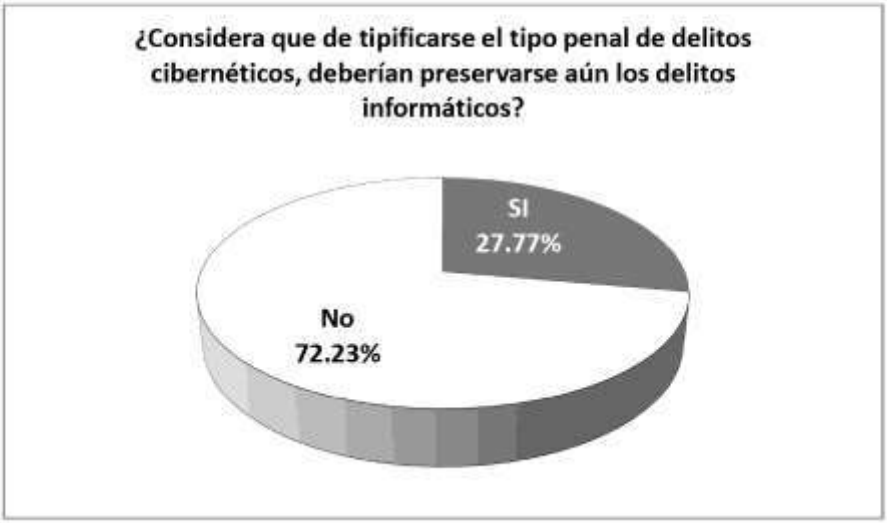
Gráfica 66



Gráfica 67

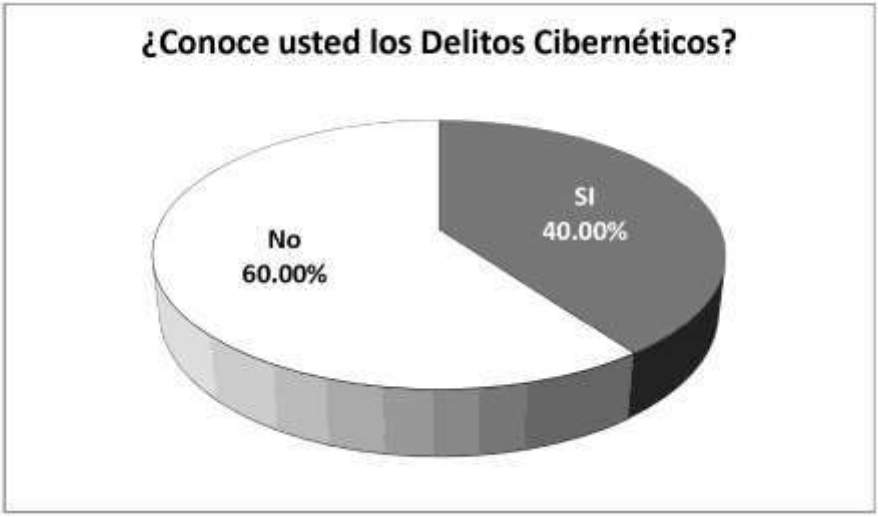
Gráfica 68

Gráfica 69

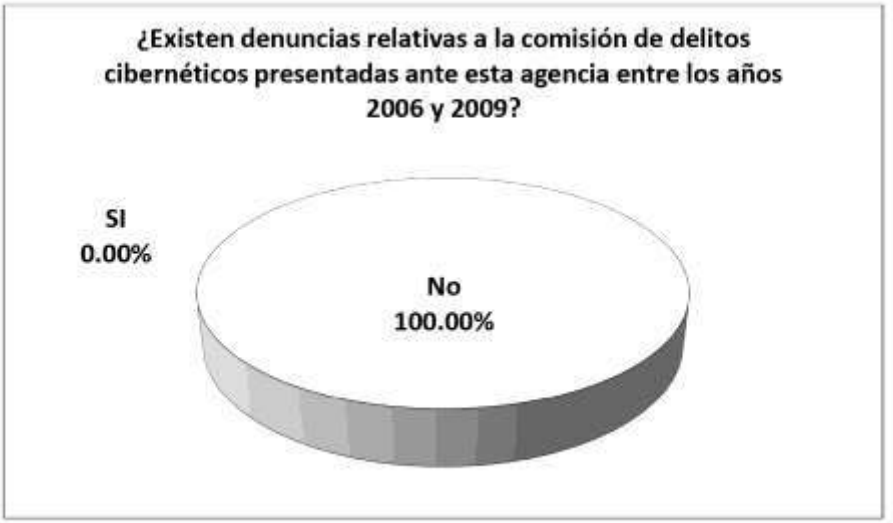


En relación a las encuestas realizadas a las agencias y dependencias procuradoras de justicia dependientes de la SUBPROCURADURÍA REGIONAL ZONA SUR COATZACOALCOS, se obtuvieron los siguientes resultados:

Gráfica 70

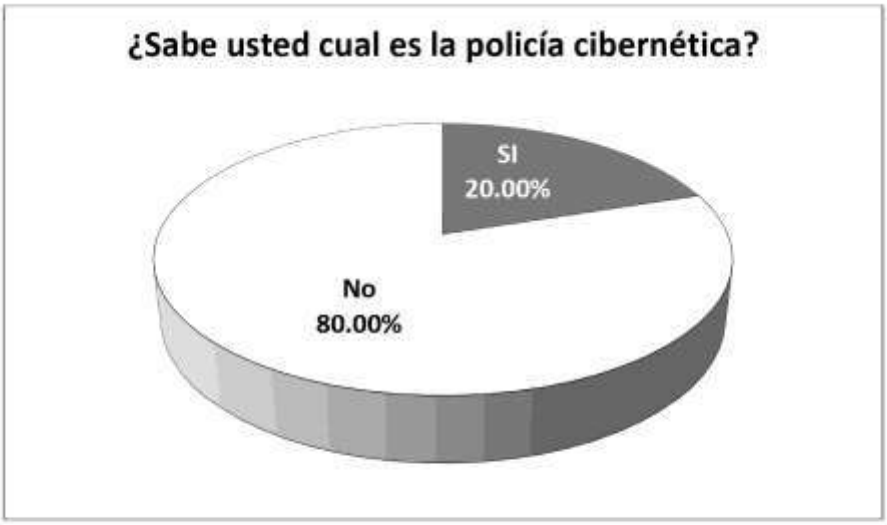


Gráfica 71



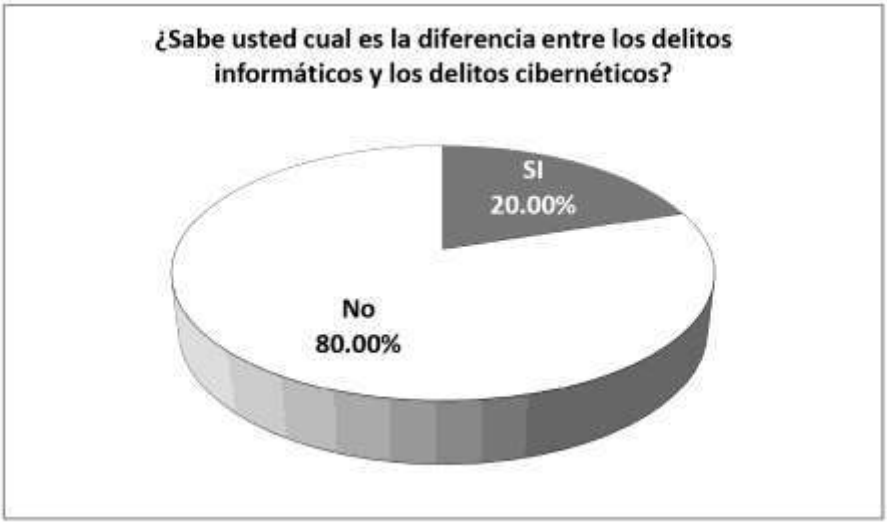
Gráfica 72

Gráfica 73



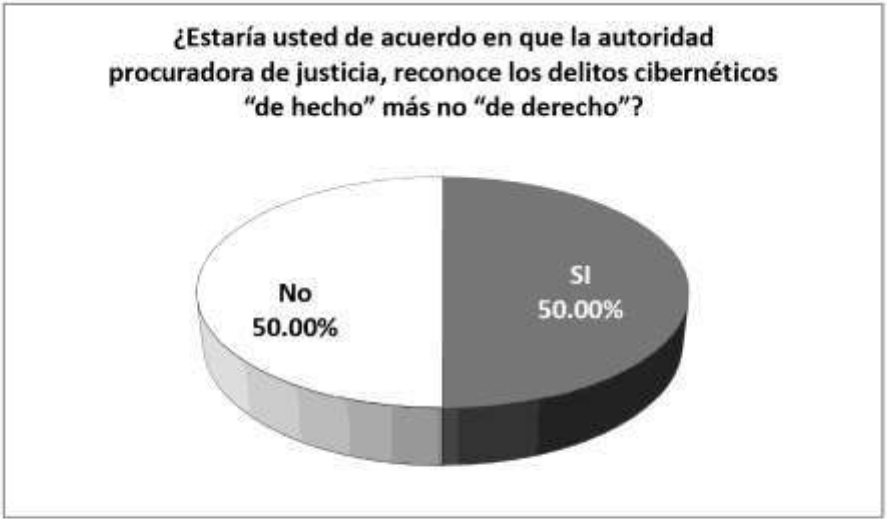
Gráfica 74

Gráfica 75

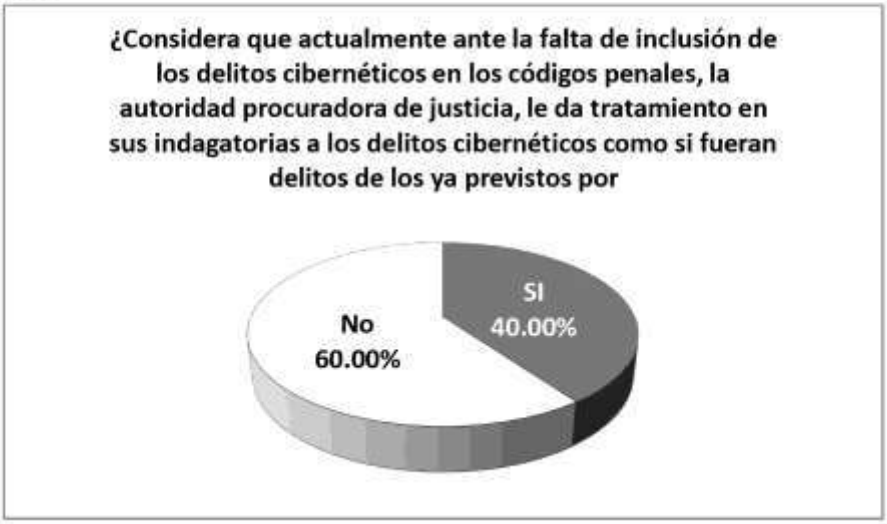


Gráfica 76

Gráfica 77



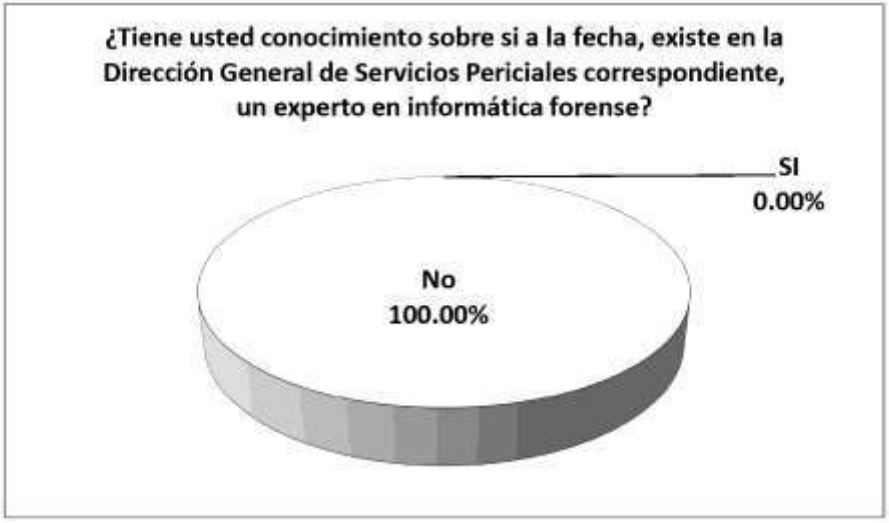
Gráfica 78



Gráfica 79

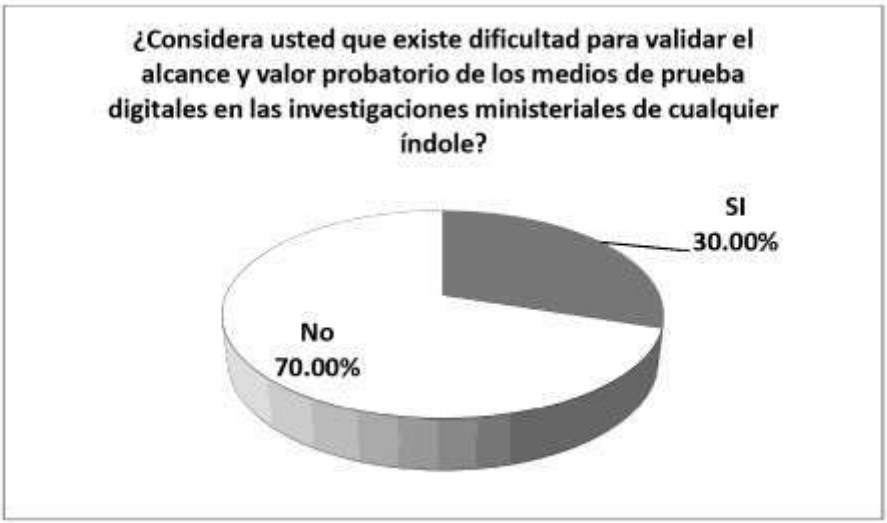
Gráfica 80

Gráfica 81



Gráfica 82

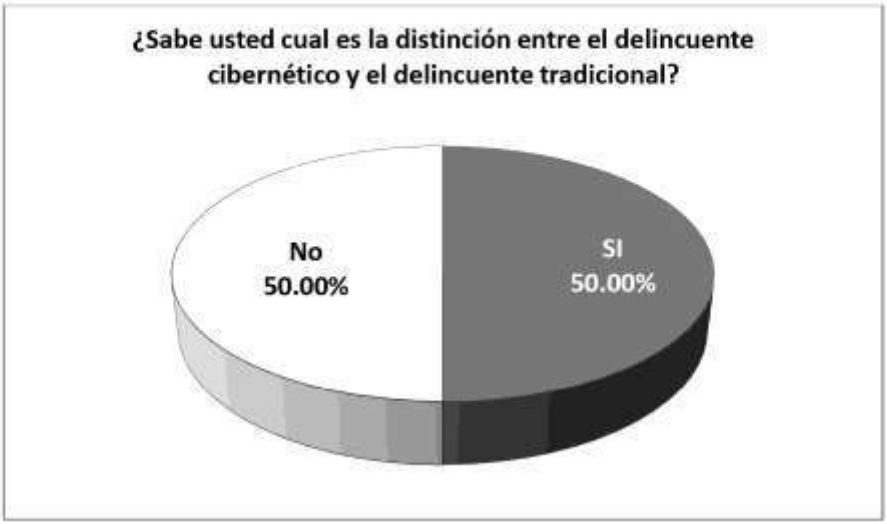
Gráfica 83



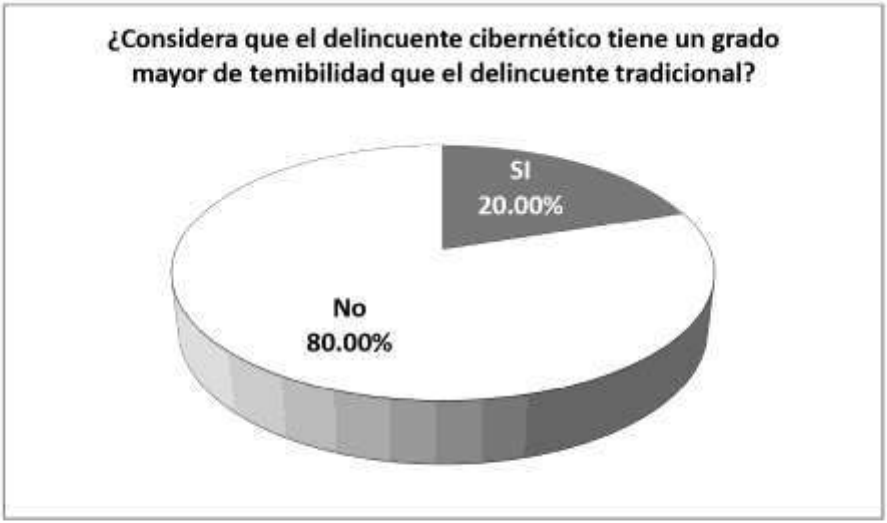
Gráfica 84

Gráfica 85

Gráfica 86

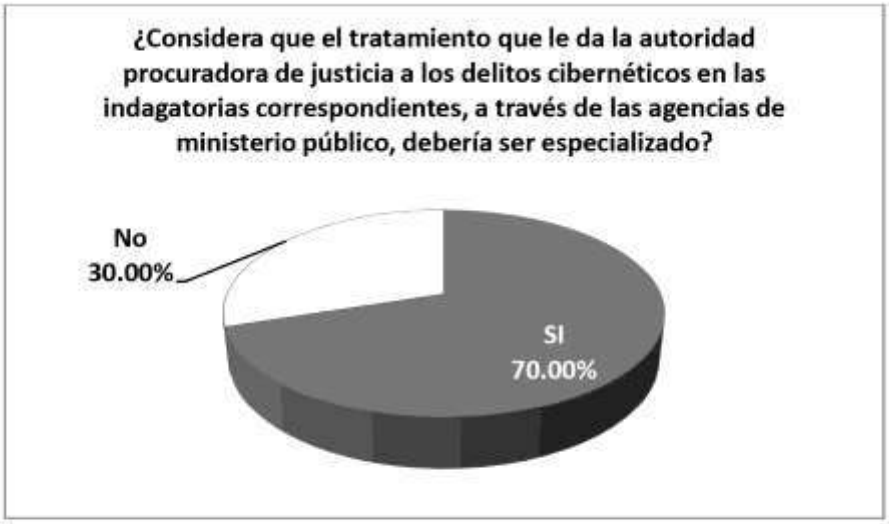


Gráfica 87



Gráfica 88

Gráfica 89



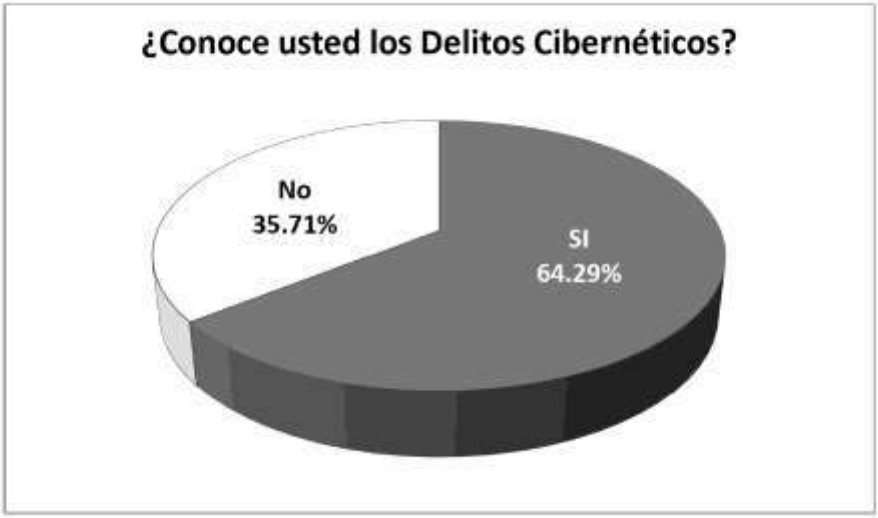
Gráfica 90

Gráfica 91

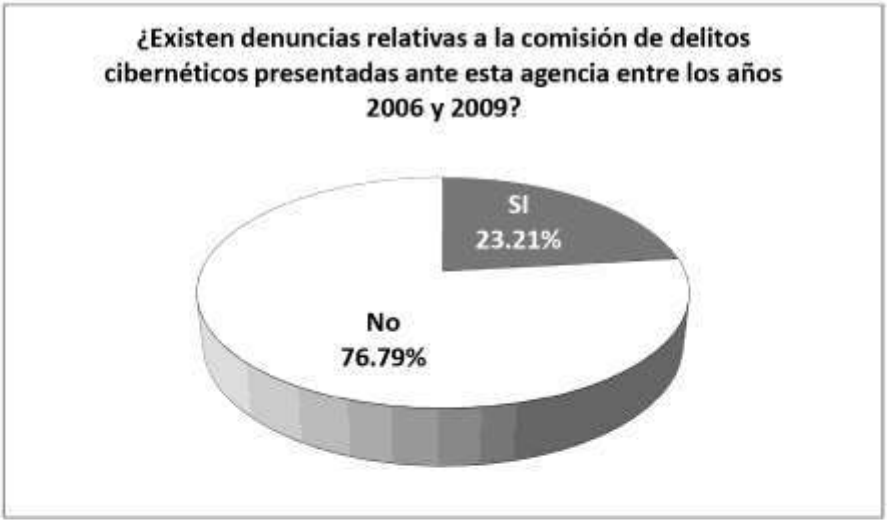
Gráfica 92

En relación a las encuestas realizadas a las agencias y dependencias procuradoras de justicia dependientes de las SUBPROCURADURÍAS REGIONALES, ZONAS SUR (COATZACOALCOS), ZONA NORTE (TANTOYUCA) Y ZONA CENTRO (VERACRUZ Y CÓRDOBA), desde una panorámica general, se obtuvieron los siguientes resultados:

