

**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**



**FACULTAD DE DERECHO**



**SEMINARIO DE DERECHO PENAL**

***ANÁLISIS GLOBAL DE LOS DELITOS INFORMÁTICOS  
CONTENIDOS EN EL TÍTULO NOVENO DEL CÓDIGO PENAL  
FEDERAL Y LA NECESIDAD DE UNA REGULACIÓN ACORDE  
AL AVANCE TECNOLÓGICO***

TESIS QUE PARA OBTENER EL TÍTULO DE

***LICENCIADA EN DERECHO***

P R E S E N T A

***SILVIA MARTÍNEZ DE ALBA ORTIZ***

DIRECTOR DE TESIS: DR. MIGUEL ÁNGEL GRANADOS ATLAÇO

CIUDAD DE MÉXICO.

2021



Universidad Nacional  
Autónoma de México

Dirección General de Bibliotecas de la UNAM

**Biblioteca Central**



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



**SEMINARIO DE DERECHO PENAL  
OFICIO INTERNO FDER/ SP/40/06/2021  
ASUNTO: APROBACIÓN DE TESIS**

**M. EN C. IVONNE RAMÍREZ WENCE  
DIRECTOR GENERAL DE LA ADMINISTRACIÓN  
ESCOLAR DE LA U.N.A.M.  
P R E S E N T E.**

La alumna **SILVIA MARTÍNEZ DE ALBA ORTIZ**, con No. de Cuenta: **091383600**, ha elaborado en este Seminario a mi cargo y bajo la dirección del Dr. **MIGUEL ÁNGEL GRANADOS ATLACO**, la tesis profesional titulada **“ANÁLISIS GLOBAL DE LOS DELITOS INFORMÁTICOS CONTENIDOS EN EL TÍTULO NOVENO DEL CÓDIGO PENAL FEDERAL Y LA NECESIDAD DE UNA REGULACIÓN ACORDE AL AVANCE TECNOLÓGICO”**, que presentará como trabajo recepcional para obtener el título de Licenciado en Derecho.

El profesor **Miguel Ángel Granados Atlaco**, en su calidad de asesor, informa que el trabajo ha sido concluido satisfactoriamente, que reúne los requisitos reglamentarios y académicos, y que lo aprueba para su presentación en examen profesional.

Por lo anterior, comunico a usted que la tesis **“ANÁLISIS GLOBAL DE LOS DELITOS INFORMÁTICOS CONTENIDOS EN EL TÍTULO NOVENO DEL CÓDIGO PENAL FEDERAL Y LA NECESIDAD DE UNA REGULACIÓN ACORDE AL AVANCE TECNOLÓGICO”** puede imprimirse para ser sometida a la consideración del H. Jurado que ha de examinar a el alumno (a) **SILVIA MARTÍNEZ DE ALBA ORTIZ**.

En la sesión del día 3 de febrero de 1998, el Consejo de Directores de Seminario acordó incluir en el oficio de aprobación la siguiente leyenda:

“El interesado deberá iniciar el trámite para su titulación dentro de los seis meses siguientes (contados de día a día) a aquél en que le sea entregado el presente oficio, en el entendido de que transcurrido dicho lapso sin haberlo hecho, caducará la autorización que ahora se le concede para someter su tesis a examen profesional, misma autorización que no podrá otorgarse nuevamente sino en el caso de que el trabajo recepcional conserve su actualidad y siempre que la oportuna iniciación del trámite para la celebración del examen haya sido impedida por circunstancia grave, todo lo cual calificará la Secretaría General de la Facultad”

Sin otro particular, agradezco anticipadamente la atención que le dé a la presente solicitud, y aprovecho para enviarle un saludo cordial.

**A T E N T A M E N T E**  
**“POR MI RAZA HABLARÁ EL ESPÍRITU”**  
Cd. Universitaria, CDMX. A 28 de junio de 2021.

**LIC. ARTURO LUIS COSSÍO ZAZUETA  
DIRECTOR DEL SEMINARIO**

## Agradecimientos

Principalmente doy gracias a Dios por permitirme tener tan buena experiencia dentro de mi Universidad, gracias a la misma por darme la oportunidad de convertirme en un ser profesional en lo que tanto me apasiona, gracias a cada maestro que fue parte de este proceso integral y al apoyo incondicional del H. Director Raúl Contreras Bustamante.. Finalmente agradezco a mi familia:

Madre; que me diste las herramientas para yo poder seguir mi camino.

Hermana Maru; por todo tu apoyo y amor desde que nací.

Tia Vicky; por tus consejos y solidaridad.

Sobrinas Andre, Dany y Mario por qué mi situación sea para ustedes un impulso en su vida y sean los mejores en todos los aspectos.

Amigas; por su apoyo, comprensión y amistad incondicional.

Jorge; porque llegaste a mi vida para unir nuestras sonrisas, formar una familia y un equipo, por tu apoyo y amor!

Renata y Regina; gracias por ser mis mejores amigas, mi mayor fuerza, mi razón de vivir y sonreír, quiero darles este ejemplo de que se puede lograr lo que se propongan si se esfuerzan, las amo!

# ANÁLISIS GLOBAL DE LOS DELITOS INFORMÁTICOS CONTENIDOS EN EL TÍTULO NOVENO DEL CÓDIGO PENAL FEDERAL Y LA NECESIDAD DE UNA REGULACIÓN ACORDE AL AVANCE TECNOLÓGICO

<b>INTRODUCCIÓN</b>	<b>I</b>
<b>Capítulo 1. Marco conceptual</b>	<b>1</b>
1.1 Antecedentes históricos.	2
1.1.1 Origen de la informática.	3
1.1.2 Características fundamentales del derecho informático.	4
1.1.3 informática jurídica. (Orígenes)	5
1.2 Evolución y clasificación.	5
1.3 La cibernética. (Orígenes)	5
1.3.1 Gobierno electrónico y ciberjusticia.	7
1.3.2 Cibertribunales.	7
1.4 Concepto de delito informático (cibernético).	7
1.4.1 Como instrumento o medio.	11
1.4.2 Como fin u objeto.	11
1.5 Problemática para la investigación de los delitos informáticos o cibernéticos.	12
1.5.1 Complejidad inherente a la propia tecnología.	13
1.5.2 La comunicación electrónica y sus complicaciones.	14
1.6 Qué son los delitos informáticos (típico y atípico).	15
1.6.1 Principales características.	15
1.6.2 Tipos de ataques contra los sistemas de información.	17
1.6.3 Clasificación de acuerdo con la Organización de las Naciones Unidas.	17
1.6.4 Tipos de delitos informáticos reconocidos por la Organización de las Naciones Unidas.	18
1.6.5 Daños o modificaciones de programas o datos computarizados.	19
1.6.6 Falsificaciones informáticas.	19

<b>Capítulo 2. Marco jurídico internacional y nacional</b>	<b>21</b>
2.1 La Organización de las Naciones Unidas y los delitos informáticos.	21
2.2 Unión Europea.	24
2.3 Alemania.	25
2.4 Estados Unidos.	26
2.5 Acuerdos internacionales suscritos por México.	27
2.6 Análisis de la legislación sobre delitos informáticos en México.	27
<b>Capítulo 3. Elementos positivos y aspectos negativos del delito</b>	<b>36</b>
3.1 Conducta y Ausencia de Conducta.	36
3.2 Tipicidad y Atipicidad.	47
3.3 Antijuridicidad y Causas de Justificación.	59
3.4 Imputabilidad e Inimputabilidad.	72
3.5 Culpabilidad e Inculpabilidad.	78
3.6 Condiciones Objetivas de Punibilidad y su Ausencia.	88
3.7 Punibilidad y Excusas Absolutorias.	91
<b>Capítulo 4. Los delitos informáticos del Título Noveno del Código Penal Federal relativos al acceso ilícito a sistemas y equipos de informática</b>	<b>97</b>
4.1 Modificar, destruir o provocar pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sin autorización.	97
4.2 Conocer o copiar información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sin autorización.	122
4.3 Modificar, destruir o provocar pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, sin autorización.	127

4.4 Conocer o copiar información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad.	153
4.5 Conocer, obtener, copiar o utilizar información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad.	157
4.6 Modificar, destruir o provocar pérdida de información que contengan indebidamente, estando autorizado para acceder a sistemas y equipos de informática del Estado.	168
4.7 Estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan.	171
4.8 Estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan.	174
4.9 Modificar, destruir o provocar pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.	180
4.10 Conocer o copiar información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.	204
4.11 Estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan.	223
4.12 Estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copien información que contengan.	234
<b>CONCLUSIONES</b>	252
<b>FUENTES CONSULTADAS</b>	254
<b>PROPUESTA DE REFORMA DE LOS DELITOS INFORMÁTICOS</b>	257

## INTRODUCCIÓN

Internet es un espacio único donde se intercambia una gran cantidad de contenidos, muchos de estos considerados lícitos o ilícitos según la legislación nacional e internacional, actualmente la tecnología está abierta a la sociedad facilitándole la propagación de información, la interacción de los individuos independientemente de su ubicación geográfica, así como la difusión mundial de información.

Este avance tecnológico sin duda ha aportado beneficios en diferentes actividades, pero también ha abierto la puerta a una serie de conductas delictivas. Internet plantea numerosas cuestiones jurídicas que se deben atender, en primer lugar, las correspondientes a la ordenación y regulación de la red; y en segundo término las relaciones jurídicas que nacen a través de la red.

Los delitos cibernéticos constituyen actos criminales que pueden afectar al gobierno y su estabilidad, la economía, la paz social.

Las tecnologías de información tienen un avance vertiginoso y el marco jurídico en México no se encuentra actualizado para poder implementar las políticas públicas que demanda la sociedad.

Resulta imposible que el derecho vaya regulándose a la par que la tecnología, ya que las conductas lícitas o ilícitas se manifiestan primero y el derecho no puede regular lo que aún no existe.

Luis Azaola nos comenta “Internet es el nombre que se le da a una red informática creada a partir de un proyecto del Departamento de Defensa de Estados Unidos llamado DARPANET (Defense Advanced Research Project Network), iniciado en 1969 y cuyo propósito principal era la investigación y desarrollo de protocolos de comunicación para redes de área amplia para ligar redes de transmisión de paquetes de diferentes tipos capaces de resistir las condiciones de operación más difíciles, y continuar funcionando aun con la pérdida de una parte de la Red general (por ejemplo en caso de guerra)”.<sup>1</sup>

---

<sup>1</sup>Azaola Calderón, Luis, *Delitos informáticos y Derecho Penal*, Editorial Ubijus, 2010, p. 1.



Los delitos informáticos, también llamados “delitos electrónicos”, “delitos relacionados con la computadora”, “crímenes por computadora”, “delincuencia relacionada con el ordenador”; son considerados por la doctrina como aquellas actividades criminales tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes, que se realizan utilizando tecnología computacional.

Estos delitos en ocasiones llegan a cruzar las fronteras, ya que la información viaja por dispositivos de manera electrónica sin control, por lo que la situación se complica al no poder perseguir y sancionar estas conductas ilícitas por carecer de regulación.

En la actualidad nos encontramos viviendo en una era informática, en la que cada vez, sofisticadas calculadoras científicas electrónicas han invadido los ámbitos más diversos de las relaciones socioeconómicas. Seguramente pocas dimensiones de nuestras vidas no se ven afectadas, dirigidas o controladas por un ordenador, de manera directa o indirecta. Sectores como la banca, los seguros, los transportes, la educación, la bolsa, el tráfico aéreo y terrestre, la administración pública, es decir, la sociedad en su conjunto, dependen, en gran medida, de los sistemas computacionales.

A ellas se les encomienda no sólo el archivo y procesamiento de la información, sino, incluso, la adopción automática de decisiones, por lo que se han convertido en el instrumento de trabajo del siglo XXI, generándose así dicha dependencia<sup>2</sup>.

En consecuencia y aunado lo anterior, podría afirmarse que el desarrollo de la tecnología informática y su enorme influencia en la vida diaria de los habitantes ha generado lo que se denomina como la “segunda revolución industrial”, y que esta revolución informática será incluso más transformadora que la revolución industrial del siglo XIX<sup>3</sup>.

La incursión del ordenador, así como de las redes informáticas en la vida del ser humano moderno, representa un giro significativo en el transcurso de su historia, que afectan de un modo positivo su realidad cotidiana. Este fenómeno

---

<sup>2</sup> RIQUELT, Marcelo A. Informática y derecho penal argentino, Ad Hoc, Buenos Aires, 1999, p.23.

<sup>3</sup> SALT, Marcos, “Delitos informáticos de carácter económico”, en delitos no convencionales, Julio B.J. Maier (comp.), Editores de Puerto, Buenos Aires, 1994, pp. 225 y ss.

informático permite fomentar la difusión de ideas entre los individuos, sin depender de la posesión de los medios de comunicación. Los beneficios de la informática<sup>4</sup>, pueden percibirse sin mayores explicaciones en el terreno del comercio, la comunicación, el transporte y la educación.

La temporalidad propia de la comunicación entre las personas sufrió un nuevo giro en sus cimientos luego de la aparición cronológica del telégrafo, el teléfono y de la televisión, todos estos instrumentos permitieron que la necesidad de comunicarse se diera de una forma sencilla, económica y rápida, lográndose así que la interacción humana alcance un nivel sin precedente.

Esta realidad, exigió evaluar las necesidades humanas de una forma perentoria y que en la medida de que vayan surgiendo se diseñen nuevas regulaciones jurídicas para las actividades de mérito, en este sentido la Comisión Europea acaba de lanzar una consulta sobre los problemas jurídicos que genera para sus empresas, el uso del internet en sus relaciones comerciales, también denominada ciber economía.

Hoy más que en ninguna otra época la tecnología nos envuelve con o sin nuestro consentimiento. La tendencia global es clara: resulta más barata la administración de transacciones bancarias y comercio por medio de Internet que tener un ejército distribuidos físicamente en locales o sucursales alrededor del mundo. Es probable que uno de los ejemplos más representativos de la globalización sea la capacidad de establecer grupos de trabajo y de intercambio de información en Internet entre estudiantes, profesionistas, investigadores y comerciantes de distintas partes del mundo en tiempo real, con la capacidad de intercambiar archivos de voz, datos y video.

Sin embargo, el mismo medio es utilizado para coordinar y programar la difusión de distintos programas maliciosos (virus informáticos) con la intención de provocarnos un dolor de cabeza al apagar nuestra computadora sin una razón aparente, o de poner a disposición de terceros nuestra información más confidencial e incluso aprovechar nuestra computadora para llevar a cabo un

---

<sup>4</sup> Comercio electrónico. Análisis jurídico multidisciplinario, B de F, Buenos Aires-Montevideo, 2003, p.1.

ataque masivo para provocar lo que se conoce como negación de servicio a un determinado servidor Web.

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

La informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial. La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos. La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos. A ello se une que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

Sensibles a lo señalado líneas arriba, el presente estudio tiene por objeto presentar el marco jurídico con el que cuenta México en materia de delitos informáticos, para después generar una propuesta de reformas al Código Penal Federal, para con ello robustecer al sistema jurídico penal mexicano e ir a la vanguardia con esta nueva realidad tecnológica.

## Capítulo 1

### Marco Conceptual

**SUMARIO:** 1.1 Antecedentes históricos. 1.1.1 Origen de la informática. 1.1.2 Características fundamentales del derecho informático. 1.1.3 informática jurídica. 1.2 Evolución. 1.2.1 Clasificación. 1.3 La cibernética. 1.3.1 Gobierno electrónico y ciberjusticia. 1.3.2 Cibertribunales. 1.4 Concepto de delito. 1.4.1 Como instrumento o medio. 1.4.2 Como fin u objeto. 1.5 Problemática para la investigación de los delitos informáticos o cibernéticos. 1.5.1 Complejidad inherente a la propia tecnología. 1.5.2 La comunicación electrónica y sus complicaciones. 1.6 Que son los delitos informáticos (típico y atípico). 1.6.1 Principales características. 1.6.2 Tipos de ataques contra los sistemas de información. 1.6.3 Clasificación de acuerdo con las Naciones Unidas. 1.6.4 tipos de delitos informáticos reconocidos por la Organización de las Naciones Unidas. 1.6.5 Daños o modificaciones de programas o datos computarizados. 1.6.6 Falsificaciones informáticas.

A la par del avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, han surgido una serie de comportamientos ilícitos denominados, de manera genérica, delitos informáticos o cibernéticos como lo expresan diferentes autores. Los delitos que se pueden cometer en la actualidad mediante el uso de la computadora son múltiples y de tipos muy variados, nadie puede estar seguro de que no va a ser víctima de alguno de ellos y por lo anterior se debe legislar este tipo de delitos. Los especialistas informáticos y legisladores deben trabajar juntos con el fin de proporcionar un instrumento confiable que permita identificar y sancionar de una manera correcta los delitos que con el uso de los equipos de cómputo se puedan presentar.

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables, la manipulación fraudulenta de las computadoras con ánimo de lucro, la destrucción de programas o datos, el acceso y la utilización indebida de la información que puede afectar la esfera de privacidad de las personas, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

No sólo la mayor cantidad de perjuicios ocasionados por el procesamiento electrónico de datos comparado con la delincuencia tradicional es lo preocupante, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos, ya que la convierten en un instrumento idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.) La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

Debido a la gran importancia que los sistemas de procesamiento de datos representan para la operación de las organizaciones tanto públicas como privadas, los sistemas se han convertido en un objetivo importante cuyo ataque provocaría un perjuicio enorme, que va mucho más allá del valor material de los sistemas mismos, además, estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

### **1.1 Antecedentes históricos**

En el año de 1975, fecha en que se creó la primera PC, para Barriuso Ruiz, "difícilmente se podría vislumbrar la complejidad en el manejo de la información que se generaría a través de la red que se originó en 1963, pero que era de pocos conocidos, dado que su

utilización se restringía al campo militar, tecnológico y universitario”;<sup>1</sup> sin embargo, la masificación y disminución en los costos de las computadoras personales, así como la apertura de la red, que cambió su denominación a Internet, dio inicio a la formación de un mundo virtual, con ilimitadas posibilidades, lo que a la postre trajo consigo grandes beneficios a la humanidad como un bien común, tan sólo por citar alguno: la ventaja de la comunicación al instante entre dos países situados en los extremos del globo terráqueo.

A la par de lo anterior, también se generaron serios problemas en relación con el uso y abuso de tal producto tecnológico la incorporación del Internet al mundo real fue avasallador de tal manera que los sistemas jurídicos de las naciones no se encontraban preparados con los mecanismos legales necesarios para afrontar dicha problemática.

México, no fue la excepción, lo que dio lugar a que se generaran congresos internacionales para intentar regular en qué casos debían considerarse ilícitas determinadas conductas ejecutadas a través del uso del Internet, se gestaron nuevas denominaciones de delito, entre otras, delito informático, ciberdelito, etcétera, en nuestro país fue hasta el año de 1999 en que se incorporó a la legislación punitiva los delitos informáticos, aunque cabe destacar que diversos ordenamientos comprenden algunas figuras lesivas genéricas en las que bien se puede integrar conductas delictivas llevadas a cabo por el uso de Internet.

### **1.1.1 Origen de la informática.**

El término de la informática surge de la misma inquietud racional del hombre, el cual, ante la continua y creciente necesidad de información para una adecuada toma de decisiones, es impulsado a formular nuevos postulados y diseñar nuevas técnicas que satisfagan nuevos propósitos.

---

<sup>1</sup> Revista de instituto de la Judicatura Federal. Versión electrónica. [http://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos\\_inform%C3%A1ticos.pdf](http://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf). 15 de marzo de 2013

### **1.1.2. Características fundamentales del derecho informático.**

El derecho informático, como una nueva rama del conocimiento jurídico, es una disciplina en constante desarrollo, que tiene hasta la fecha nuevos antecedentes a nivel histórico, podemos decir que las alusiones más específicas sobre esta interrelación existe a partir de 1949 con la obra de Norbert Wiener, en cuyo capítulo 4, dedicado al derecho y las comunicaciones, expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico.

En las primeras manifestaciones interdisciplinarias ocurrían en los términos instrumentales de las implicaciones informáticas respecto al derecho, los cuales se desarrollaron extraconceptualmente en la década de 1950. A diferencia del estudio de las implicaciones jurídicas motivadas por la informática, en los términos de un derecho informático se considera una serie de implicaciones de orden social, económico, técnico, práctico y evidentemente jurídico, suscitadas por el uso de la informática.

El derecho informático es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática).

El derecho informático obedece a dos vertientes fundamentales: la informática jurídica y el derecho de la informática.

La palabra informática es un neologismo derivado de los vocablos información y automatización, sugerido por Phillippe Dreyfus en 1962, en sentido general, la informática es un conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información con miras a una adecuada toma de decisiones.

### **1.1.3 Informática Jurídica (orígenes).**

Las primeras investigaciones en materia de recuperación de documentos jurídicos en forma automatizada se remontan a los años de la década de 1950, cuando se comienzan a utilizar las computadoras no solo con fines matemáticos, sino también lingüísticos. Estos esfuerzos fueron realizados en el Health Law Center (HLC) de la Universidad de Pittsburgh, Pensilvania. El entonces director del centro, John Harty, estaba convencido de la necesidad de encontrar medios satisfactorios para tener acceso a la información legal.

En términos generales es válido afirmar que la información jurídica es la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como a la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesaria para lograr dicha recuperación.

## **1.2 Evolución.**

La década de los años 1960 marcó el desarrollo de varios sistemas diversos de los mencionados en los orígenes de la informática jurídica. En 1964 la Corporación Americana de Recuperación de Datos comenzó a comercializar sistemas de procesamiento de datos legislativos.

Una siguiente incursión la realizó la Corporación de Investigación Automatizada de la Barra de Ohio (OBAR, por sus siglas en inglés) diferente de las dos primeras experiencias del HLC, comentadas ya que fue enfocada hacia los abogados litigantes.

### **1.2.1 Clasificación.**

En sus primeros años la informática jurídica se presentó en términos de una informática documentaria de carácter jurídico, es decir, creación y recuperación de información que contenía datos principalmente jurídicos (leyes, jurisprudencia y doctrina) o al menos de



interés jurídico. Poco a poco empezó a vislumbrarse la idea de que estos bancos de datos jurídicos se podían obtener no solo informaciones si no también, mediante programas estudiados expresamente, verdaderos actos jurídicos, como certificaciones, atribuciones de juez competente, sentencias premodeladas.

Desde hace varios años, la información jurídica ha permitido un mejor conocimiento de los fenómenos jurídicos, por lo que muchos juristas, anteriormente escépticos e indiferentes, han encontrado en la computadora un instrumento eficaz para mejorar sus actividades.

1. Informática jurídica documentaria (almacenamiento y recuperación de textos jurídicos).
2. Información jurídica de control y gestión (desarrollo de actividades jurídico-adjetivas).
3. Sistemas expertos legales o informática jurídica metadocumentaria (apoyo en la decisión, educación, investigación, redacción y previsión del derecho).

### **1.3 La Cibernética (orígenes)**

En el año de 1948, el matemático de origen Estadounidense, Norbert Wiener, escribió un libro titulado Cibernética, y empleo este término para designar a la nueva ciencia de la comunicación y control entre el hombre y la máquina.

Friedrich Engels, en su dialéctica a la naturaleza, manifestó que en los puntos de unión o de un contacto, entre las distintas ciencias, es donde se pueden esperar los mejores resultados, es decir, hablaba desde entonces, de la importancia de la disciplina.

A manera de concepto podríamos decir que el vocablo cibernética tiene su origen en la voz griega kibernetes “piloto” y kibernes, concepto referido al arte de gobernar; esta palabra alude a la función del cerebro respecto a máquinas.

### **1.3.1 Gobierno electrónico y ciberjusticia.**

Las nuevas tecnologías de la información y la comunicación (TIC) son una oportunidad y un medio excepcional para transformar de manera estratégica la administración pública en lo que se ha denominado gobierno electrónico.

El gobierno electrónico es un concepto de gestión que fusiona el empleo adecuado y acentuado de las tecnologías de la información y comunicación, con modalidades de gestión pública.

### **1.3.2 Cibertribunales.**

Los podemos definir como una propuesta muy innovadora en el ámbito de aplicación de justicia a nivel internacional, dándose el caso de que en algunos países del mundo ya existen tribunales especializados en la resolución de controversias del orden cibernético y el uso incorrecto de este mejor conocidos como Cibertribunales, que tienen como propósito servir de mediadores en los litigios derivados del uso del internet (comercio electrónico, propiedad intelectual, protección de la vida privada, etc.).

Estos tribunales permiten a las partes interesadas elegir de entre una cantidad de expertos, aquellos que propondrán soluciones a los conflictos, sustentados en los textos internacionales más avanzados en la materia.

Son particularmente frecuentes los problemas entre empresas que se interrelacionan en operaciones de comercio exterior en marketplaces digitales (importación-exportación, joint ventures, alianzas estratégicas, etc.) o problemas entre partners en redes de valor agregado en entornos Electronic Data Interchange (EDI VANS, por sus siglas en inglés). Estos conflictos son frecuentes en función de la relaciones entre consumidores finales y tiendas virtuales, bancos virtuales y sus clientes u operadoras financieras, etc.

## **1.4 Concepto de delito informático (cibernético).**

Antes que otra cosa consideramos importante hacer énfasis en que si ya tenemos una noción o cierto conocimiento de que es la informática o cibernética como algunos autores

lo describen entonces ya podemos hacer mención a algunos conceptos de delito cibernético que a continuación analizaremos

Por delito informático, suele entenderse toda aquella conducta ilícita susceptible de ser sancionada por el derecho penal, consistente en el uso indebido de cualquier medio informático.

Para Landaverde, M. L., Soto, J. G. & Torres, J. M. hablar de los delitos informáticos primero se tiene que hablar de qué es un delito, y luego de qué es la informática. Un delito es un acto u omisión sancionado por las leyes penales<sup>2</sup>.

El delito es un acto o acción humana, (ejecución u omisión) de carácter antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.

El delito debe corresponder a un tipo legal (figura de delito), definido por la ley, ha de ser un acto típico.

El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.

La ejecución u omisión del acto debe estar sancionada por una pena, por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena, mientras que la informática es, "un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones".

---

<sup>2</sup> Jurista español. Fue catedrático de derecho penal en las universidades de Barcelona y de Madrid. Escribió diversas obras, entre las que destacan Derecho penal: Penología (1920) y La nueva penología (1958).

Ahora si juntamos las definiciones tendremos que los delitos informáticos son: El conjunto de técnicas de carácter antijurídico destinadas al tratamiento lógico y automatizado de la información sancionada por las leyes penales.

Julio Téllez Valdez (1996), los define como "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)"<sup>3</sup>.

Organismos internacionales como la oced, lo define como cualquier conducta, no ética o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos.

Por lo tanto se establece como característica de dichos delitos que son conductas delictivas de cuello blanco, porque se requieren conocimientos técnicos; son acciones ocupacionales por realizarse cuando el sujeto activo labora, y son acciones de oportunidad pues se aprovecha la ocasión o el universo de funciones y organizaciones de un sistema tecnológico y económico.

Para Gabriel Andrés Campoli, los delitos informáticos "son aquéllos en los cuales el sujeto activo lesiona un bien jurídico que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo por medio de la utilización indebida de medios informáticos, agrega que delitos electrónicos o informáticos electrónicos, son una especie del género delitos informáticos, en los cuales el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos y que a la fecha por regla general no se encuentran legislados, pero que poseen como bien jurídico tutelado en forma específica la integridad de los equipos electrónicos y la intimidad de sus propietarios"<sup>4</sup>.

---

<sup>3</sup>Julio Téllez Valdés, Derecho informático, 4ª. ed., México, McGraw-Hill, 2009, p. 163.

<sup>4</sup> Campoli, Gabriel Andrés, "Hacia una correcta hermenéutica penal delitos informáticos vs. delitos electrónicos" AR: Revista de Derecho Informático núm. 048, julio de 2002, <http://www.alfa-redi.org/rdi-articulo.shtml?x=1480>.

En relación con lo anterior estimamos que deben hacerse algunas precisiones en torno a los elementos del delito; con el fin de exponer las particularidades del delito informático desde la perspectiva actual; así, desde la óptica de Díaz-Aranda, “en los cuatro sistemas del delito que fueron desarrollados en Alemania (clásico, neoclásico, finalista y funcionalista) se ha considerado que la conducta por si misma es el presupuesto o uno de los elementos del delito; sin embargo ello conduce a que en todo momento se analice la existencia de conductas y de resultados para después volver a analizarla para saber si está prohibida en la ley; es decir, si es una conducta- típica; por el contrario, cuando se intuye que un hecho puede ser constitutivo de delito, lo primero que se hace acudir a las normas para saber si eso está o no prohibido en la ley penal, lo que conduce a que el análisis no inicie con una conducta prejurídica sino con el indicio de un hecho descrito en la ley como prohibido y eso es la tipicidad entendida como juicio de adecuación de la conducta al tipo”<sup>5</sup>.

Existe una amplia discusión jurídica sobre la definición más precisa para el concepto “delito cibernético”. La UIC nos ofrece la que se apega más a la investigación de los mismos:

“Son aquellos que se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos electrónicos de comunicación”<sup>6</sup>.

Dada la enorme popularidad de Internet como medio de información y comunicación, es común asociar el concepto de delito cibernético con la red. Para todo efecto práctico, es necesario resaltar que todo lo que es delito en el mundo real, lo es también en Internet. Lo importante en toda investigación es identificar el rol que la tecnología tuvo en la comisión del ilícito, tanto como determinar cuáles tecnologías fueron utilizadas, por ejemplo, computadoras, teléfonos celulares, etcétera.

---

<sup>5</sup> Díaz-Aranda Enrique, Teoría del delito, México, Straf, 2006, p. 203.

<sup>6</sup> El efecto internet. Versión electrónica. [www.asi-mexico.org](http://www.asi-mexico.org). 14 de marzo de 2013

Según el rol de las Tecnologías de Información y Comunicación (TIC) utilizadas para la comisión de un delito cibernético, la UIC los clasifica en dos grupos:

- Cuando las TIC son un instrumento o medio comisivo.
- Cuando las TIC son el fin u objeto del delito.

#### **1.4.1 Como un instrumento o medio:**

En esta categoría se contemplan las conductas probablemente delictivas que se valen de las computadoras como medio (utilizan métodos electrónicos para llegar a un resultado ilícito), en la comisión del delito, por ejemplo las siguientes actividades:

1. Exhibición, publicación, difusión, intercambio y comercialización de pornografía infantil.
2. Extorsiones, fraudes electrónicos y amenazas.
3. Falsificación de documentos vía computarizada.
4. Negociaciones de secuestros.
5. Lectura, sustracción o copiado de información confidencial.
6. Aprovechamiento indebido o violación de código para ingresar a sistemas.
7. Variación del destino de sumas de dinero a otras cuentas (transferencias electrónicas).

Cabe señalar que en la mayoría de los casos, los delitos cibernéticos se adecuan a tipos penales vigentes.

Por ejemplo, en el caso de un fraude bancario cometido por Internet, se perseguirá con apego al tipo penal para el “fraude”, en donde Internet fue sólo el medio por el cual el ilícito se llevó a cabo.

#### **1.4.2 Como fin u objeto**

En esta categoría se contemplan las conductas probablemente delictivas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

Algunos ejemplos de estas actividades son:

1. Manipulación en los datos e información contenida en archivos o soportes físicos informáticos ajenos.
2. Acceso a los datos y utilización de los mismos por quien no está autorizado para ello.
3. Utilización del equipo y/o programas de otras personas, sin autorización, con el fin de obtener beneficios en perjuicio de otro.
4. Introducción de rutinas o programas para destruir datos, información o programas.
5. Utilización de la computadora con fines fraudulentos, con o sin conexión a Internet.

### **1.5 Problemática para la investigación de los delitos informáticos o cibernéticos.**

Muchos factores influyen para hacer compleja la investigación y esclarecimiento de los delitos cibernéticos.

En opinión de la UIC, “es necesario que los usuarios de Internet conozcan lo más posible la problemática que se crea por la falta de claridad o certeza en varias etapas de la investigación”<sup>7</sup>, por ejemplo:

La agencia del Ministerio Público debe integrar correctamente el expediente de la averiguación previa, con todos los elementos necesarios, y dando intervención a las autoridades capacitadas, servicios periciales, unidades de investigación cibernética, etcétera, en relación con lo anterior hay ocasiones en que es absolutamente necesaria la cooperación de las empresas proveedoras de acceso a Internet, mejor conocidas como ISP (Internet Service Providers, por sus siglas en inglés). Por ejemplo, cuando se comete un delito desde una computadora ubicada en un café Internet.

---

<sup>7</sup> Ídem.

### 1.5.1 Complejidad inherente a la propia tecnología

Internet nació como una plataforma de colaboración pensada para científicos y militares, por lo que los protocolos de comunicación que le dieron vida fueron desde un principio abierto y altamente configurables.

Mientras fue utilizada en este ámbito y sólo por personas de bien, esta apertura funcionó de maravilla, pero ya en la actualidad, usuarios malintencionados se aprovechan de estas características para acciones ilícitas como suplantación de identidad.

Además, existen situaciones específicas para cada clase, que también es importante tener presente. Como ejemplo veamos un caso de cuando las TIC son usadas como medio comisivo: el fraude electrónico.

La teoría del delito define dos sujetos en los delitos: el sujeto activo, que es la persona física que comete el delito, y el sujeto pasivo, que es la persona física o moral sobre quien recae el daño causado por la conducta del sujeto activo. Usualmente los definimos como delincuente y víctima, respectivamente.

Una página de Internet puede estar programada para robar información a sus visitantes y utilizarla para cometerles un fraude. Esto lo puede hacer sin su conocimiento (por ejemplo, sembrando un código malicioso en la computadora del visitante), o bien, por medio de engaños para que el propio visitante entregue su información, lo que ya de por sí modifica la forma en que deberá denunciarse en su momento.

Si bien está claro que los visitantes a los que se les roba información son las víctimas, es decir, los sujetos pasivos, ¿diríamos que la página es el sujeto activo? No, porque el sujeto activo, o delincuente, es una persona física, en este caso, el responsable de la operación de dicha página.

Dicha página puede estar alojada en otra ciudad, o en otro país, al igual que el



responsable. Cuando a una persona la roban en la calle, el sujeto pasivo está en contacto con el sujeto activo. La víctima puede entonces aportar información valiosa sobre el delincuente a la autoridad para facilitar la investigación; en los delitos cibernéticos esta complejidad recae sobre la UIC, la cual deberá investigar quién es el responsable de la página.

### **1.5.2 La comunicación electrónica y sus complicaciones**

El internet se ha convertido en un importante recurso, que resulta vital tanto para el mundo desarrollado por su función de herramienta social y comercial.

El objetivo de la cumbre mundial de la Sociedad de la Información, es garantizar que los beneficios sean accesibles para todos y fomentar ciertas ventajas específicas en algunos campos, como estrategias, comercio electrónico, gobierno electrónico, salud, educación, alfabetización, diversidad cultural, igualdad de género, desarrollo sustentable y protección del medio ambiente.

Foro de Gobernanza de internet es convocado desde el 2006 por la Organización de las Naciones Unidas en cumplimiento del mandato recibido por los acuerdos surgidos en la Cumbre Mundial de la Sociedad de la Información; el cual tiene como principal fin, efectuar una reunión que de alguna manera rompa el modelo tradicional de Naciones Unidas, en virtud de tratarse de un nuevo modelo de cooperación internacional, ya el internet está en constante evolución.

Las redes de comunicación electrónica y los sistemas de información forman parte de la vida diaria de los ciudadanos en el mundo. Los ataques contra los sistemas de información constituyen una amenaza para la creación de una sociedad de la información más segura y de un espacio de libertad, seguridad, justicia, por lo que es importante abordar este tema como tal.

## **1.6 Qué son los delitos informáticos (típico y atípico)**

Hablar de delitos en el sentido de acciones típicas (tipificadas), es decir, contempladas en textos jurídicos – penales, se requiere que la expresión delitos informáticos este consignada en los códigos penales, lo cual en algunos países no ha sido objeto de tipificación.

En el orden de las ideas, según el caso, los delitos informáticos son actitudes ilícitas que tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin (concepto típico).

### **1.6.1 Principales características.**

Según Julio Téllez Valdez, los delitos informáticos presentan las siguientes características:

1. Son conductas criminales de cuello blanco, en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
2. Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
3. Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
4. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" muy lucrativos a aquellos que las realizan.

5. Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
6. Son muchos los casos y pocas las denuncias, debido a la falta de regulación por parte del Derecho.
7. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
8. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
9. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.
10. Los sistemas mecanizados son susceptibles de pérdidas o fraudes debido a que Tratan grandes volúmenes de datos, muchas veces muy sensibles y estratégicos para las organizaciones.
11. En su mayoría son dolosos o intencionales, aunque también muchos de carácter culposos o imprudenciales.
12. Ofrecen a los menores de edad facilidades para su comisión.

Las personas que cometen estos delitos poseen ciertas características que no presentan el denominador común de los delincuentes, los sujetos activos tienen habilidad para manejar los sistemas informáticos y en general por su situación laboral se encuentran en lugares estratégicos donde la información se maneja en un carácter sensible.

De acuerdo al criminólogo estadounidense Edwin Sutherland en 1943, denomina delitos de cuello blanco, aun cuando muchos de ellas no están tipificados en los ordenamientos jurídicos como delitos, entre las cuales cabe destacar las violaciones a las leyes de patentes y fabrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas y la corrupción de altos funcionarios, etc.

### **1.6.2 Tipos de ataques contra los sistemas de información.**

La expresión sistemas de información se utiliza deliberadamente aquí en su sentido más amplio, debido a la convergencia entre las redes de comunicación electrónica y los distintos sistemas que conectan. Los sistemas de información abarcan (computadoras personales autónomas, las agendas electrónicas personales, teléfonos celulares, los intranets, los extranets, las redes, servidores y otras infraestructuras de internet).

La Comisión de la Unión Europea propuso la siguiente descripción de las amenazas contra los sistemas informáticos:

1. Acceso no autorizado a sistemas de información: Se refiere a la piratería informática, la cual consiste en tener acceso de manera no autorizada a una computadora.
2. Perturbación de los sistemas de información: Este se lleva a cabo mediante ataques mal intencionados.
3. Ejecución de programas informáticos perjudiciales que modifican o destruyen datos.
4. Intercepción de las comunicaciones: Son intercepciones mal intencionadas que afectan la confidencialidad.
5. Declaraciones falsas: Consiste en declaraciones falsas y de fraude (usurpar la identidad de otra persona en internet y utilizarla con fines malintencionados).

### **1.6.3 Clasificación de acuerdo con la Organización de las Naciones Unidas.**

De acuerdo al Manual de las Naciones Unidas para la prevención y control de delitos informáticos señala que cuando el problema aparece en el ámbito internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos

constituyen una nueva forma de delito transnacional y su combate requiere una eficaz cooperación internacional concertada.

De acuerdo a la Organización de las Naciones Unidas, se mencionan los problemas más frecuentes en delitos informáticos:

1. Falta de acuerdo globales acerca del tipo de conducta.
2. Ausencia de acuerdos globales en la definición legal de las conductas delictivas.
3. Falta de especialización del personal, en que respecta a este campo.
4. No armonización entre las diferentes leyes.
5. Carácter transnacional de múltiples delitos informáticos.
6. Ausencia de tratados de extradición.

#### **1.6.4 Tipos de delitos informáticos reconocidos por la Organización de las Naciones Unidas.**

##### **Fraudes cometidos mediante manipulación de computadoras:**

1. Manipulación de los datos de entrada:  
Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático mas común (fácil de cometer y difícil de descubrir).
2. Manipulación de programas:  
Difícil de descubrir, pasa desapercibido debido a que el delincuente cuenta con los conocimientos técnicos de informática.
3. Manipulación de los datos de salida:

Se fija un objetivo en el funcionamiento del sistema informático (el más común es el fraude, en cajeros automáticos mediante falsa instrucción a las computadoras, por medio de tarjetas bancarias robadas).

4. Fraude efectuado por manipulación informática:

Se realiza mediante repeticiones automáticas de los procesos de cómputo, es conocida como técnica del salami; que consiste en sacar dinero en repetidas ocasiones de una cuenta a otra.

### **1.6.5 Daños o modificaciones de programas o datos computarizados.**

2. Sabotaje informático:

Acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora, con intención de obstaculizar el funcionamiento normal del sistema.

3. Virus:

Es una serie de claves programáticas que pueden adherirse a los programas informáticos legítimos y propagarse a otros.

4. Gusanos:

Se fabrican de forma análoga al virus con miras a infiltrarlos en programas legítimos de procesamiento de datos o para modificar o destruir los datos.

5. Bomba lógica o cronológica:

Exige conocimientos especializados ya que requiere programar la destrucción o modificación de datos en un futuro.

### **1.6.6. Falsificaciones informáticas.**

1. Accesos no autorizados a programas o servicios:

Se da por varios motivos, por simple curiosidad, como en el caso de muchos piratas informáticos mejor conocidos como hacker, hasta el sabotaje o espionaje informático.

2. Piratas informáticos o hackers:

Este se lleva a cabo desde un lugar del exterior situado en la red de telecomunicaciones, recurriendo a diversos medios que se mencionan:

Se hacen pasar por usuarios legítimos del sistema, suele suceder en los lugares donde los empleados ocupan contraseñas comunes o de mantenimiento que están en el sistema.

3. Reproducción no autorizada de programas informáticos de protección legal:

Esta puede provocar una pérdida económica sustancial para los propietarios legítimos. Ciertas jurisdicciones la han tipificado como delito y la han sometido a sanciones penales.

El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. La reproducción de programas no autorizados no es un delito informático debido a que el bien jurídico por tutelar es la propiedad intelectual.

## Capítulo 2. Marco jurídico internacional

**SUMARIO:** 2.1 La Organización de las Naciones Unidas y los delitos informáticos. 2.2 Unión Europea. 2.3 Alemania. 2.4 Estados Unidos. 2.5 Acuerdos internacionales suscritos por México. 2.6 Análisis de la legislación sobre delitos informáticos en México.

### 2.1 La Organización de las Naciones Unidas y los delitos informáticos

El Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos señala que cuando el problema se eleva a la escena internacional, se magnifican los problemas y las insuficiencias, por cuanto, los delitos informáticos constituyen una forma de crimen transnacional y su combate requiere de una eficaz cooperación concertada. Asimismo la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- A) Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
- B) Ausencia de acuerdos globales en la definición de dichas conductas delictivas.
- C) Falta de especialización en las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- D) Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- E) Carácter transnacional de muchos delitos cometidos mediante el uso de las computadoras.
- F) Ausencia de tratados de extradición, de acuerdos de ayuda mutua y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.



En 1990 la Organización de las Naciones Unidas (ONU) en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en La Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos. La ONU ha publicado una descripción de "Tipos de Delitos Informáticos", que se transcribe al final de esta sección. En 1992 La Asociación Internacional de Derecho Penal durante el coloquio celebrado en Wurzburg en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad".

La Organización de las Naciones Unidas contempla dentro de delitos informáticos las siguientes conductas:

- Fraudes cometidos mediante la manipulación de computadoras: manipulación de datos de entrada, manipulación de programas, manipulación de datos de salida, fraude efectuado por manipulación informática
- Falsificaciones informáticas: utilizando sistemas informáticos como objetos, utilizando sistemas informáticos como instrumentos
- Daños o modificaciones de programas o datos computarizados: sabotaje informático, virus, gusanos, acceso no autorizado a sistemas o servicios, piratas informáticos o hackers, reproducción no autorizada de programas informáticos con protección legal.<sup>8</sup>

En el marco de las Naciones Unidas contiene un llamamiento a los estados miembros para que armonicen sus legislaciones a fin de castigar penalmente el uso indebido de tecnología de la información, al tiempo que los exhorta a garantizar la

---

<sup>8</sup> Flores Prada Ignacio, Criminalidad informática, Tirant lo Blanch, México, 2012.

confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos frente a los accesos no consentidos.<sup>9</sup>

En la Asamblea General del 31 de enero de 2002 figura una sección especial denominada “Medidas contra los delitos relacionados con la alta tecnología y la informática.

Como nos lo menciona Flores Prada dentro de todos los convenios o tratados que se puedan presentar el más claro luego del convenio de Budapest, es el de las naciones unidas que es de los primeros en ya tipificar y asignarle una sección especial para tratar y abordar el tema con la finalidad de la prevención, resulta interesante que las naciones unidas integren dicho tema para que así todos los sus miembros al menos tomen conciencia de la existencia de lo que ya es una realidad “LOS DELITOS INFORMATICOS”.

Se ha dicho que algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para aprehender ciertos comportamientos merecedores de pena con los medios del Derecho penal tradicional, existen, al menos en parte, relevantes dificultades. Estas proceden en buena medida, de la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas. En los Estados industriales de Occidente existe un amplio consenso sobre estas valoraciones, que se refleja en las reformas legales de los últimos diez años.

Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema sobre el particular, sin embargo con objeto de que se tomen en cuenta las medidas adoptadas por ciertos países, a continuación se presenta los siguientes casos particulares:

---

<sup>9</sup> López Betancourt, Eduardo, Revista de la judicatura Federal Número 28, p. 271.

## 2.2 Unión Europea

Acordaron sancionar con penas de uno a tres años de prisión a los responsables de delitos informáticos. Cuando quede comprobado que los ataques cibernéticos están relacionados con el crimen organizado, la pena ascenderá hasta los cinco años.

- Esta decisión marco se convierte en un gran avance dentro de la armonización de las legislaciones europeas para luchar contra los delitos informáticos. Estos delitos se han convertido en un quebradero de cabeza para los cuerpos de policía de los Estados miembros y, sobre todo, para los perjudicados por estos crímenes.
- Con este intento de unificar la legislación, las autoridades europeas podrán perseguir con una mayor efectividad a delincuentes que, hasta ahora, podían cometer sus delitos con casi total impunidad.
- Los Estados miembros distinguen tres tipos de ataques cibernéticos: el acceso ilegal a sistemas informáticos, la ocupación de sistemas a través de ejemplos como el envío de mensajes que ocupan un espacio considerable, y la difusión de virus informáticos.

La intención de la Unión Europea es doble: por un lado se trata de definir el delito; por otro pretende unificar las penas, ya que el lugar de la comisión del delito es fundamental para saber el derecho aplicable, se trata además de una medida muy sensata que evita la desprotección absoluta que presentan hoy en día las empresas del Viejo Continente. Los Quince Estados Europeos disponen ahora de un plazo de más de dos años para la adaptación de esta medida a sus textos legislativos

La comisión europea publica el 22 de mayo de 2007 que analizara el estado de la cuestión en materia de lucha contra la ciberdelincuencia , incluyendo un conjunto de propuestas a corto, medio y largo plazo destinadas a mejorar la coordinación y la eficacia de las políticas comunitarias en esta materia. En el análisis destaca la necesidad de ampliar el contenido de la delincuencia informática hacia otras formas

de criminalidad no vinculadas con el acceso e intromisión en los sistemas informáticos o la utilización indebida de datos<sup>10</sup>.

### 2.3 Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

- Espionaje de datos
- Estafa informática
- Falsificación de datos probatorios 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
- Alteración de datos es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
- Sabotaje informático Destrucción de elaboración de datos de especial significador medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causa del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio

---

<sup>10</sup> Flores Prada Ignacio, Criminalidad informática, Tirant lo Blanch, México 2012.

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.

## **2.4 Estados Unidos**

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hiper técnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya, etcétera y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, información, datos o programas, (18 U.S.C.: Sec. 1030 (a) (5) (A)). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus. El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudente la sanción fluctúa entre una multa y un año en prisión.

Nos llama la atención que el Acta de 1994 aclara que el creador de un virus no puede escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (*computercontaminant*) conceptualizándolos aunque no los limita a un grupo de instrucciones informáticas 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 o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

## 2.5 Acuerdos internacionales suscritos por México

De entre los acuerdos firmados por México relativos a la regulación del uno de los medios electrónicos y otros relacionados tenemos:

- El convenio de Berna para la protección de las obras literarias y artísticas establecido en 1886; la versión vigente del convenio de Berna data de 1971 misma que se realizó en París con la participación y firma de México entre otros tantos países.
- El Tratado de Libre Comercio de América del Norte, firmado entre Canadá, México y Estados Unidos que incluyen un capítulo sobre la propiedad intelectual
- El acuerdo de la propiedad intelectual en relación con el comercio, organización mundial del comercio
- La ley de derechos de autor o de *copyright* de cada país

Para la propiedad industrial:

- El Convenio de París para la protección industrial del 20 de marzo de 1883
- El Convenio que establece la organización de la propiedad intelectual
- El Tratado de cooperación en materia de patentes
- El Acuerdo hecho en Bruselas el 27 de mayo de 1997

## 2.6 Análisis de la legislación sobre delitos informáticos en México

Debemos advertir que cuando empleamos la expresión “ordenamiento jurídico” lo hacemos para significar la normativa de derecho público, mediante la cual se regula de manera dispersa una materia; pero que desde la perspectiva epistemológica puede ser vista como una unidad normativa.

En el ordenamiento jurídico permite conocer la clasificación legal de los delitos informáticos en México para así a su vez poder dar entrada a la existencia de previstos legales respecto a los delitos informáticos.

La doctrina del Derecho de la Informática, ha identificado tres alternativas de solución para hacer frente al problema jurídico que representa la sociedad informatizada, mismas que consisten en:

- 1) la actualización de la legislación
- 2) la evolución jurisprudencial;
- 3) la redacción de leyes de carácter particular.

Amén de ello, ha registrado los fenómenos que por una parte, distorsionan las instituciones jurídicas y por otra, erosionan el ejercicio de los derechos y libertades fundamentales.

- Delitos informáticos en la legislación mexicana

El bien jurídico que se protege es la integridad física y lógica de los equipos informáticos en un caso y la capacidad de transmisión o recepción y el procesamiento a distancia en el otro; como sabemos algunas legislaciones en México han recogido una parte de los tipos penales que nos ocupan pero en contrapartida, en la mayoría de los casos han dejado la cuestión probatoria en materia de pruebas electrónicas sin modificaciones que permitan una correcta persecución de estas conductas.

Es ahí donde nace el primer problema de las víctima ya que los medios tradicionales no existe vía de acceso a la justicia para la reparación de los daños que han sufrido, porque si bien existe el tipo penal, la acción típica y su vinculación con el sujeto resulta imposibles de reflejar en un proceso penal lo cual deja a sus víctimas en una situación de indefensión absoluta para el respeto de su elemental derecho de acceso a la justicia.

Si al hecho ya descrito de la falta de posibilidad probatoria súmanos la actual desinformación sobre el tema que existe en los ambientes policiales y aun judiciales, tendremos una situación de plena catástrofe para la víctima de este tipo de delitos.

## Conclusiones y recomendaciones<sup>4</sup>

- Se deben promover en forma urgente las reformas legislativas necesarias para la correcta aplicación de las pruebas electrónicas en los procesos penales para de esta manera, garantizar en forma fehaciente el acceso a la justicia de las víctimas de estos nuevos delitos
- Se deben establecer cursos de capacitación para jueces, magistrados y personal policial sobre estos tipos penales a fin de que puedan aconsejar a las víctimas y en su caso tomar la decisión más ajustada a derecho, para garantizar el respeto a los derechos humanos fundamentales de los sujetos pasivos.
- Se deben crear cuerpos de peritos judiciales en informática a fin de que colaboren en la información de las causas y además asesoren a las víctimas de cuáles han de ser las acciones a seguir y en su caso, las asistan durante los interrogatorios.
- Es urgente la creación de un ombudsman de la información para la protección de las posibles víctimas no conscientes de su situación o bien para los casos de violaciones múltiples en los cuales no resulte útil la intervención de todos los afectados (aunque en estos casos no se trate de delitos informáticos propiamente dichos sino de delitos de violación de la privacidad cometidos por medios informáticos.

“En primera instancia resulta muy extraño que por una parte la legislación considere a las conductas descritas como delitos graves y por la otra, las instaure como delitos de acción privada que se persiguen por querrela, digamos que dentro de la ciencia penal tradicional estas dos consideraciones resultan casi contradictorias, puesto que se supone que las conductas delictuales graves deben perseguirse de oficio toda vez que lo son por afectar un bien jurídico que el estado como garante de la paz social considera importante”.<sup>11</sup>

---

<sup>11</sup> Campoli Andrés Gabriel. *Delitos Informáticos en la legislación mexicana*, INACIPE Mex.2007.



En nuestro sistema jurídico se incluyó a los delitos informáticos justamente con las reformas que se publicaron en el Diario Oficial de la Federación el diecisiete de mayo de mil novecientos noventa y nueve.

Los novedosos ilícitos se ubicaron dentro del Título Noveno del código punitivo federal, al que se le denominó “Revelación de Secretos y Acceso Ilícito a los sistemas y Equipos de informática”.

Resulta de interés al desarrollo de estas líneas las causas medulares que se dieron origen a la exposición de motivos de la reforma al considerarse que la iniciativa propone adicionar un capítulo al código penal para sancionar al que sin autorización acceda a sistemas y equipos informáticos protegidos por algún mecanismo de seguridad, con el propósito de conocer, copiar, modificar, o provocar la pérdida de la información que contenga, por lo que se pretende tutelar la privacidad y la integridad de la información. Lo anterior refleja que para el legislador fue de suma importancia proteger el acceso no autorizado a computadoras o a sistemas electrónicos, la destrucción o alteración de la información, el sabotaje por computadora, la interceptación de correo electrónico y la transferencia de fondos ilícitos que suceden con frecuencia y que constituye un grave problema ante la revolución tecnológica que ha rebasado las estructuras de contención, control y vigilancia por parte de los estados.

## **COMPENDIO JURÍDICO DE LOS DELITOS INFORMÁTICOS**

- legislación penal federal: delitos contemplados

Se encuentran previstos los delitos de Revelación de Secretos, Acceso ilícito a equipos y sistemas de informática y los Delitos contra los Derechos de Autor.

El Delito de revelación de secretos se tipifica cuando en perjuicio de alguien, sin justa causa y sin consentimiento, se revele, divulgue o utilice algún secreto, comunicación, información o imágenes, que hayan sido conocidas o recibidas con motivo de un empleo, cargo o puesto, por la prestación de un servicio profesional o técnico, por ser funcionario o empleado público; cuando dicho secreto sea de

carácter industrial, o bien, se hubiese obtenido de una intervención de comunicación privada.

Tales ilícitos también pueden considerarse como un fin tratándose de computadoras, sobre todo cuando se trata de información de tipo industrial.

- Algunas legislaciones penales de los estados que contienen tipos penales informáticos o electrónicos

## **CIUDAD DE MÉXICO**

Producción, Impresión, Enajenación, Distribución, Alteración o Falsificación de Títulos al Portador, Documentos de Crédito Públicos o Vales de Canje

❖ **ART.336-** 3 a 9 días de prisión y de cien a cinco mil días multa al que,

IV-. Sin consentimiento de quien esté facultado para ello, 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 disposición de efectivo.

VI-. Adquiera, utilice equipos electromagnéticos para sustraer la información contenida en la cinta o banda magnética de las tarjetas.

VII-. A quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente este facultada para emitir tarjetas.

Si el sujeto es empleado o dependiente del ofendido, las penas se aumentarán en una mitad.

“Este es un nuevo ejemplo de protección solamente parcial como ya lo comentamos que contempla a los equipos informáticos como meros medios comisivos de delitos como alteración de documentos o violación de secretos”.<sup>5</sup>

## ESTADO DE MEXICO

Falsificación y utilización indebida de títulos al portador, documentos de crédito público y documentos relativos al crédito

❖ **ART 174-**4 a 10 años y de 150 a 500 días de salario mínimo de multa al que altere los medios de identificación electrónica de tarjetas, títulos o documentos para el pago de bienes y servicios.

V-. A quien acceda indebidamente a los equipos de electromagnéticos de las instituciones emisoras de tarjetas, títulos o documentos para el pago de bienes y servicios o para disposición de efectivo.

Las mismas penas se impondrán a quien utilice indebidamente información confidencial o reservada de la institución o persona que legalmente está facultada para emitir tarjetas o documentos utilizados para el pago de bienes y servicios. Si el sujeto activo es empleado o dependiente del ofendido, las penas aumentaran a la mitad.

En este caso de que se actualicen otros delitos con motivo de las conductas a que se refiere este artículo se aplicaran las reglas del concurso.

“Para este estado en particular, pareciera que el único bien a proteger de las acciones indebidas sobre los equipos es el patrimonio y los únicos sujetos pasivos posibles son las instituciones financieras o crediticias, cuando en realidad las estadísticas de todo el mundo nos orientan a que las mayores violaciones son a la intimidad o el patrimonio de las personas físicas que no poseen los medios técnicos defensivos que si estos actores económicos, despliegan creo en definitiva que han dejado una tarea inconclusa”<sup>5</sup>

## JALISCO

Delitos contra la paz, libertad y seguridad de las personas

Falsificación de Medios Electrónicos o Magnéticos

❖ ART. 170-. 3 a 9 años y de 200 a 400 días d multa al que, sin consentimiento de quien esté facultado para ello, altere, copie o reproduzca, indebidamente, los medios de identificación electrónica de boletos, contraseñas, fichas u otros documentos que no estén destinados a circular y sirvan exclusivamente para identificar a quien tiene derecho a exigir la prestación que en ellos se consigna, siempre que estos delitos no sean de competencia federal (fracción II)

III-. Acceda, obtenga, posea o detente indebidamente información de los equipos electromagnéticos o sistemas de cómputo de las organizaciones emisoras de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I de este artículo, y los destine a alguno de los supuestos que contempla el presente artículo

VI-. Y a quien adquiera, utilice, posea o detente equipos electromagnéticos o electrónicos para sustraer en forma indebida la información contenida en la cinta magnética de los boletos, contraseñas, fichas u otros documentos a los que se refiere la fracción I del artículo

## **NUEVO LEON**

Delitos en relación con el patrimonio

Falsificación de Títulos al Portador, Documentos de Crédito Público y relativos al Crédito

❖ ART 242 BIS-. 3 a 9 años y 150 a 450 días multa al que

I-. Al que, sin consentimiento de quien esté facultado para ello, altere, tarjetas de crédito o de débito, o la información contenida en éstas, esqueletos de cheque o documentos utilizados para el pago de bienes y servicios o para disposición de efectivo.

IV-. Altere los medios de identificación electrónica de cualquiera de los objetos referidos en la fracción I.

V-. Acceda indebidamente a los equipos electromagnéticos de las instituciones emisoras de cualquiera de los objetos referidos en la fracción I.

❖ ART 365-. Se equiparará robo y se castigará como tal:

IV-. 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.

“ Creo que sinceramente que este tipo penal no ha de aplicarse nunca, ya que el apoderamiento material de los documentos electrónicos suenan tan poco posible como el apoderamiento material del alma humana, ya que como sabemos, nadie se apodera de los datos ajenos poniéndolos fuera de su esfera de control sino que lo que ocurre es que alguien sin autorización accede a un equipo ajeno y copia los datos ajenos, cuestión que nada tiene que ver con el apoderamientos , ya que la copia no priva al titular del uso y goce de sus bienes sino que el daño que le produce es otro totalmente distinto, la publicidad o la competencia desleal por que el contendiente ya conoce sus datos y sabe en alguna medida como este se va a desempeñar, por ejemplo, en un mercado determinado en un momento dado”<sup>5</sup>.

## **AGUASCALIENTES**

Delitos contra la seguridad en los medios informáticos y magnéticos

❖ ART 223-. El acceso sin autorización consiste en interceptar, interferir o ingresar por cualquier medio sin la autorización debida o excediendo la que se tenga en un sistema de red de computadoras pena de 1 a 5 años y de 100 a 400 días de multa.

❖ ART 224-. El daño informático consiste en la indebida destrucción o deterioro parcial o total de programas archivos u otro elemento intangible contenido en el sistema de redes de computadoras, pena 1 a 5 años de prisión 100 a 400 días multa.

- ❖ ART 225-. 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.
- ❖ ART 226-. La falsificación informática consiste en la indebida modificación, alteración o imitación de los originales de cualquier dato, archivo o elemento contenido en el sistema de redes de computadoras, base de datos etc. Al responsable del delito se le aplicaran de 1 a 5 años de prisión y de 100 a 400 días multa.

Retomando las palabras e ideas que expone Campoli Andrés hemos de destacar que en cierta medida tiene la razón al argumentar que las leyes solo protegen al estado y a las instituciones financieras, cosa que a nuestro parecer es muy cierto porque no se prestan la misma atención que si fuera un particular que denunciara alguna afectación ya sea por el medio o la acción empleada para la comisión de un delito. Resultaría interesante que la legislación planteara una ley sobre delitos informáticos justa y equitativa para la protección de los bienes jurídicos a tutelar que no beneficie a unos cuantos sino a todos los que formamos parte de esta nación.

### Capítulo 3. Elementos positivos y aspectos negativos del delito

**SUMARIO:** 3.1 Conducta y Ausencia de Conducta. 3.2 Tipicidad y Atipicidad. 3.3 Antijuridicidad y Causas de Justificación. 3.4 Imputabilidad e Inimputabilidad. 3.5 Culpabilidad e Inculpabilidad. 3.6 Condiciones Objetivas de Punibilidad y su Ausencia. 3.7 Punibilidad y Excusas Absolutorias.

#### 3.1 Conducta y Ausencia de Conducta

El delito es antes que nada, una conducta humana, y se le han dado varias denominaciones para expresar este elemento del delito, entre ellas encontramos como denominaciones: al acto, acción, hecho. Fernando Castellanos Tena nos dice: “nosotros preferimos el termino conducta; dentro de él se puede incluir correctamente tanto el hacer positivo como el negativo”.<sup>13</sup>

#### Conducta

Dentro del elemento conducta se considera que pueden comprenderse la acción y la omisión; esto es, el hacer positivo y el negativo; que son el actuar y el abstenerse de actuar.

“La conducta es el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito”.<sup>14</sup>

Para el Derecho penal, solamente la conducta humana tiene relevancia, por lo cual sólo la acción y la omisión corresponden al hombre, porque solamente es posible que esté sea sujeto activo en las infracciones penales, ya que es el único ser capaz de tener voluntariedad.

- **Elementos.**

La conducta tiene cuatro elementos que la conforman y a saber son: la voluntad, la actividad, el resultado y la relación de causalidad, que también es conocido como nexo causal, los cuales podemos definir de la siguiente manera:

---

<sup>13</sup> Citado por Fernando Castellanos Tena, *Lineamientos elementales del derecho penal*, México, editorial Porrúa, p 137.

<sup>14</sup> Fernando castellanos Tena, *op.cit.* p.139

“Voluntad. Es el querer, por parte del sujeto activo, cometer el delito es propiamente la intención.

Actividad. Consiste en el “hacer” o actuar. Es el hecho positivo o movimiento corporal humano encaminado a producir el ilícito.

Resultado. Es la consecuencia de la conducta; el fin deseado por el agente y previsto en la ley penal.

Nexo de causalidad. Es el ligamen o nexo que une a la conducta con el resultado, el cual debe ser material. Dicho nexo es lo que une la causa con el efecto, sin el cual este último no puede atribuirse a la causa”.<sup>15</sup>

La conducta bajo el sistema clásico (causalista) se basó en conocimientos materiales y debido a eso para explicar los caracteres objetivos del delito recurrió a criterios naturalistas con lo cual se pudo concebir a la conducta “como un movimiento corporal, que es la causa de una modificación en el mundo exterior, cuya percepción se constata a través de los sentidos”.<sup>16</sup>

El funcionalismo rechaza la concepción de la acción final, el concepto de acción en el causalismo es naturalista y bajo la perspectiva de este sistema, la formación del Derecho penal, debe hacerse bajo la base de las finalidades del Derecho Penal.

Para el finalismo, la acción del ser humano, no es un proceso causal, ya que la acción del hombre es en calidad distinta a los acontecimientos naturales; por el contrario, la acción humana se distingue por su finalidad.

“Dentro de la concepción finalista, se llama acción a todo comportamiento dependiente de la voluntad humana. Sólo el acto voluntario puede ser penalmente relevante. La voluntad implica, sin embargo, siempre una finalidad. No se concibe un acto de voluntad que no vaya dirigido a un fin. El contenido de la voluntad es siempre algo que se quiere alcanzar, es decir, un fin. De ahí que la acción humana regida por

---

<sup>15</sup> Griselda Amuchategui, *Derecho penal*, México, edit. Oxford, 3ª. ed., 2005, p. 54.

<sup>16</sup> Enrique Díaz-Aranda, *Derecho Penal, Parte General*, México, edit. Porrúa 3ª. ed. 2008, p.116.



la voluntad sea siempre una acción final, una acción dirigida a la consecución de un fin. La acción es el ejercicio de la actividad final”.<sup>17</sup>

- **Formas de la conducta**

La conducta a la que también llamamos acto o acción, lato sensu; puede llegarse a manifestar mediante el hacer positivo o negativo, esto es por actos o por abstenciones.

Como todos sabemos dentro de la conducta se puede distinguir la acción y la omisión, y respecto de la acción podemos decir que es el aspecto positivo de la conducta ya que es el actuar o el hacer, lo que implica que el agente activo lleva a cabo varios movimientos corporales encaminados a cometer el injusto, y esto puede ser hecho por sí mismo o por medio de instrumentos, animales, mecanismos o mediante personas.

Por otro lado también dentro de la conducta el aspecto negativo es la omisión, y de esta podemos decir que también consiste en realizar la conducta típica pero a diferencia de la acción esta se realiza por medio de la abstención de actuar, esto es no hacer o dejar de hacer la acción que la ley exige que se realice a fin de evitar el delito por lo cual, es considerada a la omisión como la forma o el modo negativo del comportamiento.

La omisión se puede presentar de dos formas: por omisión simple o también puede haber comisión por omisión y estas a saber son:

“La omisión simple. También conocida como omisión propia, consiste en no hacer lo que se debe hacer, ya sea voluntaria o culposamente, con lo cual se produce, un delito, aunque no haya un resultado, de modo que se infringe una norma preceptiva; por ejemplo, portación de arma prohibida”.<sup>18</sup>

“comisión por omisión. También conocida como comisión impropia, es un no hacer voluntario culposo, cuya abstención produce un resultado material, y se infringen

---

<sup>17</sup> Cfr. Fernando Castellanos Tena, ob. Cit. P.145.

<sup>18</sup> Ibidem, p. 55.

una norma preceptiva y otra prohibitiva; por ejemplo, abandono de la obligación de alimentar a los hijos, con lo que se puede causar la muerte de éstos”.<sup>19</sup>

“El acto o la acción, strictu sensu, es todo hecho humano voluntario, todo movimiento voluntario del organismo humano capaz de modificar el mundo exterior o de poner en peligro dicha modificación. Según Cuello Calón, la acción en sentido estricto, es el movimiento corporal voluntario encaminado a la producción de un resultado consistente en la modificación del mundo exterior o en el peligro de que se produzca”.<sup>20</sup>

En sentido contrario podemos afirmar que la omisión consiste en un no hacer o inactividad involuntaria, violando la ley penal cuanto ésta impone el deber de hacer o de ejecutar un hecho determinado.

Así mismo Sebastián Soler, uno tratadista de Derecho penal, considera que el delincuente puede infringir o violar la ley, y que lo puede hacer sin que este mueva un solo musculo de su cuerpo, realizándolo por medio de una omisión o una abstención a la que llamamos omisión.

- **El resultado**

“El resultado no es solo el daño cometido por el delito, no consiste únicamente en el cambio material en el mundo exterior, sino también en mutaciones de orden moral. El peligro corrido de que habló elegantemente Carrara, es el resultado en la tentativa. No se produjo muerte del sujeto en el conato de homicidio, pero se alteró el mundo exterior, lesionando la seguridad, la tranquilidad de la víctima”.<sup>21</sup>

“Para nosotros no existe delito sin resultado, la vieja categoría de delitos formales es falsa. Lo que acontece en ciertas infracciones es que la manifestación de la voluntad y el resultado aparecen contemporáneamente y con aspectos inseparables”.<sup>22</sup>

---

<sup>19</sup> Ibidem, pp. 55-56.

<sup>20</sup> Fernando Castellanos tena, op.cit. p 142.

<sup>21</sup> Luis Jiménez de Asúa, la ley y el delito, Argentina, LexisNexis Abeledo-Perrot, 4ª ed., 2005, p. 214.

<sup>22</sup> Ibidem, p. 214.

“Los delitos formales son delitos de simple actividad o meros delitos de acción”.<sup>23</sup>

En los delitos de simple actividad, se agota el tipo en el movimiento corporal del agente, no siendo necesario un resultado externo. Esto es, que no es necesario que se materialice o que se altere el mundo exterior, esto es que suelen ser delitos de los que se llaman que ponen en peligro el bien jurídico tutelado, aunque el daño no se materialice.

“Los delitos materiales, son los delitos de resultado externo”.<sup>24</sup>

Otra forma de llamar a los delitos materiales, es por el nombre de delitos de lesión, y al respecto podemos decir que “La mayor parte de las conductas- típicas contenidas en el libro segundo del código penal son de lesión, y se caracterizan por requerir del daño del bien jurídico para considerarse como ‘hechos consumados’. En este sentido, la conducta-típica de violación es de lesión, porque para considerarse consumada necesita haberse impuesto la copula por medio de la violencia física o moral y de esta forma haber lesionado la libertad sexual”.<sup>25</sup>

El delito, no deja de ser una conducta humana, y durante el tiempo ha tenido varios nombres como son el acto, el hecho etc. Pero actualmente el nombre y el concepto más aceptado es el de conducta. Y dentro de esta podemos darnos cuenta de que puede desplegarse de dos maneras que a saber son, la acción y la omisión.

La acción tiene cuatro elementos que son, la voluntad, la actividad, el resultado y el nexo de causalidad, en relación al último, debemos de tomar nota que el nexo causal debe de ser material, ya que si es moral, espiritual o psicológico, será irrelevante para el derecho penal.

La acción es un movimiento corporal positivo que va encaminado a producir un resultado, mientras que la omisión es el aspecto negativo de la acción y que también puede ir encaminado a la producción de un resultado, por medio de la abstención o de un no actuar, en la omisión podemos encontrar dos tipos de omisiones, una de ellas

---

<sup>23</sup> Ibidem, p. 215.

<sup>24</sup> Ibidem, p. 215.

<sup>25</sup> Enrique Díaz-Aranda, ob.cit. p. 192

es la omisión simple, y la otra es llamada comisión por omisión. En cuanto a la voluntariedad, tanto de la acción como de la omisión requieren de la voluntad del sujeto activo para la búsqueda de ese resultado, ya que la pura acción sin la voluntad de producir un resultado, no es relevante para el Derecho penal.

Podemos decir del resultado que es la consecuencia de la conducta, el fin buscado por el sujeto activo y que está previsto en la ley penal. Y estos pueden ser de dos tipos, los cuales son los delitos de resultado formal y los delitos de resultado material, los primeros son aquellos que son considerados de simple actividad, esto es son delitos que no modifican el mundo exterior, y que nada más ponen en riesgo o en peligro el bien jurídico tutelado, un ejemplo de este tipo de delitos es la portación de armas reservadas para el uso exclusivo del ejército y de las fuerzas armadas; mientras que los delitos de resultado material, son aquellos que también son llamados de lesión, en virtud que al desplegar la conducta el agente lesiona los bienes jurídicamente tutelados por el derecho. Modificando con este resultado, el mundo exterior, un ejemplo de ello es la violación.

### **Ausencia de conducta**

Se define como un aspecto negativo del delito, la ausencia de conducta, es decir, si falta alguno de los elementos esenciales del delito, éste no se integrará; en consecuencia, si la conducta está ausente, evidentemente no habrá delito a pesar de las apariencias; impeditivo de la formación de la figura delictiva, por ser la actuación humana, positiva o negativa, la base indispensable del delito.

Hay ausencia de conducta e imposibilidad de integración del delito, cuando la acción u omisión son involuntarias, es decir, cuando el movimiento corporal o la inactividad no pueden atribuirse al sujeto, por faltar en ellos la voluntad.

Un acto u omisión es el primer elemento del delito, supone la existencia de un ser dotado de voluntad que lo ejecuta, comprensiva del aspecto positivo acción y del negativo omisión que produce un resultado.

Eugenio Zafaroni refiere que “el concepto positivo de acción, se deduce ante todo, la inexistencia de acto en cualquier hecho en que no participe un ser humano, no obstante el hombre es un ente físico, puede intervenir en un hecho sólo en este carácter y tampoco hay en este supuesto una conducta humana, de allí se deduce que no cualquier intervención de un ser humano en un acontecimiento constituye una conducta”.<sup>26</sup>

Si la conducta comprende tanto la acción como la omisión, la ausencia o falta de aquélla, abarca la ausencia de acción o de omisión, es decir, el aspecto negativo entraña la actividad y la inactividad no voluntarias.

El resultado, consiste en obrar u omitir del hombre que producen un conjunto de efectos en el mundo naturalístico, se identifica como un acontecimiento o suceso, comprendiéndose en él tanto el actuar, positivo o negativo, como los efectos producidos.<sup>27</sup>

De lo anterior, se precisa que el resultado es un efecto de la conducta, pero no todo efecto de ésta tiene tal carácter, sino sólo aquel o aquellos relevantes para el Derecho Penal por cuanto éste lo recoge dentro del tipo penal.

Al faltar la conducta no llega a configurarse el elemento objetivo y, por consiguiente, no hay antijuridicidad, y por ende no hay culpabilidad, por último punibilidad.

La ausencia de la conducta, el resultado y un nexo causal impide el nacimiento del hecho, resultando indispensable el nexo causal para atribuir un resultado a la conducta de un hombre, solo es propio hablar de nexo causal con relación a aquellas conductas productoras de un resultado material, pues únicamente en el mundo naturalístico y no en el jurídico tiene vivencia tal fenómeno; “el nexo causal es la relación existente entre la conducta y el resultado y mediante la cual se hace posible la atribución material de ésta a aquella como a su causa”.<sup>28</sup>

---

<sup>26</sup> ZAFFARONI, Eugenio Raúl. *Teoría del Delito*, Sociedad Anónima Editora, Comercial, Industrial y Financiera, Ediar, p.145.

<sup>27</sup> CASTELLANOS TENA, Fernando. *Lineamientos Elementales del Derecho Penal, Parte General*, México, Editorial Porrúa, p. 155, 2010.

<sup>28</sup> Citado por CASTELLANOS TENA, Fernando. *Lineamientos Elementales del Derecho Penal, Parte General*, México, Editorial Porrúa, 2010.

La acción y el resultado, por estar en estratos distintos dado que la acción se perfecciona sólo con la voluntad y su manifestación, y el resultado constituye en la descripción de ciertos tipos penales.

La forma en que sólo puede expresarse la conducta en acción u omisión, es decir, en una actividad o movimiento corporal, o bien en una inactividad, una abstención, un no hacer, ambas conductas tienen una íntima conexión con un factor de carácter psíquico que se identifica con la voluntad de ejecutar la acción o de no verificar la actividad esperada. Por tanto, al haber acción u omisión como movimiento corporal hay conducta, pero no todo movimiento muscular es una acción.

De la misma forma, una inactividad, es un no hacer, pero no toda inactividad es una omisión. Si acción y omisión son las formas de conducta, cabría concluir que no toda actividad o inactividad integran una conducta humana, salvo cuando ambas fueran voluntarias. La volición, constituye el elemento o coeficiente psíquico indispensable para integrar una acción o una omisión, es decir, una conducta.

El movimiento corporal sin voluntad, como la inactividad involuntaria, no conforman una conducta, considerada por el Derecho, pues la expresión puramente física o materialmente faltaría el coeficiente necesario para atribuir, la acción o la omisión a un sujeto y decir que tal conducta es suya.

- **Casos de ausencia de conducta**

Los casos significativos son los que pese a la protagonización por un hombre no hay una acción humana, tales como: la fuerza física irresistible y fuerza mayor, la involuntariedad (finca en estado de inconsciencia).

Se ejemplifica; la madre que en un agitado sueño al moverse sofoca o mata con su cuerpo a su recién nacido, colocado ahí sin su consentimiento de aquélla. El sujeto que sin saber que se encontraba su menor hijo durmiendo en el sofá, avienta su prenda ocasionándole sofocamiento o muerte del menor. Casos en los que no fue previsto.

Desde el punto de vista penal no actúa quien en una conclusión epiléptica deja caer un valioso jarrón que tenía en ese momento en la mano, a diferencia de quien aparta la mano de una placa al rojo vivo rompiendo con ello un valioso objeto.

#### **a) *Vis absoluta***

Francisco Pavón Vasconcelos refiere que ya Carrancá y Trujillo, comprendía a la *vis absoluta*, como causa de exclusión de delito.

En el Artículo 15, Fracción I, del Código Penal Federal, ha recibido en la doctrina el nombre de fuerza física irresistible, en ella el sujeto el sujeto productor de la última condición en el proceso material de la causalidad, pone a contribución en la verificación del resultado su movimiento corporal o su inactividad.

Esta debe ser exógena, proveniente del exterior y no del sujeto. Debe entenderse una fuerza de entidad, tal que haga al sujeto incapaz de dirigir sus movimientos, es decir, que lo haga obrar mecánicamente, no es una acción humana, porque supone ausencia del coeficiente psíquico en el sentido valorativo del derecho, por no existir la manifestación de la voluntad, sino “es un mero instrumento de una voluntad ajena puesta en movimiento a través de una fuerza física”.<sup>29</sup>

Esta fuerza puede provenir de una conducta humana y de una fuerza de la naturaleza, tanto una fuerza natural (viento, inundación, fuego), como una acción humana, pueden dar lugar a una causa de inculpabilidad o a una ausencia de acto, cualquiera de ambas cuando revista una entidad tal que prive al ser humano de la posibilidad de conducirse, de dirigir sus movimiento.

#### **b) *Vis maior***

En la fuerza mayor se presenta similar fenómeno al de *vis absoluta*, la actividad o inactividad involuntarias por actuación sobre el cuerpo del sujeto, de una fuerza exterior a él, de carácter irresistible, originada en la naturaleza o en seres irracionales. La fuerza mayor es una energía no humana, física, irresistible, padecida por un sujeto

---

<sup>29</sup> PAVÓN VASCONCELOS, Francisco. *Derecho Penal Mexicano*, México, Editorial Porrúa, 2010.

que se ve arrollado en la producción de un hecho cuyo resultado no es posible atribuir al sujeto, por ser patente la ausencia de su conducta.

Por fuerza mayor hay que entender en general toda fuerza externa que por su poder superior determine a la persona necesaria e inevitablemente a realizar un acto positivo o negativo.

### **c) Movimientos reflejos**

Son movimientos corporales involuntarios, puede ser que el sujeto los controle o retardarlos, pero ya no funcionan como factores negativos del delito. Los actos reflejos que ocasionan resultados lesivos a bienes jurídicos del delito y particularmente de la conducta en que está ausente la acción, en virtud de ser ajenos a la voluntad del individuo. Se les estima actos de la naturaleza inconsciente originados como respuestas del organismo a estímulos externos. Son originados por la excitación de los nervios motores y ajenos al influjo anímico; se producen de inmediato por un estímulo fisiológico corporal sin intervención de la conciencia, estímulo que pasa de un centro sensorio a uno motor productor de movimiento.

### **d) El sueño**

Conocido como “fenómeno psíquico, el sujeto realiza la actividad o inactividad sin voluntad, por hallarse en un estado en el cual su conciencia se encuentra suprimida y ha desaparecido la fuerza inhibitoria”.<sup>5</sup> Es un estado fisiológico normal de descanso del cuerpo y de la mente consciente, que puede originar movimientos involuntarios del sujeto con resultado dañoso.

### **e) El sonambulismo**

Existe una conducta más falta una verdadera conciencia, el sujeto se rige por imágenes de la sub-conciencia provocadas por sensaciones externas o internas y por estímulos somáticos o psíquicos, que sólo producen una imagen de conciencia, que no corresponde a la realidad. Parecido al sueño, éste se distingue porque el sujeto deambula dormido. Hay movimientos corporales inconscientes y por ello involuntarios.



Para algunos autores como Jiménez de Asúa el sonambulismo “es una enfermedad nerviosa, o posiblemente no es más que una manifestación parcial de otras neuropatías o de epilepsia, según han observado psiquiatras”.

#### **f) El hipnotismo**

En esta la inimputabilidad estriba derivada del estado que guarda el sujeto, en el que se dice hay una obediencia automática hacia el sugestionador, sin que tenga relevancia el argumento, sólo por el simple hecho de que se trata de un trastorno funcional de las facultades de conocer y querer, tratándose de una inimputabilidad.

Consiste en una serie de manifestaciones del sistema nervioso producidas por una causa artificial. Tales manifestaciones pueden ir, desde un simple estado de somnolencia hasta un sonambúlico, pasando por diversas fases en las cuales se acentúa en sus características externas el grado de hipnotismo. El estado sonambúlico del hipnotismo se identifica por la ausencia del dolor y del olvido de lo sucedido durante el sueño hipnótico, el sujeto animado de vida ajena obra por mandato del hipnotizador.

La fuerza irresistible es un acto de fuerza proveniente del exterior que actúa materialmente sobre el agente. La fuerza debe ser absoluta, de tal manera que al no serlo, el sujeto puede resistirla o por lo menos tiene esa posibilidad.

La involuntariedad del actuar al impulso de esa fuerza exterior e irresistible impide la integración de la conducta y por ello la fuerza mayor, como la bis absoluta, conforman casos de inexistencia del delito por ausencia de conducta.

Los movimientos reflejos tales como las convulsiones epilépticas o los movimientos instintivos de defensa, no constituyen acción, ya que el movimiento no está en estos casos controlado por la voluntad.

Los movimientos reflejos son reacciones impulsivas o explosivas, en los que la voluntad participa, así sea fugazmente, y que por lo tanto no excluye la acción.

También falta de acción en los estados de inconsciencia, tales como el sueño, el sonambulismo, en estos casos los actos que se realizan no dependen de la voluntad y, por consiguiente, no pueden considerarse acciones penalmente relevantes.

En los estados de inconsciencia falta la acción, pueden ser penalmente relevantes si el sujeto se ha colocado voluntariamente para hacerlo.

### **3.2 Tipicidad y atipicidad**

Segundo elemento del delito en la teoría heptatómica.

#### **Tipicidad**

Para la existencia del delito se requiere una conducta o hechos humanos; mas no toda conducta o hecho son delictuosos; precisa, además, que sean típicos, antijurídicos y culpables. “La tipicidad es uno de los elementos esenciales del delito cuya ausencia impide su configuración habida cuenta de que nuestra constitución federal en su artículo 14 establece en forma expresa... ‘en los juicios del orden criminal queda prohibido imponer, por simple analogía y aun por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata’, lo cual significa que no existe delito sin tipicidad.

No debe confundirse el tipo con la tipicidad. El tipo es la creación legislativa, la descripción que el estado hace de una conducta, en los preceptos penales. La tipicidad es la adecuación de una conducta concreta con la descripción legal formulada en abstracto basta que el legislador suprima de la ley penal un tipo, para que el delito quede excluido.

Hay tipos muy completos en los cuales se contienen todos los elementos del delito como ocurre, por ejemplo, en el de allanamiento de morada, en donde es fácil advertir la referencia típica a la culpabilidad, al aludir a los conceptos “con engaños ‘furtivamente’, etc. En este caso y en otros análogos, es correcto decir que el tipo consiste en la descripción legal de un delito.

Sin embargo, en ocasiones la ley se limita a formular la conducta prohibida (u ordenada en los delitos omisivos); entonces no puede hablarse de descripción del delito, sino de una parte del mismo. Lo invariable es la descripción del comportamiento antijurídico (a menos que opere un factor de exclusión del injusto, con la legítima defensa). En razón a esto, El profesor Mariano Jiménez Huerta, en su obra la tipicidad define el tipo como el injusto recogido y descrito en la ley penal.

En concreto: el tipo a veces es la descripción legal del delito y en ocasiones, la descripción del elemento objetivo (comportamiento), como sucede en el homicidio, pues según el código, lo comete (el que priva de la vida a otro).<sup>30</sup>

“La tipicidad es la adecuación de la conducta al tipo penal. En este contexto diversos autores han dado su definición de tipicidad; dentro de las más importantes tenemos la expresada por Francisco Blasco y Fernández de Moreda, la cual dice ‘la acción típica’ es solo aquella que se acomoda a la descripción objetiva, aunque saturada a veces de referencia a elementos normativos y subjetivos del injusto de una conducta generalmente se reputa delictuosa, por violar, en la generalidad de los casos, un precepto, una norma, penalmente protegida”.<sup>31</sup>

Para Laureano Landaburu “la tipicidad consiste en esa cualidad o característica de la conducta punible de ajustarse o adecuarse a la descripción formulada en los tipos de la ley penal”.<sup>32</sup>

Para Jiménez De Asúa, la tipicidad es “la exigida correspondencia entre el hecho real y la imagen rectora expresada en la ley en cada especie de infracción”.<sup>33</sup>

Y para Jiménez Huerta considero que la “adecuación típica significa, encuadramiento o subsunción de la conducta principal en un tipo de delito y subordinación o vinculación al mismo de las conductas accesorias”.<sup>34</sup>

---

<sup>30</sup> Fernando Castellanos, *Lineamientos Elementales de Derecho Penal*, México, Editorial Porrúa, 2006, pp. 167,168.

<sup>31</sup> Eduardo López Betancourt, *Teoría del Delito*, México, Editorial Porrúa, 2007, p.117.

<sup>32</sup> Laureano Landaburu, *El delito como Estructura*, Revista Penal I, Numero 1, p.443.

<sup>33</sup> Luis Jiménez de Asúa, *Tratado de Derecho penal, III, 2ed*, Editorial Lozada, S.A., Buenos Aires, 1985, p.744.

<sup>34</sup> Mariano Jiménez Huerta, *La Tipicidad*, Editorial Porrúa, México, 19955, p. 207.

“La tipicidad es el encuadramiento de una conducta con la descripción hecha en la ley; la coincidencia del comportamiento con el descrito por el legislador, es en suma la acuñación o adecuación a un hecho a la hipótesis legislativa”.<sup>35</sup>

Para Celestino Porte Petit “la tipicidad es la adecuación de la conducta al tipo, que se resume en la fórmula *nullum crimen sine tipo*.”<sup>36</sup>

“La historia de la tipicidad es, consecuentemente, la historia del tipo. El tipo era considerado antiguamente en Alemania como el conjunto de caracteres integrantes del delito, tanto los objetivos como los subjetivos; esto, incluyendo el dolo o la culpa, era para lo que los antiguos escritores españoles figura de delito.

En 1906 aparece en Alemania la doctrina de *Beling*; considera el tipo como una mera descripción. Posteriormente Max Ernesto Mayer, en su *trato de derecho penal* (1915) asegura que la tipicidad no es meramente descriptiva sino indicaría de la antijuridicidad. En otras palabras: no toda conducta típica es antijurídica pero si toda conducta típica es indiciaria de antijuridicidad; en toda conducta típica hay un principio, una probabilidad de antijuridicidad.

El concepto se modifica en Edmundo Mezger, para quien el tipo no es simple descripción en una conducta antijurídica, si no la *ratio essendi* de la antijuridicidad; es decir, la razón de ser de ella, su real fundamento no define al delito como conducta típica, antijurídica y culpable sino como acción típicamente antijurídica y culpable.”<sup>37</sup>

Según Mezger “el que actúa típicamente actúa también antijurídicamente, en tanto no exista una causa de exclusión del injusto. El tipo jurídico-penal... es fundamento real y de validez (*ratio essendi*) de la antijuridicidad, aunque a reserva siempre, de que la acción no aparezca justificada en virtud de una causa especial de exclusión del injusto si tal ocurre, la acción no es antijurídica, a pesar de su tipicidad”.<sup>38</sup>

“La tipicidad es la razón de ser de la antijuridicidad, por supuesto, con referencia a ordenamiento positivo, porque siempre hemos sostenido que, desde el punto de vista

<sup>35</sup> Fernando Castellanos, *Lineamientos Elementales de Derecho Penal*, Editorial Porrúa, 2006, p. 168.

<sup>36</sup> *Importancia de la Dogmática Jurídico Penal*, p. 37.

<sup>37</sup> Fernando Castellanos, *Lineamientos Elementales de Derecho Penal*, Editorial Porrúa, 2006, p. 169.

<sup>38</sup> Rodríguez Muñoz Traducción, *Tratado de Derecho Penal*, t .I, Madrid 1955,p. 375

del proceso formativo del derecho, la antijurídica, al contrario, es *ratio essendi* del tipo, pues el legislador crea las figuras penales por considerar antijurídicos los comportamientos en ellas descritos. En otro giro: la ley consigna los tipos y conmina con pena las conductas formuladas, por ser opuestas a los valores que el estado está obligado a tutelar.

Antaño siguiendo a Mayer, estimábamos al tipo como la *ratio cognoscendi* de la antijuridicidad; es decir, como indiciario de ella. Sin embargo, al reflexionar sobre los casos en los cuales existe certidumbre de dicha antijuridicidad (por no operar causa de justificación alguna) advertimos que no permanece a manera de mero indicio, si no como absoluta contradicción al orden jurídico. Por ende, hemos llegado a la conclusión de que asiste razón a Mezger, al observar como toda conducta típica es siempre antijurídica (salvo la presencia de una justificante por ser en los tipos en donde el legislador establece las prohibiciones y mandatos indispensables para asegurar la vida comunitaria. Solo resta hacer hincapié en que al tiempo de advertir la existencia de una justificante, no significa anulación de la antijuridicidad pues esta no existió jamás; la conducta, desde su nacimiento estuvo acorde con el derecho. Tal sucede, por ejemplo, en la legítima defensa, al descubrirla debe declararse que el comportamiento del agente estuvo justificado siempre. No se torna lícito lo que nunca fue contrario al orden jurídico”<sup>39</sup>.