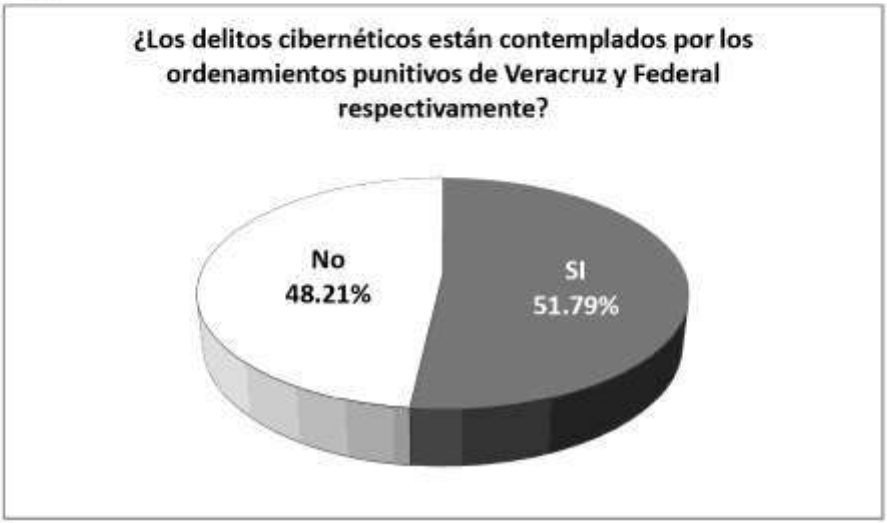
Gráfica 93



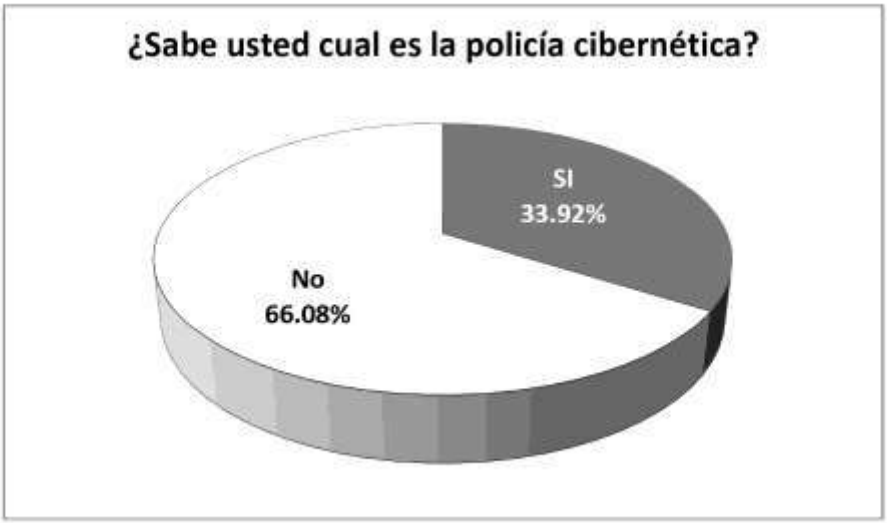
Gráfica 94



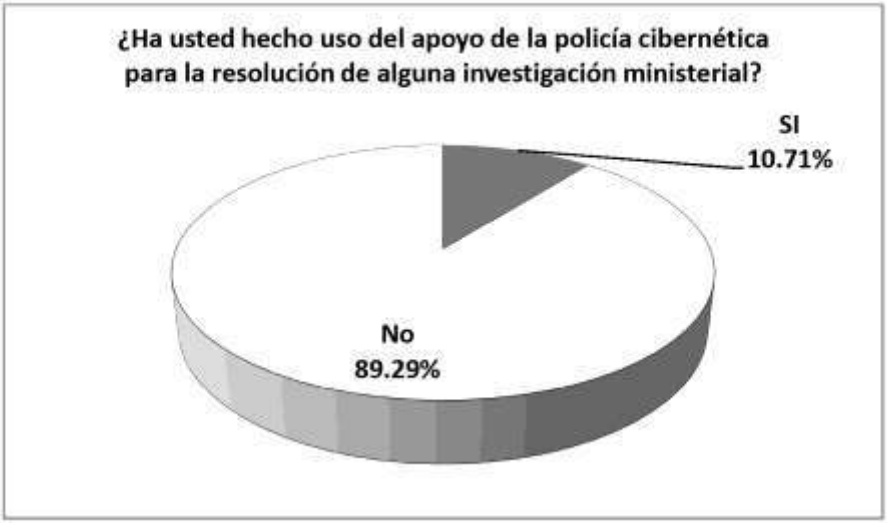
Gráfica 95



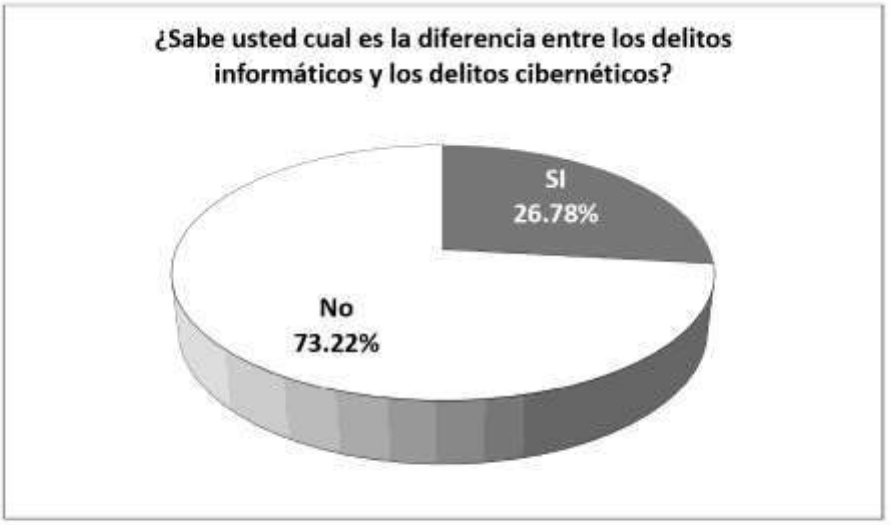
Gráfica 96



Gráfica 97

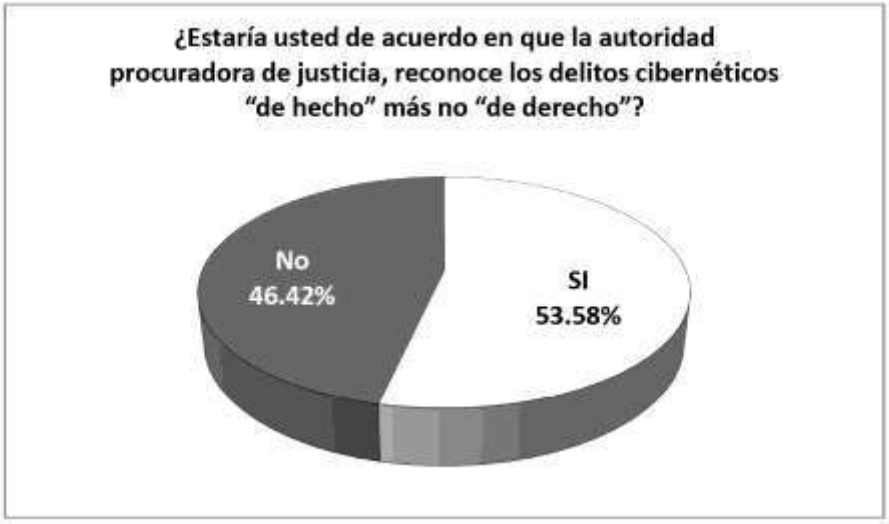


Gráfica 98

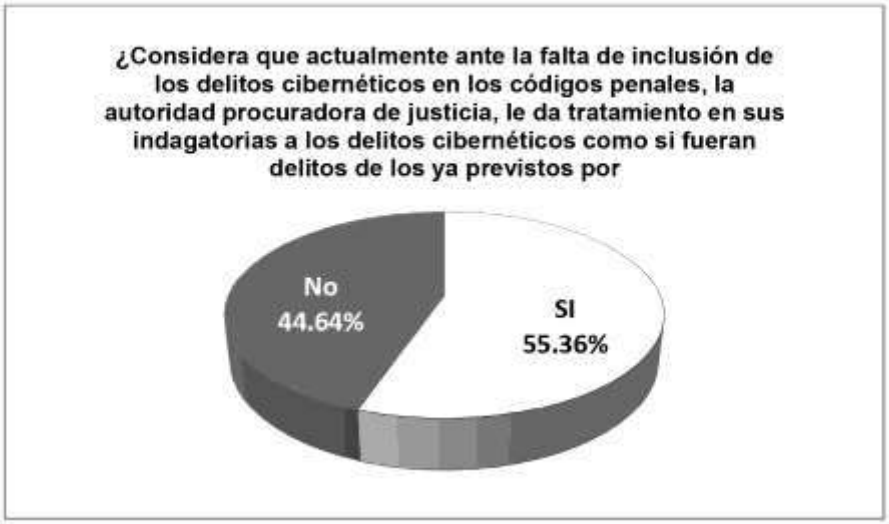


Gráfica 99

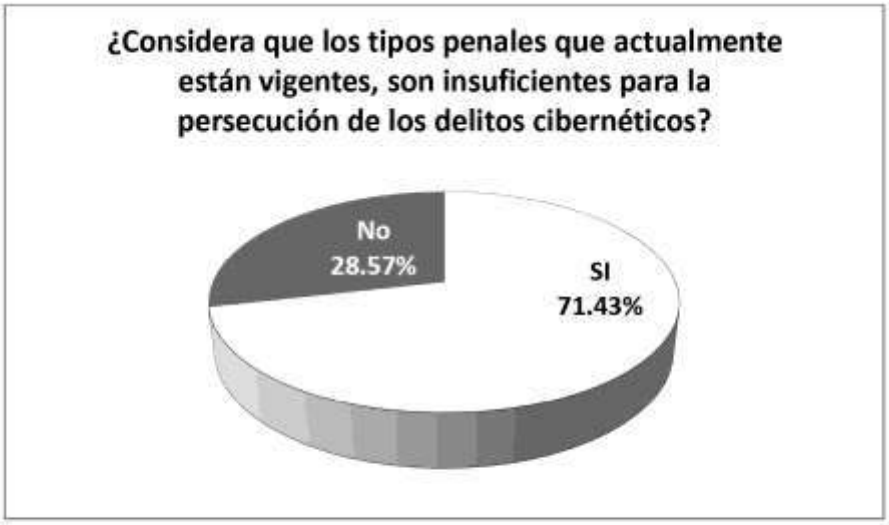
Gráfica 100



Gráfica 101

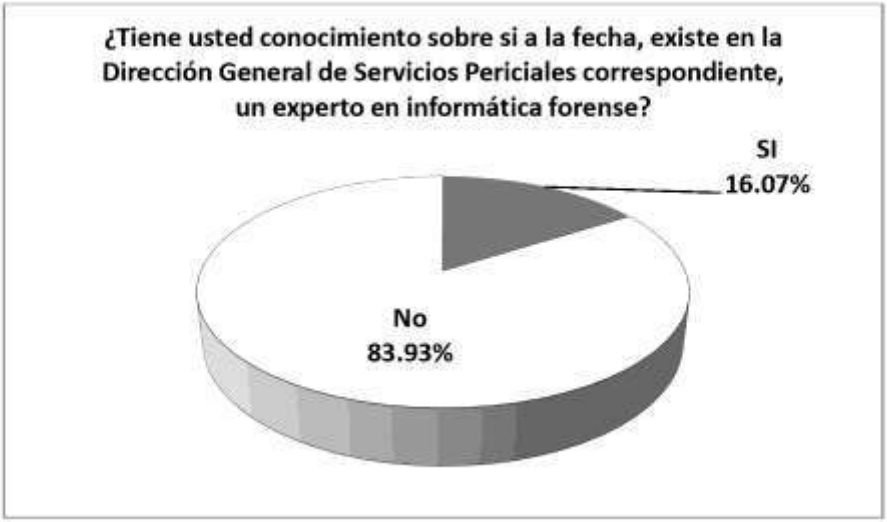


Gráfica 102



Gráfica 103

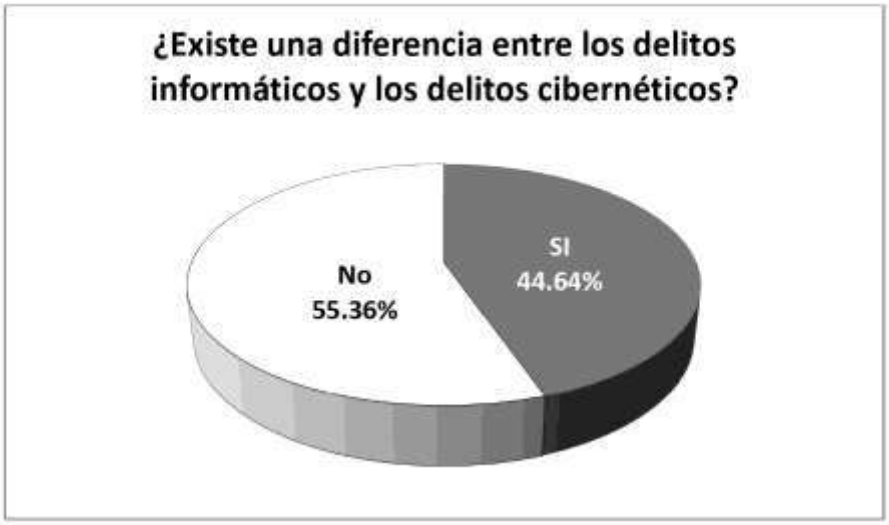
Gráfica 104



Gráfica 105

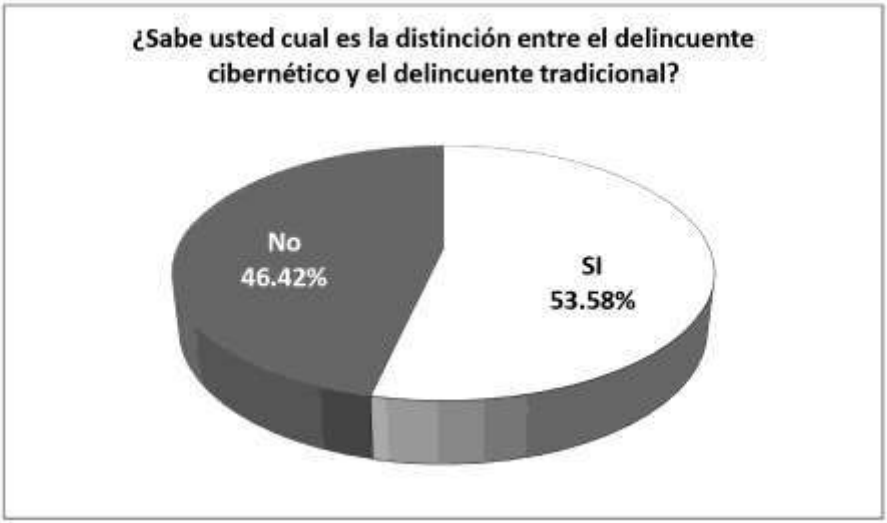
Gráfica 106

Gráfica 107

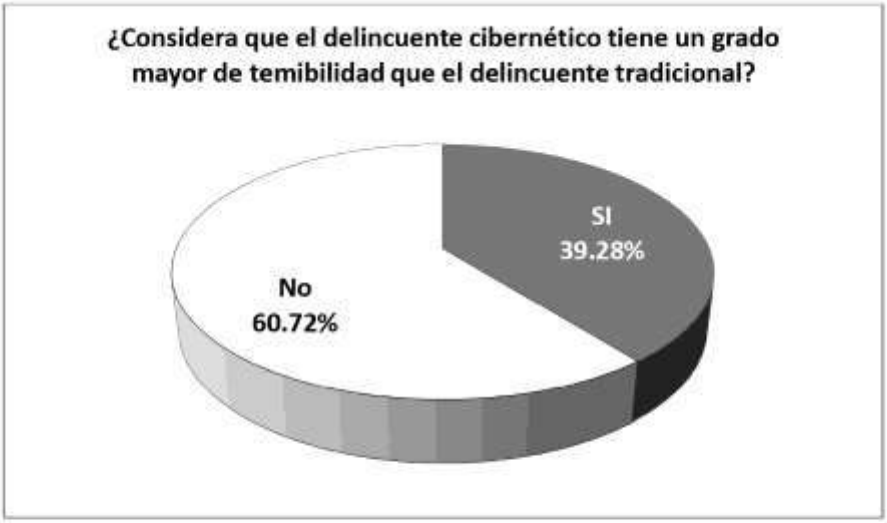


Gráfica 108

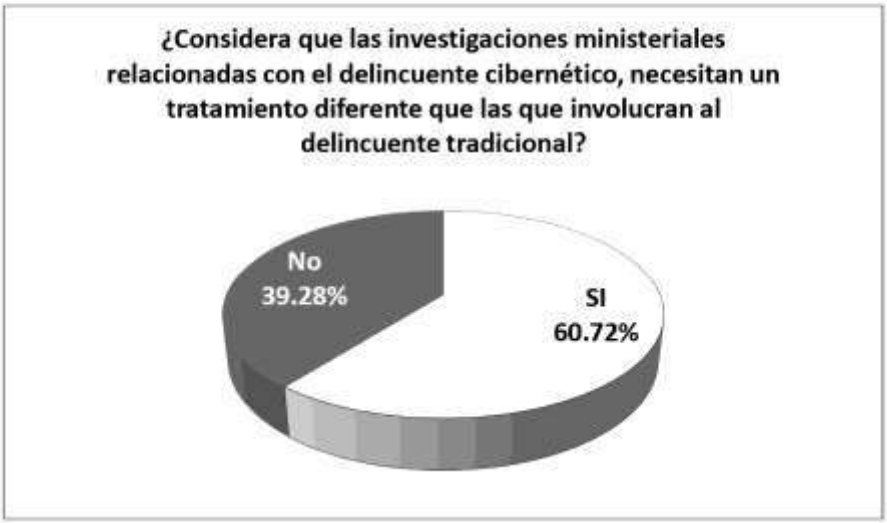
Gráfica 109



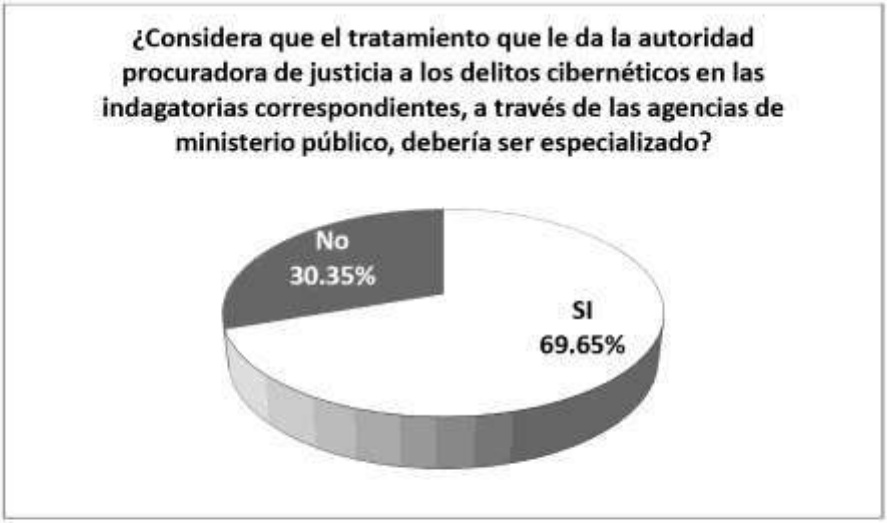
Gráfica 110



Gráfica 111

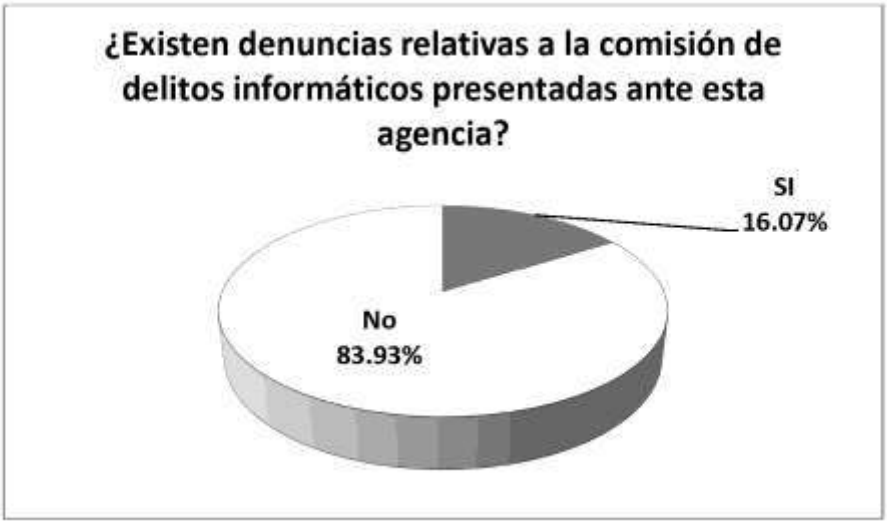


Gráfica 112



Gráfica 113

Gráfica 114



Gráfica 115

4.4. Reconocimiento de los delitos informáticos y cibernéticos en Veracruz

Como se ha sostenido a lo largo de la investigación, existe reconocimiento de los delitos informáticos y cibernéticos en Veracruz, en tratándose de los informáticos, están debidamente tipificados en el Código Penal Local Vigente, pero en tratándose de los delitos cibernéticos, estos se encuentran reconocidos de hecho, mas no de derecho y para acreditar lo que se está expresando, podemos remitirnos a los siguientes datos.

México ocupa el segundo lugar en comisión de delitos cibernéticos a nivel mundial, según datos ofrecidos en la Campaña Nacional de Prevención contra el Delito Cibernético, organizada por El Gobierno Federal, a través de la Secretaria de Seguridad Pública Federal, la Policía Federal Preventiva y los Gobiernos de los Estados.

A raíz de este tipo de delitos, México instauró la creación de la policía cibernética para prevenir y perseguir este tipo de delitos, que como se ha comentado, si están reconocidos de hecho.

De los datos obtenidos de los instrumentos de recolección de datos presentados en apartados anteriores, en lo referente a la pregunta ¿Ha usted hecho uso del apoyo de la policía cibernética para la resolución de alguna investigación ministerial?

Las respuestas según la gráfica 97, un 89.29% expresaron que no, mientras que un 10.71% dijeron que si, lo que nos indica claramente que esta policía, independientemente de la causa, en Veracruz, es poco utilizada.

La razón puede deberse a que las autoridades procuradoras de justicia en el Estado, no saben qué es la policía cibernética lo cual nos queda claro al retomar los datos obtenidos del instrumento de recolección de datos presentado en apartados anteriores, con relación a la pregunta ¿sabe usted cuál es la policía cibernética?, la respuestas según la gráfica 96, fueron: un 66.08 dijo que no, frente a un 33.92 que expresó que si, por lo que se advierte claramente que en Veracruz, hay desconocimiento en su mayoría sobre este tipo de policía.

De igual forma al responder la pregunta: ¿Considera usted que la autoridad Procuradora de Justicia, reconoce "de hecho" los delitos cibernéticos?, las respuestas en la gráfica 99, fueron, un 44.64% que no, frente a un 55.36% que sí, lo cual nos deja claro que se sabe del reconocimiento de hecho de los delitos cibernéticos en Veracruz.

Al reforzar la pregunta anterior con otra de similar naturaleza, ¿Estaría usted de acuerdo en que la autoridad procuradora de justicia, reconoce los delitos cibernéticos "de hecho" más no "de derecho"?, las respuestas, plasmadas en la gráfica 100, fueron: un 46.42% de la población expresó que No, frente a un 53.58 que Sí, lo cual nuevamente nos deja claro que la mayoría del personal encargado de la procuración de justicia en Veracruz, esta consiente del reconocimiento de hecho de los delitos cibernéticos.

4.5. Alcances de las indagatorias en tratándose de delitos cibernéticos

En Veracruz, al instaurarse una investigación ministerial, relacionada con los delitos cibernéticos, se debe tener presente primero que, independientemente de los índices de delitos de esta naturaleza denunciados en Veracruz, es importante saber qué tratamiento se les dará en la primera etapa del procedimiento penal, para lo cual, es necesario remitirse a los datos aportados en los instrumentos de recolección de datos que se presentan en apartados anteriores.

En lo referente a la pregunta: ¿Cree usted que los delitos cibernéticos merecen un tratamiento en la indagatoria diferente al que típicamente se da a los demás delitos contemplados por las leyes punitivas tanto del Estado como Federal?, las respuestas según la gráfica 103, fueron: 44.64% dijeron que No, frente a un 55.36% que expresó que Si, lo cual nos deja claro que la mayoría de los funcionarios encargados de la procuración de justicia en Veracruz, están de acuerdo en que el tratamiento en las indagatorias debe ser diferente al que típicamente se le da a los delitos tradicionales.

Por otra parte, al preguntar: ¿Considera que para la persecución de los delitos cibernéticos debe existir un experto en informática forense en la Dirección General de Servicios Periciales correspondiente?, las respuestas según la gráfica 105, fueron: 10.71% que No, frente a un 89.29% que Sí, lo cual nos deja claro que en las indagatorias relacionadas con los delitos cibernéticos, se debe acudir a un experto especializado que coadyuve con la labor de investigación.

De igual forma, existe dificultad en las indagatorias para validar el alcance y valor probatorio de los medios de convicción en las investigaciones ministeriales, lo cual se fundamentó al preguntar: ¿Considera usted que existe dificultad para validar el alcance y valor probatorio de los medios de prueba digitales en las investigaciones ministeriales de cualquier índole? Las respuestas, según la gráfica 21.42% dijeron que No, frente a un 78.58% que dijeron que Si, lo cual nos deja claro que tienen un mayor grado de dificultad el esclarecimiento de las investigaciones ministeriales relacionadas con los delitos cibernéticos, toda vez que la validación del material probatorio es más compleja.

Finalmente y atendiendo al presente apartado que refiere el alcance de las indagatorias en tratándose de delitos cibernéticos, se tiene a bien

manifestar que para que dicho alcance sea satisfactorio, deben existir agencias especializadas en delitos cibernéticos y esto se fundamenta en las respuestas provenientes de la pregunta: ¿Considera que el tratamiento que le da la autoridad procuradora de justicia a los delitos cibernéticos en las indagatorias correspondientes, a través de las agencias de ministerio público, debería ser especializado?, teniendo como respuestas plasmadas en la gráfica 112, las siguientes: el 30.35% dijo que No, frente a un 69.65% que dijo que si, lo cual nos deja claro que en Veracruz, se está a favor de una especialización en lo que a investigación ministerial se refiere, para persecución de éste tipo de delincuentes.