“Si admitimos que el tipo es la razón de ser de la antijuridicidad, hemos de atribuirle un carácter delimitador y de trascendental importancia en del derecho liberal, por no haber delito sin tipo penal (*nulum crimen sine lege, equivalente a nullum crimen sine tipo*). Para Luis Jiménez De Asúa, la tipicidad desempeña una función predominantemente descriptiva que singulariza su valor en el concepto de las características del delito y se relaciona con la antijuridicidad por concretarla en el ámbito penal. La tipicidad no solo es pieza técnica. Es, como secuela del principio legalista, garantía de la libertad”.<sup>40</sup>

---

<sup>39</sup> Fernando Castellanos, *Lineamientos Elementales de Derecho Penal*, Editorial Porrúa, 2006, pp. 169 y 170.

<sup>40</sup> *La Ley y El Delito*, Edición A. Bello, Caracas, pp. 315 y 332.

**Atipicidad.**

“Cuando no se integran los elementos descritos en el tipo legal, se presenta el aspecto negativo del delito llamado atipicidad. La tipicidad es la ausencia de adecuación de la conducta al tipo. Si la conducta no es típica, jamás podrá ser delictuosa.

Suele distinguirse entre ausencia de tipo y de tipicidad; la primera se presenta cuando el legislador, deliberada o inadvertidamente, no describe una conducta que, según el sentir general, debería ser incluida en el catálogo de los delitos. En el código penal Veracruzano presente se suprimió el tipo delictivo que figuraba en el ordenamiento anterior, integrado con un adulterio en condiciones determinadas; he ahí una ausencia de tipo”.<sup>41</sup>

“La importancia de la tipicidad es fundamental, ya que si no hay una adecuación de la conducta al tipo penal podemos afirmar que no hay delito.

Debemos tener cuidado de no confundir tipicidad con tipo; la primera se refiere a la conducta y el segundo pertenece a la ley, a la descripción o hipótesis plasmada por el legislador sobre un hecho ilícito; es la fórmula legal a la que se debe adecuar la conducta para la existencia de un delito.

En cambio, la ausencia de tipicidad surge cuando existe el tipo, pero no se amolda a él la conducta dada, como en el caso de la copula con personas mayor de dieciocho años, obteniendo su consentimiento mediante engaño; el hecho no es típico por falta de adecuación exacta a la descripción legislativa en donde precisa para configurarse el delito de estupro, que la ofendida sea menor de dieciocho años (según el precepto anterior a la reforma).

En el fondo en toda atipicidad hay falta de tipo; si un hecho específico no encuadra adecuadamente en el descrito por la ley, respecto del no existe tipo.

Ahora de manera destacada, nuestro Código Penal se refiere a la ausencia de tipicidad. Se incluyó en la fracción II del artículo 15 relativo en las causas de exclusión

---

<sup>41</sup> Fernando Castellanos, *Lineamientos Elementales de Derecho Penal*, Editorial Porrúa, 2006, p. 175.

del delito, cuando ´se demuestre la inexistencia de alguno de los elementos que integran la descripción típica del delito de que se trate.´

Las causas de atipicidad pueden reducirse a las siguientes a) ausencia de la calidad o del número exigido por la ley en cuanto a los sujetos activos y pasivo; b) si faltan el objeto material o el objeto jurídico; c) cuando no se dan las referencias temporales o espaciales referidas con el tipo; d) al no realizarse el hecho por los medios comisivos específicamente señalados en la ley; e) si faltan los elementos subjetivos del injusto legalmente exigidos; y, f) por no darse, en su caso, la antijuricidad especial.

En ocasiones el legislador, al describir el comportamiento, se refiere a cierta calidad en el sujeto activo, en el pasivo, o en ambos; tal ocurre, por ejemplo, en el delito de peculado, en el cual el sujeto activo ha de ser encargado de un servicio público (artículo 223 del Código Penal de 1931).

Sin la institución o el interés por proteger, no habrá objeto jurídico, como la falta de propiedad o posesión en delitos patrimoniales presentara una atipicidad por no existir objeto material sobre el cual recaiga la acción, como cuando se pretenda privar de la vida a quien ya no la tiene (en este caso tampoco hay objeto jurídico).

“El artículo 302 dice: ´comete el delito de homicidio el que priva de la vida a otro.´

´A veces el tipo describe el comportamiento bajo condiciones de lugar o de tiempo; si no operan, la conducta será atípica; por ejemplo, cuando la ley exige la realización del hecho ´en despoblado´; ´con violencia´, (como en el tipo del delito de asalto, a que se refiere el artículo 286; y los ilícitos contra la administración de justicia tipificados en las fracciones XIV y XVII del artículo 225 del Código Penal)´.

“Si la hipótesis legal precisa de modalidades específicas, estas han de verificarse para la integración del ilícito; por medio de la violencia física o moral..., como en el caso de la violación (artículo 265).

Hay tipos donde se contienen elementos subjetivos del injusto; estos constituyen referencias típicas a la voluntad del agente o al fin que persigue.

Diversas descripciones delictivas aluden a los conceptos: 'intencionalmente', 'a sabiendas', 'con el propósito', Su ausencia hará operar una atipicidad (como ocurre, en los tipos relativos a los artículos 199 bis. 277, 323, etcétera).

Por excepción, algunos tipos captan una especial antijuridicidad, como sucede, por ejemplo, en el artículo 285 del Código Penal (allanamiento de morada) al señalar en la descripción, que el comportamiento se efectuó 'sin motivo justificado, fuera de los casos en que la ley lo permita' entonces al lograr justificadamente, con la permisión legal, no se colma el tipo y las causas que en otros delitos serian, por su naturaleza, causas de justificación, tornándose atipicidades en estos casos."<sup>42</sup>

En el estudio de la tipicidad nos deja claro que es el encuadramiento de una conducta con la descripción hecha en la ley; la coincidencia del comportamiento con el descrito por el legislador, es en suma la acuñación o adecuación a un hecho a la hipótesis legislativa", así mismo nos explica que no debemos de confundir al tipo con la tipicidad ya que el primero es la creación legislativa, la descripción que el estado hace de una conducta, en los preceptos penales y la segunda es la adecuación de una conducta concreta con la descripción legal formulada por un abstracto basta que el legislador suprima de la ley penal un tipo, para que el delito quede excluido. La tipicidad cuenta con tipos y clasificaciones, mientras que la atipicidad carece de esos pasos y sólo cuenta con falta de ausencia, falta de elementos, todo en sentido negativo.

Ausencia de tipo y atipicidad son dos figuras diferentes, en la primera la conducta no es sancionable, no existe un tipo penal, aun cuando la sociedad considere que afecta socialmente, la ley penal no la contempla, hay una ausencia total del hecho ante la misma. Un ejemplo puede ser el adulterio que hasta hace poco era sancionable en el

---

<sup>42</sup> Fernando Castellanos, *Lineamientos Elementales de Derecho Penal*, Editorial Porrúa, 2006, pp. 176 y 177.



distrito federal, alguien podría pensar que debiera seguir vigente, sin embargo esa conducta dejó de ser delictiva.

En cuanto a la segunda se puede definir a la atipicidad como la ausencia de adecuación de la conducta al tipo. Eduardo López Betancourt la considera como “La falta de adecuación de la conducta al tipo penal. Es el aspecto negativo de la tipicidad”.<sup>43</sup>

Al respecto Luis Jiménez de Asúa manifiesta “A de afirmarse, pues, que existe ausencia de tipicidad en estos dos supuestos:

a) Cuando no concurren en un hecho concreto todos los elementos del tipo descritos en el código penal o en la leyes penales, y puesto que son varias las relaciones y elementos de los tipos, distintas son también las hipótesis que pueden concebirse (atipicidad, propiamente dicha);

b) Cuando la ley penal no ha descrito la conducta que en realidad se nos presenta con característica antijurídica (ausencia de tipicidad en sentido escrito)”.<sup>44</sup>

### **Fundamento Legal.**

El Código Penal Federal en su artículo 15 establece:

El delito se excluye cuando

II. Se demuestre la inexistencia de alguno de los elementos que integran la descripción típica del delito de que se trate.

El Código Penal del Distrito Federal en su artículo 29 nos señala:

El delito se excluye cuando:

II. (Atipicidad) Falte alguno de los elementos que integran la descripción legal del delito del que se trate

---

<sup>43</sup> Eduardo López Betancourt, *Teoría del delito*, México, Ed. Porrúa, 1994, p.140.

<sup>44</sup> Luis Jiménez de Asúa, *Tratado de derecho penal*, Buenos Aires, III edición, Ed. Losada, 1963, p. 940.

De lo anterior se puede deducir la frase *nullum poena sine lege* “No hay pena sin ley”, la conducta no llega a ser típica por falta de alguno de los elementos descriptivos del tipo, ya sea en la calidad de los sujetos (activo o pasivo), condiciones del objeto, del tiempo o lugar, así como de los elementos subjetivos o normativos del injusto.

Para Luis Jiménez de Asúa la atipicidad se dará cuando exista:

1. Ausencia de adecuación típica por falta de sujeto activo
2. Ausencia de adecuación típica por falta de sujeto pasivo o de objeto
3. Ausencia de adecuación típica por falta de las referencias temporales o espaciales
4. Ausencia de adecuación típica por falta del medio previsto
5. Ausencia de adecuación típica por carencia de los elementos subjetivos del injusto
6. Ausencia de adecuación típica por carencia de elementos normativos

Existe atipicidad, por la ausencia de elementos objetivos, porque el tipo pide determinada calidad del sujeto activo o pasivo, ejemplo: En el delito de cohecho artículo 222 del Código Penal Federal o artículo 272 del Código Penal del Distrito Federal, señalando que debe de ser un “servidor público” el que ejecute el acto.

Por la ausencia del bien jurídico tutelado en los delitos patrimoniales, por no existir la propiedad. Fernando Castellanos Tena manifiesta “sin la institución o el interés por proteger no habrá objeto jurídico, como la falta de propiedad o posesión en delitos patrimoniales. Se presentará una atipicidad por no existir objeto material sobre el cual recaiga la acción, como cuando se pretenda privar de la vida a quien ya no la tiene (en este caso tampoco hay objeto jurídico)”.<sup>45</sup>

En cuanto a las referencias de tiempo o espacio, si éstas no se dan, el delito no existe, por ejemplo en el delito de asalto artículo 286 del Código Penal Federal, establece “que debe ser en despoblado o paraje solitario”. En robo calificado la acción

---

<sup>45</sup> Fernando Castellanos Tena, *Lineamientos Elementales de Derecho Penal*, México, XVI edición, Ed. Porrúa, 1981, p. 173.

podrá ser atípica por la falta de la violencia artículo 372 del Código Penal Federal. Es importante señalar que puede faltar un elemento para integrar el tipo, pero esa conducta se puede ajustar a otro precepto legal siendo sancionado el infractor por un delito diferente del que se tenía previsto.

### **Naturaleza jurídica del consentimiento en la atipicidad.**

En las causas de atipicidad se plantea la naturaleza jurídica del consentimiento, al respecto Gerardo Armando Urosa Ramírez nos comenta: “debe precisarse que el excluyente del delito establecida en la fracción III del artículo 15 y 29 del Código Penal Federal y Código Penal del Distrito Federal, respectivamente, que prevé al consentimiento como excluyente del delito, es motivo de polémica. En efecto, se discute si se trata de una causa de atipicidad o justificación, debiendo de aclararse que la excluyente en estudio goza de una doble condición dependiendo del tipo penal en que se presente, pues si la descripción típica alude completamente al ‘consentimiento’ o un sinónimo, se estará ante una causa de atipicidad, en caso contrario operara como causa de justificación”.<sup>46</sup>

Como ejemplo de lo anterior tenemos al delito de robo previsto en el artículo 367 del Código Penal Federal “el que se apodere de una cosa ajena sin consentimiento de la persona...”

#### **Jurisprudencia.**

Quinta Época

Instancia: Sala auxiliar

Fuente: Semanario Judicial de la Federación

Tomo: GXXII

Página: 1348

CONSENTIMIENTO DEL OFENDIDO. Es sabido que el consentimiento del titular del bien jurídico lesionado a virtud del proceso delictivo, siendo anterior o coetáneo a la acción, destruye la antijuridicidad o el tipo; es decir, si el pasivo de una conducta delictiva presenta su consentimiento para que se realice ésta, no resulta afectado el bien jurídico que se tutela,

---

<sup>46</sup> Gerardo Armando Urosa Ramírez, *Teoría de la Ley Penal del Delito*, México, Ed. Porrúa, 2006, p. 143.

siempre que el consentimiento recaiga sobre bienes jurídicos disponibles. El consentimiento destruye el tipo, esto es, impide que éste se integre, cuando en la descripción legal se consagra como elemento constitutivo del delito la ausencia del consentimiento por parte del titular. Ejemplo de esto último es el robo, y de lo primero el daño en propiedad ajena, en el cual se tutela el patrimonio de las personas, que es un bien jurídico disponible. En el caso, estando demostrado el consentimiento para que la destrucción de unos cuartos se llevara a cabo, no puede sostenerse que la conducta realizada por los quejosos sea antijurídica; no hay delito sin antijuridicidad y no puede imponerse pena cuando la conducta realizada no es antijurídica. Amparo penal directo 4699/52. Scolari Llaguno Humberto y coagraviado. 22 de noviembre de 1954. Unanimidad de cuatro votos. Ausente: Rafael Matos Escobedo. La publicación no menciona el nombre del ponente.

### **La atipicidad en el delito culposo.**

Se da la atipicidad en la conducta culposa cuando falta el elemento subjetivo objetivo o normativo, cuando no se afecta al bien jurídico tutelado, por ausencia del nexo causal que acredite que el resultado le es atribuible a la gente por inexistencia a una violación del deber de cuidado o cuando no se esté en posibilidades de prever el resultado.

Eugenio Raúl Zaffaroni la describe así:

“Hay atipicidad culposa cuando el resultado no era previsible para el autor sea que no lo fuese porque se hallaba más allá de la capacidad de previsión (ignorancia vencible) o porque el sujeto se encontraba en un estado de error invencible de tipo.”<sup>47</sup>

Al respecto Gerardo Armando Urosa Ramírez nos comenta: “Habrá atipicidad conforme a nuestra legislación penal, cuando la conducta no se encuentre dentro del artículo que limitativamente señala como culposas a determinadas acciones típicas, excluyendo aquellas que no estén contempladas en dicho catálogo, acorde al sistema de numerus clausus o cerrados, reconocido por nuestra legislación penal en el segundo párrafo del artículo 60 del Código Penal Federal o el tercer párrafo del artículo 76 del Código Penal del Distrito Federal”.<sup>48</sup>

---

<sup>47</sup> Eugenio Raúl Zaffaroni, Manual de Derecho Penal, Buenos Aires, Ed. Cárdenas, 1985, p. 369

<sup>48</sup> Gerardo Armando Urosa Ramírez, Teoría de la Ley Penal del Delito, México, Ed. Porrúa, 2006, p. 164.

## **Efectos de la atipicidad.**

Eduardo López Betancourt nos señala las siguientes hipótesis:

- “a) No integración del tipo.
- b) Traslación de un tipo a otro (variación del tipo).
- c) Existencia de un delito imposible.

Se da la no integración del tipo, por ejemplo, cuando falte alguno de los elementos del estupro: La mujer sea mayor de 18 años; no haya seducción o engaño. Estamos frente a la traslación de tipo, como en el caso de faltar la relación de parentesco exigida por el tipo (parricidio) dándose un homicidio.

Se presenta una tentativa imposible cuando falta por ejemplo; el bien jurídico: la vida, o bien, el objeto material”.<sup>49</sup>

- **Ausencia de tipo.**

La ley penal no contempla la descripción de una conducta, que en ocasiones el sentir de la población es que debiera de existir el tipo penal, por considerarla dañosa socialmente hablando.

En conclusión, queda claro que la atipicidad resulta de la falta de uno o más elementos descriptivos del tipo, ya sea en cuanto a la calidad de los sujetos, la ausencia de adecuación por falta de referencias temporales o espaciales, ausencia del elemento subjetivo del injusto, ausencia del objeto material o jurídico, ausencia del elemento normativo.

La práctica en los juzgados penales está muy viciada, si los encargados de ayudar a los procesados (defensor de oficio), aplicaran el interés así como el conocimiento que se requiere para un desarrollo rápido y eficaz de un proceso, la población penitenciaria se reduciría.

---

<sup>49</sup> Eduardo López Betancourt, Teoría del delito, México, Ed. Porrúa, 1994, pp. 142, 143.

En cuanto a la ausencia de tipo, nuestros legisladores no tienen la preparación para elaborar las leyes que nuestro país necesita, su trabajo deja mucho que desear, creen que elevando las penas se puede contrarrestar la delincuencia.

Pero eso no es todo, urge una legislación acorde a los tiempos que vivimos, hecha por juristas especializados en la materia.

### **3. Antijuridicidad y causas de justificación.**

#### **Antijuridicidad.**

La antijuridicidad es un comportamiento típico en el que no concurre ninguna causa de justificación. La tipicidad es un indicio de antijuridicidad los comportamientos típicos suelen ser antijurídicos y debe ser corroborado con la ausencia de causas de justificación. Veremos más adelante cuáles son esas causas que justifican un hecho típico, dónde están reguladas y por qué se justifican.

#### **Causas de justificación**

Las causas de justificación son aquellas condiciones que tienen el poder de excluir la antijuridicidad de una conducta típica. Representa un aspecto negativo del delito; en presencia de algunas de ellas falta uno de los elementos esenciales del delito, a saber: la antijuridicidad, en tales condiciones la acción realizada a pesar de su apariencia, resulta conforme a derecho, a las causas de justificación también se les llama justificantes, causas eliminatorias de la antijuridicidad, causas de licitud.

A las justificaciones generalmente se les agrupa al lado de otras causas que anulan el delito, o mejor dicho, impeditivas de su configuración suele catalogarse bajo la denominación excluyente de responsabilidad, causas de incriminación etc. Nuestro código usa la expresión circunstancias excluyentes de responsabilidad, comprendiendo varios de naturaleza diversa.

Las justificaciones no deben ser confundidas con otras eximentes. Hay entre ellas una distinción precisa en función de los diversos elementos esenciales del delito que

anulan las causas de justificación, dice soler, son objetivas, referidas al hecho impersonales, las de inculpabilidad son de naturaleza subjetiva personal e intransitiva, los efectos de la primera, respecto de los participantes y en relación con cualquier clase de responsabilidad jurídica que se pretenda derivar del hecho en sí mismo.

### **a) Defensa legítima**

Dentro de las causas de justificación se halla la Defensa Legítima, por lo que siguiendo con un principio de orden deductivo, empezaremos por definir que son las causas de justificación: La causa de justificación es un hecho típico, el cual trae aparejado la antijuridicidad negativa, sin embargo en el momento de analizar el comportamiento antijurídico típico, nos encontramos con un desvalor de hecho típico, donde encontramos eximentes o justificaciones que lo permiten.

Desde un punto de vista material, la causa de justificación es un comportamiento típico singular, que da pie a la transgresión de un bien jurídico tutelado, con el consecuente hecho de colmar la conducta típica, es importante ser cuidadoso al analizar el tipo penal y la posible eximente justificativa, pues posiblemente se confunda la atipicidad de un tipo con la causa de justificación.

Por lo anterior, es destacable, analizar que sí falta, un elemento del tipo penal en el posible hecho singular que exima al elemento activo, o se integran todos los elementos del tipo penal y sin embargo, se encuentra dentro de las causas de justificación. Únicamente por ser parte de las causas de justificación y la defensa legítima está dentro de ellas, las mencionaré, sin entrar de modo alguno al tema por ser tópicos de otros miembros del grupo, a saber: Legítima Defensa, Estado de Necesidad, Cumplimiento de un Deber, Consentimiento del Ofendido y Ejercicio de un Derecho.

Con base en lo anterior, pasamos ahora a enfocarnos a la defensa legítima, consideramos que la misma es un comportamiento nato con el cual se trata de preservar la vida, en la antigua Roma se le consideraba como un derecho originario, el cual se limitaba al derecho por defender la vida y la integridad física del ciudadano romano, al día de hoy no sólo defiende la individualidad, sino además se contempla la

protección de la colectividad, y de otros bienes, esto se adquiere de la corriente germana, pues al defender al individuo, se defiende el orden jurídico general.

Veamos ahora su fundamento jurídico, en los numerales 29 fracción IV Del Código Penal para el Distrito Federal y el artículo 15 del Código Penal Federal, en ambos textos sustantivos se expresa el concepto de la siguiente forma:

“Art. 29 Causas de exclusión

El delito se excluye cuando:

IV. (Legítima defensa). Se repela una agresión real, actual o inminente y sin derecho, en defensa de bienes jurídicos propios o ajenos, siempre que exista necesidad de la defensa empleada y no medie provocación dolosa suficiente e inmediata por parte del agredido o de su defensor.

Se presume que existe legítima defensa, salvo prueba en contrario, cuando se cause un daño a quien por cualquier medio trate de penetrar o penetre, sin derecho, al lugar en que habite de forma temporal o permanente el que se defiende, al de su familia o al de cualquier persona respecto de las que el agente tenga la obligación de defender, a sus dependencias o al sitio donde se encuentren bienes propios o ajenos respecto de los que exista la misma obligación. Igual presunción existirá cuando el daño se cause a un intruso al momento de sorprenderlo en alguno de los lugares antes citados en circunstancias tales que revelen la posibilidad de una agresión; ...”

“Art. 15 Supuestos normativos de exclusión de los delitos

El delito se excluye cuando:

IV. Se repela una agresión real, actual o inminente, y sin derecho, en protección de bienes jurídicos propios o ajenos, siempre que exista necesidad de la defensa y racionalidad de los medios empleados y no medie provocación dolosa suficiente e inmediata por parte del agredido o de la persona a quien se defiende.

Se presumirá como defensa legítima, salvo prueba en contrario, el hecho de causar daño a quien por cualquier medio trate de penetrar, sin derecho, al hogar del agente,



al de su familia, a sus dependencias, o a los de cualquier persona que tenga la obligación de defender, al sitio donde se encuentren bienes propios o ajenos respecto de los que exista la misma obligación; o bien, lo encuentre en alguno de aquellos lugares en circunstancias tales que revelen la probabilidad de una agresión;...”

Nuestro máximo tribunal detenta esta tesis jurisprudencial, la cual a manera de guisa la transcribo, ya que los artículos en que se fundamenta la defensa legítima, son muy claros, sin embargo, llegan a generarse dudas al respecto:

“TESIS DE JURISPRUDENCIA. LEGÍTIMA DEFENSA. INEVITABILIDAD DE LA AGRESIÓN. "Doctrinalmente se ha establecido que para que la excluyente de legítima defensa pueda surtir efectos es menester que concurren, entre otros requisitos, el inherente a que la agresión, además de ilegítima y actual, debe ser inevitable". (Amparo directo 33/95. Ponente: Luis Alfonso Pérez y Pérez. Amparo en revisión 60/95. Ponente: José Pérez Troncoso. Amparo directo 562/94. Ponente: José Pérez Troncoso. Amparo directo 553/95. Ponente: Gilberto González Bozziere. Amparo directo 584/95. Ponente: José Pérez Troncoso. Novena Época. Tribunales Colegiados de Circuito. Semanario Judicial de la Federación y su Gaceta. Tomo III. Junio de 1996. Tesis VII.P. J/14. Página 647)”

Como lo podemos apreciar de manera clara en los artículos anteriores y en esta tesis, esta causa de justificación, es un elemento negativo, que excluye la antijuricidad, pues se le reconoce al individuo o individuos, en las situaciones planteadas en las leyes sustantivas, repeler una agresión para proteger sus intereses o los ajenos. Esta eximente como también las otras supra mencionadas se deberán resolver de oficio, en cualquier estado del proceso, es importante no realizar un exceso en la conducta de la defensa legítima pues esta circunstancia generaría una pena.<sup>50</sup>

### **Elementos de la defensa legítima**

La naturaleza de la legítima defensa está fundamentada en el mantenimiento del orden jurídico, constituye una delegación hipotética de la potestad que el corresponde a la

---

<sup>50</sup> Cfr. Plascencia Villanueva Raúl, *Teoría del Delito*, Editorial UNAM, 2004.

policía, ante agresiones inesperadas, en las cuales se debe actuar de forma inmediata, por la falta de la autoridad que debiera intervenir para mantener el orden social.

Fundamento Legal: Artículos 15 y 29 del Código Penal Federal y Código Penal Para el Distrito Federal, respectivamente.

Objeto: La defensa de un bien jurídico tutelado, el cual sea de igual o mayor grado del que se defiende.

Elementos Objetivos: La existencia de una agresión y no exceder la defensa, para evitar el exceso. En la cual la agresión debe contener las características siguientes: Existencia de un bien jurídicamente tutelado, los bienes jurídicamente tutelados se establecen en el Código Penal. La desprotección al bien jurídico protegido; esta situación se da al momento que el Estado no puede brindar la seguridad necesaria y el sujeto toma la decisión de defender el bien jurídicamente tutelado, esto se extiende a un bien ajeno incluso. Existencia de un riesgo para el bien jurídico; surge con la probabilidad de ser transgredido el Estado de Derecho, pues debe hacerse valer su incolumidad ante un ataque injusto. La agresión real; esto significa que la agresión se halle dentro del terreno del mundo cierto y del imaginario. Agresión actual; la agresión puede ser instantánea o duradera, sin embargo esta establece de forma inminente la puesta en peligro del bien jurídico, cuando la agresión comienza. Agresión inminente, es algo que no ha comenzado pero que puede empezar de manera inesperada. Agresión sin derecho, esa debe surgir en razón de la defensa de un bien jurídico tutelado y por último la agresión no provocada, es decir el que defiende el bien jurídico tutelado, no debe de generar la violación del mismo que defiende.<sup>3</sup>

Asimismo, en esta eximente debe de prevalecer la racionalidad en la defensa, que esta no sea excesiva, extensiva o intensiva. Es decir que no se rebasen los límites de la necesidad, que no se prolongue durante más tiempo que el justo necesario, y por último que no se lesione de manera mayor al agente que vulnera el bien jurídico tutelado.

Se arriba a la conclusión de que todos los bienes son susceptibles de defensa legítima, como quedo plasmado en este trabajo y se pueden defender los bienes propios y hasta los ajenos. Se colige que la defensa legítima se fundamenta en dos principios, que son la protección del derecho individual o colectivo y la defensa del orden jurídico. Sin embargo considero que esta eximente o justificante, da lugar a quitarle la vida a otro sujeto por el hecho de defender un bien jurídico restableciendo el *statuo legis*, pero transgrediendo un bien jurídico como lo es la vida. Bajo este tenor de ideas, podría llegar a la conclusión que quizá los bienes materiales tienen mayor jerarquía que la vida de un sujeto, y que a pesar de ser un perpetrador del derecho el delincuente, no deja de perder su condición de ser humano. Por otro lado son muy subjetivas las apreciaciones sobre el tema en el exceso de la defensa legítima, situación que los egregios jueces en su diario actuar deben estudiar el caso concreto de manera exhaustiva para arribar a sentencias correctas y apegadas a derecho.

#### **b) Ejercicio de un derecho.**

“El ejercicio de un derecho es una eximente penal que encuentra su raíz en el aforismo que señala ‘quien usa de su derecho, a nadie daña’; es decir en realidad el ejercicio de un derecho es una conducta violentas que el derecho justifica”<sup>51</sup>.

En este caso el ejercicio de un derecho es una justificante porque la conducta realizada por el sujeto se ajusta a las normas de derecho y dicha eximente concurre solo si se utiliza el derecho pues ejercen sus derechos todos los que realizan conductas que no están prohibidas, pues si el ordenamiento jurídico ha otorgado a una persona cierta facultad ello querría decir que se ha reconocido la prevalescencia de su interés sobre el de otros, por lo que dentro del presente trabajo estudiaremos que entendemos por el ejercicio de ese derecho.

---

<sup>51</sup> Cabanellas de Torres, Guillermo. *Diccionario Jurídico Elemental*, 1ª ed, Heliasta, Buenos Aires, Argentina, 1993, p.391.

La figura de excluyente de delito implica que no puede considerarse que existió un delito cuando se realicen ciertas conductas con el objetivo de proteger determinados bienes jurídicos propios o ajenos, o ante la inexistencia de la voluntad de delinquir o de alguno de los elementos que integran el tipo penal, aunque se cometa alguna de las conductas típicas, mientras que la excusa absolutoria implica que existió una conducta típica, pero se excluye la aplicación de la pena establecida para ese delito.

Es decir, las excusas absolutorias tienen como efecto la determinación de que sí existió la conducta típica y el respectivo delito (sus elementos y la responsabilidad del agente), pero por determinadas razones el legislador considera que no debe aplicarse la pena; esto es, son causas que dejando subsistente el carácter delictivo de la conducta o hecho tipificado como delito en la ley impiden la aplicación de la pena. Así, las excusas absolutorias no relevan al sujeto activo de su responsabilidad en la comisión de la conducta típica, sino que determinan su impunidad.

De lo anterior se aprecia la diferencia existente entre una excusa absolutoria y la excluyente del delito, pues en la primera se considera que efectivamente se dio un delito y que existió un responsable, pero no se aplica pena alguna, mientras en la segunda se estima que no se integra el delito y, por tanto, no existe responsable y mucho menos una pena.

Esta diferencia no es puramente teórica, sino que tiene repercusiones en todo el sistema mediante el cual se persiguen los delitos y se llevan a cabo los procesos penales, pues cuando se trata de una excusa absolutoria, puede llevarse todo un procedimiento que terminará con una declaratoria de imputabilidad del delito, de ahí que existe la posibilidad de que el titular del monopolio de la acción penal la ejerza y se consigne a los probables responsables y, posteriormente, seguido el juicio, se les pueda considerar responsables del delito, aunque no se les aplique la pena.

En México esta excusa tiene su fundamento en el artículo 29 fracción VI del Código Penal del Distrito Federal que señala:

## **CAPÍTULO V**

### **CAUSAS DE EXCLUSIÓN DEL DELITO**

**ARTÍCULO 29** (*Causas de exclusión*). El delito se excluye cuando:

VI. (*Cumplimiento de un deber o ejercicio de un derecho*). La acción o la omisión se realicen en cumplimiento de un deber jurídico o en ejercicio de un derecho, siempre que exista necesidad racional de la conducta empleada para cumplirlo o ejercerlo;

Por otro lado la legislación federal señala en su artículo 15 fracción VI señala:

## **CAPITULO IV**

### **Causas de exclusión del delito**

**Artículo 15.-** El delito se excluye cuando:

**VI.-** La acción o la omisión se realicen en cumplimiento de un deber jurídico o en ejercicio de un derecho, siempre que exista necesidad racional del medio empleado para cumplir el deber o ejercer el derecho, y que este último no se realice con el solo propósito de perjudicar a otro;

De acuerdo con esto, los elementos objetivos del ejercicio de un derecho son:

- a) El derecho debe estar previsto en la ley
- b) Que el ejercicio del derecho no se realice con el propósito de perjudicar a otro.

El ordenamiento jurídico otorga un sinnúmero de derechos al individuo en su condición de persona y a su vez regula el ejercicio de estos derechos en la forma más conveniente para lograr una convivencia social y de ahí quien actúa en el ejercicio de

un derecho está actuando conforme la ley señala; es decir, que no comete una acción antijurídica aunque su comportamiento o acción lesione o ponga en peligro los intereses de otras personas pues cuando decimos que una conducta no es antijurídica emerge la problemática de cómo distinguirla de una que si lo es, toda vez que en las distintas normas que existen, el legislador estipula consecuencias jurídicas para los que violan el deber de obediencia.

Las leyes penales no solo están integradas por normas de carácter imperativo o prohibitivo, sino que a su vez existen normas de carácter permisivo y con ellas aparecen las causas de justificación y dentro de esto encontramos el ejercicio de un derecho, pues quien obra en ejercicio de un derecho es porque previamente le asiste la facultad de obrar o el poder de voluntad establecido por el derecho objetivo para de esta manera satisfacer un interés legítimo y esta facultad no pierde su licitud mientras se dé dentro de los límites fijados por la norma jurídica, aún en el caso de que se lesionen bienes jurídicos ajenos.

### **c) Estado de necesidad.**

Es la causa de eximente de responsabilidad criminal por la que una persona para proteger un bien jurídico y evitar un mal propio o ajeno que suponga peligro actual, inminente, grave, injusto, ilegítimo, e inevitable de otra forma legítima, menoscaba otro bien jurídico cuyo daño no puede ser mayor al que pretende evitar, siempre y cuando el mal que intente evitar no haya sido provocado intencionalmente por el propio sujeto y este no tenga obligación de sacrificarse por razón de su oficio o cargo.

La naturaleza Jurídica de esta Institución es muy discutida, actualmente se hace la distinción del valor de los bienes en conflicto, si el bien sacrificado es menor que el salvado se tratará de una causa de justificación, sin embargo el conflicto inicia cuando se presenta la colisión de bienes del mismo valor, en este caso desaparece también la responsabilidad penal, no porque la conducta sea jurídica, sino porque el Estado no

exige otra actuación diversa, de tal modo que si el bien salvado es de menor cuantía que el sacrificado evidentemente se configurará el delito, a menos que intervenga un factor eximente de responsabilidad de distinta naturaleza.

El Código Penal Federal vigente, en su artículo 15, fracción V; dice: “El delito se excluye cuando: ...*Se obre por la necesidad de salvaguardar un bien jurídico propio o ajeno, de un peligro real, actual o inminente, no ocasionado dolosamente por el agente, lesionando otro bien de menor o igual valor que el salvaguardado, siempre que el peligro no sea evitable por otros medios y el agente no tuviere el deber jurídico de afrontarlo...*”<sup>52</sup>

De los conceptos anteriores podemos desprender los elementos del Estado de necesidad:

La existencia de un peligro que reúna las siguientes características:

- Que sea real.
- Que sea actual.
- Que sea inminente.
- Que no sea ocasionado dolosamente por el agente.
- Que el peligro se cierna sobre la persona o bienes propios, o la persona o bienes de otro.
- Que no exista otro medio practicable y menos perjudicial.
- Que el bien que se lesiona sea de menor o igual valor que el salvaguardado.
- Que el agente no tuviere el deber jurídico de afrontarlo.

El Código Penal Federal vigente, en su artículo 379, dice: “*No se castigará al que, sin emplear engaño ni medios violentos, se apodera una sola vez de los objetos*

---

<sup>52</sup> Código Penal Federal, [www.diputados.gob.mx/LeyesBiblio](http://www.diputados.gob.mx/LeyesBiblio). 26 Junio 2020.

*estrictamente indispensables para satisfacer sus necesidades personales o familiares del momento*".<sup>53</sup>

En este precepto encontramos los límites de esta institución jurídica, y también me parece justo que se dé seguridad jurídica a quienes puedan sufrir esta conducta de robo en sus pertenencias.

Condicionar la conducta del necesitado, es necesario para evitar que ésta se vuelva una práctica reiterativa para quienes pudieran aprovecharse del ánimo del legislador que pensó en la implementación de la institución del Estado de Necesidad, como parte integral de las políticas criminales del Estado.

Por lo antes expuesto, analizaré el contenido del artículo 379 del Código Penal Federal, que menciona claramente la forma en la que se debe presentar esta conducta para no ser sancionada.

En primer lugar, el sujeto activo *no debe emplear engaño ni medios violentos*, lo cual significa que con la presencia del engaño y la violencia en la conducta estaríamos ante una maquinación del sujeto y por lo tanto habrá sanción aun existiendo el Estado de Necesidad.

En segundo lugar, *el apoderamiento debe ser una sola vez*, lo cual evita que esta conducta sea repetida por el sujeto activo.

En tercer lugar, al referirse a que *sólo deben tomarse los objetos estrictamente indispensables para satisfacer sus necesidades personales o familiares del momento*, el legislador limita esta justificación, ya que si el sujeto activo comete la conducta, deberá desarrollarse conforme este precepto, es decir si el robo se efectúa por una causa ajena a la satisfacción de una necesidad personal o familiar habrá sanción, y por último si el robo se registra antes o después de la necesidad que lo motivo, de

---

<sup>53</sup> Ídem



igual forma se le impondrá la sanción correspondiente, toda vez que debe ser en el momento de la necesidad, no por algo que va a pasar o por lo que ya paso, ya que de el legislador tuvo a bien plasmarlo en la ley de ese modo.

Como es sabido, el Estado Mexicano ha evolucionado sus instituciones jurídicas, las cuales tienen por objeto la protección de las personas y sus bienes, en una sociedad que para cumplir con sus objetivos sociales tiene que organizar, dirigir y monitorear en forma constante su sistema de prevención del delito y su sistema penal; así como todos los actores legales.

Dentro de estas actividades de organización social que un gobierno realiza para satisfacer las necesidades de seguridad y certeza jurídica de sus gobernados, deberá incluir una política criminal, con estrategias legales que ayuden en el buen transitar de la sociedad que dirige.

Entiendo que estas políticas criminales tienen diversos matices, sin embargo también es digno reconocer que las estructuras de un gobierno normalmente se erigen con el ánimo de crecer y de hacer de su propio país un lugar con leyes que otorguen tranquilidad social y no hostigamiento y rigidez legal, o bien que abusen del poder que los ciudadanos le proporcionan a través del sufragio.

El Congreso de la Unión, ha sido sensible al implementar una serie de instituciones jurídicas con el único fin de beneficiar a quienes por una u otra razón delinquen, transgrediendo las normas penales que el mismo pueblo a través de sus representantes sociales en esa representación nacional faculta para tal fin.

Una de esas instituciones jurídicas es precisamente el Estado de Necesidad como causa de justificación o como excusa absolutoria en la comisión de una conducta delictiva, que a la luz de su análisis deja entrever su complejidad y a la vez su sencillez, que tanta importancia cobra cuando un juez impone una pena, porque en la impartición de la justicia es necesario considerar todas las herramientas jurídicas para que quien

ofende a los integrantes de una determinada sociedad sea llevado a los tribunales, con la seguridad que será oído y vencido en un juicio que tiene a su alcance, todo lo necesario para impartir en forma imparcial sus veredictos y sentencias.

En este sentido, el Estado de Necesidad busca establecer con toda claridad que dentro de las conductas delictivas que afectan los bienes jurídicos protegidos por la Constitución Política de nuestro país, existen actos, acciones y movimientos corporales que sin tener una intención de provocar un daño a las personas o patrimonio de éstas, se registran sin intención alguna de dañarlos, o bien si se presentan, atendieron a situaciones meramente circunstanciales y sin el ánimo de ofender, perjudicar y afectar esos bienes jurídicos protegidos por el Estado.

Pues bien, el Estado de Necesidad como causa de justificación, engloba todas las conductas que deben ser exoneradas por el Estado aunque se haya afectado un bien jurídico que el mismo protege.

### 3. 4 Imputabilidad e inimputabilidad

#### Imputabilidad

Para Sebastián Soler, “La Imputabilidad es la posibilidad, condicionada por la salud y la madurez espiritual del autor, de valorar correctamente los deberes y de obrar de acuerdo con ese conocimiento.”<sup>54</sup>

Según Griselda Amuchategui, ésta “es la capacidad de entender y querer en el campo del Derecho Penal. Implica salud mental, aptitud psíquica de actuar en el ámbito penal, precisamente al cometer un delito. Destacando que el sujeto debe ser primero imputable para luego ser culpable, no puede haber culpabilidad sin previamente no se es imputable”.<sup>55</sup>

Es imputable quien goza de salud mental, no se encuentra afectado por sustancias que afecten su comprensión y tienen la edad que la ley señala para considerar a las personas con capacidad mental para ser responsables de delito, en la mayoría de los estados de la República Mexicana es a partir de los 18 años.

Será imputable, dice Carranca y Trujillo, todo aquel que posea, al tiempo de la acción, las condiciones psíquicas exigidas, abstracta e indeterminadamente por la ley para desarrollar su conducta socialmente; todo el que sea apto e idóneo jurídicamente para observar una conducta que responda a las exigencias de la vida en sociedad.<sup>56</sup>

Por lo que, la imputabilidad, es pues, el conjunto de condiciones mínimas de salud y desarrollo mental del autor, en el momento del acto típico penal, que lo capacitan para responder al mismo.

La posición que ocupa la imputabilidad dentro del estudio del delito, es controvertida. Sobre la ubicación sistemática de la imputabilidad existen una serie de opiniones. Algunos autores, la entienden como presupuesto general del delito; otros, como

---

<sup>54</sup> Sebastián soler. *Derecho Penal Argentino*, Tomo 1, Tipográfica Editora Argentina, 1999, pp 51-58

<sup>55</sup> Griselda Amuchategui. *Derecho Penal*, México, Oxford, 2005, pp. 87-90

<sup>56</sup> Citado por Fernando Castellanos, *Lineamientos elementales del Derecho Penal*. México, Editorial Porrúa, 2009 pp199.-200.

elemento autónomo, mientras que para otros constituye un presupuesto de la culpabilidad.<sup>57</sup>

Las condiciones que hacen imputable a un sujeto, constituyen un *mínimum*. No es necesaria una fina conciencia valorativa para saber que el homicidio, el robo o el secuestro son malas acciones, por eso no es preciso encontrar perfecciones psíquicas en los procesados para incluir en su imputabilidad. Basta pues con un *mínimum* de condiciones, siempre que de ellas resulte que el sujeto haya tenido conciencia de la criminalidad de su acto y facultad de dirigir sus acciones.<sup>58</sup>

Comúnmente se afirma que la imputabilidad está determinada por un *mínimum* físico representado por la edad y otro psíquico, consiste en la salud mental. Son dos aspectos de tipo psicológico: salud y desarrollo mental; generalmente el desarrollo mental se relaciona estrechamente con la edad.

Son imputables quienes tienen desarrollada la mente y no padecen alguna anomalía psicológica que lo imposibilite para entender y querer, como se mencionó anteriormente, es decir, son poseedores, al tiempo de la acción, del *mínimum* de salud y desarrollo psíquico exigidos por la Ley del Estado; pero sólo son responsables quienes habiendo ejecutado el hecho, están obligados a responder por él. El término responsabilidad se utiliza para significar la situación jurídica en que se coloca el autor de un acto típicamente contrario a Derecho, si obró culpablemente; así los fallos judiciales suelen concluir en la declaración, teniendo al acusado como penalmente responsable del delito que motivó el proceso y señalan la pena respectiva.

La responsabilidad resulta entonces, una relación entre el sujeto y el Estado, según la cual éste declara que aquel obró culpablemente y se hizo acreedor a las consecuencias señaladas por la ley.<sup>59</sup>

---

<sup>57</sup> Sergio García, *Imputabilidad en el Derecho Penal Mexicano*, México, Universidad Nacional Autónoma de México, 1981, 13-21.

<sup>58</sup> Sebastián Soler, *Derecho Penal Argentino Tomo I*, Argentina, Tipográfica Editora Argentina, 1999, pp. 51-58.

<sup>59</sup> Fernando Castellanos, *Lineamientos elementales del Derecho Penal*. México, Editorial Porrúa, 2009 pp199.-200

## **Inimputabilidad.**

Son aquellas condiciones del sujeto que al presentarlas anulan la imputabilidad. Ya que derivado de esas condiciones no se le puede atribuir una responsabilidad aunque la conducta sea típica y antijurídica. A continuación expondremos dichas condiciones:

- **Trastorno mental y desarrollo intelectual retardado**

El trastorno mental y el desarrollo intelectual retardado se refieren a condiciones psíquicas que le impide al sujeto tener la capacidad y la aptitud de comprender la conducta realizada por lo cual no pueden ser responsables jurídicamente, ya que esa condición en su psique los hace no entender, ni comprender lo cual puede ser derivado de un trastorno o de una falta de madurez en el desarrollo de su intelecto. Estas condiciones se encuentran contenidas en el artículo 15 del Código Penal Federal, fracción VII.

“VII.- Al momento de realizar el hecho típico, el agente no tenga la capacidad de comprender el carácter ilícito de aquél o de conducirse de acuerdo con esa comprensión, en virtud de padecer trastorno mental o desarrollo intelectual retardado...”<sup>60</sup>

- ***Acción liberae in causa.***

Las acciones libres en su causa, se presentan cuando se produce un resultado contrario al derecho, cuando la conducta fue ocasionada por un acto (acción u omisión), doloso o culposo, cometido en estado de imputabilidad. De otra forma: conceptualmente, las acciones libres en su causa pueden entenderse como las conductas productoras de un resultado típico en un momento de inimputabilidad del sujeto actuante, pero puesta la causa en pleno estado de imputabilidad.<sup>61</sup>

Se trata, pues, de delitos, en cuyo *iter* hay un designio y una preparación reprochables, plenamente atribuibles al autor, pero cuya ejecución se desarrolla, por la maniobra y decisión de aquel, en estado de inimputabilidad. Es decir, se trata de un

<sup>60</sup> Código penal federal, <http://www.diputados.gob.mx/>. 07/05/2020.