4.6. Interpretación de los resultados obtenidos

4.6.1. Insuficiencia de los tipos penales para la persecución de los delitos cibernéticos

Los tipos penales, deben necesariamente ser suficientes para poder perseguir y sancionar a los delincuentes que actualizan conductas antisociales, antijurídicas, típicas, culpables, punibles, pero no debemos olvidar que existe el principio general del derecho que expresa: *nullo crimmen nulla pena sine lege*, es decir no hay delito ni pena sin ley, lo cual podría verse materializado cuando intentamos procesar a alguien por la comisión de un delito cibernético basados en los tipos penales tradiciones que para el caso de las nuevas tecnologías y la internet, son insuficientes.

Debe retomarse nuevamente lo expresado por los encuestados al preguntarles: ¿Considera que actualmente ante la falta de inclusión de los delitos cibernéticos en los códigos penales, la autoridad procuradora de justicia, le da tratamiento en sus indagatorias a los delitos cibernéticos como si fueran delitos de los ya previstos por los códigos?, las respuesta según la gráfica 101, fueron: un 44.64% dijeron que No, frente a un 55.36% que dijo que Si, lo que nos deja claro que

los delitos que involucran nuevas tecnologías e Internet, siguen persiguiéndose como si fueran delitos tradicionales.

Pues bien, continuando con el orden de ideas que nos ocupa, es necesario entonces aterrizar sobre si los tipos penales vigentes, son suficientes o no para dar persecución satisfactoria a los delincuentes hasta este momento conocidos como cibernéticos.

Lo anterior se responde atendiendo a lo expresado por los encuestados al referirles el siguiente tópico: ¿Considera que los tipos penales que actualmente están vigentes, son insuficientes para la persecución de los delitos cibernéticos?, las respuestas según la gráfica 102, el 28.57% dijo que No, frente a un 71.43% que dijeron que Sí, lo cual nos deja claro que se requiere una reforma de manera inmediata en tratándose de los delitos hasta este momento conocidos como cibernéticos.

Finalmente, para terminar de establecer el punto medular de la investigación, al preguntar a los encuestados: ¿Considera que con la descripción del tipo penal de delitos informáticos, es posible la persecución de los delitos cibernéticos?, las respuestas según la gráfica 108, fueron 53.58% que No, frente a un 46.42% que dijo que Sí, lo cual deja claro que los delitos cibernéticos deben tener su propio tipo penal.

4.6.2. Falta de inclusión de los delitos cibernéticos en el ordenamiento punitivo Estatal

No es necesario un análisis exhaustivo de instrumentos para determinar la falta de inclusión de los delitos cibernéticos en el ordenamiento punitivo estatal, simplemente basta y sobra con analizar el Código Penal para el Estado de Veracruz y advertir claramente como existe una ausencia de este tipo de delitos, pero lo interesante también es advertir qué conocimiento tienen al respecto las autoridades

procuradoras de justicia en el Estado, para lo cual es necesario remitirse nuevamente a los instrumentos de recolección de datos en los que advertimos respuestas como las que a continuación se retoman:

Al ser cuestionados sobre: ¿Los delitos cibernéticos están contemplados por los ordenamientos punitivos de Veracruz y Federal respectivamente?, las respuestas según la gráfica 95, fueron: 48.21% dijeron que No, frente a un 51.78% que dijeron que Si, lo cual a todas luces denota un total desconocimiento, por la mayoría de los encuestados, que son una muestra representativa del total de la población procuradora de justicia en Veracruz, porque es evidente que no existen tipificados los delitos cibernéticos.

4.6.3. Desconocimiento y confusión sobre los delitos informáticos y cibernéticos

Las autoridades procuradoras de justicia en Veracruz, actualmente tienen una confusión arraigada sobre lo que refieren los delitos cibernéticos, por tanto como podemos esperar que persiga e investiguen adecuadamente este tipo de delitos, cuando no saben siquiera que son y para demostrar lo que se está expresando en este párrafo, basta con remitirnos nuevamente a lo recabado por los instrumentos de recolección de datos que se decodifican en apartados anteriores.

Al preguntar ¿Por qué, muy a pesar de que el Estado reconoce los delitos cibernéticos “de hecho”, no los incluye dentro de la legislación penal correspondiente, para entonces reconocerlos también “de derecho”?

Las respuestas fueron:

- Porque los legisladores no tienen conocimientos claros sobre la distinción
- Se desconoce la razón
- Son delitos nuevos

Es decir, las respuestas parten del desconocimiento, tanto de las autoridades administrativas como legislativas para la implementación de este tipo de delitos, pero para seguir fundando que existe el desconocimiento, vayamos a las siguientes preguntas:

Al ser cuestionados sobre: ¿Conoce usted los Delitos Cibernéticos?, las respuestas, según la gráfica 93, fueron: 35.71% dijo que No, frente a un 64.29% que dijo que Si, lo cual aparentemente nos podría dejar entrever que si hay conocimiento sobre este tipo de delitos, pero cuando se les preguntó ¿Cuál considera que es la diferencia entre los delitos informáticos y los delitos cibernéticos?, las respuestas oscilaron de la siguiente forma:

- Ninguna
- Informáticos, información, cibernéticos, internet
- Los informáticos son a información y los cibernéticos a internet
- No se sabe
- Es poca la diferencia

Por tanto se deduce que tienen una idea, pero no saben en realidad que son, por tanto prevalece el desconocimiento y confusión sobre este tipo de delitos.

De igual forma, al preguntar: ¿Existe una diferencia entre los delitos informáticos y los delitos cibernéticos?, las respuestas según la gráfica 107, el 55.36& dijo que No, frente a un 44.64% que dijo que Sí, lo cual

no deja claro que más del cincuenta por ciento de la muestra encuestada, piensa que son lo mismo.

Finalmente se advierte con las respuestas que a continuación se analizan que, los delitos cibernéticos no se incorporan a las legislaciones punitivas vigentes por desconocimiento y confusión:

Véanse las respuestas de la siguiente pregunta: ¿Por qué el estado ha creado una policía cibernética para coadyuvar con la persecución de los delitos de ésta índole, pero no se reconocen en los ordenamientos punitivos Estatales y Federal respectivamente?, las respuestas fueron:

- Si los reconoce de manera informal
- Se desconoce
- Son delitos derivados de las computadoras

Esto deja claro también, que se sigue pensando que los delitos cibernéticos son solo un nombramiento y no un delito que debe incorporarse a los ordenamientos punitivos estatales y federal, y todo esto obedece al desconocimiento generalizado sobre los delitos cibernéticos y su confusión con los delitos informáticos.

4.7. Consideraciones finales de éste capítulo

Se logró validar la muestra obtenida de 56 agencias y dependencias del ministerio público, pertenecientes a 4 de las 7 subprocuradurías generales de justicia, abarcando las tres zonas (norte, centro y sur) que constituyen el Estado de Veracruz, con base en las formulas de Muestreo aleatorio estratificado.

Se establecieron los alcances de las preguntas cualitativas y cuantitativas del instrumento que se pretendía aplicar, teniendo las

respuestas de cada una, el objetivo de acreditar los objetivos planteados en ésta investigación.

Se establecieron los resultados de la decodificación de los instrumentos aplicados, desarrollando tablas que vaciaban los contenidos de las respuestas de forma organizada y sistematizada tanto por zonas como de una perspectiva general y se graficaron los resultados para ofrecer una visión de respuesta por porcentajes, tales resultados se tradujeron en los siguientes puntos concluyentes:

- Se demostró el reconocimiento en Veracruz, formal (de derecho) de los delitos informáticos, los cuales se encuentran contenidos en el Código Penal de Veracruz, en su artículo 181. Y existe un reconocimiento de los delitos cibernéticos en Veracruz de facto (de hecho) por parte de la autoridad procuradora de Justicia en Veracruz y de las autoridades procuradoras de Justicia Federal.
- Se demostró que resulta necesaria la especialización para la persecución de los delitos informáticos y cibernéticos, la cual se puede traducir en alguna agencia especializada en delitos cibernéticos o como posteriormente se denominaran delitos binarios.
- Se demostró que actualmente, los tipos penales que están vigentes relacionados con los delitos informáticos, son insuficientes para la persecución de los delitos cibernéticos.
- Se demostró que existe un desconocimiento y confusión por parte de las autoridades Procuradoras de Justicia en el Estado, sobre los delitos informáticos y cibernéticos, tendiendo éstas a confundir ambos delitos como si fueran los mismos e incluso expresar un desconocimiento total de tales delitos.
- Se demostró que es necesaria una reforma que incluya los delitos relacionados con las nuevas tecnologías y el Internet.

CAPÍTULO 5
PROPUESTA DE INCLUSIÓN DE LOS DELITOS BINARIOS EN LA LEY PUNITIVA DEL ESTADO DE VERACRUZ

5.1. ¿Por qué delitos binarios? y no informáticos, cibernéticos o electrónicos

Diversas propuestas han existido, para reformar los ordenamientos punitivos tanto de los estados como el federal, a fin de establecer un capítulo que pueda dar cobertura jurídica y protección a los bienes jurídicamente tutelados que se pudieran vulnerar mediante las nuevas tecnologías y las cuales se han ido fortaleciendo con base en postulados tales como los que corren a cargo de los siguientes autores:

Carlos Sarzana, en su obra Criminalitá e tecnología, los crímenes por computadora comprenden "Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo"[116]

Nidia Callegari define al "delito Informático" como "aquel que se da con la ayuda de la informática o de técnicas anexas"[117]

Rafael Fernández Calvo define al "delito Informático" como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española"[118]

María de la Luz Lima dice que el "delito electrónico" "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método,

[116] SARZANA, Carlos. "Criminalita E Tecnologia – Computer Crimes, Rasegna Penitenziaria E Criminologia", Nos 1-2, Anno 1, Gennaio – Giugno, Italia, 1979. P. 59
[117]http://www.coladic-rd.org/cms/wp-content/uploads/2008/07/los_delitos_informaticos_peter_read.pdf
[118] http://www.tribunalmmm.gob.mx/tribunalm/biblioteca/almadelia/Cap3.htm

medio o fin y que, en un sentido estricto, el delito Informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin"[119]

Julio Tellez Valdes 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" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"[120]

Como podemos darnos cuenta en líneas anteriores, los autores refieren definiciones de delitos atendiendo a una naturaleza electrónica, informática, y como en el caso de nuestro país, cibernética, pero en ninguno de los conceptos, estamos hablando de un verdadero campo de estudio que alcance siquiera a comprender todo lo que los delitos relacionados con las nuevas tecnologías infiere.

Para empezar, se analizará, que se entiende en cada concepto que antecede a los delitos que se vienen refiriendo.

Electrónica:

La electrónica es el campo de la física que se refiere al diseño y aplicación de dispositivos, por lo general circuitos electrónicos, cuyo funcionamiento depende del flujo de electrones para la generación, transmisión, recepción o almacenamiento de información. Esta información puede consistir en voz o música como en un receptor de radio, en una imagen en una pantalla de televisión, o en datos como una computadora. La electrónica como tal tiene una gran variedad de aplicaciones para la vida del hombre, como por ejemplo: las

[119] http://www.aadat.org/delitos_informaticos20.htm
[120] http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml

telecomunicaciones, la computación, la medicina, la mecánica entre otras[121].

Como se advierte de esta simple definición, la electrónica, es un campo que involucra los aparatos *per se*, por los cuales se podrían cometer los delitos, pero no involucra la realidad virtual que vivimos, es decir, cuando estamos en internet, lógicamente accedamos mediante un ordenador, pero una vez en el ciberespacio, se atiende a un leguaje que va más allá de la electrónica, es decir un leguaje binario, que rebasa el aspecto de la electrónica y pasa a un plano constituido por unos y ceros, que debe ser regulado jurídicamente y cuando un delincuente comete un delito haciendo uso de las nuevas tecnologías, no lo hace apoyándose en sus conocimientos sobre la electrónica, lo hace apoyándose en sus conocimientos sobre la utilización de las nuevas tecnologías, el cual solo puede manifestarse mediante el código binario, que es el lenguaje que las nuevas tecnologías entienden para traducir los actos de individuo, en funciones que afectan el ciberespacio u otros sistemas lógicos. Por tanto no es recomendable o suficiente hablar de delitos electrónicos.

Informática:

La informática es la ciencia que tiene como objetivo estudiar el tratamiento automático de la información a través de la computadora. Esta definición, si bien es bastante amplia, se debe a que el concepto de informática también es amplio. Para referirse a esta ciencia, también suele utilizarse el término Computación o Ciencia de la Computación, con la diferencia de orígenes. En cuanto al contenido de la Informática, se encarga de estudiar todo lo relacionado con las computadoras que incluye desde los aspectos de su arquitectura y fabricación hasta los aspectos referidos a la organización y almacenamiento de la

[121] http://www.viasatelital.com/proyectos_electronicos/definicion_electronica.htm

información. Incluso contiene las cuestiones relacionadas con la robótica y la inteligencia artificial[122].

Si se analiza el concepto de Informática, se puede aludir que, se va a un plano que involucra el tratamiento de la información mediante las computadoras, e incluso todo lo relacionado con estas, y se aterriza únicamente en lo concerniente al comportamiento del individuo respecto a esas computadoras o centro de almacenamiento de información, por tanto, cuando se habla de delitos informáticos, se infiere que son aquellos que el individuo comente con relación a las computadoras o a la información que se pudiera almacenar dentro de las mismas, pero no infiere, dada la naturaleza y alcances del concepto, el análisis de las conductas delictivas realizadas mediante las nuevas tecnologías y la internet, que solo son posibles mediante el código binario, es decir, un mensaje amenazador por celular, sería un delito binario, pero no está al alcance del campo de estudio de la informática, porque no se está vulnerando ningún ordenador o sistema de datos lógico, por tanto, se entiende que la única manera de conectar los actos del individuo con los ordenadores, las nuevas tecnologías y el ciberespacio, es el código binario, el cuál se utiliza cuando hacemos uso de las nuevas tecnologías, previo conocimiento sobre la utilización de las mismas.

Es decir, el comportamiento del individuo, verbigracia en el ciberespacio, que se logra mediante el código binario, es un aspecto que rebasa a la informática, porque no se está vulnerando un sistema lógico o de información digital, se utiliza el código binario para delinquir y si bien es cierto el código binario es objeto de estudio de la informática, no menos cierto es que el referido código, es lo que le permite a la informática su desarrollo, por tanto, tiende a ser este código la herramienta que tiene la informática para existir y por tanto se advierte como un concepto más amplio y adecuado para los delitos que

[122] http://www.mastermagazine.info/termino/5368.php

involucran las nuevas tecnologías tales como los delitos binarios y es en este sentido que tampoco se recomienda el término delitos informáticos.

Cibernética

La Cibernética es la ciencia que se ocupa de los sistemas de control y de comunicación en las personas y en las máquinas, estudiando y aprovechando todos sus aspectos y mecanismos comunes. El nacimiento de la cibernética se estableció en el año 1942, Norbert Wiener uno de los principales fundadores de esta ciencia, propuso el nombre de cibernética, derivado de una palabra griega que puede traducirse como piloto, timonel o regulador. Dentro del campo de la cibernética se incluyen las grandes máquinas calculadoras y toda clase de mecanismos o procesos de autocontrol semejantes y las máquinas que imitan la vida[123]

Los alcances del campo de estudio de la cibernética son muy amplios y van enfocados a establecer el comportamiento de las maquinas, alineado a imitar la vida humana, perfeccionarla y por supuesto facilitarla, pero indudablemente está fuera del alcance de los aspectos que interesan como disciplina de estudio que podría definir los delitos que involucran las nuevas tecnologías, puesto que, si bien es cierto, la cibernética involucra el estudio de la inteligencia artificial, que es la que da vida a los delitos que se tratan de conceptualizar, no menos cierto es que esta disciplina requiere como hilo conductor entre el hombre y la máquina, al código binario, es decir, actualmente las nuevas tecnologías están basadas en inteligencia artificial, pero hasta el momento, ésta se encuentra supeditada a la voluntad del hombre, quien brinda las instrucciones que se traducirán en actos que las máquinas realizan y la única manera en que estas instrucciones pueden ser entendidas por el ordenador, son mediante el código

[123] http://robothumano.galeon.com/productos774285.html

binario, por tanto, los delitos cibernéticos, son un concepto que quedaría cubierto por el ámbito de estudio de los delitos binarios, siendo este último el único hilo conductor entre la cibernética y el delincuente, por tanto, el concepto de delitos cibernéticos, quedaría superado y por ende, tampoco se recomienda.

Retomando lo establecido en capítulos anteriores, el Derecho Binario, es la rama del derecho que se encarga del estudio de las normas que regulan la relación entre los individuos y de ellos con su entorno social, basada en las nuevas tecnologías y la Internet.

Del ámbito de estudio anterior, se puede decir que, los Delitos Binarios, son aquellos delitos tradicionales cometidos con el uso de las nuevas tecnologías y/o el Internet, como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante, para la comisión del acto antijurídico, antisocial, típico, culpable y punible.

La comisión a la que se refiere la definición anterior, puede ser por acción, o por omisión, asimismo, al hablar de delitos tradicionales, nos referimos a los delitos tipificados como tales en los ordenamientos punitivos vigentes.

De igual forma, cuando se habla del uso de las nuevas tecnologías y el Internet, nos referimos a tres perspectivas de los Delitos Binarios: como un medio o canal para cometer el acto delictivo, como el objetivo o finalidad del acto delictivo y como el soporte o coadyuvante del acto delictivo.

Por todo lo anterior, es necesario establecer que el concepto que abarcaría todos los supuestos que pudieran ser objeto de la comisión de algún delito mediante las nuevas tecnologías y el internet, es el de Delitos Binarios.

5.2. Propuesta de reforma al Código Penal del Estado de Veracruz

La reforma que se plantea, es con relación al Capítulo III del Código Penal vigente en Veracruz, que actualmente dice:

CAPÍTULO III
DELITOS INFORMÁTICOS

Artículo 181.- Comete delito informático quien, sin derecho y con perjuicio de tercero:

I. Ingrese en una base de datos, sistema o red de computadoras para obtener, conocer, utilizar, alterar o reproducir la información, en ellos contenida; o

II. Intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático o la información contenida en el mismo o en la base, sistema o red.

Al responsable de este delito se le impondrán de seis meses a dos años de prisión y multa hasta de trescientos días de salario. Si se cometiere con fines de lucro las penas se incrementarán en una mitad.

La reforma que se plantea quedaría de la siguiente manera:

TÍTULO V
DELITOS BINARIOS

CAPÍTULO I
CONSIDERACIONES PRELIMINARES DE ESTE TÍTULO

Por delito binario, se entenderá, la comisión de un acto antijurídico, antisocial, típico, culpable y punible basado en los delitos tradicionales o independientes de estos, cometidos con el uso de las nuevas tecnologías y/o el Internet, como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante, pudiendo causar una afectación o no, a la propiedad y/o posesión binaria de que se trate, por tanto:

Se entenderá por delitos binarios basados en los delitos tradicionales, la comisión de un delito ya previsto por este código, cometido con el uso de las nuevas tecnologías y/o el Internet, como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante.

Se entenderá por delitos binarios independientes de otros delitos, la comisión de un delito que no se basa en uno tradicional, pero contemplado en el presente título, cometido con el uso de las nuevas tecnologías y/o el Internet, como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante, pudiendo causar o no una afectación a la propiedad y/o posesión binaria.

Se entenderá por delito binario en perjuicio de la propiedad y/o posesión binaria, la comisión de un acto que cause una afectación a las mismas.

La comisión a la que se refiere este título, puede ser por acción, o por omisión y cuando se habla de delitos tradicionales, se hace referencia a los delitos tipificados como tales en éste código.

Por nuevas tecnologías se entenderán los últimos desarrollos tecnológicos y sus aplicaciones.

Para efectos del presente título, se entenderá el uso de las nuevas tecnologías y el internet, como un medio o canal para cometer el acto delictivo, cuando se utilicen las mismas, como conductor entre el sujeto activo y el sujeto pasivo del delito tradicional.