<sup>61</sup> Sergio García, *imputabilidad en el Derecho Penal Mexicano*, México, Universidad Nacional Autónoma de México, 1981, 13-21.

hecho realizado por el agente en estado de inimputabilidad, pero dicho estado fue buscado libremente por él, existiendo relación de causalidad entre el acto libre y el hecho típico realizado en estado de inconsciencia. Por tanto, la ley lo considera responsable del delito. Se llaman de este modo porque son acciones libres en cuanto a su causa, pero determinadas en lo referente a su efecto.<sup>62, 63</sup>

Por ejemplo, cuando una persona decide cometer un homicidio y para darse ánimo bebe en exceso y ejecuta el delito en estado de ebriedad. Aquí sin duda, existe imputabilidad, entre el acto voluntario (decisión de matar) y el resultado, hay un enlace causal. En el momento del impulso para el desarrollo de la cadena de la causalidad, dice Cuello Calón, el sujeto era imputable. Si se acepta que al actuar el sujeto carecía de la capacidad necesaria de entender y querer, pero tal estado se procuró dolosa o culposamente, encuéntrase el fundamento en la imputabilidad en la acción o acto precedente, o sea en el cual el individuo, sin carecer de tal capacidad, movió su voluntad o actuó culposamente para colocarse en situación de inimputabilidad; por ello el resultado le es imputable y da base a declararlo culpable y, consiguientemente responsable, siendo acreedor a una pena.

Según la Suprema Corte de Justicia, aun cuando se pruebe que el sujeto se hallaba, al realizar, la conducta, en un estado de inconsciencia de sus actos, voluntariamente procurado, no se elimina la responsabilidad.<sup>64</sup>

Dichos *acciones de liberae in causa*, se hacen referencia en la segunda parte de la fracción VII del art. 15 del Código Penal Federal y el 29 fracc. VII del Código Penal del Distrito Federal. Que textualmente refieren:

**Artículos 15 CPF:** el delito se excluye cuando:

...VII. Al momento de realizar el hecho típico, el agente no tenga la capacidad de comprender el carácter ilícito de aquel o de conducirse de acuerdo con la comprensión, en virtud de padecer un trastorno mental o desarrollo mental retardado, a

---

<sup>62</sup> Griselda Amuchategui, *Derecho Penal*, México, Oxford, 2005, pp.87-90.

<sup>63</sup> Sergio García, *imputabilidad en el Derecho Penal Mexicano*, México, Universidad Nacional Autónoma de México, 1981, 13-21.

<sup>64</sup> Citado por Fernando Castellanos, *Lineamientos elementales del Derecho Penal*. México, Editorial Porrúa, 2009 pp199.-200

no ser que el agente hubiere preordenado su trastorno mental dolosa o culposamente, en cuyo caso responderá por el típico siempre y cuando lo haya previsto o le fuere previsible.

Cuando la capacidad a que se refiere el párrafo anterior sólo se encuentre considerablemente disminuida, se estará a lo dispuesto en el artículo 69 bis de este Código.

**Artículo 29 CPDF (Causas de exclusión):** el delito se excluye cuando:

... VII. (inimputabilidad y acción libre en su causa). Al momento de realizar el hecho típico, el agente no tenga la capacidad de comprender el carácter ilícito de aquel o de conducirse de acuerdo a esa comprensión, en virtud de padecer trastorno mental o de desarrollo intelectual retardado, a no ser que el sujeto hubiese provocado su trastorno mental dolosa o culposamente, en cuyo caso responderá por el resultado típico producido por tal situación.

Cuando la capacidad a que se refiere el párrafo anterior se encuentre considerablemente disminuida, se estará a lo dispuesto en el Artículo 65 de este Código.

La imputabilidad es la capacidad, condicionada por la madurez y salud mentales, de comprender el carácter antijurídico de la propia acción u omisión y de determinarse de acuerdo a esa comprensión, asumiendo la responsabilidad que derive de ello. Sin duda, que esta definición es más amplia y de carácter más técnico; nos explica que la imputabilidad tiene que ver con dos elementos: la madurez y la salud mental, ya que estos dos elementos son los que permiten comprender la conducta. Así pues, el ser imputable permite que un sujeto se pueda determinar en cuanto a sus actos y en consecuencia ser responsables de ello. De ahí se deriva que una persona solo puede "ser culpable si es imputable". Si partimos de la base que la imputabilidad consiste en aquella capacidad doble del sujeto para, por un lado comprender la ilicitud del hecho determinada por la norma, y por otro, actuar conforme a dicha comprensión, uno de los principales problemas que plantea esta categoría es establecer el límite entre el imputable y el inimputable, por lo que para mejorar la punibilidad en México, debe de

hacerse hincapié, primeramente en aquellas medidas que definan quien puede ser sometido a un proceso legal y quien, por sus características y madurez mental no.

El concepto de imputabilidad suele ser un concepto controvertido, sobre todo, teniendo en cuenta la amplia variedad de posturas diferentes que se puede tener en cuenta al abordar su significado (dogmáticas, médicas, psiquiátricas, etc.). Un primer problema que presenta la imputabilidad, es en cuanto a su ubicación dentro del campo del Derecho Penal. La mayoría de las doctrinas sostienen que la imputabilidad carece de la entidad suficiente para ser considerada como elemento de la Teoría General del Delito. Para algunos autores, no es más que un elemento que forma parte, junto con otros, de la categoría de la culpabilidad, estableciendo la imputabilidad en cuanto “capacidad cognitiva y volitiva de actuar conforme a derecho. Aquí, se engloban aquellos supuestos que se refieren a la madurez psíquica y la capacidad del sujeto de motivarse, tales como la edad o la salud mental de manera que si no se poseen las facultades psíquicas suficientes para ser motivado racionalmente no podrá haber culpabilidad, idea que comparto.

- **Minoría de edad**

En nuestro país se considera menor de edad hasta antes de cumplir 18 años de edad, sin embargo es un tema bastante debatible dado que no existe una uniformidad en general acerca de la minoría de edad, ya que en diferentes países se tienen reglamentaciones diversas, por ejemplo en algunos países se les dan ciertos derechos al cumplir los 18 años, sin embargo pueden votar hasta los 21 años de edad. En México actualmente se tiene estipulado en el artículo 18 de la Constitución Política de los Estados Unidos Mexicanos en su párrafo cuarto.

En general la minoría de edad presupone inmadurez basado en el desarrollo de la edad del sujeto y por consecuencia en su estado psíquico.



### 3.5 Culpabilidad e inculpabilidad

#### Culpabilidad

Además de ser delito una conducta típica, antijurídica e imputable, precisa ser culpable. Por tanto, de acuerdo a la anterior prelación lógica, la culpabilidad debe abordarse después de la imputabilidad que actúa como presupuesto de la primera<sup>65</sup>.

Se ha dicho también que la culpabilidad destaca en importancia respecto de los otros elementos del concepto de delito, porque es a través de esta que el derecho está en condiciones de vincular un acontecimiento con un hombre determinado<sup>66</sup>. *“Esto es de gran importancia, pues los acontecimientos que se manifiestan en el mundo exterior sólo serán relevantes para el derecho penal en tanto sea posible vincularlos o atribuirlos a un ser humano”*<sup>67</sup>. Para ilustrar de mejor manera la importancia del ser humano respecto a la culpabilidad, son pertinentes las palabras de Marco Tulio Cicerón: *“Cosa es dirá alguno, de poca importancia, pero grande la culpa: porque los pecados no se han de medir por los acontecimientos de las cosas, sino por los vicios de los hombres”*<sup>68</sup>.

Por su parte, Eduardo López Betancourt indica que el concepto de la culpabilidad dependerá, en gran medida, de la teoría que se adopte para entender este elemento del delito; estas teorías están estrechamente vinculadas con la evolución histórica de la culpabilidad.

- **Teoría Psicológica.** La culpabilidad como relación psicológica entre el hecho y su autor. El dolo y la culpa se ven como las dos formas posibles de esta conexión psíquica entre el autor y su hecho o conducta. Para la teoría psicológica, la culpabilidad se produce en cuanto existe el nexo psicológico.
- **Teoría normativa.** Se funda en el reproche (basado en el acto psicológico, en los motivos y en la caracterología del agente) y en la exigibilidad. Nexo psicológico entre el autor, la conducta y el resultado material (hecho) y la reprochabilidad.

<sup>65</sup> Cfr. Eduardo López Betancourt, *Imputabilidad y Culpabilidad*, México D.F., Ed. Porrúa, 2002, p. 61.

<sup>66</sup> Cfr. Sergio Vela Treviño, *Culpabilidad e Inculpabilidad*, México D.F., Ed. Trillas, 2007, p. 4.

<sup>67</sup> *Ibidem*, p. 138.

<sup>68</sup> Citado por Vela Treviño, *Ibidem*, p. 140.

Por su parte, Sergio Vela Treviño describe a la teoría psicológica como aquella en que lo predominante es la causalidad psíquica, que se entiende como la vinculación subjetiva por la cual quedan unidos un hecho y su agente. Asimismo, el mismo autor, citando al maestro argentino Sebastián Soler, refiere que el contenido de la culpabilidad en la teoría psicológica lo constituye la conciencia de la criminalidad del acto. De esto se desprende que “*hay culpabilidad cuando un imputable, con conciencia del contenido de la antijuridicidad*<sup>69</sup> *de su conducta, lleva a cabo, dolosa o culposamente un hecho que produce un resultado típico*”<sup>70</sup>.

Por lo que hace a la teoría normativista, el autor de *Culpabilidad e Inculpabilidad* enumera sus características de la siguiente manera:

- i. La culpabilidad es un juicio de referencia, por referirse al hecho psicológico;
- ii. La culpabilidad es un proceso atribuible a una motivación reprochable del agente;
- iii. La reprochabilidad de la conducta únicamente podrá formularse cuando se demuestre la exigibilidad de otra conducta a la emitida por el sujeto; y
- iv. En consecuencia, la culpabilidad tiene como fundamentos, la reprochabilidad y la exigibilidad.

- **Concepto de Culpabilidad**

Como lo menciona Eduardo López Betancourt, este concepto habrá de fijarse según la teoría que se adopte; entonces, según la teoría psicologista, la culpabilidad sería el vínculo subjetivo entre el agente y el hecho causado.

Por lo que hace al concepto según la teoría normativa, este sería: “*Culpabilidad es el resultado del juicio por el cual se reprocha a un sujeto imputable haber realizado*

---

<sup>69</sup> Cfr. Resulta interesante la construcción lógica que lleva a cabo Sebastián Soler, en el sentido de explicar que la referencia a la conciencia del contenido antijurídico no implica un conocimiento previo y exacto de la transgresión a una norma específica del orden jurídico, sino a una conciencia general de que se está incurriendo en una conducta reprobable, contraria a la moral o las buenas costumbres. *Culpabilidad e Inculpabilidad*, obra citada, p. 181.

<sup>70</sup> *Ibidem*.

*un comportamiento típico y antijurídico, cuando le era exigible la realización de otro comportamiento diferente, adecuado a la norma”<sup>71</sup>.*

- **Naturaleza**

Dilucidar la naturaleza de las cosas o de los seres implica siempre llegar a conocer sus orígenes, sus causas y sus fines. El mismo vocablo naturaleza, puede significar: esencia y propiedad característica de cada ser; virtud, calidad o propiedad de las cosas<sup>72</sup>.

Así pues, tenemos como acepciones de la palabra “culpa”, a las siguientes: 1) Imputación a alguien de una determinada acción como consecuencia de su conducta; 2) Hecho de ser causante de algo; 3) Desde la perspectiva del derecho, omisión de la diligencia exigible a alguien que implica que el hecho injusto o dañoso resultante, motive su responsabilidad civil o penal; 4) Para la psicología sería la acción u omisión que provoca un sentimiento de responsabilidad por un daño causado; y, finalmente, desde una perspectiva teológica, 5) Pecado o transgresión voluntaria de la ley de Dios.

En esta materia, el suscrito estima necesario - a fin de dilucidar la naturaleza de la culpa desde un punto de vista jurídico - considerar que esta es uno de los elementos de la teoría del delito y, tomando en cuenta ese origen, es como debe entenderse su naturaleza.

Entonces, sí para determinar la naturaleza de algo es necesario conocer cómo está formado, entonces es relevante buscar los elementos de la culpabilidad, a saber:

*“i. La imputabilidad (como presupuesto de la culpabilidad);*

*ii. Las formas de culpabilidad, dolo y culpa, consideradas como parte de la culpabilidad y que constituyen la referencia psíquica entre la conducta o hecho y su autor;*

---

<sup>71</sup> *Ibidem.*, p. 201.

<sup>72</sup> Diccionario en Línea de la Real Academia Española de la Lengua, disponible en: [http://buscon.rae.es/draeI/SrvltConsulta?TIPO\\_BUS=3&LEMA=apartado](http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=apartado), última consulta, 28/12/19.

*iii. La ausencia de causas de exclusión de la culpabilidad*<sup>73</sup>.

Por otro lado, la teoría finalista enumera a los elementos de la culpabilidad de la siguiente manera:

- i. La exigibilidad de una conducta distinta conforme a la ley;
- ii. La imputabilidad; y
- iii. La posibilidad concreta de reconocer el carácter ilícito del hecho realizado.

Asimismo, la importancia que tiene la culpabilidad para el derecho penal y, por lo tanto, la esencia de la culpabilidad, radica en la manera en que su participación es relevante para conocer la existencia del delito y, específicamente, como lo señalan varios autores, el hombre específico a quien debe atribuirse el acto típico y antijurídico, verificándose la existencia del elemento culpable, una vez que ha concluido el juicio de reproche.

- **Grados o Tipos de Culpabilidad**

Los grados de la culpabilidad son, desde un punto de vista estrictamente doctrinal, el dolo, la culpa y la preterintención.

**a) El dolo**

Para los clásicos, dolo es la intención de ejecutar un acto que se sabe contrario a derecho, mientras que para los positivistas el dolo requiere para su existencia de voluntad, intención y fin<sup>74</sup>.

Por su parte, Francisco Pavón Vasconcelos, aceptando la definición de dolo de Luis Jiménez de Asúa, la endosa y la reproduce en su obra: “...*dolo es la producción de un resultado típicamente antijurídico con consciencia de que se quebranta el deber, con conocimiento de las circunstancias del hecho y del curso esencial de la relación de causalidad existente entre la manifestación humana y el cambio en el mundo*”.

<sup>73</sup> Francisco Pavón Vasconcelos, *Derecho Penal Mexicano*, México D.F., Ed. Porrúa, 1999, p. 407.

<sup>74</sup> Cfr. *Imputabilidad y Culpabilidad*, citando a Eugenio Cuello Calón “*Dolo es la voluntad consciente dirigida a la ejecución de un hecho que es delictuoso*”, obra citada, pp.87-89.

*exterior, con voluntad de realizar la acción y con representación del resultado que se quiere o ratifica”.*

### **b) La culpa**

Francisco Pavón Vasconcelos nos dice que estamos en presencia de la culpa, cuando la actitud del sujeto, enjuiciada a través del imperativo de los deberes impuestos por la ley, es reprochable a virtud de la falta de observancia de la prudencia, atención, pericia, reglas, órdenes, disciplinas, etc., necesarias para evitar la producción de resultados previstos en la ley como delictuosos. Y la define como *“aquel resultado típico y antijurídico, no querido ni aceptado, previsto o previsible, derivado de una acción u omisión voluntarias, y evitable si se hubieran observado los deberes impuestos por el ordenamiento jurídico y aconsejables por los usos y costumbres”*<sup>75</sup>. A esta definición, Eduardo López Betancourt le agrega *...y evitable si se hubieran observado los deberes impuestos por el ordenamientos jurídico y aconsejables por los usos y costumbres y también por la cultura del sujeto*<sup>76</sup>.

### **c) La preterintencionalidad**

Francisco Pavón Vasconcelos nos dice que, en la doctrina penal, el término genérico de preterintencionalidad comprende una serie de casos en los cuales, concurriendo algún elemento de culpabilidad, no existe plena coincidencia entre dicho elemento y el resultado típico producido por el autor. Citando a Ángel Reyes Navarro, Pavón Vasconcelos endosa la descripción de preterintencionalidad hecha por este último: *“cuando el daño causado es mayor de aquel que tenía intención de causar el agente, o dicho en otras palabras, cuando el resultado ha sobrepasado a la intención del autor”*<sup>77</sup>.

A manera de conclusión, en lo que se refiere al concepto de culpabilidad, el suscrito considera preferible el de la teoría normativa, basada en el aspecto subjetivo-psicológico, en los motivos y características del agente y la exigibilidad de la conducta que, valorados en conjunto, nos permitirán concluir de forma adecuada el juicio de

<sup>75</sup> *Derecho Penal Mexicano*, obra citada, p. 447.

<sup>76</sup> *Cfr. Imputabilidad y Culpabilidad*, obra citada, p. 119.

<sup>77</sup> *Derecho Penal Mexicano*, obra citada, p. 464.

reproche. Esto, en mi opinión, va de la mano de la naturaleza jurídica de la culpabilidad, en tanto que, elemento del delito, corresponde a la culpabilidad atribuir a determinado hombre el acto típico y antijurídico, dicho de forma coloquial, asignarle a dicho acto un nombre y un rostro.

## **Inculpabilidad**

Es el aspecto negativo de la Culpabilidad. La inculpabilidad es la ausencia de culpabilidad. Esta definición, expresa con razón Jiménez de Asúa, es tautológica. “El penalista hispano, consecuente con su concepción normativa de la culpabilidad, sostiene que la inculpabilidad consiste en la absolución del sujeto en el juicio de reproche”.<sup>78</sup>

“Es la falta de reprochabilidad ante el derecho penal, por faltar la voluntad o el conocimiento del hecho”.<sup>79</sup>

La inculpabilidad opera al hallarse ausentes los elementos esenciales de la culpabilidad que son conocimiento y voluntad.

- **Causas de inculpabilidad**

Griselda Amuchategui Requena define las causas de inculpabilidad son las circunstancias que anulan la voluntad o el conocimiento:

Error esencial de hecho invencible (ataca el elemento intelectual)

Eximentes putativas

No exigibilidad de otra conducta

Temor fundado

Caso fortuito

### **A. Error esencial del hecho**

---

<sup>78</sup> *La ley y el Delito*, p.480, Caracas, 1945 citado por Fernando Castellanos Tena, *Lineamientos Elementales de Derecho Penal*, Editorial Porrúa, 2010, p.260.

<sup>79</sup> Amuchategui Requena, Griselda, *Derecho Penal*, México, Editorial Oxford University Press México, S.A. de C.V., 2010, p.95.

El *error esencial del hecho invencible* es la incorrecta concepción de la realidad, el sujeto está imposibilitado para conocer que la acción u omisión realizada es ilícita, es decir, cree que está realizando una actuación lícita.

*Error.* Es falsa concepción de la realidad; no es la ausencia de conocimiento, sino un conocimiento deformado o incorrecto. El error se conoce pero se conoce mal.

*Error de hecho:* El error recae en condiciones del hecho; así puede ser de tipo o de prohibición.

*Error esencial.* Es un error sobre un elemento de hecho que impide que se dé el dolo. Vannini, dice, es el que, recayendo sobre un extremo esencial del delito, impide al agente conocer, advertir la relación del hecho realizado con hecho formulado en forma abstracta en el precepto penal<sup>80</sup>. El sujeto actúa antijurídicamente.

- a) Error esencial vencible. Cuando subsiste la culpa a pesar del error.
- b) Error esencial invencible. Cuando no hay culpabilidad. Este error constituye una causa de inculpabilidad. El sujeto está imposibilitado para conocer la ilicitud de su acción u omisión. Considera lícita su actuación.

*Error accidental.* Cuando recae sobre circunstancias accesorias y secundarias del hecho.

- a) *Aberratio ictus.* Es el error en el golpe.
- b) *Aberratio in persona.* Es el error sobre la persona que aplicaba el delito.
- c) *Aberratio in delicti.* Es el error en el delito; se produce otro ilícito que no era el querido.

Es causa de inculpabilidad únicamente el error de hecho, esencial invencible.

El texto vigente del CPF establece, en su artículo 15, fracción VIII, lo siguiente:  
VIII. Se realice la acción o la omisión bajo un error invencible:

- a) Sobre alguno de los elementos esenciales que integran el tipo penal; o
- b) Respecto de la ilicitud de la conducta, ya sea porque el sujeto desconozca la existencia de la ley o el alcance de la misma, o porque crea que está justificada su conducta.

Si los errores a que se refieren los incisos anteriores son vencibles, se estará a lo dispuesto por el artículo 66 de este Código.

---

<sup>80</sup> Citado por Fernando Castellanos Tena, *Lineamientos Elementales de Derecho Penal*, Editorial Porrúa, 2010, p.260.

## B. Eximentes putativas

“Por eximentes putativas se entienden las situaciones en las cuales el agente, por error esencial de hecho insuperable, cree fundadamente, al realizar un hecho típico del Derecho Penal, hallarse amparado por una justificante, o ejecutar una conducta atípica, permitida, lícita, sin serlo”.<sup>81</sup>

*Legítima defensa putativa.* El sujeto cree obrar en legítima defensa por un error esencial invencible de hecho.

*Legítima defensa putativa recíproca.* Dos personas pueden obrar por error esencial invencible de hecho, ante la creencia de una agresión injusta, y obrar cada una de ellas en legítima defensa por error.

*Legítima defensa real contra la legítima defensa putativa.* Puede ocurrir también una conducta típica resultante de obrar una persona en legítima defensa real contra otra que actúa en legítima defensa putativa. Habrá dos resultados típicos y dos excluyentes de responsabilidad: al primero le beneficiará una causa de justificación y al otro, una causa de inculpabilidad.

*Cumplimiento de un deber putativo.* El sujeto puede creer que actúa en delito por un error de la misma naturaleza de los casos anteriores, cuando el sujeto cree que actúa en ejercicio de un derecho.

*Ejercicio de un deber putativo.* Esta figura será factible si se produce un delito por un error de la misma naturaleza de los casos anteriores, cuando el sujeto actúa en ejercicio de un derecho.

## C. No exigibilidad de otra conducta

“Cuando se produce una consecuencia típica, por las circunstancias, condiciones, características, relaciones, parentesco, etc., de la persona, no puede esperarse y menos exigirse otro comportamiento”.<sup>82</sup>

---

<sup>81</sup> Fernando Castellanos Tena, *Lineamientos Elementales de Derecho Penal*, Editorial Porrúa, 2010, p.266.

<sup>82</sup> Amuchategui Requena, Griselda, *Derecho Penal*, México, Editorial Oxford University Press México, S.A. de C.V., 2010, p.98



Se reglamenta en forma destacada la inexigibilidad en el artículo 15 del CPF: “El delito se excluye cuando: IX. *Atentas las circunstancias que concurren en la realización de una conducta ilícita, no sea racionalmente exigible al agente una conducta diversa a la que realizó, en virtud de no haberse podido determinar a actuar conforme a derecho*”.

#### **D. Estado de necesidad**

Estado de Necesidad: La comisión de un delito puede existir cuando el agente, por error esencial de hecho invencible, cree encontrarse en un estado de necesidad. Para algunos autores, cuando los bienes jurídicos (el sacrificado y el salvado) son de igual jerarquía, se trata del estado de necesidad como causa de inculpabilidad.

#### **E. Obediencia jerárquica**

Obediencia jerárquico-legítima: “Los tratadistas distinguen entre la obediencia que responde a subordinación espiritual, o política, o doméstica o legítima. Sólo la última puede dar lugar a la excluyente, porque obedece a una jerarquía impuesta por la ley para que ésta sea eficazmente obedecida”.<sup>83</sup>

#### **F. Temor fundado**

Actualmente el Código Penal Federal ya no reglamenta el temor fundado entre las causas de exclusión del delito. El cual consistía en causar daño por que el sujeto se creía amenazado de un mal grave.

Antes recogía la fracción VI del artículo 15 entre las excluyentes de responsabilidad: “... el temor fundado e irresistible de un mal inminente y grave en bienes jurídicos, propios o ajenos, siempre que no exista otro medio practicable y menos perjudicial al alcance del agente”. Como en realidad se trata de la vis compulsiva o coacción moral, queda comprendida como un caso de no exigibilidad de

---

<sup>83</sup> Raúl Carrancá y Trujillo, Raúl Carranca y Rivas, *Derecho Penal Mexicano*, México, Editorial Porrúa, 2007, p.673.

otra conducta (Art. 15-IX). Para la mayor parte de los especialistas, el fundado temor es uno de los casos típicos de la no exigibilidad de otra conducta, en virtud de que el Estado, según afirman, no puede exigir un obrar diverso, heroico.

### **G. Caso fortuito**

Es causar un daño por mero accidente, sin intención ni prudencia alguna, al realizar un hecho lícito con todas las precauciones debidas.

Está prevista en la fracción X del art. 15 del CPF: *El resultado típico se produce por causa fortuito.*

Para algunos autores el caso fortuito es una causa de inculpabilidad, mientras que para otros es una excluyente de responsabilidad ajena a la culpa, pues se obra con precaución y al realizar un hecho lícito; así, se produce un resultado sólo por mero accidente, lo cual deja absolutamente fuera la voluntad del sujeto.

Inculpabilidad es un aspecto negativo del delito, es la ausencia del delito. Están ausentes los elementos esenciales de la culpabilidad que son el conocimiento y la voluntad.

Las causas de inculpabilidad son las circunstancias que anulan el elemento del conocimiento o de la voluntad, como puede ser el error de hecho invencible, eximentes putativas (aquel que disculpa el castigo), no exigibilidad de otra conducta, temor fundado, caso fortuito.

En la no exigibilidad de la conducta se encuentra el estado de necesidad y la obediencia jerárquica.

El temor fundado ya no está reglamentado, pues no se podía obligar a una conducta de tipo heroica.

El caso fortuito es un accidente y no debe ser considerado como incriminante.

### 3.6 Condiciones objetivas de punibilidad y su ausencia.

#### Condiciones objetivas de punibilidad.

Es el nombre que reciben los requisitos que la ley señala eventualmente para que pueda perseguirse el delito. Vamos a encontrar que constituyen circunstancias de cuya existencia depende la aplicación de la pena prevista para la conducta desplegada.

Von Liszt considera a la punibilidad como "coercibilidad penal, que permite distinguir el injusto penal de cualquiera otra rama jurídica; constituye la consecuencia de la conducta típica, antijurídica y culpable, no existe la punibilidad por innecesaria, en la medida que a través de la tipicidad se reconoce la característica definitoria del delito como la conducta que implica la transgresión a la ley penal."<sup>84</sup>

Analizamos que para que exista un delito lo primero que se requiere es que exista una conducta humana, la cual va a consistir en un hecho material, exterior, positivo o negativo, producido por el hombre, respecto de la cual Jiménez de Asúa afirma que: "es la manifestación de la voluntad que mediante acción provoca un cambio que el mundo exterior(o pone en peligro de que se produzca), o bien, que por no hacer lo que se espera deja sin mudanza ese mundo externo cuya modificación se aguarda. El acto es pues, una conducta humana voluntaria que produce un resultado."<sup>85</sup>

- **La acción penal.**

Esta es la suma de las relaciones causales que necesariamente debe contener los siguientes elementos:

- a. Modificación en el mundo exterior perceptible a través de los sentidos, en los delitos de acción o resultado material.
- b. Un simple movimiento corporal sin que exija además la producción del resultado.

---

<sup>84</sup> Malo Camacho, Gustavo, *Derecho Penal Mexicano*, México, 1998.p.249, 2ª, Ed. Porrúa.

<sup>85</sup> Jiménez De Asúa, Luis. *La Ley y el Delito*. España, 1967. p.210. Edit. Sudamericana.

c. La no evitación de un resultado en los de omisión.

La no realización de una determinada actividad (omisión por socorro) causada por la voluntad, en los de comisión por omisión.

Vamos a ver que estas son circunstancias extrínsecas e independientes del acto punible. Por ello, para algunos autores carecen de relevancia dentro de la teoría del delito. Pueden ser consideradas como requisitos de procedibilidad o como cuestiones prejudiciales y se refieren más a cuestiones procesales que a sustantivas.

Otros autores nos dicen que constituyen modalidades del tipo penal que si forman parte del derecho sustantivo, cuando se presenta, puede decirse que el delito es condición necesaria para la responsabilidad penal, pero no condición suficiente.

- **Requisitos para determinar la pena al sujeto activo.**

Dado que para la aplicación de las penas, el juez deberá sujetarse a los límites fijados por el legislador en la ley penal, la que no podrá determinar arbitrariamente, sino siguiendo las reglas, generales o específicas y cumpliendo con los requisitos que la propia ley determine.

Para aplicar la pena justa, el juez deberá precisar en la sentencia los requisitos previstos por la ley;

- I. La naturaleza de la acción u omisión y de los medios empleados para ejecutarla.
- II. La magnitud del daño causado al bien jurídico y el peligro al que hubiese sido expuesto.
- III. Las circunstancias del tiempo, lugar modo u ocasión del hecho realizado.
- IV. La forma y grado de intervención del agente en la comisión del delito, así como su calidad y la de la víctima y ofendido.

- V. La edad, la educación, la ilustración, las costumbres, las condiciones sociales y económicas del sujeto, así como los motivos que lo impulsaron o determinaron a delinquir.
- VI. El comportamiento posterior del sentenciado con relación al delito cometido.
- VII. Las demás condiciones especiales y personales en que se encontraba el agente en el momento de la comisión del delito.

### **Ausencia Condiciones Objetivas de Punibilidad**

Hablamos de usar el término causas excluyentes del delito, que resulta inadecuado, ya que de acuerdo a la ley, el delito solo podrá excluirse, siempre y cuando se haya justificado el comportamiento del autor o en su defecto se haya probado alguna causa excluyente de responsabilidad.

- **Causas Permisivas**

a.) se actúe con el consentimiento del titular del bien jurídico afectado, siempre que se llenen los siguientes requisitos:

1. Delito perseguible por querrela;
2. que el titular del bien tenga capacidad de disponer libremente del mismo, y
3. Que el consentimiento sea expreso o tácito y sin que medie algún vicio de la voluntad.

b.) Se repele una agresión real, actual o inminente y sin derecho en protección de bienes jurídicos propios o ajenos, siempre que exista necesidad de la defensa y racionalidad de los medios empleados y no medie provocación dolosa, suficiente o inmediata por parte del agredido o de la persona a quien se defiende.

Podemos encontrar las excusas absolutorias en el artículo 139 del Código Penal para el Distrito Federal.

- **Causas de inculpabilidad**

a.) Al momento de realizar el hecho típico el agente padezca un trastorno mental transitorio que le impida comprender el carácter ilícito del hecho.

b.) Respecto de la ilicitud de la conducta, ya sea porque el sujeto desconozca el alcance de la ley, o porque crea que está justificada su conducta.

Vamos a encontrar que doctrinalmente se encuentra dividida la punibilidad, algunos autores consideran que la punibilidad es un elemento del delito, mientras que para otros autores, la punibilidad no es más que una consecuencia del delito.

Considero que del tema lo más importante que debemos tomar en cuenta es que, para que una acción constituya un delito o varios delitos debe necesariamente que se halle en una ley con una pena.

En consecuencia encontramos que la punibilidad es resultado de la reunión de varios elementos.

Por el contrario vemos que también existen las excusas absolutorias de la punibilidad, en ese sentido, se entiende que pueden ser conductas antijurídicas que no necesariamente van a ser sancionadas por el Estado. Y que dichas excusas van a operar en función de los intereses públicos.

### **3.7 Punibilidad y Excusas Absolutorias**

#### **Punibilidad**

El diccionario jurídico<sup>86</sup> refiere que, la voz "punibilidad" tiene dos sentidos: 1) puede significar merecimiento de pena y en este, sentido todo delito es punible; 2) también puede significar posibilidad de aplicar penas; y de la mano no a cualquier delito se le puede aplicar pena.

Para Jiménez Huerta la *punibilidad* "es la consecuencia lógico jurídica del juicio de reproche: *nulla poena sine culpa*"<sup>87</sup>. Otros autores igualmente refieren este latinismo como base del aspecto negativo de la *punibilidad*.

---

<sup>86</sup> *Diccionario Jurídico Espasa*. P. 221.

<sup>87</sup> Jiménez Huerta, Mariano. *Derecho Penal Mexicano*. Tomo I, México, Editorial Porrúa, 1983, p. 473.

Por otro lado el jurista Castellanos Tena<sup>88</sup> refiere en este tema que: “es el merecimiento de una pena en la función de la realización de una conducta.”

Considero que las definiciones son ejemplificativas y varían a capricho de cada autor según su propio estudio, sin embargo es entendible que la *punibilidad* va de la mano con el merecimiento de una pena o sanción establecida en la legislación vigente.

Finalmente para Miguel Ángel Granados Atlaco<sup>89</sup> es la amenaza de aplicación de una pena en concreto sobre quien cometa un acto delictivo.

- **Punición, pena y Sanción**

El diccionario jurídico<sup>90</sup> nos refiere por punición como el castigo que se impone por algo. Zaffaroni<sup>91</sup> al respecto refiere en este marco que: “*es la facultad potestativa del estado para ejercer su poder de imperium*”. Aunque de la mano con la pena, la punición es como se ha dicho es propia del estado a través del poder judicial para sancionar la conducta delictiva. Por otro lado la pena ya es la sanción dictada y ejecutable, o sea, es la conducta sancionada.

Finalmente la sanción entendida como tal es usada como sinónimo de pena pero se aplica generalmente a actos de índole administrativo o acciones delictuosas que no merecen pena sino un castigo mínimo que puede ser: una medida de seguridad, multa, trabajos a favor de la comunidad u otra similar.

Como se ha mencionado en reiteradas ocasiones, tanto la sanción y la pena la determinan el tipo penal y en algunos casos, las condiciones generales de aplicabilidad de la norma.

- **Variación de la Pena. Circunstancias atenuantes o privilegiadas**

La punibilidad tiene alcances limitados. Esto es que no se puede imponer la pena en condiciones que no lo permitan; tal es el caso de esta figura que se actualiza

---

<sup>88</sup> Castellanos Tena, Fernando. *Lineamientos Elementales de Derecho penal*. Editorial Porrúa, 2010, p. 277.

<sup>89</sup> Granados Atlaco, Miguel Ángel. *Derecho Penal Electoral Mexicano*. Editorial Porrúa, 2009, p. 209.

<sup>90</sup> idem

<sup>91</sup> Zaffaroni, Eugenio. Apuntes de derecho penal.

cuando muere el activo del delito (art 98 CPDF), sustitución de prisión art 84 CPDF. Por sustitución de la multa art 85 (por trabajo en beneficio de la comunidad), sustitución de la sanción privativa de libertad (por reparación del daño cuando esta proceda (art. 86 CPDF), Indulto, amnistía, prescripción, rehabilitación, reconocimiento de inocencia, perdón del ofendido (art. 94 CPDF) por el beneficio que le otorgue una ley penal nueva a la anterior.

- **Circunstancias Agravantes**

Las condiciones objetivas que tienden a hacer gravosa la conducta punible, nos la da la hipótesis normativa misma establecida por la autoridad legislativa y en algunos casos, la jurisprudencia.

A manera de conclusión, la *punibilidad* ha existido desde que el hombre consideró la necesidad de sancionar una conducta que afecta o puede dañar al grupo colectivo o en lo individual.

La *punibilidad* coinciden los autores, en que no es otra cosa que la pena o sanción establecida por el legislador en las leyes penales con evidentes limitantes discrecionales de aplicación. De igual manera la imposición de la pena es exclusiva de la autoridad jurisdiccional y esta puede determinar la forma de cumplir la sanción impuesta y de igual manera los criterios jurisprudenciales emitidos por la autoridad federal, permiten la modalidad discrecional del juez para aplicar la sanción de mérito.

Sin pena previa y expresamente establecida en la ley de la materia, no puede existir sanción y con ello, la conducta no es castigable.

### **Excusas Absolutorias**

Son aquellas en donde el legislador contempló para que un delito carezca de una punición, aunque el mismo se haya configurado y actualizado en el mundo material.



El Maestro Castellanos Tena, dice: “son aquellas causas que dejando subsistente el carácter delictivo de la conducta de hecho, impiden la aplicación de la pena.”<sup>92</sup> Derivadas de cuestiones de justicia, equidad y/o costumbre o necesidad específica de una determinada demarcación geográfica en algún momento de la historia.

Aunque la conducta antisocial contenida en un tipo específico sea culpable y antijurídica, o sea que reúne los elementos indispensables para que se configure dicha conducta como un delito, en casos específicos la Ley exonera al autor de la acción dolosa o culposa, por ende no se aplica la sanción.

Meramente tiene una razón de utilidad pública, siendo que en otro contexto u otra demarcación, las excusas que sean en una entidad no serán necesariamente en otra, dado que las normas penales atienden a las necesidades sociales de una demarcación en específico.

Como bien refiere el Doctor Miguel Ángel Granados Atlaco, las excusas absolutorias son creadas con base en una política criminal, con el objeto de coadyuvar al interés de una colectividad.

Las mismas no se encuentran legisladas en la parte general del Código Penal, sino en particulares disposiciones de la parte especial, y sin afectar la tipicidad, la antijuridicidad o la culpabilidad, eximen de pena al autor de determinados delitos.

No obstante que el delito se encuentra completo en sus elementos dogmáticos, y haberse comprobado autoría y responsabilidad del agente, no corresponde aplicar pena.

El Profesor Carrancá y Trujillo, expone una clasificación de las Excusas Absolutorias, las cuales son; “en razón de los móviles afectivos revelados; en razón de la

---

<sup>92</sup> Fernando, Castellanos Tena. Lineamientos Elementales de Derecho Penal, México, Editorial Porrúa, 1974, p 271.

copropiedad familiar; en razón de la maternidad conciente; en razón del interés social; en razón de la temibilidad.”<sup>93</sup>

En primer término tenemos los móviles afectivos revelados, que no son más que las excusas que el legislador pasmó en virtud de los lazos existentes entre la filiación y la familiaridad de las personas y hasta personas con vínculos de estrecha amistad o de afectividad. El ejemplo más claro es la circunstancia contenida en el artículo 139 del Código Penal del Distrito Federal, que a la letra reza: “No se impondrá pena alguna a quien por culpa ocasione lesiones u homicidio en agravio de un ascendiente o descendiente consanguíneo en línea recta, hermano, adoptante o adoptado, cónyuge, concubina, concubinario o cuando entre el agente y el pasivo exista relación de pareja permanente, amistad o de familia, salvo que el agente se encuentre bajo el efecto de bebidas embriagantes, de estupefacientes o psicotrópicos, sin que medie prescripción médica, o bien que se diere a la fuga y no auxiliare a la víctima.”

Es claro que el legislador al crear este tipo penal, trata de salvaguardar los intereses familiares ante un suceso trágico, ya que evita la pena del familiar que culposamente prive de la vida a otro de sufrir, además las consecuencias del evento típico y antijurídico.

Por lo que en concreto se puede decir que las excusas absolutorias atienden a aspectos como el de desanimar del camino del delito como la excusa por motivos de arrepentimiento; las tendientes a la paz colectiva; al resguardo familiar, como las lesiones o en su momento la violación entre cónyuges y/o el encubrimiento de parientes; y las fundadas en la mínima temibilidad.

En síntesis, las excusas absolutorias son aquellas circunstancias que no estando relacionadas directamente con la conducta del autor descrita en el tipo penal excluyen la pena cuando se dan, pueden referir tanto a la calidad personal del agente o a su propia actividad fuera del tipo o a la actividad de un tercero, o a la situación en que el hecho se comete. Se trata de causas personales de impunidad, que

---

<sup>93</sup> Raúl, Carrancá y Trujillo. Derecho Penal. Parte General, México, Editorial Porrúa, 2001, p 652.

genéricamente obedecen a razones de política criminal o de utilidad, es decir cuando aparezca evidentemente inconveniente la sanción de un hecho.

Para finalizar, las excusas absolutorias son un elemento importante para tratar de evitar el castigo de la ley al cometer una conducta típica y antijurídica; el legislador debería de seguir con la aplicación de políticas criminales con el objeto de crear más supuestos eximentes de punibilidad, dado que hay circunstancias que el propio legislador debería de observar en su totalidad las necesidades de la sociedad, para el caso las del conglomerado del Distrito Federal, todo esto con el fin de no cometer injustos al aplicar las sanciones penales que ordena el tipo penal para el caso de la no obediencia de la norma penal.

## **Capítulo 4. Los delitos informáticos del Título Noveno del Código Penal Federal relativos al acceso ilícito a sistemas y equipos de informática**

**SUMARIO:** 4.1 Modificar, destruir o provocar pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sin autorización. 4.2 Conocer o copiar información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sin autorización. 4.3 Modificar, destruir o provocar pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, sin autorización. 4.4 Conocer o copiar información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad. 4.5 Conocer, obtener, copiar o utilizar información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad. 4.6 Modificar, destruir o provocar pérdida de información que contengan indebidamente, estando autorizado para acceder a sistemas y equipos de informática del Estado. 4.7 Estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente copiar información que contengan. 4.8 Estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtener, copiar o utilizar información que contengan. 4.9 Modificar, destruir o provocar pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. 4.10 Conocer o copiar información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. 4.11 Estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modificar, destruir o provocar pérdida de información que contengan. 4.12 Estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copiar información que contengan.

### **4.1 Modificar, destruir o provocar pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sin autorización.**

El artículo 211 bis 1 del Código Penal Federal establece en su primer párrafo lo siguiente:

“Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida 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 de cien a trescientos días multa.”

Como podemos ver del texto anterior, se derivan una serie considerable de hipótesis, las cuales procederemos a ilustrar:

ACCIÓN ESPECÍFICA DEL SUJETO ACTIVO	HIPÓTESIS
MODIFIQUE	<ul style="list-style-type: none"> <li>· Información contenida en sistemas de informática protegidos por algún mecanismo de seguridad.</li> <li>· Información contenida en equipos de informática protegidos por algún mecanismo de seguridad.</li> </ul>
DESTRUYA	<ul style="list-style-type: none"> <li>· Información contenida en sistemas de informática protegidos por algún mecanismo de seguridad.</li> <li>· Información contenida en equipos de informática protegidos por algún mecanismo de seguridad.</li> </ul>
PROVOQUE PÉRDIDA	<ul style="list-style-type: none"> <li>· Información contenida en sistemas de informática protegidos por algún mecanismo de seguridad.</li> <li>· Información contenida en equipos de informática protegidos por algún mecanismo de seguridad.</li> </ul>

TOTAL DE HIPÓTESIS PREVISTAS EN EL PRIMER  
PÁRRAFO DEL ARTÍCULO 211 BIS 1 DEL CÓDIGO  
PENAL FEDERAL

6

Como podemos observar este artículo consta de varios supuestos, por lo que se hará el estudio dogmático de una manera general, definiendo antes diversos conceptos claves para poder entender de manera correcta el párrafo, tomando los supuestos de este precepto para este ejercicio.

Debido a que la legislación mexicana no define que debemos entender por “modificar”, “destruir”, “provocar” y “pérdida”, que son los verbos núcleos del primer párrafo del artículo 211 bis 1, nos mantendremos apegados a la definición que nos brinda, tanto el Diccionario de la Real Academia de la Lengua Española (DRAE), así como el Diccionario del Español de México (DEM), que son:

- **Modificar:**  
**DRAE:** Transformar o cambiar algo mudando alguna de sus características.  
**DEM:** Cambiar algunas partes o aspectos de una cosa sin que se modifique o altere del todo o se transforme en otra.
- **Destruir:**  
**DRAE:** 1. Reducir a pedazos o a cenizas algo material, u ocasionarle un grave daño.  
2. Deshacer o inutilizar algo no material.  
**DEM:** Poner fin a algo haciéndolo pedazos, dañándolo gravemente o dejándolo inservible.
- **Provocar:**  
**DRAE:** Producir o causar algo.  
**DEM:** Hacer que ocurra una cosa como consecuencia de otra.
- **Perder:**  
**DRAE:** Dejar de tener, o no hallar, aquello que poseía, sea por culpa o descuido del poseedor, sea por contingencia o desgracia.  
**DEM:** Dejar de tener algo, no saber dónde quedó una cosa que se tenía o alguna persona con la que se estaba, no conseguir algo que se esperaba.

Ahora bien, nos atañe hacer la diferenciación entre lo que es un “sistema de informática” y un “equipo de informática”. Son términos que van de la mano, pero que es muy importante su diferencia.

***1. Modifique información contenida en sistemas de informática protegidos por algún mecanismo de seguridad.***

La conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “modificar”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, es decir, una fuerza física superior e irresistible proveniente de otro hombre.

Referente a la tipicidad, se debe dar el exacto encuadramiento de la conducta respecto al tipo penal, que es el “modificar” información contenida en sistemas de informática protegidos por algún mecanismo de seguridad. El tipo

señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema; en lo que respecta al sujeto pasivo, puede ser cualquier persona, ya sea física o moral, y no se establece ninguna calidad específica para el sujeto pasivo.

El elemento objetivo de la hipótesis es todo aquel atentado que prevea dañar o desviar el uso correcto de un sistema de informática con la finalidad de obtener un beneficio, ya sea material o inmaterial, ya sea moral, para sí o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un sistema de informática protegido por algún mecanismo de seguridad.

El elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa con que actúa el sujeto activo que modifique información contenida en sistemas de informática protegidos por algún mecanismo de seguridad.

También, existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba con autorización o no. La atipicidad en este supuesto encajaría en 2 supuestos, el primero es que el sujeto activo cuente con autorización para realizar la modificación de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad, y, la segunda, sería que el que sin autorización, modifique información contenida en sistemas de informática que no esté protegida por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

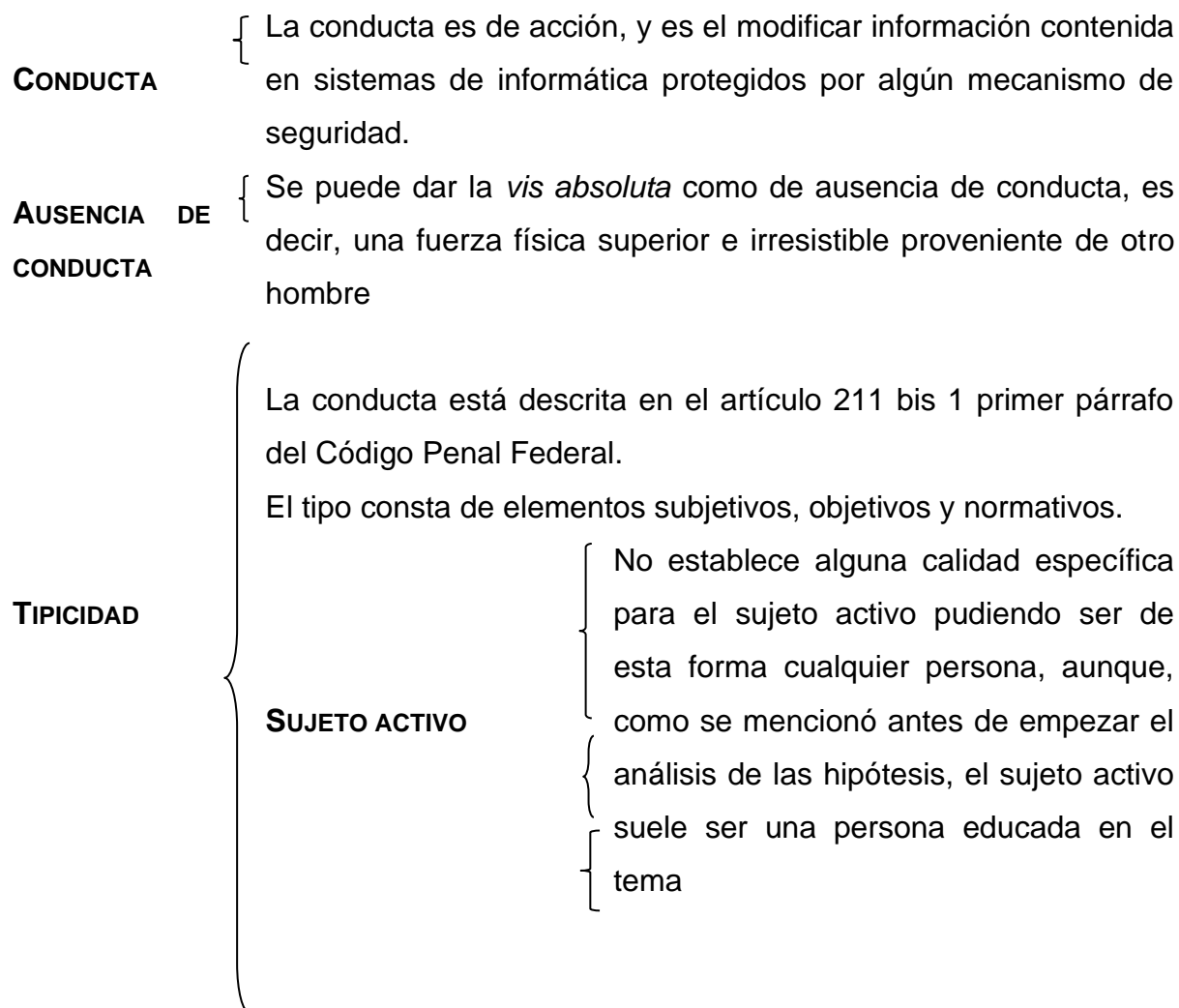
Para la acción realizada en esta hipótesis, como se ha mencionado con anterioridad, el sujeto activo de los delitos informáticos se ha observado que por lo general son personas de un determinado nivel de inteligencia y educación,

superior al común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis analizada se da de forma dolosa o culposa, mismo que nos ayuda a evidenciar la realización de la conducta. La inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podía presentar una amenaza de un daño grave si no se realiza la conducta en el tipo de mérito.

Este delito se persigue de oficio, teniendo una sanción de seis meses a dos años de prisión y de cien a trescientos días multa; no teniendo ninguna excusa absolutoria.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación se esquematiza lo anteriormente explicado.





	<b>SUJETO PASIVO</b>	El sujeto pasivo, puede ser cualquier persona, ya sea física o moral, y no se establece ninguna calidad específica para ser sujeto pasivo.
	<b>BIEN JURÍDICO TUTELADO</b>	{ La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
	<b>OBJETO JURÍDICO</b>	{ Sistemas de informática.
	<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	constituido por el dolo o la culpa con que actúa el sujeto activo que modifique información contenida en sistemas de informática protegidos por algún mecanismo de seguridad
	<b>ELEMENTO NORMATIVO</b>	{ Que atente contra los sistemas de informática.
<b>ATIPICIDAD</b>	{	Encajaría en 2 hipótesis, el primero es que el sujeto activo cuente con autorización para realizar la modificación de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad, y, la segunda, sería que el que, sin autorización, modifique información contenida en sistemas de informática que no esté protegida por algún mecanismo de seguridad.
<b>ANTI JURIDICIDAD</b>	{	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 1 primer párrafo del Código Penal Federal) y es contraria a la sociedad.
<b>CAUSAS DE JUSTIFICACIÓN</b>	{	No se puede aplicar ninguna.
<b>IMPUTABILIDAD</b>	{	La capacidad de querer y entender.
<b>INIMPUTABILIDAD</b>	{	Se puede presentar que una persona no imputable realice la conducta, pero sería difícil que pasara.

<b>CULPABILIDAD</b>	{	Se puede dar de manera dolosa o culposa.
<b>INCULPABILIDAD</b>	{	Se puede presentar por dos razones, siendo la primera la vis compulsiva, y la segunda, por obediencia jerárquica
<b>CONDICIONES OBJETIVAS DE</b>	{	Se persigue de oficio.
<b>PUNIBILIDAD</b>		
<b>PUNIBILIDAD</b>	{	De seis meses a dos años de prisión y de cien a trescientos días multa
<b>EXCUSAS ABSOLUTORIAS</b>	{	No tiene excusa absolutoria alguna

***2. Modifique información contenida en equipos de informática protegidos por algún mecanismo de seguridad.***

La conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “modificar”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, es decir, una fuerza física superior e irresistible proveniente de otro hombre.

Referente a la tipicidad, se debe dar el exacto encuadramiento de la conducta respecto al tipo penal, que es el “modificar información contenida en equipos de informática protegidos por algún mecanismo de seguridad. El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema; en lo que respecta al sujeto pasivo, puede ser cualquier persona, ya sea física o moral, y no se establece ninguna calidad específica para el sujeto pasivo.

El elemento objetivo de la hipótesis es todo aquel atentado que prevea dañar o desviar el uso correcto de un equipo de informática con la finalidad de obtener un beneficio, ya sea material o inmaterial, ya sea moral, para sí o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un equipo de informática protegido por algún mecanismo de seguridad.

El elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa con que actúa el sujeto activo que modifique información contenida en equipos de informática protegidos por algún mecanismo de seguridad.

También, existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba con autorización o no. La atipicidad en este supuesto encajaría en 2 supuestos, el primero es que el sujeto activo cuente con autorización para realizar la modificación de información contenida en equipos de informática protegidos por algún mecanismo de seguridad, y, la segunda, sería que el que, sin autorización, modifique información contenida en equipos de informática protegidos por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

Para la acción realizada en esta hipótesis, como se ha mencionado con anterioridad, el sujeto activo de los delitos informáticos se ha observado que por lo general son personas de un determinado nivel de inteligencia y educación, superior al común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis analizada se da de forma dolosa o culposa, mismo que nos ayuda a evidenciar la realización de la conducta. La inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podía presentar una amenaza de un daño grave si no se realiza la conducta en el tipo de mérito.

Este delito se persigue de oficio, teniendo una sanción de seis meses a dos años de prisión y de cien a trescientos días multa; no teniendo ninguna excusa absolutoria.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación se esquematiza lo anteriormente explicado.

<b>CONDUCTA</b>	{	La conducta es de acción, y es el modificar información contenida en equipos de informática protegidos por algún mecanismo de seguridad.
<b>AUSENCIA DE CONDUCTA</b>	{	Se puede dar la <i>vis absoluta</i> como de ausencia de conducta, es decir, una fuerza física superior e irresistible proveniente de otro hombre
<b>TIPICIDAD</b>	{	<p>La conducta está descrita en el artículo 211 bis 1 primer párrafo del Código Penal Federal.</p> <p>El tipo consta de elementos subjetivos, objetivos y normativos.</p> <p><b>SUJETO ACTIVO</b> {</p> <p style="margin-left: 20px;">No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema</p> <p><b>SUJETO PASIVO</b> {</p> <p style="margin-left: 20px;">El sujeto pasivo, puede ser cualquier persona, ya sea física o moral, y no se establece ninguna calidad específica para ser sujeto pasivo.</p> <p><b>BIEN JURÍDICO TUTELADO</b> {</p> <p style="margin-left: 20px;">La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.</p> <p><b>OBJETO JURÍDICO</b> {</p> <p style="margin-left: 20px;">Equipos de informática.</p> <p><b>ELEMENTO SUBJETIVO DEL ILÍCITO</b> {</p> <p style="margin-left: 20px;">Constituido por el dolo o la culpa con que actúa el sujeto activo que modifique información contenida en equipos de informática protegidos por algún mecanismo de seguridad</p>

	<b>ELEMENTO NORMATIVO</b>	{ Que atente contra los equipos de informática.
<b>ATIPICIDAD</b>	{	Encajaría en 2 hipótesis, el primero es que el sujeto activo cuente con autorización para realizar la modificación de información contenida en equipos de informática protegidos por algún mecanismo de seguridad, y, la segunda, sería que el que, sin autorización, modifique información contenida en equipos de informática que no esté protegida por algún mecanismo de seguridad.
<b>ANTI JURIDICIDAD</b>	{	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 1 primer párrafo del Código Penal Federal) y es contraria a la sociedad.
<b>CAUSAS DE JUSTIFICACIÓN</b>	{	No se puede aplicar ninguna.
<b>IMPUTABILIDAD</b>	{	La capacidad de querer y entender.
<b>INIMPUTABILIDAD</b>	{	Se puede presentar que una persona no imputable realice la conducta, pero sería difícil que pasara.
<b>CULPABILIDAD</b>	{	Se puede dar de manera dolosa o culposa.
<b>INCULPABILIDAD</b>	{	Se puede presentar por dos razones, siendo la primera la vis compulsiva, y la segunda, por obediencia jerárquica
<b>CONDICIONES OBJETIVAS DE PUNIBILIDAD</b>	{	Se persigue de oficio.
<b>PUNIBILIDAD</b>	{	De seis meses a dos años de prisión y de cien a trescientos días multa
<b>EXCUSAS ABSOLUTORIAS</b>	{	No tiene excusa absolutoria alguna

***3. Destruir información contenida en sistemas de informática protegidos por algún mecanismo de seguridad.***

La conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “destruir”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, es decir, una fuerza física superior e irresistible proveniente de otro hombre.

Referente a la tipicidad, se debe dar el exacto encuadramiento de la conducta respecto al tipo penal, que es el “destruir” información contenida en sistemas de informática protegidos por algún mecanismo de seguridad. El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema; en lo que respecta al sujeto pasivo, puede ser cualquier persona, ya sea física o moral, y no se establece ninguna calidad específica para el sujeto pasivo.

El elemento objetivo de la hipótesis es todo aquel atentado que prevea dañar o desviar el uso correcto de un sistema de informática con la finalidad de obtener un beneficio, ya sea material o inmaterial, ya sea moral, para sí o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un sistema de informática protegido por algún mecanismo de seguridad.

El elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa con que actúa el sujeto activo que destruya información contenida en sistemas de informática protegidos por algún mecanismo de seguridad.

También, existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba con autorización o no. La atipicidad en este supuesto encajaría en 2 supuestos, el primero es que el sujeto activo cuente con autorización para destruir información contenida en sistemas de informática protegidos por algún mecanismo de seguridad, y, la segunda, sería que el que, sin autorización, destruya información contenida en sistemas de informática que no esté protegida por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

Para la acción realizada en esta hipótesis, como se ha mencionado con anterioridad, el sujeto activo de los delitos informáticos se ha observado que por lo general son personas de un determinado nivel de inteligencia y educación, superior al común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis analizada se da de forma dolosa o culposa, mismo que nos ayuda a evidenciar la realización de la conducta. La inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podía presentar una amenaza de un daño grave si no se realiza la conducta en el tipo de mérito.

Este delito se persigue de oficio, teniendo una sanción de seis meses a dos años de prisión y de cien a trescientos días multa; no teniendo ninguna excusa absolutoria.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación se esquematiza lo anteriormente explicado.

<b>CONDUCTA</b>	{	La conducta es de acción, y es el destruir información contenida en sistemas de informática protegidos por algún mecanismo de seguridad.
<b>AUSENCIA DE CONDUCTA</b>	{	Se puede dar la <i>vis absoluta</i> como de ausencia de conducta, es decir, una fuerza física superior e irresistible proveniente de otro hombre.
<b>TIPICIDAD</b>	{	La conducta está descrita en el artículo 211 bis 1 primer párrafo del Código Penal Federal. El tipo consta de elementos subjetivos, objetivos y normativos.

<b>SUJETO ACTIVO</b>	<p>{ No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema</p>
<b>SUJETO PASIVO</b>	<p>{ El sujeto pasivo, puede ser cualquier persona, ya sea física o moral, y no se establece ninguna calidad específica para ser sujeto pasivo.</p>
<b>BIEN JURÍDICO TUTELADO</b>	<p>{ La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.</p>
<b>OBJETO JURÍDICO</b>	<p>{ Sistemas de informática. Constituido por el dolo o la culpa con que actúa el sujeto activo que modifique información contenida en sistemas de informática protegidos por algún mecanismo de seguridad</p>
<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	<p>{ Que atente contra los sistemas de informática.</p>
<b>ATIPICIDAD</b>	<p>{ Encajaría en 2 hipótesis, el primero es que el sujeto activo cuente con autorización para realizar la destrucción de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad, y, la segunda, sería que el que, sin autorización, destruya información contenida en sistemas de informática que no esté protegida por algún mecanismo de seguridad.</p>
<b>ANTI JURIDICIDAD</b>	<p>{ Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 1 primer párrafo del Código Penal Federal) y es contraria a la sociedad.</p>



<b>CAUSAS DE JUSTIFICACIÓN</b>	{	No se puede aplicar ninguna.
<b>IMPUTABILIDAD</b>	{	La capacidad de querer y entender.
<b>INIMPUTABILIDAD</b>	{	Se puede presentar que una persona no imputable realice la conducta, pero sería difícil que pasara.
<b>CULPABILIDAD</b>	{	Se puede dar de manera dolosa o culposa.
<b>INCULPABILIDAD</b>	{	Se puede presentar por dos razones, siendo la primera la vis compulsiva, y la segunda, por obediencia jerárquica
<b>CONDICIONES OBJETIVAS DE PUNIBILIDAD</b>	{	Se persigue de oficio.
<b>PUNIBILIDAD</b>	{	De seis meses a dos años de prisión y de cien a trescientos días multa
<b>EXCUSAS ABSOLUTORIAS</b>	{	No tiene excusa absolutoria alguna

#### ***4. Destruir información contenida en equipos de informática protegidos por algún mecanismo de seguridad.***

La conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “destruir”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, es decir, una fuerza física superior e irresistible proveniente de otro hombre.

Referente a la tipicidad, se debe dar el exacto encuadramiento de la conducta respecto al tipo penal, que es el “destruir” información contenida en equipos de informática protegidos por algún mecanismo de seguridad. El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema; en lo que respecta al sujeto pasivo, puede ser cualquier persona, ya sea física o moral, y no se establece ninguna calidad específica para el sujeto pasivo.

El elemento objetivo de la hipótesis es todo aquel atentado que prevea dañar o desviar el uso correcto de un sistema de informática con la finalidad de obtener un beneficio, ya sea material o inmaterial, ya sea moral, para sí o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un equipo de informática protegido por algún mecanismo de seguridad.

El elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa con que actúa el sujeto activo que destruya información contenida en equipos de informática protegidos por algún mecanismo de seguridad.

También, existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba con autorización o no. La atipicidad en este supuesto encajaría en 2 supuestos, el primero es que el sujeto activo cuente con autorización para destruir información contenida en equipos de informática protegidos por algún mecanismo de seguridad, y, la segunda, sería que el que, sin autorización, destruya información contenida en equipos de informática que no esté protegida por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

Para la acción realizada en esta hipótesis, como se ha mencionado con anterioridad, el sujeto activo de los delitos informáticos se ha observado que por lo general son personas de un determinado nivel de inteligencia y educación, superior al común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis analizada se da de forma dolosa o culposa, mismo que nos ayuda a evidenciar la realización de la conducta. La inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podía presentar una amenaza de un daño grave si no se realiza la conducta en el tipo de mérito.

Este delito se persigue de oficio, teniendo una sanción de seis meses a dos años de prisión y de cien a trescientos días multa; no teniendo ninguna excusa absolutoria.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación se esquematiza lo anteriormente explicado.

<b>CONDUCTA</b>	{	La conducta es de acción, y es el destruir información contenida en equipos de informática protegidos por algún mecanismo de seguridad.
<b>AUSENCIA DE CONDUCTA</b>	{	Se puede dar la <i>vis absoluta</i> como de ausencia de conducta, es decir, una fuerza física superior e irresistible proveniente de otro hombre
<b>TIPICIDAD</b>	{	La conducta está descrita en el artículo 211 bis 1 primer párrafo del Código Penal Federal. El tipo consta de elementos subjetivos, objetivos y normativos.
	{	<b>SUJETO ACTIVO</b>
	{	No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema
	{	<b>SUJETO PASIVO</b>
	{	El sujeto pasivo, puede ser cualquier persona, ya sea física o moral, y no se establece ninguna calidad específica para ser sujeto pasivo.
	{	<b>BIEN JURÍDICO TUTELADO</b>
	{	La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
	{	<b>OBJETO JURÍDICO</b>
	{	Equipos de informática.

	<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	Constituido por el dolo o la culpa con que actúa el sujeto activo que modifique información contenida en equipos de informática protegidos por algún mecanismo de seguridad
	<b>ELEMENTO NORMATIVO</b>	{ Que atente contra los equipos de informática.
<b>ATIPICIDAD</b>	{	Encajaría en 2 hipótesis, el primero es que el sujeto activo cuente con autorización para realizar la destrucción de información contenida en equipos de informática protegidos por algún mecanismo de seguridad, y, la segunda, sería que el que, sin autorización, destruya información contenida en equipos de informática que no esté protegida por algún mecanismo de seguridad.
<b>ANTI JURIDICIDAD</b>	{	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 1 primer párrafo del Código Penal Federal) y es contraria a la sociedad.
<b>CAUSAS DE JUSTIFICACIÓN</b>	{	No se puede aplicar ninguna.
<b>IMPUTABILIDAD</b>	{	La capacidad de querer y entender.
<b>INIMPUTABILIDAD</b>	{	Se puede presentar que una persona no imputable realice la conducta, pero sería difícil que pasara.
<b>CULPABILIDAD</b>	{	Se puede dar de manera dolosa o culposa.
<b>INCULPABILIDAD</b>	{	Se puede presentar por dos razones, siendo la primera la vis compulsiva, y la segunda, por obediencia jerárquica
<b>CONDICIONES OBJETIVAS DE PUNIBILIDAD</b>	{	Se persigue de oficio.
<b>PUNIBILIDAD</b>	{	De seis meses a dos años de prisión y de cien a trescientos días multa

EXCUSAS  
ABSOLUTORIAS { No tiene excusa absolutoria alguna

**5. Provoque pérdida información contenida en sistemas de informática protegidos por algún mecanismo de seguridad.**

La conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “provoque pérdida”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, es decir, una fuerza física superior e irresistible proveniente de otro hombre.

Referente a la tipicidad, se debe dar el exacto encuadramiento de la conducta respecto al tipo penal, que es el “provocar pérdida” información contenida en sistemas de informática protegidos por algún mecanismo de seguridad. El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema; en lo que respecta al sujeto pasivo, puede ser cualquier persona, ya sea física o moral, y no se establece ninguna calidad específica para el sujeto pasivo.

El elemento objetivo de la hipótesis es todo aquel atentado que prevea dañar o desviar el uso correcto de un sistema de informática con la finalidad de obtener un beneficio, ya sea material o inmaterial, ya sea moral, para sí o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un sistema de informática protegido por algún mecanismo de seguridad.

El elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa con que actúa el sujeto activo que provoque pérdida de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad.

También, existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba con autorización o no. La atipicidad en este supuesto encajaría en 2 supuestos, el primero es que el sujeto activo cuente con autorización provoque la pérdida de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad, y, la segunda, sería que el que, sin autorización, provoque pérdida información contenida en sistemas de informática que no esté protegida por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

Para la acción realizada en esta hipótesis, como se ha mencionado con anterioridad, el sujeto activo de los delitos informáticos se ha observado que por lo general son personas de un determinado nivel de inteligencia y educación, superior al común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis analizada se da de forma dolosa o culposa, mismo que nos ayuda a evidenciar la realización de la conducta. La inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podía presentar una amenaza de un daño grave si no se realiza la conducta en el tipo de mérito.

Este delito se persigue de oficio, teniendo una sanción de seis meses a dos años de prisión y de cien a trescientos días multa; no teniendo ninguna excusa absolutoria.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación se esquematiza lo anteriormente explicado.

**CONDUCTA** { La conducta es de acción, y es el provocar la pérdida de

información contenida en sistemas de informática protegidos por algún mecanismo de seguridad.

<b>AUSENCIA DE CONDUCTA</b>	{	Se puede dar la <i>vis absoluta</i> como de ausencia de conducta, es decir, una fuerza física superior e irresistible proveniente de otro hombre	
		La conducta está descrita en el artículo 211 bis 1 primer párrafo del Código Penal Federal. El tipo consta de elementos subjetivos, objetivos y normativos.	
<b>TIPICIDAD</b>	{	<b>SUJETO ACTIVO</b>	{ No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema
			{ El sujeto pasivo, puede ser cualquier persona, ya sea física o moral, y no se establece ninguna calidad específica para ser sujeto pasivo.
		<b>SUJETO PASIVO</b>	{ El sujeto pasivo, puede ser cualquier persona, ya sea física o moral, y no se establece ninguna calidad específica para ser sujeto pasivo.
			{ La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
		<b>BIEN JURÍDICO TUTELADO</b>	{ La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
			{ Sistemas de informática.
<b>OBJETO JURÍDICO</b>	{	Sistemas de informática.	
	{	Constituido por el dolo o la culpa con que actúa el sujeto activo que provoque pérdida de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad	
<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	{	Constituido por el dolo o la culpa con que actúa el sujeto activo que provoque pérdida de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad	
	{	Que atente contra los sistemas de informática.	
<b>ELEMENTO NORMATIVO</b>	{	Que atente contra los sistemas de informática.	
	{	informática.	

<b>ATIPICIDAD</b>	{ Encajaría en 2 hipótesis, el primero es que el sujeto activo cuente con autorización para provocar la pérdida de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad, y, la segunda, sería que el que, sin autorización, provoque pérdida de información contenida en sistemas de informática que no esté protegida por algún mecanismo de seguridad.
<b>ANTI JURIDICIDAD</b>	{ Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 1 primer párrafo del Código Penal Federal) y es contraria a la sociedad.
<b>CAUSAS DE JUSTIFICACIÓN</b>	{ No se puede aplicar ninguna.
<b>IMPUTABILIDAD</b>	{ La capacidad de querer y entender.
<b>INIMPUTABILIDAD</b>	{ Se puede presentar que una persona no imputable realice la conducta, pero sería difícil que pasara.
<b>CULPABILIDAD</b>	{ Se puede dar de manera dolosa o culposa.
<b>INCULPABILIDAD</b>	{ Se puede presentar por dos razones, siendo la primera la vis compulsiva, y la segunda, por obediencia jerárquica
<b>CONDICIONES OBJETIVAS DE PUNIBILIDAD</b>	{ Se persigue de oficio.
<b>PUNIBILIDAD</b>	{ De seis meses a dos años de prisión y de cien a trescientos días multa
<b>EXCUSAS ABSOLUTORIAS</b>	{ No tiene excusa absolutoria alguna

**6. Provoque pérdida información contenida en equipos de informática protegidos por algún mecanismo de seguridad.**

La conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “provoque pérdida”, pudiéndose presentar una ausencia de conducta de tipo *vis*



*absoluta*, es decir, una fuerza física superior e irresistible proveniente de otro hombre.

Referente a la tipicidad, se debe dar el exacto encuadramiento de la conducta respecto al tipo penal, que es el “provocar pérdida” información contenida en equipos de informática protegidos por algún mecanismo de seguridad. El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema; en lo que respecta al sujeto pasivo, puede ser cualquier persona, ya sea física o moral, y no se establece ninguna calidad específica para el sujeto pasivo.

El elemento objetivo de la hipótesis es todo aquel atentado que prevea dañar o desviar el uso correcto de un equipo de informática con la finalidad de obtener un beneficio, ya sea material o inmaterial, ya sea moral, para sí o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un equipo de informática protegido por algún mecanismo de seguridad.

El elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa con que actúa el sujeto activo que destruya información contenida en equipos de informática protegidos por algún mecanismo de seguridad.

También, existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba con autorización o no. La atipicidad en este supuesto encajaría en 2 supuestos, el primero es que el sujeto activo cuente con autorización para destruir información contenida en equipos de informática protegidos por algún mecanismo de seguridad, y, la segunda, sería que el que, sin autorización, destruya información contenida en equipos de informática que no esté protegida por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

Para la acción realizada en esta hipótesis, como se ha mencionado con anterioridad, el sujeto activo de los delitos informáticos se ha observado que por lo general son personas de un determinado nivel de inteligencia y educación, superior al común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis analizada se da de forma dolosa o culposa, mismo que nos ayuda a evidenciar la realización de la conducta. La inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podía presentar una amenaza de un daño grave si no se realiza la conducta en el tipo de mérito.

Este delito se persigue de oficio, teniendo una sanción de seis meses a dos años de prisión y de cien a trescientos días multa; no teniendo ninguna excusa absolutoria.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación se esquematiza lo anteriormente explicado.

<b>CONDUCTA</b>	{	La conducta es de acción, y es el destruir información contenida en equipos de informática protegidos por algún mecanismo de seguridad.
<b>AUSENCIA DE CONDUCTA</b>	{	Se puede dar la <i>vis absoluta</i> como de ausencia de conducta, es decir, una fuerza física superior e irresistible proveniente de otro hombre
<b>TIPICIDAD</b>	{	La conducta está descrita en el artículo 211 bis 1 primer párrafo del Código Penal Federal. El tipo consta de elementos subjetivos, objetivos y normativos.

<b>SUJETO ACTIVO</b>	<p>No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema</p>
<b>SUJETO PASIVO</b>	<p>El sujeto pasivo, puede ser cualquier persona, ya sea física o moral, y no se establece ninguna calidad específica para ser sujeto pasivo.</p>
<b>BIEN JURÍDICO TUTELADO</b>	<p>La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.</p>
<b>OBJETO JURÍDICO</b>	<p>{ Equipos de informática.</p>
<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	<p>Constituido por el dolo o la culpa con que actúa el sujeto activo que modifique información contenida en equipos de informática protegidos por algún mecanismo de seguridad</p>
<b>ELEMENTO NORMATIVO</b>	<p>{ Que atente contra los equipos de informática.</p>
<b>ATIPICIDAD</b>	<p>{ Encajaría en 2 hipótesis, el primero es que el sujeto activo cuente con autorización provoque pérdida de información contenida en equipos de informática protegidos por algún mecanismo de seguridad, y, la segunda, sería que el que, sin autorización, provoque pérdida de información contenida en equipos de informática que no esté protegida por algún mecanismo de seguridad.</p>
<b>ANTI JURIDICIDAD</b>	<p>{ Cuenta con la formal y material, ya que la conducta transgrede</p>

una norma dictada por el Estado (art. 211 bis 1 primer párrafo del Código Penal Federal) y es contraria a la sociedad.

<b>CAUSAS DE JUSTIFICACIÓN</b>	{	No se puede aplicar ninguna.
<b>IMPUTABILIDAD</b>	{	La capacidad de querer y entender.
<b>INIMPUTABILIDAD</b>	{	Se puede presentar que una persona no imputable realice la conducta, pero sería difícil que pasara.
<b>CULPABILIDAD</b>	{	Se puede dar de manera dolosa o culposa.
<b>INCULPABILIDAD</b>	{	Se puede presentar por dos razones, siendo la primera la vis compulsiva, y la segunda, por obediencia jerárquica
<b>CONDICIONES OBJETIVAS DE PUNIBILIDAD</b>	{	Se persigue de oficio.
<b>PUNIBILIDAD</b>	{	De seis meses a dos años de prisión y de cien a trescientos días multa
<b>EXCUSAS ABSOLUTORIAS</b>	{	No tiene excusa absolutoria alguna

#### **4.2 Conocer o copiar información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sin autorización.**

En el artículo 211 bis 1 segundo párrafo del Código Penal Federal se establece lo siguiente:

“Al que sin autorización conozca o copie 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 de cincuenta a ciento cincuenta días multa.”

Como podemos ver del texto anterior, se derivan una serie considerable de hipótesis, las cuales procederemos a ilustrar:

	HIPÓTESIS
Acción	<ul style="list-style-type: none"> <li>• Conozca información</li> <li>• Copie información</li> </ul>
Consentimiento	<ul style="list-style-type: none"> <li>• Sin autorización</li> </ul>
Seguridad	<ul style="list-style-type: none"> <li>• Los sistemas de informática estén protegidos por algún mecanismo de seguridad</li> <li>• Los equipos de informática estén protegidos por algún mecanismo de seguridad</li> </ul>
Información	<ul style="list-style-type: none"> <li>• La información esté contenida en sistemas de informática</li> <li>• La información esté contenida en equipos de informática</li> </ul>

Para comenzar con el análisis se debe precisar que cuando se habla del verbo “*conocer*” cómo conducta es por la calidad de los mecanismos de seguridad, la cual es de seguridad, por lo que al conocer de la información

contenida en equipos informáticos y protegidos por mecanismos, se estará hablando del engaño que se tuvo que dar para tener acceso a ella.

Como se puede observar, se habla de una falta de consentimiento, donde la conducta de esta fracción denota que es acción, ya que se habla de la falta de cuyos verbos núcleos son “conocer” o “copiar” la información, en estos casos no se puede pensar en que por una fuerza física superior e irresistible proveniente de la naturaleza o de otro ser humano o por medio de movimientos reflejos se conozca o copie la información.

En lo que respecta a la tipicidad se debe dar el exacto encuadramiento de la conducta al tipo, el cual contiene como tipo fundamental la conducta de conocer o copiar información, no obstante encontramos que es un tipo especial ya que tiene como cualidad que para el encuadramiento de la conducta tendrá que darse esta última sin autorización, la información debe estar contenida en equipos de informática y estos a su vez tendrán que estar protegidos por algún mecanismo de seguridad.

La atipicidad se puede dar bastará con que falte alguno de los elementos mencionados. En el caso de que no se lleve a cabo las acciones de conocer o copiar, se podrá decir que el hecho ilícito no corresponde al tipo, de igual forma en el caso de que se realice la acción pero con autorización; si la información no está contenida en sistemas informáticos; así también en el caso de que esta información no esté protegida por un mecanismo de seguridad.

El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo, pudiendo ser de esta forma cualquier persona.

Hablando de elemento objetivo encontramos la relación en que se habla de quien copie o conozca la información contenida y protegida por mecanismos informáticos, de tal suerte que esta acción sea sin previa autorización.

Se establece como elemento subjetivo del ilícito el que la conducta sea realizada con dolo, al tratarse de la manipulación de mecanismos de seguridad se necesita tener el conocimiento necesario y por lo tanto resulta imposible que el sujeto activo no tenga la intención del acto ilícito.

En el elemento normativo encontramos que al existir la necesidad de una valoración jurídico cultural, se habla como elemento normativo el que atente contra una herramienta que se utiliza para fortalecer la confidencialidad , la integridad y la disponibilidad de un grupo de aparatos que realizan mediante un programa el tratamiento automático de datos.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación. Recordemos que el bien tutelado mediante la sanción de estos delitos informáticos es la pureza de la técnica que presupone la informática, el resguardo de los medios involucrados en la computación electrónica y la información o datos contenida en ellos.

Como sabemos, para ser imputable se requiere la capacidad de querer y entender, la conducta de la hipótesis no puede ser realizada por alguna persona inimputable, ya que este delito es sumamente sofisticado, hasta tal punto que por ser de carácter tan técnico presentan grandes dificultades para su comprobación. No obstante a lo antes explicado, en el artículo no se habla de una cualidad específica del sujeto activo y por lo tanto cualquier persona puede ser objeto de esta conducta.

Esta hipótesis se puede dar únicamente de forma dolosa, lo cual ayuda a evidenciar la intención del sujeto activo en la realización de la conducta. No se habla de culpa y por lo tanto no aplica la inculpabilidad.

Este delito se persigue por oficio, teniendo una sanción de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa; mientras que como excusas absolutorias tenemos que no serán consideradas.

Para una mejor comprensión del estudio dogmático de esta fracción, a continuación se esquematiza lo anteriormente explicado.

<b>CONDUCTA</b>	{ La conducta es conocer o copiar la información.
<b>AUSENCIA DE CONDUCTA</b>	{ No se puede dar ninguna de las formas de ausencia de conducta.

	<p>La conducta está descrita en el segundo párrafo del artículo 211 bis 1 del Código Penal Federal.</p> <p>El tipo consta de elementos subjetivos, objetivos y normativos.</p>	
<b>TIPICIDAD</b>	<b>SUJETO ACTIVO</b>	<p>El tipo no establece alguna calidad específica por lo que puede ser cualquier persona.</p>
	<b>SUJETO PASIVO</b>	<p>No se</p>
	<b>BIEN JURÍDICO TUTELADO</b>	<p>La pureza de la técnica que presupone la informática, el resguardo de los medios involucrados en la computación electrónica y la información o datos contenida en ellos.</p>
	<b>OBJETO JURÍDICO</b>	<p>La confidencialidad, integridad y disponibilidad</p>
	<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	<p>Que con dolo o culpa accediera o copiara la información.</p>
	<b>ELEMENTO NORMATIVO</b>	<p>Que atente contra la seguridad de un mecanismo informático</p>
<b>ATIPICIDAD</b>	<p>Se puede presentar si llega a faltar algún elemento del tipo penal, por lo que podría existir la ausencia de los elementos objetivos, subjetivos y normativos del ilícito.</p>	
<b>ANTI JURIDICIDAD</b>	<p>Cuenta con la formal, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 1 segundo párrafo del Código Penal Federal) y es contraria a la sociedad.</p>	
<b>CAUSAS DE JUSTIFICACIÓN</b>	<p>No se puede aplicar ninguna.</p>	
<b>IMPUTABILIDAD</b>	<p>La capacidad de querer y entender.</p>	
<b>INIMPUTABILIDAD</b>	<p>No aplica</p>	



<b>CULPABILIDAD</b>	{	Se puede dar únicamente de manera dolosa.
<b>INCULPABILIDAD</b>	{	No aplica
<b>CONDICIONES OBJETIVAS DE PUNIBILIDAD</b>	{	Se persigue por oficio.
<b>PUNIBILIDAD</b>	{	De tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.
<b>EXCUSAS ABSOLUTORIAS</b>	{	No serán consideradas.

### 4.3 Modificar, destruir o provocar pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, sin autorización.

El artículo 211 bis 2 del Código Penal Federal establece en su primer párrafo lo siguiente:

“Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.”

Del texto anterior podemos encontrar una serie de hipótesis que derivan en la conducta delictiva, éstas podrían ser:

ACCIÓN ESPECÍFICA DEL SUJETO ACTIVO	HIPÓTESIS
MODIFIQUE	<ul style="list-style-type: none"> <li>· Información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad.</li> <li>· Información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad.</li> </ul>
DESTRUYA	<ul style="list-style-type: none"> <li>· Información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad.</li> <li>· Información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad.</li> </ul>
PROVOQUE PÉRDIDA	<ul style="list-style-type: none"> <li>· Información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad.</li> <li>· Información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad.</li> </ul>

ACCIÓN ESPECÍFICA DEL SUJETO ACTIVO	HIPÓTESIS
TOTAL DE HIPÓTESIS PREVISTAS EN EL PRIMER PÁRRAFO DEL ARTÍCULO 211 BIS 2 DEL CÓDIGO PENAL FEDERAL	6

Tal y como lo vemos esquematizado en el cuadro anterior, este artículo plantea una serie de supuestos que pueden derivar en este tipo penal, éstos se explicarán en un sentido dogmático de forma general, para ello definiremos con antelación diversos conceptos que son clave para poder entender perfectamente este párrafo.

Ya que la legislación no define expresamente lo que se debe entender por “modificar”, “destruir”, “provocar” y “pérdida”, que son los verbos núcleos del párrafo en estudio, debemos recurrir a la definición que de estas palabras nos hace el Diccionario de la Real Academia de la Lengua Española (DRAE), así como el Diccionario Jurídico Mexicano (DJM) del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, a continuación podemos encontrar las definiciones que ambos textos nos brindan:

- **Modificar:**

**DRAE:** Transformar o cambiar algo mudando alguna de sus características.

**DJM:** Es la acción de cambiar algo en relación a un estado inicial.

- **Destruir:**

**DRAE:** 1. Reducir a pedazos o a cenizas algo material, u ocasionarle un grave daño.

2. Deshacer o inutilizar algo no material.

**DJM:** Es el acto que se lleva a cabo con el fin de extinguir algo, sea con intención o por mero accidente.

- **Provocar**

**DRAE:** Producir o causar algo.

**DJM:** Excitar, producir o fomentar que una cosa exista.

- **Perder**

**DRAE:** Dejar de tener, o no hallar, aquello que poseía, sea por culpa o descuido del poseedor, sea por contingencia o desgracia.

**DJM:** Es el extravío de aquello que se poseía anteriormente.

Una vez explicados los verbos núcleo, debemos hacer la diferenciación entre lo que es un “sistema de informática” y un “equipo de informática”. Son términos que van de la mano, pero que a la vez son distintos.

Un sistema de informática puede ser definido como un conjunto constituido tanto por elementos físicos como lógicos (es decir los *software*) necesarios para captar, almacenar y procesar información. Por otro lado, un equipo de informático es un dispositivo electrónico que permite la ejecución de programas informáticos, es decir, hablamos únicamente de las computadoras.

***1.- Modifique información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad.***

La conducta que se denota en esta hipótesis es un acto positivo, cuyo verbo núcleo es “modificar”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, es decir, una fuerza física superior e irresistible proveniente de otro ser humano.

En lo que respecta a la tipicidad, se deben de presentar todos los elementos que el tipo describe para que la conducta se pueda encuadrar, en especial el “modificar” información contenida en sistemas de informática del Estado que se encuentran protegidos por algún mecanismo de seguridad. El tipo en cuestión cuenta con elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona la que lleve a cabo la conducta delictiva, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema; en lo que respecta al sujeto pasivo, debe ser forzosamente el Estado, ya que a quien se afecta en la invasión de un sistema de

informática es al mismo pues es de su pertenencia dicho sistema y la información que allí se encuentra es del Estado.

El elemento objetivo de la hipótesis es todo aquel atentado que prevea dañar o desviar el uso debido de un sistema de informática que le pertenezca al Estado con la finalidad de obtener un beneficio particular, ya sea material o inmaterial, ya sea moral, para sí o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un sistema de informática del Estado protegido por algún mecanismo de seguridad.

El elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa con que actúa el sujeto activo que modifique información contenida en sistemas de informática pertenecientes al Estado protegidos por algún mecanismo de seguridad.

También es necesaria una valoración jurídica cultural, pues se tiene que corroborar si el elemento de si el sujeto activo obró con autorización o sin ella.

La atipicidad en este supuesto encajaría en tres hipótesis, la primera es que el sujeto activo cuente con autorización para realizar la modificación de información contenida en sistemas de informática pertenecientes al Estado protegidos por algún mecanismo de seguridad; la segunda, sería que el que sin autorización, modifique información contenida en sistemas de informática que estén protegidos por algún mecanismo de seguridad, pero que no sean propiedad del Estado, ya que en este supuesto estaríamos hablando de otro tipo, pero no del descrito en el artículo 211 bis 2 párrafo primero; y la última sería que el que sin autorización se modifique información contenida en sistemas de informática del Estado, pero que no esté protegida por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

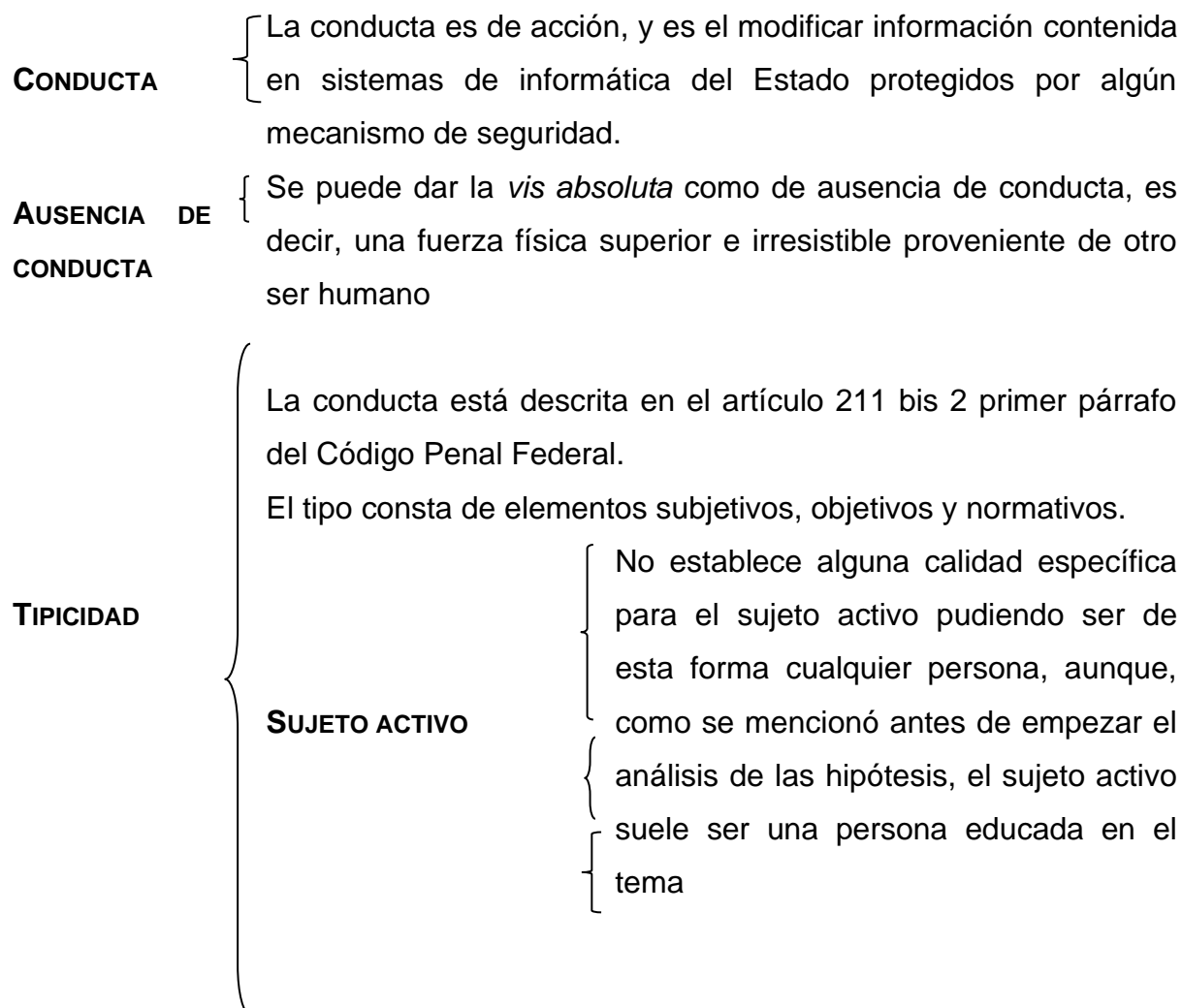
Para la acción descrita en esta hipótesis, como se ha mencionado con anterioridad, el sujeto activo de este tipo de delitos se ha observado que por lo

regular son personas de un determinado nivel de inteligencia y educación superior al común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis analizada se da de forma dolosa o culposa, mismo que nos ayuda a evidenciar la realización de la conducta. La inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podía presentar una amenaza de un daño grave si no se realiza la conducta descrita en el tipo penal.

Este delito se persigue de oficio, teniendo una sanción de uno a cuatro años de prisión y de doscientos a seiscientos días multa; no existiendo ninguna excusa absolutoria.

A continuación se presenta un esquema donde se presenta lo anteriormente explicado respecto al estudio dogmático de esta hipótesis:



	<b>SUJETO PASIVO</b>	El sujeto pasivo, debe ser forzosamente el Estado ya que se está modificando información de sistemas pertenecientes al mismo.
	<b>BIEN JURÍDICO TUTELADO</b>	{ La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
	<b>OBJETO JURÍDICO</b>	{ Sistemas de informática.
	<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	{ constituido por el dolo o la culpa con que actúa el sujeto activo que modifique información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad
	<b>ELEMENTO NORMATIVO</b>	{ Que atente contra los sistemas de informática.
<b>ATIPICIDAD</b>	{	Encajaría en 3 hipótesis, la primera es que el sujeto activo cuente con autorización para realizar la modificación de información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad; la segunda, sería que sin autorización se modifique información contenida en sistemas de informática protegidos por algún mecanismo de seguridad, pero que no sean pertenecientes al Estado, ya que entonces no sería el tipo descrito en el artículo 211 bis 2 primer párrafo, y la última, sería que el que, sin autorización, modifique información contenida en sistemas de informática del Estado que no esté protegida por algún mecanismo de seguridad.
<b>ANTI JURIDICIDAD</b>	{	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 1 primer párrafo del Código Penal Federal) y es contraria a la sociedad.
<b>CAUSAS DE</b>	{	No se puede aplicar ninguna.

**JUSTIFICACIÓN**

**IMPUTABILIDAD** { La capacidad de querer y entender.

**INIMPUTABILIDAD** { Se puede presentar que una persona no imputable realice la conducta, pero sería difícil que pasara.

**CULPABILIDAD** { Se puede dar de manera dolosa o culposa.

**INCULPABILIDAD** { Se puede presentar por dos razones, siendo la primera la vis compulsiva, y la segunda, por obediencia jerárquica

**CONDICIONES OBJETIVAS DE** { Se persigue de oficio.

**PUNIBILIDAD**

**PUNIBILIDAD** { De uno a cuatro años de prisión y de doscientos a seiscientos días multa.

**EXCUSAS ABSOLUTORIAS** { No tiene excusa absolutoria alguna.

***2.- Modifique información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad.***

La conducta que se denota en esta hipótesis es de un acto positivo, cuyo verbo núcleo es “modificar”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, es decir, una fuerza física superior e irresistible proveniente de otro hombre.

Referente a la tipicidad, se debe dar el exacto encuadramiento de la conducta respecto al tipo penal, que es el “modificar información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad.” El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema; en lo que respecta al sujeto pasivo, debe ser forzosamente el Estado, ya que a quien se afecta en la invasión de un equipo de informática es al mismo pues es de su pertenencia dicho equipo y la información que allí se encuentra es del Estado.



El elemento objetivo de la hipótesis es todo aquel atentado que prevea dañar o desviar el uso correcto de un equipo de informática con la finalidad de obtener un beneficio, ya sea material o inmaterial, ya sea moral, para sí o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un equipo de informática del Estado protegido por algún mecanismo de seguridad.

El elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa con que actúa el sujeto activo que modifique información contenida en equipos de informática protegidos por algún mecanismo de seguridad.

También, existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba con autorización o no. La atipicidad en este supuesto encajaría en tres hipótesis, la primero es que el sujeto activo cuente con autorización para realizar la modificación de información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad; la segunda, sería que el que sin autorización, modifique información contenida en equipos de informática que estén protegidos por algún mecanismo de seguridad, pero que no sean propiedad del Estado, ya que en este supuesto estaríamos hablando de otro tipo, pero no del descrito en el artículo 211 bis 2 párrafo primero; y la última sería que el que sin autorización se modifique información contenida en equipos de informática del Estado, pero que no esté protegida por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

Para la acción realizada en esta hipótesis, como se ha mencionado con anterioridad, el sujeto activo de los delitos informáticos se ha observado que por lo general son personas de un determinado nivel de inteligencia y educación, superior al común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis analizada se da de forma dolosa o culposa, mismo que nos ayuda a evidenciar la realización de la conducta. La inculpabilidad se puede

considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podía presentar una amenaza de un daño grave si no se realiza la conducta en el tipo de mérito.

Este delito se persigue de oficio, teniendo una sanción de uno a cuatro años de prisión y de doscientos a seiscientos días multa; no existiendo ninguna excusa absolutoria.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación se esquematiza lo anteriormente explicado:

<b>CONDUCTA</b>	{	La conducta es de acción, y es el modificar información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad.						
<b>AUSENCIA DE CONDUCTA</b>	{	Se puede dar la <i>vis absoluta</i> como de ausencia de conducta, es decir, una fuerza física superior e irresistible proveniente de otro ser humano						
<b>TIPICIDAD</b>	{	<p>La conducta está descrita en el artículo 211 bis 2 primer párrafo del Código Penal Federal.</p> <p>El tipo consta de elementos subjetivos, objetivos y normativos.</p> <table border="0" style="margin-left: 20px;"> <tr> <td style="vertical-align: top;"><b>SUJETO ACTIVO</b></td> <td style="vertical-align: top;">{</td> <td>No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema</td> </tr> <tr> <td style="vertical-align: top;"><b>SUJETO PASIVO</b></td> <td style="vertical-align: top;">{</td> <td>El sujeto pasivo, debe ser forzosamente el Estado ya que se está modificando información de equipos pertenecientes al mismo.</td> </tr> </table>	<b>SUJETO ACTIVO</b>	{	No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema	<b>SUJETO PASIVO</b>	{	El sujeto pasivo, debe ser forzosamente el Estado ya que se está modificando información de equipos pertenecientes al mismo.
<b>SUJETO ACTIVO</b>	{	No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema						
<b>SUJETO PASIVO</b>	{	El sujeto pasivo, debe ser forzosamente el Estado ya que se está modificando información de equipos pertenecientes al mismo.						

<b>BIEN TUTELADO</b>	<b>JURÍDICO</b>	{ La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
	<b>OBJETO JURÍDICO</b>	{- Equipos de informática. constituido por el dolo o la culpa con que actúa el sujeto activo que modifique
	<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	{ información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad
	<b>ELEMENTO NORMATIVO</b>	{- Que atente contra los equipos de informática.
<b>ATIPICIDAD</b>		{ Encajaría en 3 hipótesis, la primera es que el sujeto activo cuente con autorización para realizar la modificación de información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad; la segunda, sería que sin autorización se modifique información contenida en equipos de informática protegidos por algún mecanismo de seguridad, pero que no sean pertenecientes al Estado, ya que entonces no sería el tipo descrito en el artículo 211 bis 2 primer párrafo, y la última, sería que el que, sin autorización, modifique información contenida en equipos de informática del Estado que no esté protegida por algún mecanismo de seguridad.
<b>ANTI JURIDICIDAD</b>		{ Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 1 primer párrafo del Código Penal Federal) y es contraria a la sociedad.
<b>CAUSAS DE JUSTIFICACIÓN</b>		{- No se puede aplicar ninguna.
<b>IMPUTABILIDAD</b>		{- La capacidad de querer y entender.
<b>INIMPUTABILIDAD</b>		{- Se puede presentar que una persona no imputable realice la conducta, pero sería difícil que pasara.

<b>CULPABILIDAD</b>	{	Se puede dar de manera dolosa o culposa.
<b>INCULPABILIDAD</b>	{	Se puede presentar por dos razones, siendo la primera la vis compulsiva, y la segunda, por obediencia jerárquica
<b>CONDICIONES OBJETIVAS DE</b>	{	Se persigue de oficio.
<b>PUNIBILIDAD</b>		
<b>PUNIBILIDAD</b>	{	De uno a cuatro años de prisión y de doscientos a seiscientos días multa.
<b>EXCUSAS ABSOLUTORIAS</b>	{	No tiene excusa absolutoria alguna.

### ***3.- Destruir información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad.***

La conducta que se denota en esta hipótesis es de un acto positivo, cuyo verbo núcleo es “destruir”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, es decir, una fuerza física superior e irresistible proveniente de otro hombre.

Referente a la tipicidad, se debe dar el exacto encuadramiento de la conducta respecto al tipo penal, que es el “destruir” información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad. El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema; en lo que respecta al sujeto pasivo, debe ser forzosamente el Estado, ya que a quien se afecta en la invasión de un sistema de informática es al mismo pues es de su pertenencia dicho sistema y la información que allí se encuentra es del Estado.

El elemento objetivo de la hipótesis es todo aquel atentado que prevea dañar o desviar el uso correcto de un sistema de informática del Estado con la finalidad de obtener un beneficio, ya sea material o inmaterial, ya sea moral, para sí o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un sistema de informática del Estado protegido por algún mecanismo de seguridad.

El elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa con que actúa el sujeto activo que destruya información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad.

También es necesaria una valoración jurídica cultural, pues se tiene que corroborar si el elemento de si el sujeto activo obró con autorización o sin ella.

La atipicidad en este supuesto encajaría en tres hipótesis, la primera es que el sujeto activo cuente con autorización para destruir información contenida en sistemas de informática pertenecientes al Estado protegidos por algún mecanismo de seguridad; la segunda, sería que el que sin autorización, destruya información contenida en sistemas de informática que estén protegidos por algún mecanismo de seguridad, pero que no sean propiedad del Estado, ya que en este supuesto estaríamos hablando de otro tipo, pero no del descrito en el artículo 211 bis 2 párrafo primero; y la última sería que el que sin autorización se destruya información contenida en sistemas de informática del Estado, pero que no esté protegida por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

Para la acción realizada en esta hipótesis, como se ha mencionado con anterioridad, el sujeto activo de los delitos informáticos se ha observado que por lo general son personas de un determinado nivel de inteligencia y educación, superior al común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis analizada se da de forma dolosa o culposa, mismo que nos ayuda a evidenciar la realización de la conducta. La inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podía presentar una amenaza de un daño grave si no se realiza la conducta en el tipo de mérito.

Este delito se persigue de oficio, teniendo una sanción de uno a cuatro años de prisión y de doscientos a seiscientos días multa; no existiendo ninguna excusa absolutoria.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación se esquematiza lo anteriormente explicado.

**CONDUCTA** { La conducta es de acción, y es el destruir información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad.

**AUSENCIA DE CONDUCTA** { Se puede dar la *vis absoluta* como de ausencia de conducta, es decir, una fuerza física superior e irresistible proveniente de otro ser humano

La conducta está descrita en el artículo 211 bis 2 primer párrafo del Código Penal Federal.

El tipo consta de elementos subjetivos, objetivos y normativos.

**TIPICIDAD**

**SUJETO ACTIVO** { No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema

			<p><b>SUJETO PASIVO</b> { El sujeto pasivo, debe ser forzosamente el Estado ya que se está destruyendo información de sistemas pertenecientes al mismo.</p>
	<b>BIEN</b>	<b>JURÍDICO</b>	<p>{ La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.</p>
	<b>TUTELADO</b>		
	<b>OBJETO JURÍDICO</b>		<p>{ Sistemas de informática.</p>
	<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>		<p>{ constituido por el dolo o la culpa con que actúa el sujeto activo que destruya información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad</p>
	<b>ELEMENTO NORMATIVO</b>		<p>{ Que atente contra los sistemas de informática.</p>
<b>ANTIPICIDAD</b>			<p>{ Encajaría en 3 hipótesis, la primera es que el sujeto activo cuente con autorización para destruir información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad; la segunda, sería que sin autorización se destruya información contenida en sistemas de informática protegidos por algún mecanismo de seguridad, pero que no sean pertenecientes al Estado, ya que entonces no sería el tipo descrito en el artículo 211 bis 2 primer párrafo, y la última, sería que el que, sin autorización, se destruya información contenida en sistemas de informática del Estado que no esté protegida por algún mecanismo de seguridad.</p>
<b>ANTI JURIDICIDAD</b>			<p>{ Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 1 primer párrafo del Código Penal Federal) y es contraria a la sociedad.</p>
<b>CAUSAS</b>	<b>DE</b>		<p>{ No se puede aplicar ninguna.</p>

**JUSTIFICACIÓN**

**IMPUTABILIDAD** { La capacidad de querer y entender.

**INIMPUTABILIDAD** { Se puede presentar que una persona no imputable realice la conducta, pero sería difícil que pasara.

**CULPABILIDAD** { Se puede dar de manera dolosa o culposa.

**INCULPABILIDAD** { Se puede presentar por dos razones, siendo la primera la vis compulsiva, y la segunda, por obediencia jerárquica

**CONDICIONES OBJETIVAS DE** { Se persigue de oficio.

**PUNIBILIDAD**

**PUNIBILIDAD** { De uno a cuatro años de prisión y de doscientos a seiscientos días multa.

**EXCUSAS ABSOLUTORIAS** { No tiene excusa absolutoria alguna.

***4.- Destruir información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad.***

La conducta que se denota en esta hipótesis es de un acto positivo, cuyo verbo núcleo es “destruir”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, es decir, una fuerza física superior e irresistible proveniente de otro hombre.

Referente a la tipicidad, se debe dar el exacto encuadramiento de la conducta respecto al tipo penal, que es el “destruir información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad.” El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema; en lo que respecta al sujeto pasivo, debe ser forzosamente el Estado, ya que a quien se afecta en la invasión de un equipo de informática es al mismo pues es de su pertenencia dicho equipo y la información que allí se encuentra es del Estado.



El elemento objetivo de la hipótesis es todo aquel atentado que prevea dañar o desviar el uso correcto de un equipo de informática con la finalidad de obtener un beneficio, ya sea material o inmaterial, ya sea moral, para sí o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un equipo de informática del Estado protegido por algún mecanismo de seguridad.

El elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa con que actúa el sujeto activo que modifique información contenida en equipos de informática protegidos por algún mecanismo de seguridad.

También, existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba con autorización o no. La atipicidad en este supuesto encajaría en tres hipótesis, la primero es que el sujeto activo cuente con autorización para destruir la información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad; la segunda, sería que el que sin autorización, destruya información contenida en equipos de informática que estén protegidos por algún mecanismo de seguridad, pero que no sean propiedad del Estado, ya que en este supuesto estaríamos hablando de otro tipo, pero no del descrito en el artículo 211 bis 2 párrafo primero; y la última sería que el que sin autorización destruya información contenida en equipos de informática del Estado, pero que no esté protegida por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

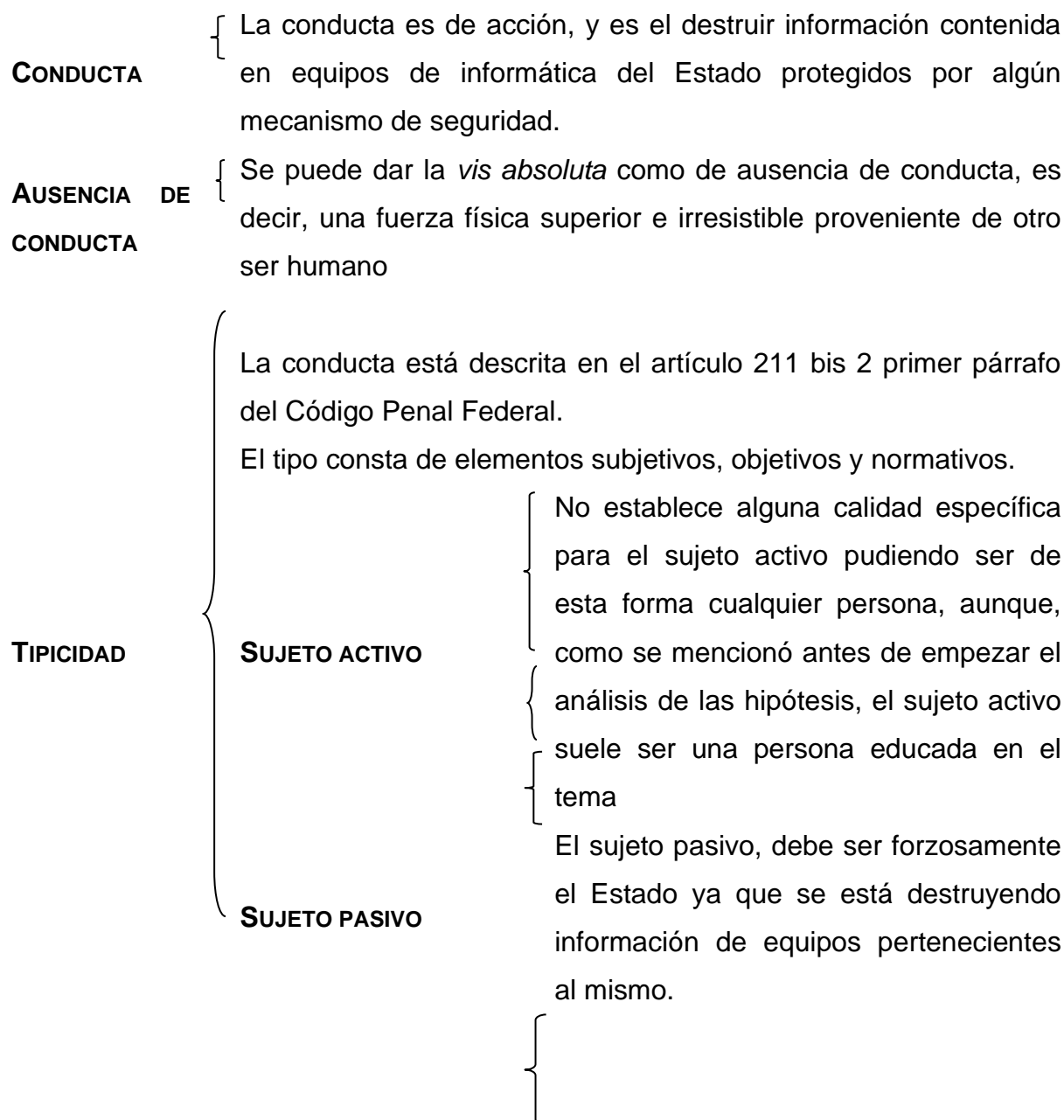
Para la acción realizada en esta hipótesis, como se ha mencionado con anterioridad, el sujeto activo de los delitos informáticos se ha observado que por lo general son personas de un determinado nivel de inteligencia y educación, superior al común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis analizada se da de forma dolosa o culposa, mismo que nos ayuda a evidenciar la realización de la conducta. La inculpabilidad se puede

considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podía presentar una amenaza de un daño grave si no se realiza la conducta en el tipo de mérito.

Este delito se persigue de oficio, teniendo una sanción de uno a cuatro años de prisión y de doscientos a seiscientos días multa; no existiendo ninguna excusa absolutoria.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación se esquematiza lo anteriormente explicado:



<b>BIEN TUTELADO</b>	<b>JURÍDICO</b>	{ La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
<b>OBJETO JURÍDICO</b>	{	Equipos de informática.
<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	{	constituido por el dolo o la culpa con que actúa el sujeto activo que destruya información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad
<b>ELEMENTO NORMATIVO</b>	{	Que atente contra los equipos de informática.
<b>ATIPICIDAD</b>	{	Encajaría en 3 hipótesis, la primera es que el sujeto activo cuente con autorización para destruir la información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad; la segunda, sería que sin autorización se destruya información contenida en equipos de informática protegidos por algún mecanismo de seguridad, pero que no sean pertenecientes al Estado, ya que entonces no sería el tipo descrito en el artículo 211 bis 2 primer párrafo, y la última, sería que el que, sin autorización, destruya información contenida en equipos de informática del Estado que no esté protegida por algún mecanismo de seguridad.
<b>ANTI JURIDICIDAD</b>	{	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 1 primer párrafo del Código Penal Federal) y es contraria a la sociedad.
<b>CAUSAS DE JUSTIFICACIÓN</b>	{	No se puede aplicar ninguna.
<b>IMPUTABILIDAD</b>	{	La capacidad de querer y entender.
<b>INIMPUTABILIDAD</b>	{	Se puede presentar que una persona no imputable realice la conducta, pero sería difícil que pasara.

<b>CULPABILIDAD</b>	{	Se puede dar de manera dolosa o culposa.
<b>INCULPABILIDAD</b>	{	Se puede presentar por dos razones, siendo la primera la vis compulsiva, y la segunda, por obediencia jerárquica
<b>CONDICIONES OBJETIVAS DE</b>	{	Se persigue de oficio.
<b>PUNIBILIDAD</b>		
<b>PUNIBILIDAD</b>	{	De uno a cuatro años de prisión y de doscientos a seiscientos días multa.
<b>EXCUSAS ABSOLUTORIAS</b>	{	No tiene excusa absolutoria alguna.

***5.- Provoque pérdida de información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad.***

La conducta que se denota en esta hipótesis es un acto positivo, cuyo verbo núcleo es “provocar la pérdida”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, es decir, una fuerza física superior e irresistible proveniente de otro ser humano.

En lo que respecta a la tipicidad, se deben de presentar todos los elementos que el tipo describe para que la conducta se pueda encuadrar, en especial el “provocar la pérdida” de información contenida en sistemas de informática del Estado que se encuentran protegidos por algún mecanismo de seguridad. El tipo en cuestión cuenta con elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona la que lleve a cabo la conducta delictiva, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema; en lo que respecta al sujeto pasivo, debe ser forzosamente el Estado, ya que a quien se afecta en la invasión de un sistema de informática es al mismo pues es de su pertenencia dicho sistema y la información que allí se encuentra es del Estado.

El elemento objetivo de la hipótesis es todo aquel atentado que prevea dañar o desviar el uso debido de un sistema de informática que le pertenezca al

Estado con la finalidad de obtener un beneficio particular, ya sea material o inmaterial, ya sea moral, para sí o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un sistema de informática del Estado protegido por algún mecanismo de seguridad.

El elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa con que actúa el sujeto activo que modifique información contenida en sistemas de informática pertenecientes al Estado protegidos por algún mecanismo de seguridad.

También es necesaria una valoración jurídica cultural, pues se tiene que corroborar si el elemento de si el sujeto activo obró con autorización o sin ella.

La atipicidad en este supuesto encajaría en tres hipótesis, la primera es que el sujeto activo cuente con autorización para provocar la pérdida de información contenida en sistemas de informática pertenecientes al Estado protegidos por algún mecanismo de seguridad; la segunda, sería que el que sin autorización, se provoque la pérdida de información contenida en sistemas de informática que estén protegidos por algún mecanismo de seguridad, pero que no sean propiedad del Estado, ya que en este supuesto estaríamos hablando de otro tipo, pero no del descrito en el artículo 211 bis 2 párrafo primero; y la última sería que el que sin autorización provoque la pérdida de información contenida en sistemas de informática del Estado, pero que no esté protegida por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

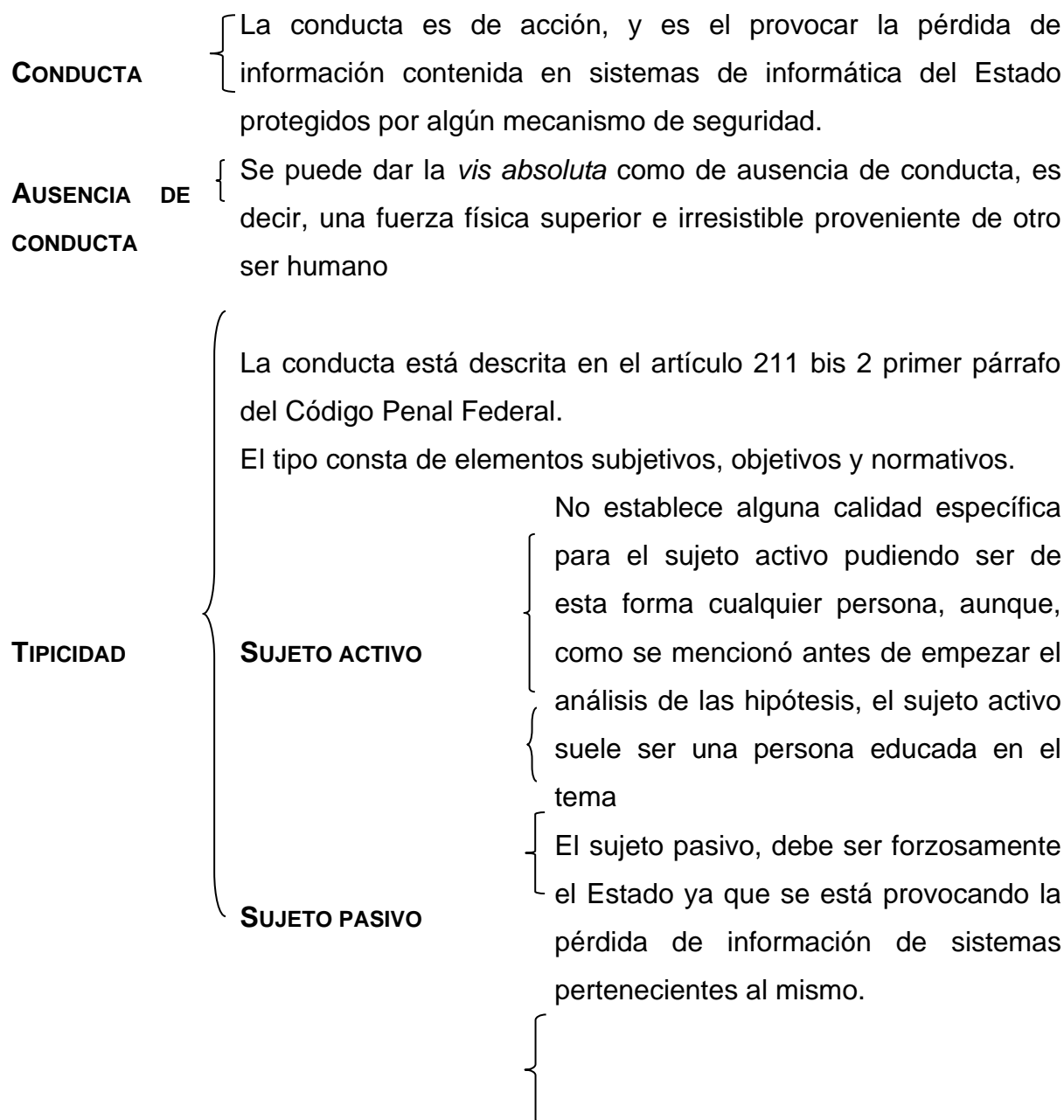
Para la acción descrita en esta hipótesis, como se ha mencionado con anterioridad, el sujeto activo de este tipo de delitos se ha observado que por lo regular son personas de un determinado nivel de inteligencia y educación, superior al común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis analizada se da de forma dolosa o culposa, mismo que nos ayuda a evidenciar la realización de la conducta. La inculpabilidad se puede

considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podía presentar una amenaza de un daño grave si no se realiza la conducta descrita en el tipo penal.

Este delito se persigue de oficio, teniendo una sanción de uno a cuatro años de prisión y de doscientos a seiscientos días multa; no existiendo ninguna excusa absolutoria.

A continuación se presenta un esquema donde se presenta lo anteriormente explicado respecto al estudio dogmático de esta hipótesis:



<b>BIEN TUTELADO</b>	<b>JURÍDICO</b>	{ La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
	<b>OBJETO JURÍDICO</b>	{ Sistemas de informática. constituido por el dolo o la culpa con que actúa el sujeto activo que provoque
	<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	{ la pérdida de información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad
	<b>ELEMENTO NORMATIVO</b>	{ Que atente contra los sistemas de informática.
<b>ATIPICIDAD</b>		{ Encajaría en 3 hipótesis, la primera es que el sujeto activo cuente con autorización para provocar la pérdida de información contenida en sistemas de informática del Estado protegidos por algún mecanismo de seguridad; la segunda, sería que sin autorización se provoque la pérdida de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad, pero que no sean pertenecientes al Estado, ya que entonces no sería el tipo descrito en el artículo 211 bis 2 primer párrafo, y la última, sería que el que, sin autorización, provoque la pérdida de información contenida en sistemas de informática del Estado que no esté protegida por algún mecanismo de seguridad.
<b>ANTI JURIDICIDAD</b>		{ Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 1 primer párrafo del Código Penal Federal) y es contraria a la sociedad.
<b>CAUSAS DE JUSTIFICACIÓN</b>		{ No se puede aplicar ninguna.
<b>IMPUTABILIDAD</b>		{ La capacidad de querer y entender.
<b>INIMPUTABILIDAD</b>		{ Se puede presentar que una persona no imputable realice la

AD	conducta, pero sería difícil que pasara.
CULPABILIDAD	{ Se puede dar de manera dolosa o culposa.
INCULPABILIDAD	{ Se puede presentar por dos razones, siendo la primera la vis
D	compulsiva, y la segunda, por obediencia jerárquica
CONDICIONES	{
OBJETIVAS DE	
PUNIBILIDAD	
PUNIBILIDAD	{ De uno a cuatro años de prisión y de doscientos a seiscientos días multa.
EXCUSAS	{
ABSOLUTORIAS	

**6.- Provoque pérdida de información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad.**

La conducta que se denota en esta hipótesis es de un acto positivo, cuyo verbo núcleo es “provocar la pérdida”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, es decir, una fuerza física superior e irresistible proveniente de otro hombre.

Referente a la tipicidad, se debe dar el exacto encuadramiento de la conducta respecto al tipo penal, que es el “provocar la pérdida de información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad.” El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, aunque, como se mencionó antes de empezar el análisis de las hipótesis, el sujeto activo suele ser una persona educada en el tema; en lo que respecta al sujeto pasivo, debe ser forzosamente el Estado, ya que a quien se afecta en la invasión de un equipo de informática es al mismo pues es de su pertenencia dicho equipo y la información que allí se encuentra es del Estado.

El elemento objetivo de la hipótesis es todo aquel atentado que prevea dañar o desviar el uso correcto de un equipo de informática con la finalidad de



obtener un beneficio, ya sea material o inmaterial, ya sea moral, para sí o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un equipo de informática del Estado protegido por algún mecanismo de seguridad.

El elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa con que actúa el sujeto activo que modifique información contenida en equipos de informática protegidos por algún mecanismo de seguridad.

También, existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba con autorización o no. La atipicidad en este supuesto encajaría en tres hipótesis, la primero es que el sujeto activo cuente con autorización para provocar la pérdida de la información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad; la segunda, sería que el que sin autorización, provoque la pérdida de información contenida en equipos de informática que estén protegidos por algún mecanismo de seguridad, pero que no sean propiedad del Estado, ya que en este supuesto estaríamos hablando de otro tipo, pero no del descrito en el artículo 211 bis 2 párrafo primero; y la última sería que el que sin autorización provoque la pérdida de información contenida en equipos de informática del Estado, pero que no esté protegida por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

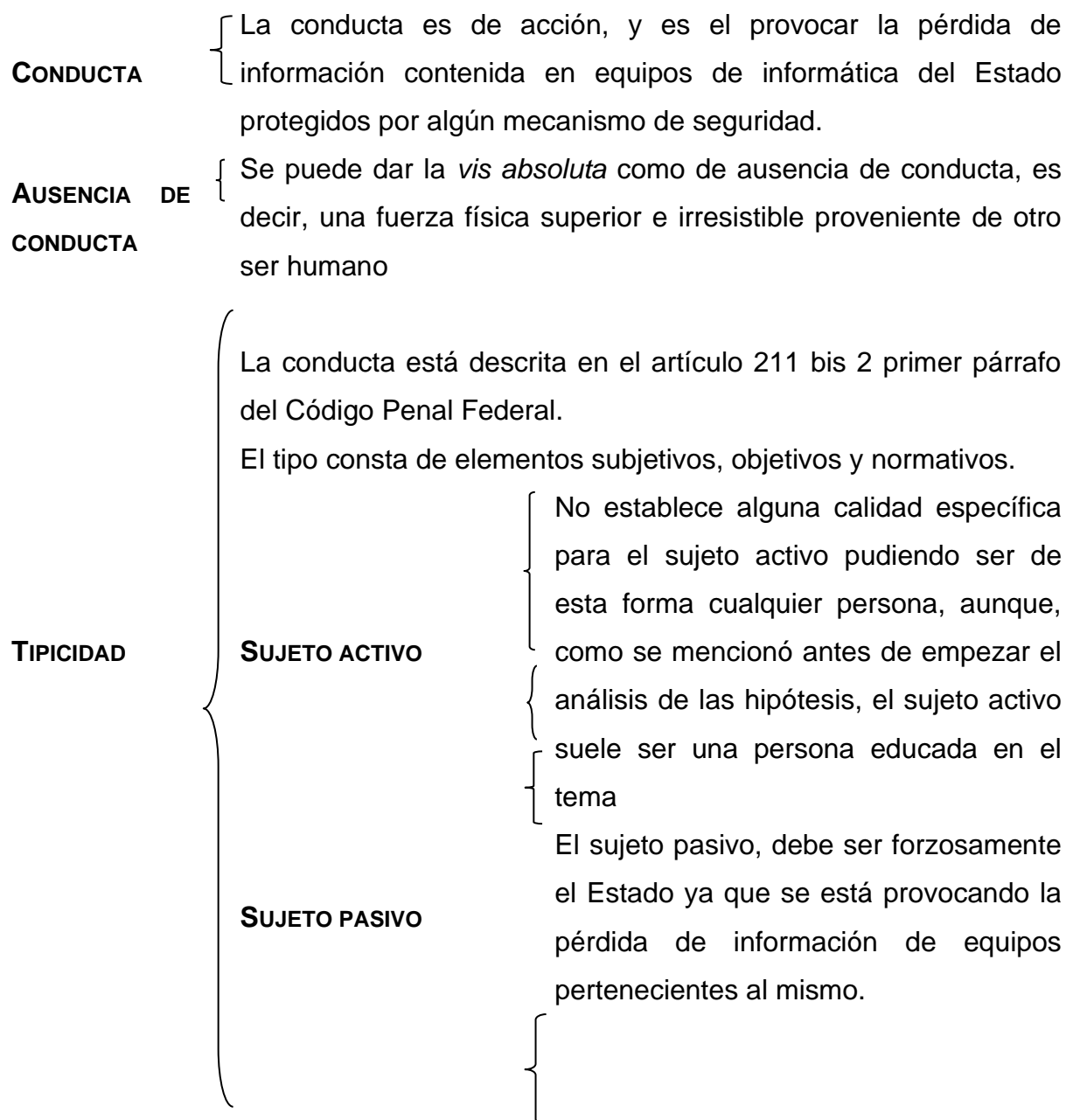
Para la acción realizada en esta hipótesis, como se ha mencionado con anterioridad, el sujeto activo de los delitos informáticos se ha observado que por lo general son personas de un determinado nivel de inteligencia y educación, superior al común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis analizada se da de forma dolosa o culposa, mismo que nos ayuda a evidenciar la realización de la conducta. La inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podía

presentar una amenaza de un daño grave si no se realiza la conducta en el tipo de mérito.

Este delito se persigue de oficio, teniendo una sanción de uno a cuatro años de prisión y de doscientos a seiscientos días multa; no existiendo ninguna excusa absoluta.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación se esquematiza lo anteriormente explicado:



<b>BIEN TUTELADO</b>	<b>JURÍDICO</b>	{ La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
<b>OBJETO JURÍDICO</b>	{	Equipos de informática. constituido por el dolo o la culpa con que actúa el sujeto activo que provoque
<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	{	la pérdida de información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad
<b>ELEMENTO NORMATIVO</b>	{	Que atente contra los equipos de informática.
<b>ATIPICIDAD</b>	{	Encajaría en 3 hipótesis, la primera es que el sujeto activo cuente con autorización para provocar la pérdida de información contenida en equipos de informática del Estado protegidos por algún mecanismo de seguridad; la segunda, sería que sin autorización provoque la pérdida de información contenida en equipos de informática protegidos por algún mecanismo de seguridad, pero que no sean pertenecientes al Estado, ya que entonces no sería el tipo descrito en el artículo 211 bis 2 primer párrafo, y la última, sería que el que, sin autorización, provoque la pérdida de información contenida en equipos de informática del Estado que no esté protegida por algún mecanismo de seguridad.
<b>ANTI JURIDICIDAD</b>	{	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 1 primer párrafo del Código Penal Federal) y es contraria a la sociedad.
<b>CAUSAS DE JUSTIFICACIÓN</b>	{	No se puede aplicar ninguna.
<b>IMPUTABILIDAD</b>	{	La capacidad de querer y entender.
<b>INIMPUTABILIDAD</b>	{	Se puede presentar que una persona no imputable realice la

<b>AD</b>	conducta, pero sería difícil que pasara.
<b>CULPABILIDAD</b>	{ Se puede dar de manera dolosa o culposa.
<b>INCULPABILIDAD</b>	{ Se puede presentar por dos razones, siendo la primera la vis
<b>D</b>	compulsiva, y la segunda, por obediencia jerárquica
<b>CONDICIONES</b>	{ Se persigue de oficio.
<b>OBJETIVAS DE</b>	
<b>PUNIBILIDAD</b>	
<b>PUNIBILIDAD</b>	{ De uno a cuatro años de prisión y de doscientos a seiscientos días multa.
<b>EXCUSAS</b>	{ No tiene excusa absolutoria alguna.
<b>ABSOLUTORIAS</b>	

#### **4.4 Conocer o copiar información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad.**

##### **Artículo 211 bis 2 párrafo segundo**

“Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.”

La conducta en esta hipótesis es de acción cuyos verbos núcleos son “conocer” o “copiar” información contenida en sistemas o equipos de informática del Estado sin autorización y que se encuentren protegidos por algún mecanismo de seguridad.

No se puede presentar la ausencia de conducta porque no se puede pensar en que por una fuerza física superior e irresistible proveniente de la naturaleza o de otro ser humano o por medio de movimientos reflejos se conozca o copie sin autorización información contenida en sistemas o equipos de Informática del Estado.

La tipicidad consiste es el encuadramiento de la conducta al tipo, y en lo que respecta a este artículo el cual contiene la conducta de conocer o copiar información sin autorización de equipos informáticos del Estado. El tipo señalado

consta de elementos objetivos y subjetivos; además no establece alguna calidad específica para el sujeto activo, pudiendo ser de esta forma cualquier persona; en lo que respecta al sujeto pasivo, el tipo nos indica que es el Estado, por lo tanto no hay calidad específica, ya que de él depende la función y control de la información que se maneja a través de los equipos o sistemas informáticos y se ve afectado al difundirse información que se encuentra protegida.

Se establece como elemento subjetivo del ilícito el que la conducta tenga por objeto conocer o copiar información contenida y protegida en sistemas informáticos del Estado.

La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar los verbos núcleos de la conducta.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y contraria a la sociedad, se puede aplicar alguna causa de justificación como en el cumplimiento de un deber o el ejercicio de un derecho, incluso en un estado de necesidad justificante.

Como sabemos, para ser imputable se requiere la capacidad de querer y entender, pero la conducta de la hipótesis en cuestión puede ser realizada por alguna persona inimputable, teniendo como ejemplo algún menor de edad, ante lo cual será importante aplicar las medidas de seguridad del caso.

Esta hipótesis se puede dar de forma dolosa y culposa, respecto a la inculpabilidad, se puede considerar el error de hecho e invencible, cuando se dé un falso conocimiento de la verdad, un estado de necesidad que permita salvaguardar un bien jurídico tutelado alterando a otro bien jurídico y por obediencia jerárquica, bajo la instrucción de un superior jerárquico.

Este delito se persigue de oficio, teniendo una sanción de seis meses a dos años de prisión y de cien a trescientos días de multa.

A continuación, se esquematiza lo explicado anteriormente:

<b>Conducta</b>	La conducta es de acción, y es el conocer o copiar sin autorización información contenida y protegida en sistemas o
-----------------	---

	equipos de informática del Estado.
<b>Ausencia de conducta</b>	No se puede dar ninguna de las formas de ausencia de conducta.
<b>Tipicidad</b>	<p>La conducta esta descrita en el artículo 211 bis párrafo segundo del código penal federal El tipo consta de elementos objetivos y normativos.</p> <p><b>SUJETO ACTIVO</b></p> <p>el tipo no establece alguna calidad especifica por lo que puede ser cualquier persona.</p> <p><b>SUJETO PASIVO</b></p> <p>El tipo establece como sujeto pasivo al Estado</p> <p><b>BIEN JURÍDICO TUTELADO</b></p> <p>Información del Estado contenida en sistemas o equipos de informática.</p> <p><b>OBJETO JURÍDICO</b></p> <p>Información del Estado</p> <p><b>ELEMENTO SUBJETIVO DEL ILÍCITO</b></p> <p>ilícito el que la conducta tenga por objeto conocer o copiar información contenida y protegida en sistemas informáticos del Estado.</p>

<b>Atipicidad</b>	Se puede presentar si llega a faltar algún elemento del tipo penal, por lo que podría existir la ausencia de los objetos jurídico y material.
<b>Antijuridicidad</b>	La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y contraria a la sociedad
<b>Causas de justificación</b>	se puede aplicar en el estado de necesidad justificante ,el cumplimiento de un deber o el ejercicio de un derecho
<b>Imputabilidad</b>	la capacidad de querer y entender
<b>Inimputabilidad</b>	se puede presentar que una persona no imputable realice la conducta. Por ejemplo un menor de edad
<b>Culpabilidad</b>	se puede dar de manera dolosa y culposa
<b>Inculpabilidad</b>	se podría presentar el error esencial de hecho e invencible o la obediencia jerárquica y el estado de necesidad
<b>Condiciones objetivas de punibilidad</b>	no se especifica, por lo que puede interpretarse, esto quiere decir que se podría perseguir de oficio, por parte del Estado
<b>Punibilidad</b>	6 meses a 2 años de prisión y de 100 a 300 días multa.
<b>Excusas absolutorias</b>	No se pueden dar en esta hipótesis.
<b>SUJETO ACTIVO</b>	el tipo no establece alguna calidad específica por lo que puede ser cualquier persona.
<b>SUJETO PASIVO</b>	El tipo establece como sujeto pasivo al Estado
<b>BIEN JURÍDICO TUTELADO</b>	Información del Estado contenida en sistemas o equipos de informática.
<b>OBJETO JURÍDICO</b>	Información del Estado

<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	ilícito el que la conducta tenga por objeto conocer o copiar información contenida y protegida en sistemas informáticos del Estado.
---	---

#### **4.5 Conocer, obtener, copiar o utilizar información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad**

Art. 211 Bis 2 párrafo 3 del Código Penal Federal establece:

*“A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.”*

En el párrafo específico del artículo se plantean distintas hipótesis, las cuales serán ilustradas.



CALIDAD ESPECÍFICA DEL SUJETO PASIVO	CALIDAD ESPECÍFICA DEL SUJETO ACTIVO	HIPÓTESIS
Estado	Cualquier persona	<ul style="list-style-type: none"> <li>-Conozca información contenida en cualquier sistema de almacenamiento informático</li> <li>-Obtenga información contenida en cualquier sistema de almacenamiento informático</li> <li>-Copie información contenida en cualquier sistema de almacenamiento informático</li> <li>-Utilice información contenida en cualquier sistema de almacenamiento informático</li> </ul>
Estado	Cualquier persona	<ul style="list-style-type: none"> <li>-Conozca información contenida en cualquier equipo de almacenamiento informático</li> <li>-Obtenga información contenida en cualquier equipo de almacenamiento informático</li> <li>-Copie información contenida en cualquier equipo de almacenamiento informático</li> <li>-Utilice información contenida en cualquier equipo de almacenamiento informático</li> </ul>
		<ul style="list-style-type: none"> <li>-Conozca información contenida en cualquier medio de almacenamiento informático</li> <li>-Obtenga información contenida</li> </ul>

Estado	Cualquier persona	<p>en cualquier medio de almacenamiento informático</p> <ul style="list-style-type: none"> <li>-Copie información contenida en cualquier medio de almacenamiento informático</li> <li>-Utilice información contenida en cualquier medio de almacenamiento informático</li> </ul>
Estado	Servidor público en una institución de seguridad pública	<ul style="list-style-type: none"> <li>-Conozca información contenida en cualquier sistema de almacenamiento informático</li> <li>-Obtenga información contenida en cualquier sistema de almacenamiento informático</li> <li>-Copie información contenida en cualquier sistema de almacenamiento informático</li> <li>-Utilice información contenida en cualquier sistema de almacenamiento informático</li> </ul>
Estado	Servidor público en una institución de seguridad pública	<ul style="list-style-type: none"> <li>-Conozca información contenida en cualquier equipo de almacenamiento informático</li> <li>-Obtenga información contenida en cualquier equipo de almacenamiento informático</li> <li>-Copie información contenida en cualquier equipo de almacenamiento informático</li> <li>-Utilice información contenida en cualquier equipo de</li> </ul>

		almacenamiento informático
Estado	Servidor público en una institución de seguridad pública	-Conozca información contenida en cualquier medio de almacenamiento informático -Obtenga información contenida en cualquier medio de almacenamiento informático -Copie información contenida en cualquier medio de almacenamiento informático -Utilice información contenida en cualquier medio de almacenamiento informático

Lo anterior nos da un total de **24 hipótesis** del párrafo tercero perteneciente al art. 211 Bis 2.