Se entenderá el uso de las nuevas tecnologías y el internet, como el objetivo o finalidad del acto delictivo, cuando se utilicen las mismas, como el receptor de la actualización del tipo penal que se configure.

Para efectos del presente título, se entenderá el uso de las nuevas tecnologías y el internet, como soporte o coadyuvante del acto delictivo, cuando se utilicen las mismas, como apoyo para la consumación del acto ilícito sin ser necesariamente un medio o la finalidad.

Para efectos de este título, por propiedad binaria, se entiende, el derecho que se tiene de uso, goce, usufructo y disfrute sobre bases de datos, sistemas de red, carpetas de información, archivos, programas, cuentas de correo electrónico, cuentas de redes sociales, sitios de internet, espacios virtuales y toda aquella información digital o sitios digitales, resguardados en el ciberespacio o en algún medio de almacenamiento, sin que necesariamente se tenga la posesión de las mismas.

Por posesión binaria, se entiende el derecho que se tiene de uso, goce, usufructo y disfrute sobre bases de datos, sistemas de red, carpetas de información, archivos, programas, cuentas de correo electrónico,

cuentas de redes sociales, sitios de internet, espacios virtuales y toda aquella información digital o sitios digitales, resguardados en el ciberespacio o en algún medio de almacenamiento, sin que necesariamente se acredite la propiedad de las mismas.

Para efectos de este título, se entenderá como afectación a la propiedad binaria, la alteración, daño, modificación, uso sin autorización, reconfiguración, desconfiguración, intrusión no autorizada, interceptación, y/o todo aquello que tienda al deterioro y/o aprovechamiento y/o difusión indebida de la propiedad binaria.

También se entenderá como afectación a la posesión binaria, la restricción del acceso que haga una o mas personas en un sitio virtual, base de datos, archivo, carpeta y/o sistema operativo ubicado en internet o en un ordenador o sistema de computo, a quien tenga derecho para tener dicho acceso.

CAPÍTULO II
DELITOS BINARIOS
BASADOS EN LOS DELITOS TRADICIONALES

Artículo 181.- A quien cometa un delito de los ya previstos por este código, con el uso de las nuevas tecnologías y/o el Internet, como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante, serán sancionado con la pena prevista por el delito tradicional del que se trate, incrementándose hasta en una mitad.

CAPÍTULO III
DELITOS BINARIOS EN PERJUICIO DE
LA PROPIEDAD Y LA POSESIÓN BINARIA

Artículo 181 Bis.- A quien cometa un acto que cause una afectación a la propiedad y/o posesión binaria, se le impondrán de seis meses a

doce años de prisión y multa hasta de trescientos días de salario.

Si la afectación a la que se refiere este título, es con ánimo de lucro y/o en perjuicio de terceros, las penas previstas en el párrafo anterior, se incrementarán hasta en una mitad.

CAPÍTULO IV
DELITOS BINARIOS
INDEPENDIENTES DE OTROS DELITOS

Artículo 181 Ter.- Se impondrán de seis meses a doce años de prisión y multa hasta de trescientos días de salario al que actualice alguno de los siguientes supuestos:

I.- Recolección no autorizada de datos.- Comete este delito binario, quien, con cualquier fin y sin autorización de quien deba otorgarla, desarrolle, utilice, adquiera o propague, en cualquier sistema operativo conectado a un sistema de red interna o a la internet, un software que recolecte información ubicada en dicho sistema operativo o en cualquier otro.

II.- Instalación no autorizada de software.- Comete este delito binario, quien sin autorización de quien deba otorgarla e independientemente del fin, instale cualquier tipo de software o descargue algún tipo de archivo en un ordenador, sistema operativo o sistema lógico de cómputo.

III.- Almacenamiento no autorizado de información.- Comete este delito binario quien, sin contar con autorización de quien debiera otorgarla, almacene, en algún tipo de medio de almacenamiento o en internet, cualquier tipo de información digital.

IV.- Suplantación de identidad.- Comete este delito binario quien, con

el animo de recolectar datos, independientemente del fin, hospede en internet un dominio igual o similar a otro con las diferencias suficientes en el nombre del sitio para generar en los cibernautas la creencia de que se encuentran en el sitio original, propiciando que de manera voluntaria el sujeto pasivo otorgue sus datos o revele información.

También comete este delito, quien con autorización o sin ella, ingrese a una cuenta de correo electrónico, pagina web, cuenta de red social, o cualquier sitio web, realizando actos a nombre de quien tenga el derecho sobre las mismas, siempre que dichos actos causen una afectación al sujeto pasivo y/o un beneficio al sujeto activo de este delito.

V.- Secuestro de cuentas de correo, sitios web y redes sociales.- Comete este delito, quien, con autorización de quien deba darla o sin ella, ingrese a una cuenta de correo electrónico, sitio web o red social y cambie la contraseña o código de acceso, generando que quien tenga derecho a ingresar quede impedido de hacerlo.

VI.- Implantación de Software o archivo malicioso.- Comete este delito binario quien, mediante algún tipo de medio de almacenamiento digital, memoria USB, o mediante una transferencia de datos digitales, instale, propague, difunda o haga circular, en un ordenador, sistema lógico de computo, en el internet o en una red interna, un virus, un software o archivo que, al ser abierto, o al ser instalado, implante un virus digital en un ordenador, sistema operativo, base de datos o sistema lógico de computo.

VII.- Neutralización de seguridad y antivirus.- Comete este delito binario quien, sin autorización de quien deba darla, por medio de internet o directamente en un ordenador, sistema operativo o sistema lógico de computo, desactive un antivirus, una pared de fuego o cualquier sistema de seguridad que se encuentre activado.

VIII.- Implantación de archivos espías.- Comete este delito binario, quien envíe mediante internet o instale directamente un archivo espía en un ordenador, sistema operativo o sistema lógico de computo, con el fin de conocer todo aquello que acontezca en los mismos.

IX.- Manipulación de ordenadores o programas.- Comete este delito binario, quien mediante un ordenador, sistema operativo o sistema lógico de cómputo, manipule, configure, desconfigure, altere, utilice o modifique un ordenador, sistema operativo o sistema lógico de cómputo, inhabilitando el uso de quien tenga derecho a hacerlo.

X.- Transferencia de correos electrónicos basura.- Comete este delito binario, quien de manera reiterada, mande correos electrónicos a través de la internet, a uno o mas destinatarios, cuyos contenidos, sean cadenas, publicidades u otros considerados perjudiciales o improductivos para el usuario, con el fin de causar una afectación a los destinatarios. Este delito se perseguirá por querella de parte.

Si la afectación a la que se refiere este título, es con ánimo de lucro y/o en perjuicio de terceros, las penas previstas en este artículo, se incrementarán hasta en una mitad.

CAPÍTULO V
CONSIDERACIONES RELATIVAS A LOS DELITOS BINARIOS

Los delitos binarios, se actualizan independientemente de que causen una afectación o no, pero en caso de existir, la reparación del daño se basará en el daño ocasionado o las consecuencias que traiga consigo la perdida de la información, los archivos, programas o cualquier daño lógico del que se trate.

Al sujeto activo del delito binario basado en los delitos tradicionales, se

le aplicará la pena a la que haya lugar según lo establecido por este título, sin que proceda aplicarle adicionalmente la pena que el delito tradicional de origen contemple.

Al sujeto activo del delito binario independiente de otros delitos, se le aplicará la pena a la que haya lugar, independientemente de la sanción que pudiera existir, en caso de actualizarse alguna otra conducta delictiva prevista por este código.

5.3. Cuestiones anexas a la reforma

La reforma que se viene planteando, involucra necesariamente una trasformación de la visión que actualmente se tiene sobre los delitos y se debe comenzar a entender que estamos en medio de una evolución sin precedentes, que requiere adaptar las leyes a las nuevas necesidades que enfrentamos y evidentemente la era digital, es el principal reto.

Asimismo, esta reforma, requiere el establecimiento de nuevas leyes que permitan la salvaguarda de la propiedad binaria y de la realidad virtual, puesto que actualmente, no existen mecanismos jurídicos de salvaguarda para ello.

Requiere también, el reconocimiento por parte de los doctrinarios, de nuevas normas que rebasan lo establecido por Eduardo García Máynez entre otros juristas destacados, quien establecía la existencia de normas jurídicas, morales, religiosas, de trato social y técnicas, pero ahora, debemos incorporar las normas binarias.

Las normas binarias, son aquellas que regulan la conducta del individuo y de él con otros individuos en la realidad virtual.

Ya en capítulos anteriores, hemos establecido que es la realidad virtual, entendiendo por ésta, una realidad que vivimos a la par de nuestra realidad material, intangible y transportable, basada en un código binario y en muchos casos es una realidad en la que interactuamos la mayor parte de nuestro tiempo y refiere aquella donde realizamos todas nuestras actividades sociales, familiares, emocionales, laborales, de recreación, entre otras, mediante las nuevas tecnologías y la Internet.

Por lo anterior, una de las cuestiones que deben de surgir con la reforma propuesta, es la regulación de la realidad virtual mediante normas binarias, ya que no es posible tutelar nada en el ciberespacio y para muestra nos podemos remitir a los siguientes ejemplos:

Una cuenta de correo electrónico, nos atrevemos a decir que es nuestra, pero ¿cómo acreditamos la propiedad de la misma?, si alguien vulnera nuestra cuenta e ingresa de forma ilegal a ella hackeandola, además de la intrusión no autorizada a sistemas lógicos de los que hablan los delitos informáticos, pero ¿por qué no autorizada?... también debemos tener presente que se está invadiendo la privacidad y se está allanando un espacio virtual, pero todo lo anterior, no es posible acreditarlo si no es posible primero acreditar la propiedad de la cuenta o la posesión siquiera.

De quien es propiedad la información que se sube al ciberespacio, es decir, si subo una fotografía y alguien la toma, y yo no lo autorizó, ¿puedo exigir jurídicamente algo?, la verdad es que no, porque sabido es por los cibernautas, que lo que se sube a internet sin las precauciones de los derechos de autor, se vuelve del dominio público, pero esto ¿Quién lo estableció?

Cuáles son las políticas de navegación que debemos observar o que pasa si alguna página, mediante engaños, me hace descargar un virus perjudicial a mi máquina, que puedo hacer jurídicamente hablando, si

los virus no son otra cosa que programas diseñados para causar afectaciones lógicas. ¿Puedo proceder por daños? Que dice el tipo penal de daños en Veracruz:

Artículo 226.- A quien, en perjuicio de tercero, por cualquier medio destruya o deteriore una cosa, total o parcialmente ajena o propia, se le impondrán de seis meses a ocho años de prisión y multa hasta de ciento cincuenta días de salario.
Este delito se perseguirá por querella. (Reformado, primer párrafo; g.o. 24 de agosto de 2004)

Artículo 227.- Si el daño se ocasiona con motivo del tránsito de vehículos y el conductor se hallare en estado de ebriedad o bajo el influjo de estupefacientes u otras sustancias tóxicas, se sancionará con prisión de tres a nueve años, multa hasta de trescientos días de salario y suspensión del derecho para conducir vehículos hasta por tres años. Esta conducta se perseguirá de oficio.

Artículo 228.-La prisión podrá aumentarse hasta diez años y la multa hasta trescientos días de salario, si el daño recae en bienes de valor científico, artístico, cultural o de utilidad pública.

En el tipo penal descrito con antelación, se habla de la destrucción o deterioro de una cosa total o parcialmente ajena… para empezar, regresamos al problema de la acreditación de la propiedad, pero también nos enfrentamos al problema de la definición de cosa, puesto que cosa, jurídicamente hablando, puede ser un bien, una obligación o un derecho, pero si hablamos de bien, ¿cómo establecemos que tipo de bien?

Para efectos de la presente investigación se deben acuñar también como parte de la clasificaron a los bienes binarios, que no son ni los bienes incorpóreos, ni los intangibles, puesto que estos dos últimos,

hacen referencia a la realidad material mientras que el primero de los mencionados, hace referencia a la realidad virtual.

Pero esto que se comenta en el presente apartado, no es ni la punta del iceberg de lo que se tiene que enfrentar en tratándose del Derecho binario, puesto que el ciberespacio involucra infinidad de nuevos retos que solo se podrán ir subsanando con el trascurso de la actual evolución.

Finalmente nos permitimos presentar en este apartado, algunas medidas que pudieran mejorar algunos de los problemas más comunes jurídicamente hablando, con respecto al ciberespacio.

- Implementar como forma de acceso al correo electrónico u otras páginas de internet la huella digital para efectos de identificar al usuario sin lugar dudas.
- En páginas para adultos, solicitar el número de folio de la credencial de elector para acreditar la mayoría de edad de los visitantes
- Establecer una cuenta de correo electrónico oficial por cada ciudadano, de un servidor de gobierno, para un mayor control y diversos usos tales como las notificaciones personales.
- Establecimiento de una división política y por ende de competencia por naciones en el ciberespacio.
- La creación de un registro nacional de cibernautas
- La creación de una base de datos nacional de páginas de internet con registro de los que tiene derechos sobre los respectivos dominios y hospedajes.

Somos conscientes en la presente investigación que las recomendaciones aquí expresadas, son complicadas de llevarse a la práctica, pero de hacerse, tenderían a mejorar las conductas del individuo en el ciberespacio.

5.4. Expectativas de la reforma

La reforma tiene las expectativas de que se tienda a mejorar la persecución de los delitos binarios, actualmente conocidos como informáticos y cibernéticos.

Pero esto involucra, capacitación al personal encargado de la procuración de justicia mediante programas de mejora continua, además involucra también la creación de agencias especializadas en delitos binarios, puesto que como ya ha quedado demostrado en capítulos anteriores, los que se encuentran al frente del aparato de administración de justicia en el Estado, manifiestan que es necesario que se establezca personal especializado para la atención a este tipo de delitos.