Como podemos observar este artículo consta de varios supuestos, por lo que se hará el estudio dogmático de una manera general, sin importar la calidad del sujeto pasivo, tomando las fracciones de este precepto para este ejercicio.

### **1. Conozca información contenida**

Como podemos observar, en este supuesto de acción, cuyo verbo núcleo es “conocer”, en donde no se puede presentar la ausencia de conducta porque no se puede pensar en que por una fuerza física superior e irresistible proveniente de la naturaleza o de otro ser humano o por medio de movimientos reflejos se conozca sin autorización información contenida en medios, sistemas o equipos de informática del Estado.

Tipicidad consiste en el encuadramiento de la conducta al tipo, y en lo que respecta a este artículo el cual contiene la conducta de conocer información sin autorización de medios, sistemas o equipos informáticos del Estado. El tipo señalado consta de elementos objetivos; además se establece alguna calidad específica para el sujeto activo, contemplando a cualquier persona y a servidores

públicos; en lo que respecta al sujeto pasivo, el tipo nos indica que es el Estado, por lo tanto no hay calidad específica, ya que de él depende la función y control de la información que se maneja a través de los medios, equipos o sistemas informáticos y se ve afectado al difundirse información que se encuentra protegida.

Se establece como elemento subjetivo del ilícito el que la conducta tenga por objeto conocer información contenida y protegida en medios, sistemas y equipos informáticos del Estado.

La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar los verbos núcleos de la conducta.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y contraria a la sociedad, se puede aplicar alguna causa de justificación como en el cumplimiento de un deber o el ejercicio de un derecho, incluso en un estado de necesidad justificante.

Como sabemos, para ser imputable se requiere la capacidad de querer y entender, pero en la conducta de la hipótesis en cuestión no se especifica, por lo que se pueden contemplar tanto adultos como menores de edad.

Esta hipótesis se puede dar de forma dolosa y culposa, respecto a la inculpabilidad, se puede considerar el error de hecho e invencible, cuando se dé un falso conocimiento de la verdad, un estado de necesidad que permita salvaguardar un bien jurídico tutelado alterando a otro bien jurídico y por obediencia jerárquica, bajo la instrucción de un superior jerárquico.

Este delito se persigue de oficio, teniendo una pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal, y si el delito lo cometiera un servidor público se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

## **2. Obtenga información contenida**

Como podemos observar, en este supuesto de acción, cuyo verbo núcleo es “obtener”, en donde no se puede presentar la ausencia de conducta porque no se

puede pensar en que por una fuerza física superior e irresistible proveniente de la naturaleza o de otro ser humano o por medio de movimientos reflejos se obtenga sin autorización información contenida en medios, sistemas o equipos de informática del Estado.

Tipicidad consiste en el encuadramiento de la conducta al tipo, y en lo que respecta a este artículo el cual contiene la conducta de obtener información sin autorización de medios, sistemas o equipos informáticos del Estado. El tipo señalado consta de elementos objetivos; además se establece alguna calidad específica para el sujeto activo, contemplando a cualquier persona y a servidores públicos; en lo que respecta al sujeto pasivo, el tipo nos indica que es el Estado, por lo tanto no hay calidad específica, ya que de él depende la función y control de la información que se maneja a través de los medios, equipos o sistemas informáticos y se ve afectado al difundirse información que se encuentra protegida.

Se establece como elemento subjetivo del ilícito el que la conducta tenga por objeto obtener información contenida y protegida en medios, sistemas y equipos informáticos del Estado.

La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar los verbos núcleos de la conducta.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y contraria a la sociedad, se puede aplicar alguna causa de justificación como en el cumplimiento de un deber o el ejercicio de un derecho, incluso en un estado de necesidad justificante.

Como sabemos, para ser imputable se requiere la capacidad de querer y entender, pero en la conducta de la hipótesis en cuestión no se especifica, por lo que se pueden contemplar tanto adultos como menores de edad.

Esta hipótesis se puede dar de forma dolosa y culposa, respecto a la inculpabilidad, se puede considerar el error de hecho e invencible, cuando se dé un falso conocimiento de la verdad, un estado de necesidad que permita salvaguardar un bien jurídico tutelado alterando a otro bien jurídico y por obediencia jerárquica, bajo la instrucción de un superior jerárquico.

Este delito se persigue de oficio, teniendo una pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal, y si el delito lo cometiera un servidor público se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

### **3. Copie información contenida**

Como podemos observar, en este supuesto de acción, cuyo verbo núcleo es “copiar”, en donde no se puede presentar la ausencia de conducta porque no se puede pensar en que por una fuerza física superior e irresistible proveniente de la naturaleza o de otro ser humano o por medio de movimientos reflejos se obtenga sin autorización información contenida en medios, sistemas o equipos de informática del Estado.

Tipicidad consiste en el encuadramiento de la conducta al tipo, y en lo que respecta a este artículo el cual contiene la conducta de copiar información sin autorización de medios, sistemas o equipos informáticos del Estado. El tipo señalado consta de elementos objetivos; además se establece alguna calidad específica para el sujeto activo, contemplando a cualquier persona y a servidores públicos; en lo que respecta al sujeto pasivo, el tipo nos indica que es el Estado, por lo tanto no hay calidad específica, ya que de él depende la función y control de la información que se maneja a través de los medios, equipos o sistemas informáticos y se ve afectado al difundirse información que se encuentra protegida.

Se establece como elemento subjetivo del ilícito el que la conducta tenga por objeto copiar información contenida y protegida en medios, sistemas y equipos informáticos del Estado.

La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar los verbos núcleos de la conducta.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y contraria a la sociedad, se puede

aplicar alguna causa de justificación como en el cumplimiento de un deber o el ejercicio de un derecho, incluso en un estado de necesidad justificante.

Como sabemos, para ser imputable se requiere la capacidad de querer y entender, pero en la conducta de la hipótesis en cuestión no se especifica, por lo que se pueden contemplar tanto adultos como menores de edad.

Esta hipótesis se puede dar de forma dolosa y culposa, respecto a la inculpabilidad, se puede considerar el error de hecho e invencible, cuando se dé un falso conocimiento de la verdad, un estado de necesidad que permita salvaguardar un bien jurídico tutelado alterando a otro bien jurídico y por obediencia jerárquica, bajo la instrucción de un superior jerárquico.

Este delito se persigue de oficio, teniendo una pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal, y si el delito lo cometiera un servidor público se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

#### **4. Utilice información contenida**

Como podemos observar, en este supuesto de acción, cuyo verbo núcleo es “utilizar”, en donde no se puede presentar la ausencia de conducta porque no se puede pensar en que por una fuerza física superior e irresistible proveniente de la naturaleza o de otro ser humano o por medio de movimientos reflejos se obtenga sin autorización información contenida en medios, sistemas o equipos de informática del Estado.

Tipicidad consiste en el encuadramiento de la conducta al tipo, y en lo que respecta a este artículo el cual contiene la conducta de utilizar información sin autorización de medios, sistemas o equipos informáticos del Estado. El tipo señalado consta de elementos objetivos; además se establece alguna calidad específica para el sujeto activo, contemplando a cualquier persona y a servidores públicos; en lo que respecta al sujeto pasivo, el tipo nos indica que es el Estado, por lo tanto no hay calidad específica, ya que de él depende la función y control de

la información que se maneja a través de los medios, equipos o sistemas informáticos y se ve afectado al difundirse información que se encuentra protegida.

Se establece como elemento subjetivo del ilícito el que la conducta tenga por objeto utilizar información contenida y protegida en medios, sistemas y equipos informáticos del Estado.

La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar los verbos núcleos de la conducta.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y contraria a la sociedad, se puede aplicar alguna causa de justificación como en el cumplimiento de un deber o el ejercicio de un derecho, incluso en un estado de necesidad justificante.

Como sabemos, para ser imputable se requiere la capacidad de querer y entender, pero en la conducta de la hipótesis en cuestión no se especifica, por lo que se pueden contemplar tanto adultos como menores de edad.

**CONDUCTA** { La conducta es de acción, y es el conocer, obtener, copiar y utilizar sin autorización información contenida y protegida en sistemas, equipos o medios de informática del Estado.

Esta hipótesis se puede dar de forma dolosa y culposa, respecto a la inculpabilidad, se puede considerar el error de hecho e invencible, cuando se dé un falso conocimiento de la verdad, un estado de necesidad que permita salvaguardar un bien jurídico tutelado alterando a otro bien jurídico y por obediencia jerárquica, bajo la instrucción de un superior jerárquico.

Este delito se persigue de oficio, teniendo una pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal, y si el delito lo cometiera un servidor público se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

**A continuación, se ejemplifica lo dicho con anterioridad a través de una tabla**



**AUSENCIA  
CONDUCTA**

DE { No se puede dar ninguna de las formas de ausencia de conducta.

**TIPICIDAD**

La conducta esta descrita en el artículo 211 bis 2 párrafo tercero del código penal federal

El tipo consta de elementos objetivos y normativos.

**SUJETO ACTIVO**

{ Establece que puede ser cualquier persona o un servidor público.

**SUJETO PASIVO**

{ El tipo establece como sujeto pasivo al Estado

**BIEN JURÍDICO  
TUTELADO**

{ Información del Estado contenida en sistemas, equipos o medios de informática.

**OBJETO JURÍDICO**

{ Información del Estado

**ELEMENTO  
SUBJETIVO  
ILÍCITO**

**DEL**

{ Ilícito el que la conducta tenga por objeto conocer, obtener, copiar o utilizar información contenida y protegida en sistemas informáticos del Estado.

<b>ATIPICIDAD</b>	{	Se puede presentar si llega a faltar algún elemento del tipo penal, por lo que podría existir la ausencia de los objetos jurídico y material.
<b>ANTI JURIDICIDAD</b>	{	La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y contraria a la sociedad
<b>CAUSAS DE JUSTIFICACIÓN</b>	{	se puede aplicar en el estado de necesidad justificante, el cumplimiento de un deber o el ejercicio de un derecho
<b>IMPUTABILIDAD</b>	{	la capacidad de querer y entender
<b>INIMPUTABILIDAD</b>	{	Se puede presentar que una persona no imputable realice la conducta. Por ejemplo un menor de edad
<b>CULPABILIDAD</b>	{	se puede dar de manera dolosa y culposa
<b>INCULPABILIDAD</b>	{	se podría presentar el error esencial de hecho e invencible o la obediencia jerárquica y el estado de necesidad
<b>CONDICIONES OBJETIVAS DE PUNIBILIDAD</b>	{	no se especifica, por lo que puede interpretarse, esto quiere decir que se podría perseguir de oficio, por parte del Estado
<b>PUNIBILIDAD</b>	{	4 a 10 años de prisión y multa de 500 mil días de salario mínimo general vigente en el Distrito Federal, cuando se tratase de un servidor público se impondrá la destitución e inhabilitación de 4 a 10 años para desempeñarse en otro empleo, puesto, cargo o comisión pública.
<b>EXCUSAS ABSOLUTORIAS</b>	{	No se pueden dar en esta hipótesis.

#### **4.6. Modificar, destruir o provocar pérdida de información que contengan indebidamente, estando autorizado para acceder a sistemas y equipos de informática del Estado.**

Artículo 211 bis 3.- Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Como se puede observar, la conducta en esta fracción denota que es de acción, cuyos verbos núcleos son “modifique”, “destruya” o “provoque”, si se puede presentar una ausencia de conducta, poniendo el supuesto que el sujeto activo sea amenazado para realizar la conducta, presentándose así la Vis Absoluta.

Con respecto a la tipicidad se debe dar un exacto encuadramiento de la conducta al tipo, el cual contiene la conducta de modificar, destruir o provocar la pérdida de información.

El tipo señalado consta de solamente de un elemento objetivo; si se establece una calidad específica con respecto al sujeto activo, ya que se establece que es aquel que este autorizado para acceder a sistemas y equipos de informática del estado, así mismo también se establece una calidad específica para el sujeto pasivo ya que se establece que debe ser el Estado el afectado. Se establece como elemento objetivo del ilícito el que la conducta tenga por resultado la pérdida de información del estado o la alteración de esta. Tomando en cuenta esto, podemos observar que solamente el Estado puede ser objeto de esta conducta.

La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar los verbos núcleos de la conducta.

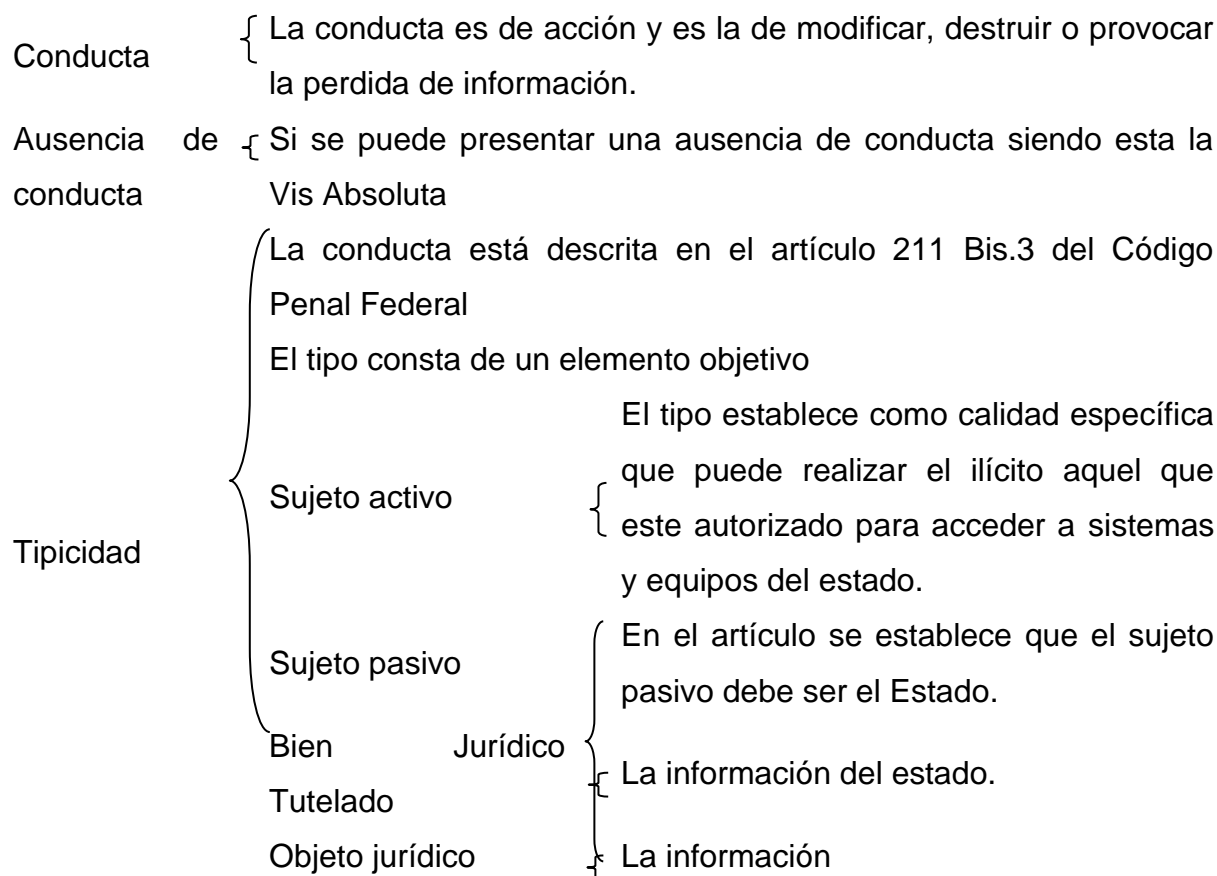
La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal al constituir una transgresión a la norma dictada por el Estado, pudiéndose aplicar solamente como causa de justificación el estado de necesidad, en la salvaguarda de un bien jurídico de mayor valía.

Para ser imputable además de tener la capacidad de querer y entender, se necesita tener la calidad específica de ser autorizado para acceder a sistemas y equipos de informática del estado, por lo anterior esta hipótesis no puede ser cometida por algún inimputable.

Esta hipótesis se puede dar únicamente de forma dolosa, lo cual ayuda a evidenciar la intención del sujeto activo en la realización de la conducta; en lo que respecta a la inculpabilidad, se puede considerar la vis absoluta como la no exigibilidad de otra conducta, al presentarse una amenaza de un daño grave si no se realiza la conducta descrita en el tipo de mérito.

Este delito se persigue por oficio, teniendo una sanción de dos a ocho años de prisión y de trescientos a novecientos días multa, mientras que como excusa absolutoria tenemos que se necesita que el sujeto activo sea personal autorizado para tener acceso a la información del Estado si el delito lo cometiera alguien que no esté autorizado no se podría aplicar esta fracción.

A continuación, se esquematiza lo explicado en párrafos anteriores.



Atipicidad	{	Se puede presentar si llega a faltar la calidad específica del sujeto activo.
Antijuridicidad	{	Cuenta con la formal, ya que la conducta transgrede una norma dictada por el Estado (art 211 Bis. 3 fr. I del Código Penal Federal)
Causas de justificación	{	Se puede aplicar el Estado de necesidad siempre que se vea comprometido un bien jurídico tutelado mayor
Imputabilidad	{	La capacidad de querer y entender.
Inimputabilidad	{	Se puede presentar que una persona no imputable realice la conducta, o alguien que no esté autorizado para tener acceso a los sistemas y equipos de informática del estado
Culpabilidad	{	Se puede dar únicamente de manera dolosa.
Inculpabilidad	{	Se podría presentar la <i>vis absoluta</i> .
Condiciones objetivas de punibilidad	{	Se persigue por oficio.
Punibilidad	{	De 2 a 8 años de prisión y de 300 a 900 días de multa.
Excusas absolutorias	{	Se necesita que el sujeto activo sea personal autorizado para tener acceso a la información del Estado si el delito lo cometiera alguien que no esté autorizado no se podría aplicar esta fracción del artículo.

#### **4.7. Estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan**

En el segundo párrafo del artículo 211 bis 3 del Código Penal Federal se establece lo siguiente:

“Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos días de multa.”

De acuerdo con lo descrito anteriormente por el artículo mencionado se derivan diferentes hipótesis:

	HIPOTESIS
CONDUCTA	<ul style="list-style-type: none"> <li>- Acceda a sistemas o equipos</li> <li>- Copie información</li> </ul>
CONSENTIMIENTO	- Autorizado para acceder a sistemas y equipos del Estado
INFORMACION	- De manera indebida copie información que contengan

Comenzando este análisis debemos puntualizar que se habla del verbo “acceder” que en materia de este estudio se refiere a que aún quién tenga el privilegio de tener esa información copie y haga mal uso de la misma, estaremos entrando en la acción de traicionar la confianza del Estado.

Siguiendo la misma línea de estudio pasamos con la condición del sujeto activo que en este caso es el que se encuentre autorizado para acceder a sistemas y equipos de informática, que lo denominamos consentimiento ya que siendo capaz de acceder a esta información la ocupe para fines lascivos o de lucro.

Como siguiente punto a abordar será la tipicidad y para ello debemos de ser muy puntuales de poder dar de manera exacta el encuadramiento de esta conducta que como punto primordial será el que estado autorizado copie información que contengan sin embargo debemos de poner especial atención en que la acción se haga indebidamente y que sea información específica del Estado y se encuentre protegida por el mismo.

Proseguiremos con la atipicidad que desafortunadamente en este caso es muy común que se presente ya que al no contener alguno de los elementos como acceder, indebidamente, copiar información podremos tener un caso de atipicidad.

Consta de elementos objetivos, subjetivos y normativos; y la calidad específica del sujeto activo es el que esté autorizado por eje de estamos en presencia de que quien realice este ilícito debe tener un nexo con el Estado en calidad de trabajador ya que especifique quién esté autorizado.

Como elemento subjetivo de este delito es la manera en que se realice la acción que en este caso será de una forma indebida donde acceda y copie información.

Como elemento normativo que es la valoración jurídico cultural, tomamos que se atente contra un sistema que cuida la confidencialidad del Estado y la posición de datos.

La antijuridicidad queda establecida desde que se encuentra tipificada, que de manera directa se transgrede la norma y que es una afectación directa al Estado.

Como lo hemos visto reiteradas ocasiones para ser imputable se requiere el poder comprender la conducta que se está realizando de tal forma que en este caso no aplica la imputabilidad ya que presenta grandes dificultades técnicas y de accesibilidad de manejo de información y confidencialidad del Estado.

En este caso si menciona que debe de existir una calidad específica del sujeto activo la cual es que esté autorizado para realizar este ilícito.

Este delito sólo se puede realizar de manera dolosa que podrá facilitar la acción del sujeto de transgredir la confidencialidad del Estado.

La forma de perseguir este ilícito es por oficio teniendo la sanción de 1 a 4 años de prisión o de ciento cincuenta a cuatrocientos días de multa. Y que será imposible aplicar alguna de las excusas absolutorias para este.

Para esclarecer cualquier duda se anexa un cuadro con lo antes mencionado:

<b>CONDUCTA</b>	{ Acceda y copie información de manera indebida
<b>AUSENCIA DE CONDUCTA</b>	{ No aplicará la ausencia de conducta
<b>TIPICIDAD</b>	<p>La conducta está descrita en el segundo párrafo del artículo 211 bis 3 del Código Penal. El tipo consta de elementos subjetivos, objetivos y normativos</p> <p><b>SUJETO ACTIVO</b> { El tipo especifica que sea quien con autorización acceda y copie indebidamente información</p> <p><b>SUJETO PASIVO</b> { Es una afectación directa al Estado</p> <p><b>BIEN JURÍDICO TUTELADO</b> { La información del Estado</p> <p><b>OBJETO JURÍDICO</b> { La confidencialidad</p> <p><b>ELEMENTO SUBJETIVO DEL ILÍCITO</b> { Que obre de manera dolosa</p> <p><b>ELEMENTO NORMATIVO</b> { Que traicione la confianza del Estado.</p>
<b>ATIPICIDAD</b>	{ Se puede presentar si llega a faltar algún elemento del tipo penal, por lo que podría existir la ausencia de los elementos objetivos, subjetivos y normativos del ilícito.
<b>ANTI JURIDICIDAD</b>	{ Se toma la formal se encuentra en el Art. 211 bis 3 párrafo 2 del Código Penal Federal.
<b>CAUSAS DE</b>	{ No son aplicables



**JUSTIFICACIÓN**

**IMPUTABILIDAD** { La capacidad de querer y entender.

**INIMPUTABILIDAD** { No aplica

**CULPABILIDAD** { Solo se puede consumir de manera dolosa

**INCULPABILIDAD** { No aplica

**CONDICIONES OBJETIVAS DE** { Se persigue por oficio.

**PUNIBILIDAD**

**PUNIBILIDAD** { De 1 a 4 años de prisión y de ciento cincuenta a cuatrocientos días de multa

**EXCUSAS ABSOLUTORIAS** { No serán aplicables.

**S**

**4.8 Estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan.**

El artículo 211 bis 3 del Código Penal Federal establece en su tercer párrafo lo siguiente:

“A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad

más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.”

En el análisis de este texto podemos encontrar que los verbos núcleos son obtenga, copie y utilice, cada uno de estos verbos tienen 3 hipótesis a considerar cada uno. La primera cuando la información se encuentre contenida en sistemas informáticos en materia de seguridad pública, la segunda cuando la información se encuentre en equipos informáticos en materia de seguridad pública y la tercera cuando la información se encuentre contenida en medios de almacenamiento informáticos en materia de seguridad pública. Lo cual nos da un total de 9 conductas hipotéticas ilustradas a continuación:

Acción Específica del Sujeto Activo	Conducta hipotética sancionada
<ul style="list-style-type: none"> <li>· Obtenga</li> </ul>	<ul style="list-style-type: none"> <li>· Cuando la información se encuentre contenida en sistemas informáticos en materia de seguridad pública.</li> <li>· Cuando la información se encuentre en equipos informáticos en materia de seguridad pública.</li> <li>· Cuando la información se encuentre contenida en medios de almacenamiento informáticos en materia de seguridad pública.</li> </ul>
<ul style="list-style-type: none"> <li>· Copie</li> </ul>	<ul style="list-style-type: none"> <li>· Cuando la información se encuentre contenida en sistemas informáticos en materia de seguridad pública.</li> <li>· Cuando la información se encuentre en equipos</li> </ul>

	<p>informáticos en materia de seguridad pública.</p> <ul style="list-style-type: none"> <li>· Cuando la información se encuentre contenida en medios de almacenamiento informáticos en materia de seguridad pública.</li> </ul>
<ul style="list-style-type: none"> <li>· Utilice</li> </ul>	<ul style="list-style-type: none"> <li>· Cuando la información se encuentre contenida en sistemas informáticos en materia de seguridad pública.</li> <li>· Cuando la información se encuentre en equipos informáticos en materia de seguridad pública.</li> <li>· Cuando la información se encuentre contenida en medios de almacenamiento informáticos en materia de seguridad pública.</li> </ul>

Para fines dogmáticos se muestran las definiciones de la RAE (Real Academia Española) de los verbos núcleo.

Obtener:

1. tr. Alcanzar, conseguir y lograr algo que se merece, solicita o pretende.
2. tr. Tener, conservar y mantener.
3. tr. Fabricar o extraer un material o un producto con ciertas cosas o de cierta manera

Copiar:

1. tr. Escribir en una parte lo que está escrito en otra.
2. tr. Trasladar a un escrito lo que alguien dice de viva voz.
3. tr. Reproducir textos, imágenes, sonidos u objetos.

Utilizar:

1. tr. Hacer que algo sirva para un fin.
2. tr. Aprovecharse de algo o de alguien.

Podemos decir que la conducta consiste en un hacer, ya que los verbos núcleo nos expresa que el sujeto activo debe de realizar una acción específica la cual en este caso es obtener, copiar y/o utilizar información en materia de seguridad pública de manera indebida por lo cual denota necesariamente la intervención de un ente o voluntad humana.

El sujeto activo debe tener la calidad de estar autorizado para manejar la información en materia de seguridad pública, la conducta ilícita se presenta en el momento en el que este sujeto realiza un uso indebido de sus funciones respecto de la información antes mencionada dando a entender que el fin de esto es diferente a las responsabilidades que le fueron confiadas.

Una vez dicho lo anterior podemos decir que la tipicidad requiere del exacto encuadramiento de la conducta la cual tiene como tipo fundamental la conducta de obtener, copiar o utilizar indebidamente información en materia de seguridad pública, cabe mencionar la existencia de un tipo especial ya que la información debe ser utilizada indebidamente y encontrarse en equipos o medios de almacenamiento informáticos y que el sujeto activo tenga la calidad de persona autorizada.

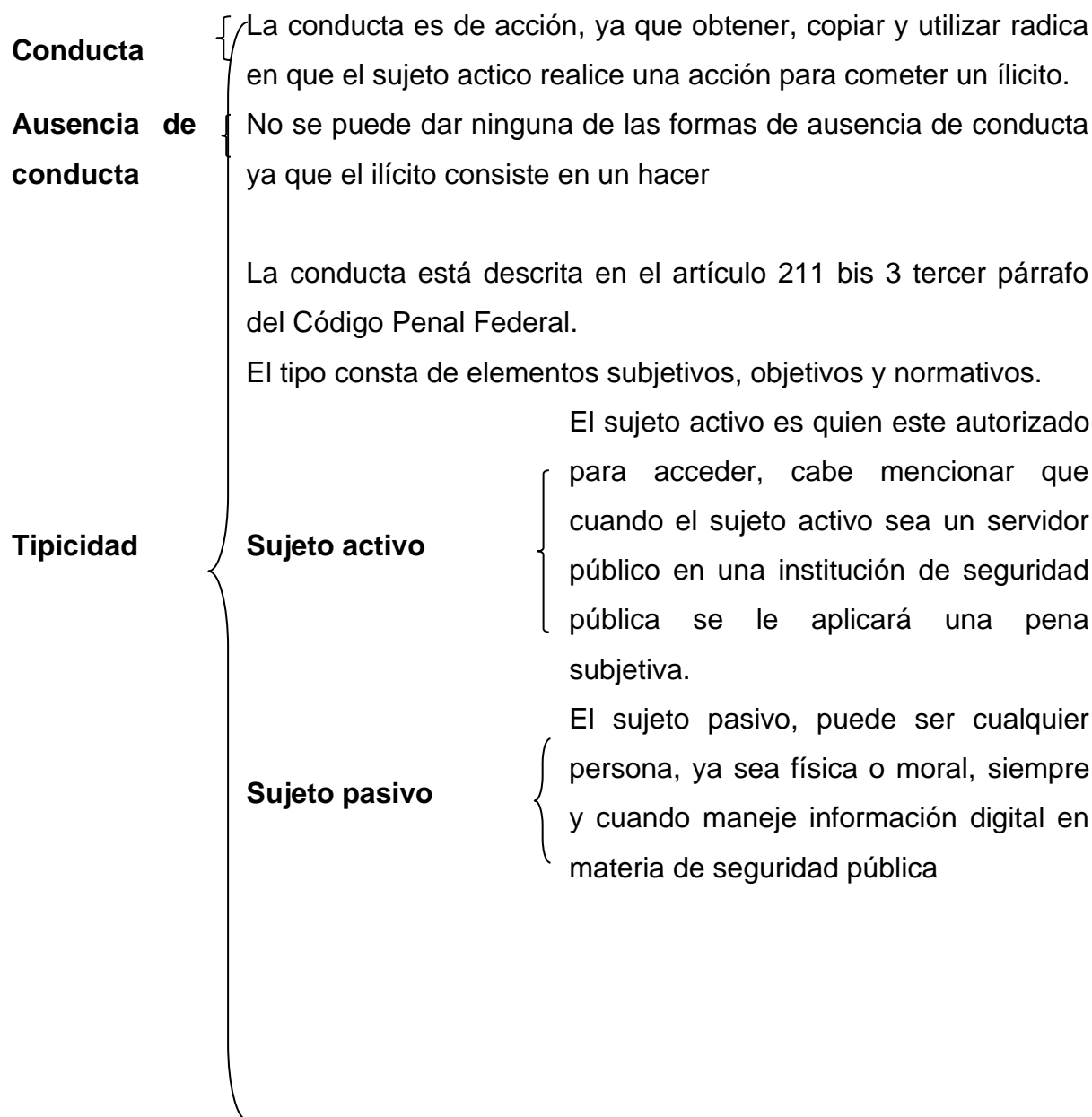
La atipicidad se puede dar bastará con que falte alguno de los elementos mencionados. En el caso de que no se lleve a cabo las acciones de conocer o copiar, se podrá decir que el hecho ilícito no corresponde al tipo.

Se establece como elemento subjetivo del ilícito el que la conducta sea realizada con dolo, al tratarse de la manipulación de información contenida en medios

informáticos se necesita tener el conocimiento necesario y por lo tanto resulta imposible que el sujeto activo no tenga la intención del acto ilícito.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

De igual manera se habla de una pena adjetiva en la cual el sujeto activo debe de tener la calidad de servidor público activo o no activo en una institución de seguridad pública.



<b>Bien Tutelado</b>	<b>Jurídico</b>	El bien jurídico tutelado es el resguardo de la información en materia de seguridad pública, este bien jurídico tutelado tiene particular importancia ya que garantiza el ejercicio de los derechos y las libertades de colectividad.
<b>Objeto jurídico</b>		Sistemas, equipos y medios de almacenamiento informáticos, equipos o medios de almacenamiento informáticos en materia de seguridad pública
<b>Elemento subjetivo del ilícito</b>		Constituido por el dolo o la culpa con que actúa el sujeto activo que obtenga, copie o utilice contenida en sistemas informáticos, equipos o medios de almacenamiento informáticos en materia de seguridad pública
<b>Elemento normativo</b>		Que atente contra los sistemas de informática.
<b>Atipicidad</b>		Cuando el sujeto activo no sea una persona autorizada y/o cuando la información manipulada no sea en materia de seguridad pública
<b>Antijuridicidad</b>		Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 3 tercer párrafo del Código Penal Federal) y es contraria a la sociedad.
<b>Causas de justificación</b>		No se puede aplicar ninguna.
<b>Imputabilidad</b>		La capacidad de querer y entender.
<b>Inimputabilidad</b>		Se puede presentar que una persona no imputable realice la conducta, pero sería difícil que pasara ya que debería tener

		manejo de las tecnologías de la información.
<b>Culpabilidad</b>	{	Se puede dar de manera dolosa o culposa.
<b>Inculpabilidad</b>	{	Se puede presentar por la primera la vis compulsiva,
<b>d</b>		
<b>Condiciones objetivas de punibilidad</b>	{	Se persigue de oficio.
<b>Punibilidad</b>	{	<p>Penal: Pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal.</p> <p>Penal Adjetiva: se impondrá, además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública la cual se aplica cuando se satisfacen la siguiente agravante: El sujeto activo es un servidor público en una institución de seguridad pública.</p>
<b>Excusas absolutorias</b>	{	No tiene excusa absoluta alguna

#### **4.9 Modificar, destruir o provocar pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.**

Art. 211 bis 4. párrafo primero del Código Penal Federal:

“Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.”

Como podemos ver del texto anterior, se derivan una serie considerable de hipótesis, las cuales procederemos a ilustrar:

<b>Acción específica del sujeto activo</b>	<b>Hipótesis</b>
Modifique	<ul style="list-style-type: none"><li>• Información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.</li><li>• de información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.</li></ul>
Destruya	<ul style="list-style-type: none"><li>• Información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.</li><li>• de información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.</li></ul>



Provoque pérdida	<ul style="list-style-type: none"> <li>• Información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.</li> <li>• de información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.</li> </ul>		
	<table border="1" style="width: 100%;"> <tr> <td data-bbox="561 806 1036 1020">Total de hipótesis previstas en el primer párrafo del artículo 211 bis 4 del Código Penal Federal</td> <td data-bbox="1040 806 1421 1020" style="text-align: center;"><b>6</b></td> </tr> </table>	Total de hipótesis previstas en el primer párrafo del artículo 211 bis 4 del Código Penal Federal	<b>6</b>
Total de hipótesis previstas en el primer párrafo del artículo 211 bis 4 del Código Penal Federal	<b>6</b>		

Como podemos observar este artículo consta de varios supuestos, por lo que se hará el estudio dogmático de una manera general, no sin antes dar un breve contexto para mejor entendimiento del tema.

Las TIC se ha caracterizada por el dinamismo de las tecnologías de la información y la comunicación, y la masiva producción de información a velocidades y cantidades inusitadas, así surgen nuevas formas de convivencia, trayendo consigo una serie de conductas ilícitas relacionadas con el uso de estas tecnologías.

Elas se han convertido en herramientas para concretar delitos, en el ambiente virtual, existen diversas conductas que son catalogadas de la misma forma, por ello, el derecho penal informático o derecho penal de las nuevas tecnologías de la información y comunicación se encarga de su estudio.

Davara Rodríguez define al Delito informático como, “la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea

llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.”

Se ha observado que por lo general el sujeto activo del delitos es una persona con un determinado nivel de inteligencia y educación, superior al común, mismos que pueden ser los programadores que violan o inutilizan controles protectores del programa o sistema, los analistas de sistemas que generalmente son los únicos que conocen la operación completa de ellos; los analistas de comunicaciones que diseñan la seguridad del sistema de comunicaciones, supervisores que tienen conocimiento integral de las operaciones y debilidades del sistema de seguridad; personal técnico y de mantenimiento, que suele tener libre acceso a los centros de cómputo y conoce los sistemas operativos y bases de datos; etcétera.

Lo anterior, sería aplicable a los denominados delitos computacionales que se identifican así, porque el medio de comisión son las tecnologías de la información o la comunicación y el valor protegido es distinto al valor económico de la información.

***1. Modifique información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.***

Como se puede observar, la conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “modificar”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, una fuerza física superior e irresistible proveniente de otro hombre.

De acuerdo con la tipicidad se debe dar el perfecto y cabal encuadramiento de la conducta al tipo penal, el cual es “modificar” información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona experta en el tema que no esté autorizada para acceder a la información, en lo

que respecta al sujeto pasivo, podemos ver en el párrafo que refiere a las Instituciones que integran el sistema financiero.

El elemento objetivo refiere a quien comete el delito, es todo atentado que signifique dañar o desviar el correcto uso de la máquina con la finalidad de causar un perjuicio moral o material, para sí o para otro por el uso indebido de un sistema de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

El elemento subjetivo debe estar constituido por el dolo o la culpa con que actúa el sujeto activo del delito que modifique información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. Existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba o no con autorización. La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar el verbo núcleo de la conducta, ocurre en el supuesto de que el sujeto activo tenga autorización para acceder a la información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

Se tiene en cuenta que para ser imputable se requiere la capacidad de querer y entender, teniendo en cuenta que para la acción realizada, como se mencionó antes la ejecuta una persona experta en el tema, es por ello por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis se da de forma dolosa, misma que nos ayuda a evidenciar la realización de la conducta.; en lo que respecta a la inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podía presentar una amenaza de un daño grave si no se realiza la conducta.

Este delito se persigue de oficio, teniendo una sanción de seis meses a cuatro años de prisión y de cien a seiscientos días multa; no encontrando alguna excusa absoluta.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación se esquematiza lo anteriormente explicado.

<b>Conducta</b>	La conducta es de acción, y es modificar información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.	
<b>Ausencia de conducta</b>	Se puede dar la <i>vis absoluta</i> como de ausencia de conducta, es decir, una fuerza física superior e irresistible proveniente de otro hombre.	
<b>Tipicidad</b>	La conducta está descrita en el artículo 211 bis 4 párrafo primero del Código Penal Federal. El tipo consta de elementos subjetivos, objetivos y normativos.	
	<b>Sujeto activo</b>	No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, educada en el tema.
	<b>Sujeto pasivo</b>	Las Instituciones que integran el sistema financiero.
	<b>Bien Jurídico Tutelado</b>	La seguridad de la información del sistema financiero.
	<b>Objeto jurídico</b>	Sistemas de informática

	<b>Elemento subjetivo del ilícito</b>	Está constituido por el dolo con que actúa el sujeto activo del delito que modifique información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.
	<b>Elemento normativo</b>	Que atente contra los sistemas de informática.
<b>Atipicidad</b>	Que el sujeto activo cuente con autorización para realizar la modificación de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad, y, al que sin autorización, modifique información contenida en sistemas de informática que no esté protegida por algún mecanismo de seguridad.	
<b>Antijuridicidad</b>	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 4 párrafo primero del Código Penal Federal) y es contraria a la sociedad.	
<b>Causas de justificación</b>	No aplica.	
<b>Imputabilidad</b>	La capacidad de querer y entender.	
<b>Inimputabilidad</b>	Se puede presentar que una persona no imputable realice la conducta, aunque sería poca la probabilidad.	
<b>Culpabilidad</b>	Se puede dar únicamente de manera dolosa	
<b>Inculpabilidad</b>	Se podría presentar la <i>vis compulsiva</i> o por obediencia jerárquica	
<b>Condiciones objetivas de punibilidad</b>	Se persigue de oficio.	
<b>Punibilidad</b>	De seis meses a cuatro años de prisión y de cien a seiscientos días multa.	

<b>Excusas absolutorias</b>	No tiene excusas absolutorias.
-----------------------------	--------------------------------

**2. Modifique de información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.**

Como se puede observar, la conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “modificar”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, una fuerza física superior e irresistible proveniente de otro hombre.

De acuerdo con la tipicidad se debe dar el perfecto y cabal encuadramiento de la conducta al tipo penal, el cual es “modificar” información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona experta en el tema que no esté autorizada para acceder a la información, en lo que respecta al sujeto pasivo, podemos ver en el párrafo que refiere a las Instituciones que integran el sistema financiero.

El elemento objetivo refiere a quien comete el delito, es todo atentado que signifique dañar o desviar el correcto uso de la máquina con la finalidad de causar un perjuicio moral o material, para sí o para otro por el uso indebido de un equipo de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

El elemento subjetivo debe estar constituido por el dolo con que actúa el sujeto activo del delito que modifique información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. Existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba o no con autorización. La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar el verbo núcleo de la conducta, ocurre en el

supuesto de que el sujeto activo tenga autorización para acceder a la información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

Se tiene en cuenta que para ser imputable se requiere la capacidad de querer y entender, teniendo en cuenta que para la acción realizada, como se mencionó antes, la ejecuta una persona experta en el tema, es por ello por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis se da de forma dolosa, misma que nos ayuda a evidenciar la realización de la conducta.; en lo que respecta a la inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podría presentar una amenaza de un daño grave si no se realiza la conducta.

Este delito se persigue de oficio, teniendo una sanción de seis meses a cuatro años de prisión y de cien a seiscientos días multa; no encontrando alguna excusa absolutoria.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación se esquematiza lo anteriormente explicado.

<b>Conducta</b>	La conducta es de acción, y es modificar información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.
<b>Ausencia de conducta</b>	Se puede dar la <i>vis absoluta</i> como de ausencia de conducta, es decir, una fuerza física superior e irresistible proveniente de otro hombre.

<b>Tipicidad</b>	<p>La conducta está descrita en el artículo 211 bis 4 párrafo primero del Código Penal Federal.</p> <p>El tipo consta de elementos subjetivos, objetivos y normativos.</p>	
	<b>Sujeto activo</b>	No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, educada en el tema.
	<b>Sujeto pasivo</b>	Las Instituciones que integran el sistema financiero.
	<b>Bien Jurídico Tutelado</b>	La seguridad de la información del sistema financiero.
	<b>Objeto jurídico</b>	Sistemas de informática
	<b>Elemento subjetivo del ilícito</b>	Está constituido por el dolo con que actúa el sujeto activo del delito que modifique información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.
	<b>Elemento normativo</b>	Que atente contra los equipos de informática.
<b>Atipicidad</b>	<p>Que el sujeto activo cuente con autorización para realizar la modificación de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad, y, al que sin autorización, modifique información contenida en sistemas de informática que no esté protegida por algún mecanismo de seguridad.</p>	
<b>Antijuridicidad</b>	<p>Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 4 párrafo primero del Código Penal Federal) y es contraria a la sociedad.</p>	



<b>Causas de justificación</b>	No aplica.
<b>Imputabilidad</b>	La capacidad de querer y entender.
<b>Inimputabilidad</b>	Se puede presentar que una persona no imputable realice la conducta, aunque sería poca la probabilidad.
<b>Culpabilidad</b>	Se puede dar únicamente de manera dolosa
<b>Inculpabilidad</b>	Se podría presentar la <i>vis compulsiva</i> o por obediencia jerárquica
<b>Condiciones objetivas de punibilidad</b>	Se persigue de oficio.
<b>Punibilidad</b>	De seis meses a cuatro años de prisión y de cien a seiscientos días multa.
<b>Excusas absolutorias</b>	No tiene excusas absolutorias.

**3. Destruya información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.**

Como se puede observar, la conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “destruir”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, una fuerza física superior e irresistible proveniente de otro hombre.

De acuerdo con la tipicidad se debe dar el perfecto y cabal encuadramiento de la conducta al tipo penal, el cual es “destruir” información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona

experta en el tema que no esté autorizada para acceder a la información, en lo que respecta al sujeto pasivo, podemos ver en el párrafo que refiere a las Instituciones que integran el sistema financiero.

El elemento objetivo refiere a quien comete el delito, es todo atentado que signifique dañar o desviar el correcto uso de la máquina con la finalidad de causar un perjuicio moral o material, para sí o para otro por el uso indebido de un sistema de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

El elemento subjetivo debe estar constituido por el dolo con que actúa el sujeto activo del delito que destruya información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. Existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba o no con autorización. La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar el verbo núcleo de la conducta, ocurre en el supuesto de que el sujeto activo tenga autorización para destruir información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

Se tiene en cuenta que para ser imputable se requiere la capacidad de querer y entender, teniendo en cuenta que para la acción realizada, como se mencionó antes la ejecuta una persona experta en el tema, es por ello por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis se da de forma dolosa, misma que nos ayuda a evidenciar la realización de la conducta.; en lo que respecta a la inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podría presentar una amenaza de un daño grave si no se realiza la conducta.

Este delito se persigue de oficio, teniendo una sanción de seis meses a cuatro años de prisión y de cien a seiscientos días multa; no encontrando alguna excusa absoluta.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación se esquematiza lo anteriormente explicado.