También involucra, que en las universidades preparen a los estudiantes ante los retos jurídicos que involucran las nuevas tecnologías y el internet, pues prácticamente todas las disciplinas de estudio que se desprenden de la ciencia del derecho, son objeto de las nuevas tecnologías y la internet, por ejemplo, en el ámbito del comercio, tenemos el comercio tradicional y el comercio electrónico, en el ámbito civil, tenemos los contratos tradicionales y los contratos electrónicos revestidos de una firma electrónica, en el ámbito fiscal, tenemos incorporado el pago de impuestos por internet, en el ámbito bancario tenemos las trasferencias electrónicas y en suma, prácticamente en todas las ramas del derecho es posible la incorporación del enfoque de nuevas tecnologías y el internet, y todo esto es campo de estudio del derecho binario.

Por lo anterior, se espera que la reforma, traiga consigo el reconocimiento de una nueva rama del derecho como lo es el derecho binario y que consecuencia de esto se mejoren los mecanismos

jurídicos de protección para los derechos binarios, siendo estos últimos aquellos inherentes al individuo en el ciberespacio.

5.5. Consideraciones finales de éste capítulo

Se demostró que el término adecuado para vislumbrar el campo de acción que infieren los delitos que involucran las nuevas tecnologías y la internet es el de Delitos Binarios, toda vez que abarca toda la actividad humana, tendiente a delinquir, relacionada con las nuevas tecnologías y el internet.

Se estableció una reforma que logra cubrir con todos los supuestos delictivos que se pudieran actualizar, con el uso de las nuevas tecnologías y el Internet.

Se argumentó que anexo a la reforma, se requieren otras reformas que tutelen los derechos en la realidad virtual tales como los que involucran la propiedad binaria, que se alberga en las redes, bases de datos y el propio ciberespacio.

Se demostró que es necesaria la incorporación de una nueva rama del derecho denominada Derecho Binario, la cual trae como campo de estudio todo el orden jurídico tendiente a regular al individuo con relación a su entorno y a otros individuos, basado en las nuevas tecnologías y el internet.

CONCLUSIONES GENERALES

Finalmente, se arriba a las siguientes conclusiones generales que son producto del desarrollo de esta investigación:

- Se demostró que en el Estado de Veracruz, no se contempla el tipo penal de delitos cibernéticos, sino únicamente el tipo penal de delitos informáticos, lo cual quedó acreditado en el Capítulo II de la presente investigación, al analizar el Código Penal del Estado de Veracruz y de las respuestas que brindaron en las encuestas el personal de las dependencias procuradoras de justicia del estado, quienes afirmaron que no se contempla el tipo penal de delitos cibernéticos, sino únicamente el tipo penal de delitos informáticos.

- Se demostró que los delitos cibernéticos si están reconocidos de hecho por las autoridades procuradoras de justicia estatal y federal, así como por las corporaciones policiacas federales, lo cual quedó acreditado en el Capítulo II de la presente investigación, al establecer los datos presentados en la campaña nacional de prevención contra el delito cibernético y de las respuestas que brindaron en las encuestas el personal de las dependencias procuradoras de justicia del estado, quienes afirmaron que hay un reconocimiento de hecho de los delitos cibernéticos mas no de derecho.

- Se demostró que existe desconocimiento, por parte de las autoridades procuradoras de justicia en el Estado, sobre los delitos informáticos y los delitos cibernéticos, lo cual quedó acreditado en el Capítulo II de la presente investigación, al presentar las respuestas que brindaron en las encuestas el personal de las dependencias procuradoras de justicia del

estado, quienes no pudieron expresar una definición o idea que se asemejara lo que son los delitos informáticos y cibernéticos.

- Se demostró que las autoridades procuradoras de justicia en el Estado, confunden los delitos informáticos y los delitos cibernéticos, lo cual quedó acreditado en el Capítulo II de la presente investigación, al presentar las respuestas que brindaron en las encuestas el personal de las dependencias procuradoras de justicia del estado, quienes no pudieron expresar la diferencia que existe entre los delitos informáticos y cibernéticos e incluso en muchos casos expresando que son lo mismo.

- Se conoció la labor de persecución de los delitos cibernéticos, lo cual quedó acreditado en el Capítulo I de la presente investigación, estableciendo la descripción de casos prácticos que refieren el desarrollo de las investigaciones ministeriales en tratándose de diversos delitos incluyendo los delitos informáticos y cibernéticos.

- Se analizaron las respuestas de las autoridades procuradoras de justicia con relación a la persecución de los delitos cibernéticos, lo cual quedó acreditado en el Capítulo II de la presente investigación; dichas respuestas se presentaron de forma ordenada y sistematizada en tablas y gráficas que permitieron el análisis y argumentación de los contenidos que se presentan en esta investigación.

- Se compararon las legislaciones de diferentes países de todo el mundo y las legislaciones de los Estados y el Distrito Federal que integran nuestro país, con relación a la contemplación de los delitos informáticos y cibernéticos, lo cual quedó acreditado en el Capítulo III de la presente investigación, determinando que

países tales como Austria, Chile, China, España, Estados Unidos, Francia, Holanda e Inglaterra, incluyen dentro de sus ordenamientos punitivos el reconocimiento de los delitos informáticos y cibernéticos y en lo que respecta a México, se demostró que todos los Códigos Penales del país, incluyen dentro de sus tipos penales la comisión de delitos mediante las nuevas tecnologías y la internet, todo lo anterior mediante el análisis de los diversos ordenamientos punitivos de cada Estado en nuestro país, el Distrito Federal y de los países antes mencionados.

- Se estableció una nueva rama del derecho que permitirá el estudio del ámbito digital, informático y cibernético, desde una perspectiva jurídica, lo cual quedó acreditado en el Capítulo IV de la presente investigación, estableciendo que, el Derecho Binario, es una nueva rama del derecho, que es necesario reconocer y comenzar a estudiar, puesto que su campo de estudio, involucra un nuevo mundo, el mundo digital, la realidad virtual, de los cuales actualmente sólo podemos ver una reminiscencia, pero que en pocos años, será lo más estudiado del derecho.

- Se propuso una reforma al Código Penal Estatal, para la inclusión de los delitos binarios, lo cual quedó acreditado en el Capítulo V de la presente investigación, estableciendo que el término adecuado para vislumbrar el campo de acción que infieren los delitos que involucran las nuevas tecnologías y la internet es el de Delitos Binarios, toda vez que abarca toda la actividad humana, tendiente a delinquir, relacionada con las nuevas tecnologías y el internet.

REFERENCIAS BIBLIOGRÁFICAS

AMUCHATEGUI REQUENA, Irma Griselda, Derecho Penal, 3ª edición, Oxford, México, 2009

ARROYO GUTIÉRREZ, José Manuel, Teoría de la Pena, La Ejecución Penal en: Reflexiones sobre el nuevo Proceso, Editorial Tecnos, Madrid, 2005.

BECERRA RAMÍREZ, Manuel, La propiedad intelectual en transformación, IIJ-UNAM, México, 2004

BEUCHOT, Mauricio, Derechos humanos, Iuspositivismo y Iusnaturalismo, Editorial UNAM, México 1995.

BOBBIO, Norberto, Contribución a la Teoría del Derecho, Ciencia del Derecho y Análisis del Lenguaje, Editorial Combate, Madrid España 1990.

BOBBIO, Norberto, Justicia, validez y eficacia, Teoría general del derecho, Debate, Madrid 1990.

BOBBIO, Norberto, Teoría general del Derecho, Editorial Temis, Bogotá 1997.

BRIESKORN, Norbert, “Filosofía del Derecho”, Editorial Herder, Barcelona 1993.

CARRANZA LUCERO, Elías, Criminalidad: ¿Prevención o promoción?, Editorial EUNED, 3ª Edición, San José de Costa Rica, 2001

CASTELLANOS, Fernando, Lineamientos elementales del Derecho Penal, Editorial Porrúa, México, 2008.

CISNEROS FARÍAS, Germán, Teoría del Derecho, 2da edición, Editorial Trillas, México 2000.

Conocimiento e Innovación en México: Hacia una Política de Estado; Elementos para el Plan Nacional de Desarrollo y el Programa de Gobierno 2006-2012, Ed. Foro Consultivo Científico y Tecnológico, A.C., México 2006.

DE LA TORRE, José María, *Filosofía Cristiana,* Editorial Palabra, Madrid 1982.

DE PINA, Rafael, DE PINA VARA, Rafae, "Diccionario de Derecho", Editorial Porrua, México 1965.

DÍAZ, Elías, Sentido actual de la concepción normativa del derecho, Sociología y filosofía del derecho, Taurus, Madrid, 1971.

DWORKIN, R.M. (Compilador), Filosofía del Derecho. trad. J. Saínz, col. Breviarios, Fondo de Cultura Económica, México, 1998.

ESQUIVEL PÉREZ, Javier y Coautores, Formalismo y realismo en la teoría del derecho, UNAM, México 1980.

FERNÁNDEZ CARRASQUILLA, Juan, Concepto y límites del Derecho de Penal, Editorial Temis, Colombia, 1993.

GARCÍA HUIDOBRO, Joaquín, Filosofía y retórica del iusnaturalismo, Editorial UNAM, México 2002.

GARCÍA MAYNES, Eduardo, Positivismo jurídico, realismo sociológico y iusnaturalismo, Editorial UNAM, México 1986.

GARCÍA MÁYNEZ, Eduardo, "Filosofía del Derecho", Editorial Porrua, Sexta Edición, México 1989.

GARCÍA MÁYNEZ, Eduardo, Introducción al Estudio del Derecho, 60ª Edición, Porrúa, México, 2008.

GARCÍA-PABLOS DE MOLINA, Antonio, Criminología, Una Introducción a sus fundamentos teóricos, Editorial Tirant Lo Blanch. 5ª Edición, Barcelona, España, 2005.

GÓNGORA PIMENTEL, Génaro David, Derecho penal mexicano, Editorial Porrúa. 4ª Edición, México, 2003.

GUTIÉRREZ GARCÍA, José Luis, *Introducción a la Doctrina Social de la Iglesia,* Editorial Ariel, Barcelona 2001.

GUTIÉRREZ, Miguel Ángel, "La Globalización del Conocimiento" y "Exportación de Servicios Universitarios", Universidad de Buenos Aires, Buenos Aires, 1999.

HERNÁNDEZ SAMPIERI, Roberto, FERNÁNDEZ-COLLADO, Carlos y BAPTISTA LUCIO, Pilar, Metodología de la Investigación. 4ª edición, Mc Graw Hill, México, 2006.

INSTITUTO DE INVESTIGACIONES JURÍDICAS DE LA UNAM, Diccionario Jurídico Mexicano, Editorial UNAM-Porrua, México 1982

KANT, Immanuel, Crítica de la razón pura, Tomo II, Editorial Losada, Buenos Aires 1960.

KAPLAN, Marcos, Ciencia, Estado y Derecho en la Tercera Revolución, UNAM, México, 2000.

KAUFMANN, Arthur, Filosofía del Derecho, Editorial Universidad Extermado de Colombia, Colombia, 1999.

KELSEN, Hans, Teoría General del Derecho y del Estado, Editorial UNAM, México 1988.

MARX, Carlos y ENGELS, Federico, “Manifiesto Comunista”, Editorial Ciencias Sociales, Instituto cubano del libro, La Habana, 1971.

MEDINA, Rangel, Derecho intelectual, México, McGraw-Hill-UNAM, Instituto de Investigaciones Jurídicas, 1998, colección Panorama del Derecho Mexicano.

OCHOA SÁNCHEZ, Miguel Ángel, VALDÉS MARTÍNEZ, Jacinto, VEYTIA PALOMINO, Hernany, Derecho Positivo Mexicano, 2a Ed., Editorial McGrawHill, México 2002.

ORTIZ SÁNCHEZ, Leonides, México y la Propiedad Intelectual, Ed. Convergencia, Partido Político Nacional, México 2006.

OSORIO Y NIETO, César Augusto, Derecho Penal, 4ª edición, Trillas. México, 2002

PAVÓN VASCONCELOS, Francisco, Derecho Penal Mexicano, 20ª edición, Porrúa, México 2008.

PAVÓN VASCONCELOS, Francisco, Manual de Derecho Penal Mexicano, Parte General, Editorial Porrúa, México, 2004.

PRECIADO HERNÁNDEZ, Rafael, Lecciones de filosofía del derecho, UNAM, México 1984.

PUY, Francisco, Derechos Humanos, Derechos Políticos, Vol. 3, Editorial Paredes, Santiago de Compostela 1983.

REALE, Miguel, Filosofia do Directo, Saraiva, São Paulo 1962.

REALE, Miguel, Introducción al Derecho, Sexta edición, Ediciones Pirámide S.A., Madrid 1984.

REALE, Miguel, Teoría Tridimensional do Directo, Editorial Saraiva, São Paulo 1968.

RECASÉNS SICHES, Luis, Introducción al estudio del derecho, Porrúa, México 1985.

RECASENS SICHES, Luís, La Filosofía del Derecho de Francisco Suárez, Editorial IUS, México 1947.

RECASÉNS SICHES, Luis, Tratado general de filosofía del derecho, Porrúa, México 1991.

ROA, Consuelo L., La OMPI y la propiedad intelectual en Internet, Enero 2006, www.mati.unam.mx.

ROJAS AMANDI, Víctor Manuel, Filosofía del Derecho, Editorial Oxford, México 2005.

ROSS, Alf, On Law and Justice, Editorial University of California, Berkeley 1959.

ROUSSEAU, Jean-Jacques, El Contrato Social, Altaya, Madrid 1992.

SANZ MORÁN, Ángel José, Teorías de la pena y límites al ius puniendi desde el Estado democrático, Editorial Dykinson, España, 2006.

SQUELLA, Agustín, Positivismo jurídico, Democracia y Derechos Humanos, Fontamara, México 1998.

TÉLLEZ VALDÉS, Julio, Derecho informático, UNAM, México, 1991

TERÁN, Juan Manuel, Filosofía del Derecho, 17 edición, Editorial Porrua, México, 2003.

TORAL, Pedro Carrillo, El Derecho Intelectual en México, Ed. Plaza y Valdés, México, 2002.

VASCONCELOS, José, Teoría dinámica del derecho, Libreros Mexicanos Unidos, México 1957.

VILLORO Luis, Creer, saber, conocer, Siglo XXI, México, 2004

VILLORO TORANZO, Miguel, Introducción al Estudio del Derecho, Porrúa, México, 2002

ZAFFARONI EUGENIO, Raúl, Derecho Penal. 2ª edición, Porrúa, México, 2005.

LEGISGRAFÍA, INTERNETGRAFÍA Y HEMEROGRAFÍA

Revista de Derecho Privado, nueva época, año II, núm. 6, septiembre-diciembre de 2003.

Organización Mundial de la Propiedad Intelectual, http://www2.medioambiente.gov.ar/acuerdos/organismos/onu/Ompi/InfGral.htm, Agosto 2008.

Acuerdo Nacional Contra la Piratería, http://pirateria.pgr.gob.mx/Docs/Acuerdo%20Nacional%20VS.%20Piratería.pdf.

DELGADO RODRÍGUEZ, Margarita, Plagio de la Información, 2007, http://infoetica.blogspot.com/2007/03/blog-post.html.

Ley de Propiedad Industrial, vigente en México

Ley Federal de Derechos de Autor, vigente en México
RADBRUCH, Gustav, “El fin del derecho”, Primera edición cibernética, noviembre del 2004, Captura y diseño, Chantal López y Omar Cortés, en: http://www.antorcha.net/biblioteca_virtual/derecho/fin/fin.html#2

Sábado mundial contra la piratería, CNN 2008: http://www.cnnexpansion.com/actualidad/2008/04/26/sabado-mundial-de-la-antipirateria.

Redacción de: El universal, http://eluniversal.com.mx, martes 10 de julio de 2007.

http://noticias.juridicas.com/articulos/00-Generalidades/200309-42551018810342601.html, Enero 2007

http://realidadjuridica.uabc.mx/realidad/files/derechoshumanoscon.doc, p. 23, 02 de Agosto 2006.

http://usuarios.lycos.es/christianlr/01d51a93a00bc2104/01d51a93a00c2c02b.html, 14 de agosto 2006.

http://www.juridicas.unam.mx/publica/librev/rev/jurid/cont/20/pr/pr31.pdf

Mabel García, Silvana, el derecho como ciencia, Invenio, vol. 14, núm. 26, Universidad del Centro Educativo Latinoamericano, Rosario, Argentina, junio 2011

Declaración Universal de los Derechos Humanos.

Constitución Política de los Estados Unidos Mexicanos.

Legislación y Delitos Informáticos – Estados Unidos, http://www.segu-info.com.ar/delitos/francia.htm

Legislación y Delitos Informáticos – Estados Unidos, http://www.segu-info.com.ar/delitos/holanda.htm

Legislación y Delitos Informáticos – Estados Unidos, http://www.segu-info.com.ar/delitos/inglaterra.htm

Legislación y Delitos Informáticos – Estados Unidos, http://www.segu-info.com.ar/delitos/estadosunidos.htm

Legislación Penal del Estado de Querétaro

Legislación y Delitos Informáticos – Chile, http://www.segu-info.com.ar/delitos/chile.htm

Legislación y Delitos Informáticos – China, http://www.segu-info.com.ar/delitos/china.htm

Legislación y Delitos Informáticos – España, http://www.segu-info.com.ar/delitos/espania.htm

http://www.psico.uniovi.es/Dpto_Psicologia/metodos/tutor.7/p2.html

Legislación y Delitos Informáticos – Alemania, http://www.segu-info.com.ar/delitos/alemania.htm

http://www.feedbacknetworks.com/cas/experiencia/sol-preguntar-calcular.htm

http://www.infoleg.gov.ar/infolegInternet/anexos/15000-19999/16546/texact.htm,
Cosido Penal de Baja California Sur

Agregan fraude informático al Código Penal de Colima; http://www.eseguridad.gob.mx/wb2/eMex/eMex_2e98c_not969_agregan_fraud

Código de Defensa Social para el Estado Libre y Soberano de Puebla

Código Penal Alemán, López Díaz, Claudia, traductora, http://www.unifr.ch/ddp1/derechopenal/obrasjuridicas/oj_20080609_13.pdf,

Legislación y Delitos Informáticos – Austria, http://www.segu-info.com.ar/delitos/austria.htm

Código Penal de Aguas Calientes

Código Penal de Baja California Norte

Código Penal de Campeche

Código Penal de Chiapas

Código Penal de Chihuahua

Código Penal de Coahuila

Código Penal de Colima

Código Penal de Guerrero

Código Penal de Jalisco

Código Penal de la Nación Argentina

Código Penal de Morelos

Código Penal de Nuevo León

Código Penal del Estado de México

Código Penal del Estado de Oaxaca

Código Penal del Estado de Sinaloa

Código Penal del Estado de Tlaxcala

Código Penal del Estado de Veracruz

Código Penal del Estado de Yucatán

Código Penal del Estado de Zacatecas

Código Penal para el Distrito Federal

Código Penal para el Estado de San Luis Potosí

Código Penal para el Estado de Tabasco

Código Penal para el Estado de Tamaulipas

Código Penal para el Estado Libre y Soberano de Quintana Roo

ANEXO

ENCUESTA REALIZADA AL PERSONAL DE LAS INSTITUCIONES PROCURADORAS DE JUSTICIA Y DE LAS DIVERSAS AGENCIAS DEL MINISTERIO PÚBLICO DE LAS SUBPROCURADURÍAS DEL ESTADO DE VERACRUZ, ZONA NORTE, ZONA CENTRO Y ZONA SUR

LA PERSECUCIÓN DE LOS DELITOS CIBERNÉTICOS (XALAPA 2006 - 2009) Y SU INCLUSIÓN COMO DELITOS BINARIOS DENTRO DEL ORDENAMIENTO PUNITIVO DEL ESTADO DE VERACRUZ			
INSTRUMENTO DE RECOLECCIÓN DE DATOS CUALITATIVO			
DESCRIPCIÓN.- El presente instrumento, tiene como objetivo, recolectar datos cualitativos y cuantitativos, relacionados con el combate a la delincuencia cibernética. Es importante resaltar que la información aquí recolectada, bajo ninguna circunstancia será utilizada para otros fines que no sean exclusivamente de investigación.			
INSTRUCCIONES.- Lea detalladamente cada cuestionamiento y conteste de la manera que considere correcta, encerrando en un circulo las respuestas que así lo ameritan y/o contestando en el espacio destinado, aquellas que requieren el desarrollo de su respuesta. Muchas gracias por su valioso tiempo y contribución a la Ciencia.			
DATOS DEL ENCUESTADO			
NOMBRE			
AGENCIA		**FUERO DE COMPETENCIA**	
DEMARCACIÓN	**Xalapa, Veracruz, México**	**FECHA DE ENCUESTA**	**Mayo de 2010**

1. ¿Conoce usted los Delitos Cibernéticos? Si su respuesta es no pase a la pregunta 3			
	SI	**NO**	

2. ¿Como podría usted definir a los delitos cibernéticos?
_____
_____
_____
_____
_____
_____

3. ¿Existen denuncias relativas a la comisión de delitos cibernéticos presentadas ante esta agencia entre los años 2006 y 2009? Si su respuesta es no pase a la pregunta 6.			
	SI	**NO**	

4. ¿Con qué frecuencia se presentan denuncias relativas a la comisión de delitos cibernéticos?

_____
_____
_____
_____
_____
_____

5. ¿Con qué frecuencia son consignados los presuntos responsables por la comisión de delitos cibernéticos?

_____
_____
_____
_____
_____
_____

6. ¿Los delitos cibernéticos están contemplados por los ordenamientos punitivos de Veracruz y Federal respectivamente?

7. ¿Por qué la legislación punitiva del Estado de Veracruz y la Federal, no contemplan dentro de sus tipos penales a los delitos cibernéticos?

_____
_____
_____
_____
_____

8. ¿Sabe usted cual es la policía cibernética?			
	SI	**NO**	

9. ¿Ha usted hecho uso del apoyo de la policía cibernética para la resolución de alguna investigación ministerial?			
	SI	**NO**	

10. ¿Sabe usted cual es la diferencia entre los delitos informáticos y los delitos cibernéticos?		
SI ¿Diga Cuál?	_____ _____ _____ _____	**NO**

11. ¿Considera usted que la autoridad Procuradora de Justicia, reconoce "de hecho" los delitos cibernéticos?			
	SI	**NO**	

12. ¿Estaría usted de acuerdo en que la autoridad procuradora de justicia, reconoce los delitos cibernéticos "de hecho" más no "de derecho"?			
	SI	**NO**	

13. ¿Considera que actualmente ante la falta de inclusión de los delitos cibernéticos en los códigos penales, la autoridad procuradora de justicia, le da tratamiento en sus indagatorias a los delitos cibernéticos como si fueran delitos de los ya previstos por los códigos?			
	SI	**NO**	

14. ¿Considera que los tipos penales que actualmente están vigentes, son insuficientes para la persecución de los delitos cibernéticos?			
	SI	**NO**	

15. ¿Cree usted que los delitos cibernéticos merecen un tratamiento en la indagatoria diferente al que típicamente se da a los demás delitos contemplados por las leyes punitivas tanto del Estado como Federal? Si su respuesta es no pase a la pregunta 18.			
	SI	**NO**	

16. ¿Cómo considera que debe ser el tratamiento en la indagatoria para la persecución de los delitos cibernéticos?
_____ _____ _____ _____ _____

17. ¿Tiene usted conocimiento sobre si a la fecha, existe en la Dirección General de Servicios Periciales correspondiente, un experto en informática forense?			
	SI	**NO**	

18. ¿Considera que para la persecución de los delitos cibernéticos debe existir un experto en informática forense en la Dirección General de Servicios Periciales correspondiente?			
	SI	**NO**	

19. ¿Considera usted que existe dificultad para validar el alcance y valor probatorio de los medios de prueba digitales en las investigaciones ministeriales de cualquier índole?			
	SI	**NO**	

20. ¿Quién es el encargado de validar el alcance y valor probatorio de los medios de prueba digitales en las investigaciones ministeriales?
_____ _____

21. ¿Quien es el perito experto de la correspondiente Dirección General de Servicios Periciales que valida el alcance y valor probatorio de los medios digitales en tratándose de la comisión de los delitos cibernéticos?
_____ _____ _____ _____

22. ¿Quien es el perito experto de la correspondiente Dirección General de Servicios Periciales que valida los daños a los medios digitales, electrónicos y de nuevas tecnologías, en tratándose de la comisión de los delitos cibernéticos?
_____ _____ _____ _____ _____

23. ¿Cuando usted dirige un oficio a la Dirección General de Servicios Periciales, para efectos de solicitar el apoyo de un perito experto en tratándose de una indagatoria relativa a la comisión de delitos cibernéticos, ¿De que perito específicamente requiere el apoyo?
_____ _____ _____ _____ _____

24. ¿Existe una diferencia entre los delitos informáticos y los delitos cibernéticos? Si su respuesta es no pase a la pregunta 26.			
	SI	**NO**	

25. ¿Cuál considera que es la diferencia entre los delitos informáticos y los delitos cibernéticos?

_____
_____
_____
_____
_____

26. ¿Considera que con la descripción del tipo penal de delitos informáticos, es posible la persecución de los delitos cibernéticos?			
	SI	**NO**	

27. ¿Qué es para usted el delincuente cibernético?
_____ _____ _____ _____ _____

28. ¿Sabe usted cual es la distinción entre el delincuente cibernético y el delincuente tradicional?			
	SI	**NO**	

29. ¿Considera que el delincuente cibernético tiene un grado mayor de temibilidad que el delincuente tradicional?			
	SI	**NO**	

30. ¿Considera que las investigaciones ministeriales relacionadas con el delincuente cibernético, necesitan un tratamiento diferente que las que involucran al delincuente tradicional?			
	SI	**NO**	

31. ¿Por qué, muy a pesar de que el Estado reconoce los delitos cibernéticos "de hecho", no los incluye dentro de la legislación penal correspondiente, para entonces reconocerlos también "de derecho"?

_____
_____
_____
_____
_____

32. ¿Por qué el estado ha creado una policía cibernética para coadyuvar con la persecución de los delitos de esta índole, pero no se reconocen en los ordenamientos punitivos Estatales y Federal respectivamente?

_____
_____
_____
_____

33. ¿Cuál es el tratamiento que la autoridad procuradora de justicia le da a los delitos cibernéticos en las indagatorias correspondientes, a través de las agencias de ministerio público?

_____
_____
_____
_____
_____

34. ¿Considera que el tratamiento que le da la autoridad procuradora de justicia a los delitos cibernéticos en las indagatorias correspondientes, a través de las agencias de ministerio público, debería ser especializado?

	SI	**NO**	

35. ¿Considera que los delitos informáticos son un tipo penal que podría incluirse dentro de los delitos cibernéticos de estar estos últimos tipificados?

	SI	**NO**	

36. ¿Existen denuncias relativas a la comisión de delitos informáticos presentadas ante esta agencia? Si su respuesta es no pase a la pregunta número 39.			
	SI	**NO**	

37. ¿Con qué frecuencia se presentan denuncias relativas a la comisión de delitos informáticos?
_____ _____ _____ _____

38. ¿Con que frecuencia son consignados los presuntos responsables por la comisión de delitos informáticos?
_____ _____ _____ _____

39. ¿Considera que de tipificarse el tipo penal de delitos cibernéticos, deberían preservarse aún los delitos informáticos?			
	SI	**NO**	

¡Muchas Gracias!
LE REITERAMOS UN PROFUNDO AGRADECIMIENTO POR SU CONTRIBUCIÓN A LA PRESENTE INVESTIGACIÓN.