<b>Conducta</b>	La conducta es de acción, y es destruir información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.	
<b>Ausencia de conducta</b>	Se puede dar la <i>vis absoluta</i> como de ausencia de conducta, es decir, una fuerza física superior e irresistible proveniente de otro hombre.	
<b>Tipicidad</b>	La conducta está descrita en el artículo 211 bis 4 párrafo primero del Código Penal Federal. El tipo consta de elementos subjetivos, objetivos y normativos.	
	<b>Sujeto activo</b>	No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, educada en el tema.
	<b>Sujeto pasivo</b>	Las Instituciones que integran el sistema financiero.
	<b>Bien Jurídico Tutelado</b>	La seguridad de la información del sistema financiero.
	<b>Objeto jurídico</b>	Sistemas de informática

	<b>Elemento subjetivo del ilícito</b>	Está constituido por el dolo con que actúa el sujeto activo del delito que destruya información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.
	<b>Elemento normativo</b>	Que atente contra los sistemas de informática.
<b>Atipicidad</b>	Que el sujeto activo cuente con autorización para realizar la destrucción de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad, y, al que sin autorización, destruya información contenida en sistemas de informática que no esté protegida por algún mecanismo de seguridad.	
<b>Antijuridicidad</b>	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 4 párrafo primero del Código Penal Federal) y es contraria a la sociedad.	
<b>Causas de justificación</b>	No aplica.	
<b>Imputabilidad</b>	La capacidad de querer y entender.	
<b>Inimputabilidad</b>	Se puede presentar que una persona no imputable realice la conducta, aunque sería poca la probabilidad.	
<b>Culpabilidad</b>	Se puede dar únicamente de manera dolosa	
<b>Inculpabilidad</b>	Se podría presentar la <i>vis compulsiva</i> o por obediencia jerárquica	
<b>Condiciones objetivas de punibilidad</b>	Se persigue de oficio.	
<b>Punibilidad</b>	De seis meses a cuatro años de prisión y de cien a seiscientos días multa.	

<b>Excusas absolutorias</b>	No tiene excusas absolutorias.
-----------------------------	--------------------------------

**4. Destruya información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.**

Como se puede observar, la conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “destruir”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, una fuerza física superior e irresistible proveniente de otro hombre.

De acuerdo con la tipicidad se debe dar el perfecto y cabal encuadramiento de la conducta al tipo penal, el cual es “destruir” información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona experta en el tema que no esté autorizada para acceder a la información, en lo que respecta al sujeto pasivo, podemos ver en el párrafo que refiere a las Instituciones que integran el sistema financiero.

El elemento objetivo refiere a quien comete el delito, es todo atentado que signifique dañar o desviar el correcto uso de la máquina con la finalidad de causar un perjuicio moral o material, para sí o para otro por el uso indebido de un equipo de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

El elemento subjetivo debe estar constituido por el dolo con que actúa el sujeto activo del delito que destruya información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. Existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba o no con autorización. La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar el verbo núcleo de la conducta, ocurre en el

supuesto de que el sujeto activo tenga autorización para destruir información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

Se tiene en cuenta que para ser imputable se requiere la capacidad de querer y entender, teniendo en cuenta que para la acción realizada, como se mencionó antes la ejecuta una persona experta en el tema, es por ello por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis se da de forma dolosa, misma que nos ayuda a evidenciar la realización de la conducta.; en lo que respecta a la inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podría presentar una amenaza de un daño grave si no se realiza la conducta. Este delito se persigue de oficio, teniendo una sanción de seis meses a cuatro años de prisión y de cien a seiscientos días multa; no encontrando alguna excusa absoluta.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación, se esquematiza lo anteriormente explicado.

<b>Conducta</b>	La conducta es de acción, y es destruir información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.
<b>Ausencia de conducta</b>	Se puede dar la <i>vis absoluta</i> como de ausencia de conducta, es decir, una fuerza física superior e irresistible proveniente de otro hombre.

<b>Tipicidad</b>	La conducta está descrita en el artículo 211 bis 4 párrafo primero del Código Penal Federal. El tipo consta de elementos subjetivos, objetivos y normativos.	
	<b>Sujeto activo</b>	No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, educada en el tema.
	<b>Sujeto pasivo</b>	Las Instituciones que integran el sistema financiero.
	<b>Bien Jurídico Tutelado</b>	La seguridad de la información del sistema financiero.
	<b>Objeto jurídico</b>	Sistemas de informática
	<b>Elemento subjetivo del ilícito</b>	Está constituido por el dolo con que actúa el sujeto activo del delito que destruya información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.
	<b>Elemento normativo</b>	Que atente contra los equipos de informática.
<b>Atipicidad</b>	Que el sujeto activo cuente con autorización para destruir información contenida en equipos de informática protegidos por algún mecanismo de seguridad, y, al que sin autorización, destruya información contenida en equipos de informática que no esté protegida por algún mecanismo de seguridad.	
<b>Antijuridicidad</b>	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 4 párrafo primero del Código Penal Federal) y es contraria a la sociedad.	
<b>Causas de justificación</b>	No aplica.	

<b>Imputabilidad</b>	La capacidad de querer y entender.
<b>Inimputabilidad</b>	Se puede presentar que una persona no imputable realice la conducta, aunque sería poca la probabilidad.
<b>Culpabilidad</b>	Se puede dar únicamente de manera dolosa
<b>Inculpabilidad</b>	Se podría presentar la <i>vis compulsiva</i> o por obediencia jerárquica
<b>Condiciones objetivas de punibilidad</b>	Se persigue de oficio.
<b>Punibilidad</b>	De seis meses a cuatro años de prisión y de cien a seiscientos días multa.
<b>Excusas absolutorias</b>	No tiene excusas absolutorias.

***5. Provoque pérdida de información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.***

Como se puede observar, la conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “provoque pérdida”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, una fuerza física superior e irresistible proveniente de otro hombre.

De acuerdo con la tipicidad se debe dar el perfecto y cabal encuadramiento de la conducta al tipo penal, el cual es “provocar pérdida” de información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona experta en el tema que no esté autorizada para provocar pérdida de información, en lo que respecta al sujeto pasivo, podemos ver en el párrafo que refiere a las Instituciones que integran el sistema financiero.



El elemento objetivo refiere a quien comete el delito, es todo atentado que signifique dañar o desviar el correcto uso de la máquina con la finalidad de causar un perjuicio moral o material, para sí o para otro por el uso indebido de un sistema de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

El elemento subjetivo debe estar constituido por el dolo con que actúa el sujeto activo del delito que provoque pérdida de información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. Existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba o no con autorización. La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar el verbo núcleo de la conducta, ocurre en el supuesto de que el sujeto activo tenga autorización para provocar pérdida de información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

Se tiene en cuenta que para ser imputable se requiere la capacidad de querer y entender, teniendo en cuenta que para la acción realizada, como se mencionó antes la ejecuta una persona experta en el tema, es por ello por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis se da de forma dolosa, misma que nos ayuda a evidenciar la realización de la conducta.; en lo que respecta a la inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podía presentar una amenaza de un daño grave si no se realiza la conducta.

Este delito se persigue de oficio, teniendo una sanción de seis meses a cuatro años de prisión y de cien a seiscientos días multa; no encontrando alguna excusa absolutoria.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación se esquematiza lo anteriormente explicado.

<b>Conducta</b>	La conducta es de acción, y es provocar pérdida de información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.	
<b>Ausencia de conducta</b>	Se puede dar la <i>vis absoluta</i> como de ausencia de conducta, es decir, una fuerza física superior e irresistible proveniente de otro hombre.	
<b>Tipicidad</b>	La conducta está descrita en el artículo 211 bis 4 párrafo primero del Código Penal Federal. El tipo consta de elementos subjetivos, objetivos y normativos.	
	<b>Sujeto activo</b>	No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, educada en el tema.
	<b>Sujeto pasivo</b>	Las Instituciones que integran el sistema financiero.
	<b>Bien Jurídico Tutelado</b>	La seguridad de la información del sistema financiero.
	<b>Objeto jurídico</b>	Sistemas de informática

	<b>Elemento subjetivo del ilícito</b>	Está constituido por el dolo con que actúa el sujeto activo del delito que provoque pérdida de información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.
	<b>Elemento normativo</b>	Que atente contra los sistemas de informática.
<b>Atipicidad</b>	Que el sujeto activo cuente con autorización para provocar la pérdida de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad, y, al que sin autorización, provoque pérdida información contenida en sistemas de informática que no esté protegida por algún mecanismo de seguridad.	
<b>Antijuridicidad</b>	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 4 párrafo primero del Código Penal Federal) y es contraria a la sociedad.	
<b>Causas de justificación</b>	No aplica.	
<b>Imputabilidad</b>	La capacidad de querer y entender.	
<b>Inimputabilidad</b>	Se puede presentar que una persona no imputable realice la conducta, aunque sería poca la probabilidad.	
<b>Culpabilidad</b>	Se puede dar únicamente de manera dolosa	
<b>Inculpabilidad</b>	Se podría presentar la <i>vis compulsiva</i> o por obediencia jerárquica	
<b>Condiciones objetivas de punibilidad</b>	Se persigue de oficio.	
<b>Punibilidad</b>	De seis meses a cuatro años de prisión y de cien a seiscientos días multa.	

<b>Excusas absolutorias</b>	No tiene excusas absolutorias.
-----------------------------	--------------------------------

**6. Provoque pérdida de información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.**

Como se puede observar, la conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “provoque pérdida”, pudiéndose presentar una ausencia de conducta de tipo *vis absoluta*, una fuerza física superior e irresistible proveniente de otro hombre.

De acuerdo con la tipicidad se debe dar el perfecto y cabal encuadramiento de la conducta al tipo penal, el cual es “provocar pérdida” de información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. El tipo señalado consta de elementos objetivos, subjetivos y normativos; además no establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona experta en el tema que no esté autorizada para acceder a la información, en lo que respecta al sujeto pasivo, podemos ver en el párrafo que refiere a las Instituciones que integran el sistema financiero.

El elemento objetivo refiere a quien comete el delito, es todo atentado que signifique dañar o desviar el correcto uso de la máquina con la finalidad de causar un perjuicio moral o material, para sí o para otro por el uso indebido de un equipo de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

El elemento subjetivo debe estar constituido por el dolo con que actúa el sujeto activo del delito que provoque pérdida de información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad. Existe la necesidad de una valoración jurídico cultural, pues se tiene que verificar el elemento de si el sujeto activo contaba o no con autorización. La atipicidad se puede dar cuando falte alguno de los elementos

mencionados, pudiéndose no agotar el verbo núcleo de la conducta, ocurre en el supuesto de que el sujeto activo tenga autorización para provocar pérdida de información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

La antijuridicidad de esta conducta queda establecida al momento de estar tipificada, presentándose ésta de manera formal y material al constituir una transgresión a la norma dictada por el Estado y al ser contraria a la sociedad, no pudiéndose aplicar alguna causa de justificación.

Se tiene en cuenta que para ser imputable se requiere la capacidad de querer y entender, teniendo en cuenta que para la acción realizada, como se mencionó antes la ejecuta una persona experta en el tema, es por ello por lo que sería difícil encajar la imputabilidad en esta hipótesis.

La hipótesis se da de forma dolosa, misma que nos ayuda a evidenciar la realización de la conducta.; en lo que respecta a la inculpabilidad se puede considerar por dos razones, siendo la primera la *vis compulsiva*, y la segunda, por obediencia jerárquica, como la no exigibilidad de otra conducta, pues se podría presentar una amenaza de un daño grave si no se realiza la conducta.

Este delito se persigue de oficio, teniendo una sanción de seis meses a cuatro años de prisión y de cien a seiscientos días multa; no encontrando alguna excusa absolutoria.

Para una mejor comprensión del estudio dogmático de esta hipótesis, a continuación, se esquematiza lo anteriormente explicado.

<b>Conducta</b>	La conducta es de acción, y es provocar pérdida de información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.
<b>Ausencia de conducta</b>	Se puede dar la <i>vis absoluta</i> como de ausencia de conducta, es decir, una fuerza física superior e irresistible proveniente de otro hombre.

<b>Tipicidad</b>	<p>La conducta está descrita en el artículo 211 bis 4 párrafo primero del Código Penal Federal.</p> <p>El tipo consta de elementos subjetivos, objetivos y normativos.</p>	
	<b>Sujeto activo</b>	No establece alguna calidad específica para el sujeto activo pudiendo ser de esta forma cualquier persona, educada en el tema.
	<b>Sujeto pasivo</b>	Las Instituciones que integran el sistema financiero.
	<b>Bien Jurídico Tutelado</b>	La seguridad de la información del sistema financiero.
	<b>Objeto jurídico</b>	Sistemas de informática
	<b>Elemento subjetivo del ilícito</b>	Está constituido por el dolo con que actúa el sujeto activo del delito que provoque pérdida de información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.
	<b>Elemento normativo</b>	Que atente contra los equipos de informática.
<b>Atipicidad</b>	<p>Que el sujeto activo cuente con autorización de provocar pérdida de información contenida en sistemas de informática protegidos por algún mecanismo de seguridad, y, al que sin autorización, provoque pérdida de información contenida en sistemas de informática que no esté protegida por algún mecanismo de seguridad.</p>	
<b>Antijuridicidad</b>	<p>Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 4 párrafo primero del Código Penal Federal) y es contraria a la sociedad.</p>	

<b>Causas de justificación</b>	No aplica.
<b>Imputabilidad</b>	La capacidad de querer y entender.
<b>Inimputabilidad</b>	Se puede presentar que una persona no imputable realice la conducta, aunque sería poca la probabilidad.
<b>Culpabilidad</b>	Se puede dar únicamente de manera dolosa
<b>Inculpabilidad</b>	Se podría presentar la <i>vis compulsiva</i> o por obediencia jerárquica
<b>Condiciones objetivas de punibilidad</b>	Se persigue de oficio.
<b>Punibilidad</b>	De seis meses a cuatro años de prisión y de cien a seiscientos días multa.
<b>Excusas absolutorias</b>	No tiene excusas absolutorias.

#### **4.10 Conocer o copiar información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.**

El artículo 211 Bis 4 segundo párrafo del Código Penal Federal se establece lo siguiente:

“Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.”

Como podemos ver del párrafo anterior, se encuentran una serie de hipótesis, las cuales podemos ilustrar en estas:

<b>Acción del sujeto activo</b>	<b>Hipótesis</b>
Conozca	<ul style="list-style-type: none"> <li>● Información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.</li> <li>● Información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.</li> </ul>
Copie	<ul style="list-style-type: none"> <li>● Información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.</li> <li>● Información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.</li> </ul>

Total de Hipótesis previstas en el primer párrafo del Artículo 211 Bis 4 segundo párrafo del Código Penal Federal.

4
---

Para poder dar pie al análisis de este párrafo es indispensable que conozcamos la definición de los verbos utilizados, puesto que el artículo no nos los define. Todos los párrafos al describir la acción utilizan verbos núcleos como lo son en este caso “conocer” y “copiar”.



Comenzaré con el verbo “conocer” según el Diccionario de la Real Academia Española lo define como la acción de averiguar por el ejercicio de las facultades intelectuales la naturaleza, cualidades y relaciones de las cosas.

Por el verbo “copiar” el Diccionario de la Real Academia Española lo define como Escribir en una parte lo que está escrito en otra o reproducir textos, imágenes, sonidos u objetos.

**1. Conozca información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, sin autorización.**

Entendemos por sistema de informática como el conjunto constituido por los elementos físicos y lógicos (software) necesarios para captar información, almacenarla y procesarla.

La conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “conocer”, pudiéndose presentar una ausencia de conducta de tipo vis absoluta, la cual es la fuerza física superior e irresistible proveniente de otro hombre.

Es importante saber que respecta a la tipicidad, primero entendemos por tipicidad a la adecuación de una conducta concreta con la descripción legal formulada en abstracto, por lo que la conducta del sujeto activo debe ser de conocer la información, pero aquí nos encontramos con un tipo especial puesto que su única cualidad es que deberán ser sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

Así mismo la atipicidad la entendemos como la falta de adecuación de la conducta al tipo penal, es decir que solo nos bastará con que falte alguno de los elementos especificados en el párrafo para no corresponder con el tipo, como podría ser que la acción de conocer con autorización, si la información no se

encuentra contenida en sistemas de informática de las instituciones que integran el sistema financiero, o que estos no se encuentren protegidos por algún mecanismo de seguridad.

Este tipo tiene elementos objetivos, subjetivos y normativos, pero no establece ninguna calidad específica para el sujeto activo lo cual nos da a comprender que este hecho ilícito podría llevarse a cabo por cualquier persona.

Nuestro elemento objetivo de esta hipótesis sería todo aquel atentado que prevea conocer la información contenida en sistemas de informática de las instituciones con la finalidad de obtener un beneficio, ya sea material o inmaterial, moral, para si o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un sistema financiero protegidos por algún mecanismo de seguridad.

Como elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa en la conducta con la que actuará el sujeto activo que conoce la información contenida en sistemas de informática de las instituciones que integran el sistema financiero protegidos por algún mecanismo de seguridad.

Por otra parte, también es necesaria una valoración jurídico cultural, donde se verificará el elemento de si el sujeto activo contaba con autorización para llevar a cabo la conducta o no.

Dicha atipicidad de la hipótesis tiene 2 supuestos:

1. Que el sujeto activo cuente con autorización para conocer información contenida en los sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo.
2. Que el sujeto activo sin autorización conozca la información contenida en los sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo.

Podemos saber que esta conducta tiene antijuridicidad desde el momento en que se encuentra establecida y tipificada de manera formal y material, pues

esta es dictada por el Estado y es contraria a la sociedad, por lo que no es posible aplicar una causa de justificación para el sujeto activo, nuestro bien tutelado como bien se ha mencionado será la conservación de los sistemas de informática de las instituciones que integran el sistema financiero que se encuentren protegidos por algún mecanismo de seguridad, buscando el resguardo de la información y elementos contenidos en ellos.

Esta conducta deber ser realizada por una persona con capacidad de querer y entender, la conducta de esta requiere de una serie de conductas sofisticadas, con un determinado nivel de inteligencia y educación de carácter técnico y electrónico superior a lo común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

Esta hipótesis se da de forma dolosa o culposa, lo que nos ayuda a evidenciar la intención del sujeto activo en la ejecución de la conducta. La inculpabilidad se podría considerar por la razón de Vis compulsiva o por obediencia jerárquica, como la no exigibilidad de otra conducta, pues podría presentarse una amenaza con gravedad si no se realiza la conducta.

Este delito tiene una sanción de tres meses a dos años de prisión y de cincuenta a trescientos días multa, también es importante decir que este se persigue por oficio es decir el Estado tendrá la obligación de perseguirlo, por lo que no tiene ninguna excusa absolutoria.

A continuación, podremos analizar en esquema y de mejor manera el estudio dogmático de esta hipótesis.

**Conducta** { La conducta es de acción que sin autorización se conoce la información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

**Ausencia de conducta** { Podríamos hablar de la vis absoluta como ausencia de conducta

**Tipicidad** { La conducta está descrita en el artículo 211 bis 4 segundo párrafo del Código Penal Federal.

El tipo consta de elementos subjetivos, objetivos y normativos.

**Sujeto activo** { No se establece ninguna cualidad específica del sujeto activo, por lo que podría ser cualquier persona

**Sujeto pasivo** { Las instituciones que integran el sistema financiero pertenecientes de los sistemas

**Bien Jurídico Tutelado** { La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica y la información o datos contenida en ellos.

**Objeto jurídico** { La confidencialidad, integridad y disponibilidad

**Elemento subjetivo del ilícito** { Que el sujeto actúe con dolo o culpa mientras conoce la información contenida en los sistemas.

**Elemento normativo** { Que atente contra la integridad de la información de los sistemas.

### **Atipicidad**

{ Podríamos presentar hipótesis las cuales serían, si se tiene la autorización, si la información no se encuentra protegida por algún mecanismo de seguridad, si no pertenece a alguna institución que integre el sistema financiero, si no se conoce información contenida en sistemas de informática y por ende no correspondería al tipo descrito en el artículo 211 Bis 4 segundo párrafo.

### **Antijuridicidad**

{ Cuenta con la formal y material ya que la conducta transgrede

<b>ad</b>	una norma dictada por el Estado (art. 211 bis 4 segundo párrafo del Código Penal Federal) y es contraria a la sociedad.
<b>Causas de justificación</b>	{ No se puede aplicar ninguna.
<b>Imputabilidad</b>	{ La capacidad de querer y entender.
<b>Inimputabilidad</b>	{ Si el sujeto activo es no imputable
<b>Culpabilidad</b>	{ Se puede dar únicamente de manera dolosa o culposa.
<b>Inculpabilidad</b>	{ Por vis compulsiva o por obediencia jerárquica.
<b>Condiciones objetivas de punibilidad</b>	{ Se persigue por oficio.
<b>Punibilidad</b>	{ De tres meses a dos años de prisión y de cincuenta a trescientos días multa.
<b>Excusas absolutorias</b>	{ No tiene.

## **2. Conozca información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, sin autorización.**

Entendemos por equipos de informática a los distintos dispositivos electrónicos que permiten la ejecución de programas informáticos, como podrían ser una computadora.

La conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “conocer”, pudiéndose presentar una ausencia de conducta de tipo vis absoluta, la cual es la fuerza física superior e irresistible proveniente de otro hombre.

Referente a la tipicidad, primero entendemos por tipicidad a la adecuación de una conducta concreta con la descripción legal formulada en abstracto, por lo que la conducta del sujeto activo deberá encuadrar exactamente con el tipo penal, que es conocer la información, pero aquí nos encontramos con un tipo especial puesto que su única cualidad es que deberán ser equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

Así mismo la atipicidad la entendemos como la falta de adecuación de la conducta al tipo penal, es decir que solo nos bastará con que falte alguno de los elementos especificados en el párrafo para no corresponder con el tipo, como podría ser que la acción de conocer con autorización, si la información no se encuentra contenida en equipos de informática de las instituciones que integran el sistema financiero, o que estos no se encuentren protegidos por algún mecanismo de seguridad.

Este tipo tiene elementos objetivos, subjetivos y normativos, pero no establece ninguna calidad específica para el sujeto activo lo cual nos da a comprender que este hecho ilícito podría llevarse a cabo por cualquier persona.

Nuestro elemento objetivo de esta hipótesis sería todo aquel atentado que prevea conocer la información contenida en equipos de informática de las instituciones con la finalidad de obtener un beneficio, ya sea material o inmaterial, moral, para si o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un sistema financiero protegidos por algún mecanismo de seguridad.

Como elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa en la conducta con la que actuará el sujeto activo que conoce la información contenida en equipos de informática de las instituciones que integran el sistema financiero protegidos por algún mecanismo de seguridad.

También es necesaria hacer una valoración jurídico cultural, pues se tendrá que verificar el elemento de si el sujeto activo contaba con autorización para llevar a cabo la conducta o no.

Dicha atipicidad de la hipótesis tiene 2 supuestos:

1. Que el sujeto activo cuente con autorización para conocer información contenida en los equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo.
2. Que el sujeto activo sin autorización conozca la información contenida en los equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo.

Podemos saber que esta conducta tiene antijuridicidad desde el momento en que se encuentra establecida y tipificada de manera formal y material, pues esta es dictada por el Estado y es contraria a la sociedad, por lo que no es posible aplicar una causa de justificación para el sujeto activo, nuestro bien tutelado como bien se ha mencionado será la conservación de los equipos de informática de las instituciones que integran el sistema financiero que se encuentren protegidos por algún mecanismo de seguridad, buscando el resguardo de la información y elementos contenidos en ellos.

Esta conducta deber ser realizada por una persona con capacidad de querer y entender, la conducta de esta requiere de una serie de conductas sofisticadas, con un determinado nivel de inteligencia y educación de carácter técnico y electrónico superior a lo común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

Esta hipótesis se da de forma dolosa o culposa, lo que nos ayuda a evidenciar la intención del sujeto activo en la ejecución de la conducta. La inculpabilidad se podría considerar por la razón de Vis compulsiva o por obediencia jerárquica, como la no exigibilidad de otra conducta, pues podría presentarse una amenaza con gravedad si no se realiza la conducta.

Este delito se persigue de oficio y tiene una sanción de tres meses a dos años de prisión y de cincuenta a trescientos días multa, por lo que no tiene ninguna excusa absolutoria.

Para una mejor comprensión, podremos analizar en esquema el estudio dogmático de esta hipótesis.

<b>Conducta</b>	{	La conducta es de acción que sin autorización se conoce la información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.
<b>Ausencia de conducta</b>	{	Podríamos hablar de la vis absoluta como ausencia de conducta
<b>Tipicidad</b>	{	<p>La conducta está descrita en el artículo 211 bis 4 segundo párrafo del Código Penal Federal.</p> <p>El tipo consta de elementos subjetivos, objetivos y normativos.</p>
	{	<p><b>Sujeto activo</b> { No se establece ninguna cualidad específica del sujeto activo, por lo que podría ser cualquier persona</p>
	{	<p><b>Sujeto pasivo</b> { Las instituciones que integran el sistema financiero a los que les pertenecen los equipos</p>
	{	<p><b>Bien Jurídico Tutelado</b> { La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica y la información o datos contenida en ellos.</p>
	{	<p><b>Objeto jurídico</b> { La confidencialidad, integridad y disponibilidad</p>



**Elemento subjetivo del ilícito** { Que el sujeto actúe con dolo o culpa mientras conoce la información contenida en los equipos.

**Elemento normativo** { Que atente contra la integridad de la información de los equipos.

**Atipicidad** { Podríamos presentar hipótesis las cuales serían, si se tiene la autorización, si la información no se encuentra protegida por algún mecanismo de seguridad, si no pertenece a alguna institución que integre el sistema financiero, si no se conoce información contenida en los equipos de informática y por ende no correspondería al tipo descrito en el artículo 211 Bis 4 segundo párrado.

**Antijuridicidad** { Cuenta con la formal y material ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 4 segundo párrafo del Código Penal Federal) y es contraria a la sociedad.

**Causas de justificación** { No se puede aplicar ninguna.

**Imputabilidad** { La capacidad de querer y entender.

**Inimputabilidad** { Si el sujeto activo es no imputable

**Culpabilidad** { Se puede dar únicamente de manera dolosa o culposa.

**Inculpadad** { Por vis compulsiva o por obediencia jerárquica.

**Condiciones objetivas de punibilidad** { Se persigue por oficio.

<b>Punibilidad</b>	{ De tres meses a dos años de prisión y de cincuenta a trescientos días multa.
<b>Excusas absolutorias</b>	{ No tiene.

### **3. Copie información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, sin autorización.**

La conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “copiar”, pudiéndose presentar una ausencia de conducta de tipo vis absoluta, la cual es la fuerza física superior e irresistible proveniente de otro hombre.

Referente a lo que respecta a la tipicidad, se debe dar el exacto encuadramiento de la conducta del sujeto activo respecto al tipo penal, debe copiar la información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

Así mismo la atipicidad la entendemos como la falta de adecuación de la conducta al tipo penal, es decir que solo nos bastará con que falte alguno de los elementos especificados en el párrafo para no corresponder con el tipo, como podría ser que la acción de copiar con autorización, si la información no se encuentra contenida en sistemas de informática de las instituciones que integran el sistema financiero, o que estos no se encuentren protegidos por algún mecanismo de seguridad.

Este tipo tiene elementos objetivos, subjetivos y normativos, pero no establece ninguna calidad específica para el sujeto activo lo cual nos da a comprender que este hecho ilícito podría llevarse a cabo por cualquier persona.

Nuestro elemento objetivo de esta hipótesis sería todo aquel atentado que prevea copiar la información contenida en sistemas de informática de las instituciones con la finalidad de obtener un beneficio, ya sea material o inmaterial, moral, para si o para un tercero, esto derivado un perjuicio causado al sujeto

pasivo, por el uso indebido de un sistema financiero protegidos por algún mecanismo de seguridad.

Como elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa en la conducta con la que actuará el sujeto activo que copia la información contenida en sistemas de informática de las instituciones que integran el sistema financiero protegidos por algún mecanismo de seguridad.

Por otra parte, también es necesaria una valoración jurídico cultural, donde se verificará el elemento de si el sujeto activo contaba con autorización para llevar a cabo la conducta o no.

Dicha atipicidad de la hipótesis tiene 2 supuestos:

1. Que el sujeto activo cuente con autorización para copiar la información contenida en los sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo.
2. Que el sujeto activo sin autorización copie la información contenida en los sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo.

La antijuridicidad de esta conducta queda establecida desde el momento en que está tipificada de manera formal y material, pues esta es dictada por el Estado y es contraria a la sociedad, por lo que no es posible aplicar una causa de justificación para el sujeto activo, nuestro bien tutelado como bien se ha mencionado será la conservación de los sistemas de informática de las instituciones que integran el sistema financiero que se encuentren protegidos por algún mecanismo de seguridad, buscando el resguardo de la información y elementos contenidos en ellos.

Esta conducta deber ser realizada por una persona con capacidad de querer y entender, la conducta de esta requiere de una serie de conductas sofisticadas, con un determinado nivel de inteligencia y educación de carácter técnico y electrónico superior a lo común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

Esta hipótesis se da de forma dolosa o culposa, lo que nos ayuda a evidenciar la intención del sujeto activo en la ejecución de la conducta. La inculpabilidad se podría considerar por la razón de Vis compulsiva o por obediencia jerárquica, como la no exigibilidad de otra conducta, pues podría presentarse una amenaza con gravedad si no se realiza la conducta.

Este delito tiene una sanción de tres meses a dos años de prisión y de cincuenta a trescientos días multa, también es importante decir que este se persigue por oficio es decir el Estado tendrá la obligación de perseguirlo, por lo que no tiene ninguna excusa absolutoria.

A continuación, podremos analizar en esquema y de mejor manera el estudio dogmático de esta hipótesis.

<b>Conducta</b>	{	La conducta es de acción que sin autorización se copie la información contenida en sistemas de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.									
<b>Ausencia de conducta</b>	{	Podríamos hablar de la vis absoluta como ausencia de conducta									
<b>Tipicidad</b>	{	<p>La conducta está descrita en el artículo 211 bis 4 segundo párrafo del Código Penal Federal.</p> <p>El tipo consta de elementos subjetivos, objetivos y normativos.</p> <table border="0" style="margin-left: 20px;"> <tr> <td style="vertical-align: middle;"><b>Sujeto activo</b></td> <td style="font-size: 3em; vertical-align: middle;">{</td> <td>No se establece ninguna cualidad específica del sujeto activo, por lo que podría ser cualquier persona</td> </tr> <tr> <td style="vertical-align: middle;"><b>Sujeto pasivo</b></td> <td style="font-size: 3em; vertical-align: middle;">{</td> <td>Las instituciones que integran el sistema financiero pertenecientes de los sistemas</td> </tr> <tr> <td style="vertical-align: middle;"><b>Bien Tutelado</b></td> <td style="font-size: 3em; vertical-align: middle;">{</td> <td>La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación</td> </tr> </table>	<b>Sujeto activo</b>	{	No se establece ninguna cualidad específica del sujeto activo, por lo que podría ser cualquier persona	<b>Sujeto pasivo</b>	{	Las instituciones que integran el sistema financiero pertenecientes de los sistemas	<b>Bien Tutelado</b>	{	La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación
<b>Sujeto activo</b>	{	No se establece ninguna cualidad específica del sujeto activo, por lo que podría ser cualquier persona									
<b>Sujeto pasivo</b>	{	Las instituciones que integran el sistema financiero pertenecientes de los sistemas									
<b>Bien Tutelado</b>	{	La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación									

		electrónica y la información o datos contenida en ellos.
	<b>Objeto jurídico</b>	{ La confidencialidad, integridad y disponibilidad
	<b>Elemento subjetivo del ilícito</b>	{ Que el sujeto actúe con dolo o culpa mientras copie la información contenida en los sistemas.
	<b>Elemento normativo</b>	{ Que atente contra la integridad de la información de los sistemas.
<b>Atipicidad</b>	{	Podríamos presentar hipótesis las cuales serían, si se tiene la autorización, si la información no se encuentra protegida por algún mecanismo de seguridad, si no pertenece a alguna institución que integre el sistema financiero, si no se copie la información contenida en sistemas de informática y por ende no correspondería al tipo descrito en el artículo 211 Bis 4 segundo párrafo.
<b>Antijuridicidad</b>	{	Cuenta con la formal y material ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 4 segundo párrafo del Código Penal Federal) y es contraria a la sociedad.
<b>Causas de justificación</b>	{	No se puede aplicar ninguna.
<b>Imputabilidad</b>	{	La capacidad de querer y entender.
<b>Inimputabilidad</b>	{	Si el sujeto activo es no imputable
<b>Culpabilidad</b>	{	Se puede dar únicamente de manera dolosa o culposa.
<b>Inculpabilidad</b>	{	Por vis compulsiva o por obediencia jerárquica.

**ad**

**Condiciones  
objetivas de  
punibilidad** { Se persigue por oficio.

**Punibilidad** { De tres meses a dos años de prisión y de cincuenta a trescientos días multa.

**Excusas  
absolutorias** { No tiene.

**4. Copie información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, sin autorización.**

La conducta que se denota en esta hipótesis es de acción, cuyo verbo núcleo es “copiar”, pudiéndose presentar una ausencia de conducta de tipo vis absoluta, la cual es la fuerza física superior e irresistible proveniente de otro hombre.

Referente a la tipicidad, se debe cumplir con lo establecido de la conducta respecto al tipo penal, que es el “copiar la información” contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.

Así mismo la atipicidad la entendemos como la falta de adecuación de la conducta al tipo penal, es decir que solo nos bastará con que falte alguno de los elementos especificados en el párrafo para no corresponder con el tipo, como podría ser que la acción de copiar con autorización, si la información no se encuentra contenida en equipos de informática de las instituciones que integran el sistema financiero, o que estos no se encuentren protegidos por algún mecanismo de seguridad.

Este tipo tiene elementos objetivos, subjetivos y normativos, pero no establece ninguna calidad específica para el sujeto activo lo cual nos da a comprender que este hecho ilícito podría llevarse a cabo por cualquier persona.

El elemento objetivo de esta hipótesis sería todo aquel atentado que prevea copiar la información contenida en equipos de informática de las instituciones con la finalidad de obtener un beneficio, ya sea material o inmaterial, moral, para si o para un tercero, esto derivado un perjuicio causado al sujeto pasivo, por el uso indebido de un sistema financiero protegidos por algún mecanismo de seguridad.

Como elemento subjetivo de la hipótesis debe estar constituido por el dolo o la culpa en la conducta con la que actuará el sujeto activo que copie la información contenida en equipos de informática de las instituciones que integran el sistema financiero protegidos por algún mecanismo de seguridad.

También es necesaria hacer una valoración jurídico cultural, pues se tendrá que verificar el elemento de si el sujeto activo contaba con autorización para llevar a cabo la conducta o no.

Dicha atipicidad de la hipótesis tiene 2 supuestos:

1. Que el sujeto activo cuente con autorización para copiar información contenida en los equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo.
2. Que el sujeto activo sin autorización copie la información contenida en los equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo.

Podemos saber que esta conducta tiene antijuridicidad desde el momento en que se encuentra establecida y tipificada de manera formal y material, pues esta es dictada por el Estado y es contraria a la sociedad, por lo que no es posible aplicar una causa de justificación para el sujeto activo, nuestro bien tutelado como

bien se ha mencionado será la conservación de los equipos de informática de las instituciones que integran el sistema financiero que se encuentren protegidos por algún mecanismo de seguridad, buscando el resguardo de la información y elementos contenidos en ellos.

Esta conducta deber ser realizada por una persona con capacidad de querer y entender, la conducta de esta requiere de una serie de conductas sofisticadas, con un determinado nivel de inteligencia y educación de carácter técnico y electrónico superior a lo común, por lo que sería difícil encajar la imputabilidad en esta hipótesis.

Esta hipótesis se da de forma dolosa o culposa, lo que nos ayuda a evidenciar la intención del sujeto activo en la ejecución de la conducta. La inculpabilidad se podría considerar por la razón de Vis compulsiva o por obediencia jerárquica, como la no exigibilidad de otra conducta, pues podría presentarse una amenaza con gravedad si no se realiza la conducta.

Este delito se persigue de oficio y tiene una sanción de tres meses a dos años de prisión y de cincuenta a trescientos días multa, por lo que no tiene ninguna excusa absolutoria.

Para una mejor comprensión, podremos analizar en esquema el estudio dogmático de esta hipótesis.

<b>Conducta</b>	{	La conducta es de acción que sin autorización copie la información contenida en equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad.
<b>Ausencia de conducta</b>	{	Podríamos hablar de la vis absoluta como ausencia de conducta



	<p>La conducta está descrita en el artículo 211 bis 4 segundo párrafo del Código Penal Federal.</p> <p>El tipo consta de elementos subjetivos, objetivos y normativos.</p>	
	<b>Sujeto activo</b>	<p>No se establece ninguna cualidad específica del sujeto activo, por lo que podría ser cualquier persona</p>
	<b>Sujeto pasivo</b>	<p>Las instituciones que integran el sistema financiero a los que les pertenecen los equipos</p>
<b>Tipicidad</b>	<b>Bien Jurídico Tutelado</b>	<p>La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica y la información o datos contenida en ellos.</p>
	<b>Objeto jurídico</b>	<p>La confidencialidad, integridad y disponibilidad</p>
	<b>Elemento subjetivo del ilícito</b>	<p>Que el sujeto actúe con dolo o culpa mientras copie la información contenida en los equipos.</p>
	<b>Elemento normativo</b>	<p>Que atente contra la integridad de la información de los equipos.</p>
<b>Atipicidad</b>	<p>Podríamos presentar hipótesis las cuales serían, si se tiene la autorización, si la información no se encuentra protegida por algún mecanismo de seguridad, si no pertenece a alguna institución que integre el sistema financiero, si no se copia la información contenida en los equipos de informática y por ende no correspondería al tipo descrito en el artículo 211 Bis 4</p>	

segundo párrafo.

<b>Antijuridicidad</b>	{ Cuenta con la formal y material ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 4 segundo párrafo del Código Penal Federal) y es contraria a la sociedad.
<b>Causas de justificación</b>	{ No se puede aplicar ninguna.
<b>Imputabilidad</b>	{ La capacidad de querer y entender.
<b>Inimputabilidad</b>	{ Si el sujeto activo es no imputable
<b>Culpabilidad</b>	{ Se puede dar únicamente de manera dolosa o culposa.
<b>Inculpadad</b>	{ Por vis compulsiva o por obediencia jerárquica.
<b>Condiciones objetivas de punibilidad</b>	{ Se persigue por oficio.
<b>Punibilidad</b>	{ De tres meses a dos años de prisión y de cincuenta a trescientos días multa.
<b>Excusas absolutorias</b>	{ No tiene.

**4.11 Estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan.**

Artículo 211 Bis 5 Párrafo 1:

“Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque

pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.”

El artículo en su totalidad cuenta con 3 párrafos en los que se dan a conocer la calidad específica de los sujetos, las hipótesis y la punibilidad. Sin embargo, en este apartado solo compete el primer párrafo por lo que el estudio será solo de:

CALIDAD ESPECÍFICA DEL SUJETO PASIVO	HIPÓTESIS	
INSTITUCIÓN DEL SISTEMA FINANCIERO	<ul style="list-style-type: none"> <li>• <b>Modificar.</b></li> <li>• <b>Destruir.</b></li> <li>• <b>Provocar perdida.</b></li> </ul>	
TOTAL DE HIPÓTESIS PREVISTAS EN EL ARTÍCULO 211 BIS 5, PÁRRAFO PRIMERO DEL CÓDIGO PENAL FEDERAL.		<b>3</b>

Como se logra apreciar, en el párrafo correspondiente y a su vez resaltado, sólo se pueden identificar un sujeto pasivo, tres hipótesis correspondientes y las características del sujeto activo, por lo tanto, es imperativo el detenerse a desarrollar las hipótesis; siguiendo el orden correspondiente se dividirá en párrafo por partes y así obtener de mejor manera cada punto tocado en la redacción del artículo.

1. El antes mencionado se desarrolla de la siguiente manera: “**Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique**

[...]" ; desde este apartado se puede retomar tanto al sujeto pasivo como el primer verbo núcleo.

En el párrafo del artículo se encuentra el verbo núcleo "modificar", esto no alcanza por sí mismo para entender el ilícito, por lo que va acompañado de "datos", ahora bien, si se juntan ambos quedaría "modificar los datos contenidos" que sería el primer supuesto ilícito al que se refiere el párrafo y una vez con el primer verbo núcleo bien delimitado se pueden llegar a las siguientes conclusiones; en primera no puede haber ausencia de conducta ya que se trata de un hecho de acción para ser concebido; después, no hay cabida al apercibimiento de los movimientos reflejo pues para llevar a cabo el hecho es necesario estar consiente del acto, así mismo, no se puede pensar en que el hecho es resultado de una fuerza física superior e irresistible proveniente de la naturaleza o de otro ser humano.

En cuanto a la tipicidad, se debe de hacer un perfecto encuadramiento en la acción precisa que es el "modificar", y a su vez, se le podría encuadrar en las modalidades de la conducta que son el dolo y la preterintencionalidad, exceptuando la culpa puesto que este no permite la culpa por las cualidades que debe de tener el sujeto activo. Con respecto a las cualidades del sujeto activo me basare a lo que expresa el licenciado Lucerito Ludmila Flores Salgado en su libro sobre Derecho Informático en el cual se plantea lo siguiente:

***"Tocante al sujeto activo de los delitos informáticos se ha observado que por lo general son personas de un determinado nivel de inteligencia y educación, superior al común, mismos que pueden ser los programadores que violan o inutilizan controles protectores del programa o sistema, los analistas de sistemas que generalmente son los únicos que conocen la operación completa de ellos; los analistas de comunicaciones que diseñan la seguridad del sistema de comunicaciones, supervisores que tienen conocimiento integral de las operaciones y debilidades del sistema de seguridad; personal técnico y de mantenimiento, que suele tener libre acceso a los centros de cómputo y conoce los sistemas operativos y bases de datos; etcétera."***

De acuerdo a lo antes planteado se entiende que la calidad del sujeto activo no es general pues debe de contar con características específicas como lo son la “educación superior”, “inteligencia”, ser un “programador”, “analista de sistemas”, “supervisores”, etcétera; sin embargo, se entiende por la formula del artículo que cualquier persona “autorizada” por lo que se caracterizaría por ser un delito de cuello blanco y esto determina que no puede ser cualquier persona.

Ahora bien, en cuanto al sujeto pasivo se entiende que es aquella institución que cuente con la característica de ser parte del sistema financiero, esto delimita la calidad específica del sujeto a todas aquellas instituciones que están reguladas por la secretaria de Hacienda y Crédito Público de acuerdo con el artículo 400 Bis. La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar el verbo núcleo de la conducta o no cubrir el elemento subjetivo del ilícito.

Con respecto a la antijuricidad se entiende que cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 Bis 5 fr. I del Código Penal Federal) y es contraria a la sociedad.

Así también en cuanto a las causas de justificación no hay alguna forma de que se presente puesto que no hay forma alguna de que mediante el cumplimiento de un deber o el ejercicio de un derecho se realice el acto, así como tampoco se podría dar el consentimiento del titular, siendo específico ya que en el artículo se menciona que el sujeto cuenta con el consentimiento para tener acceso, sin embargo, no puede disponer del bien jurídico que en este aspecto es la información pues no está legitimado por no ser dueño del bien y mucho menos tiene la capacidad jurídica como lo plantea el artículo 29 del Código Penal Federal. Este delito es perseguido por la Secretaria de Hacienda y Crédito Público con una denuncia previa para después proceder legalmente ante el ámbito penal, esto de acuerdo con el artículo 211 Bis 6 y el artículo 400 Bis del Código Penal Federal.

Todo lo explicado queda sintetizado de la siguiente manera.

**CONDUCTA**        { La conducta es de modificar los datos contenidos.

**AUSENCIA DE CONDUCTA**    { No se puede dar ninguna de las formas de ausencia de conducta.

		<p>La conducta está descrita en el artículo 211 Bis 5, párrafo primero del Código Penal Federal.</p> <p>El tipo consta de elementos subjetivos, objetivos y normativos.</p>
<b>TIPICIDAD</b>	<b>SUJETO ACTIVO</b>	<p>Se establece que debe ser una persona autorizada y al ser un delito de cuello blanco se entiende que hay características específicas del sujeto activo.</p>
	<b>SUJETO PASIVO</b>	<p>Solo se especifica que debe de ser una institución del sistema financiero mexicano.</p>
	<b>BIEN JURÍDICO TUTELADO</b>	<p>La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.</p>
	<b>OBJETO JURÍDICO</b>	<p>{ La información.</p>
	<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	<p>{ Que tenga por objeto el sacar provecho del acto mediante el dolo.</p>
	<b>ATIPICIDAD</b>	<p>{ Se puede presentar si llega a faltar algún elemento del tipo penal, por lo que podría existir la ausencia de los objetos jurídico y material, así como la del elemento subjetivo del ilícito.</p>
<b>ANTI JURIDICIDAD</b>	<p>{ Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 Bis 5 fr. I del Código Penal Federal) y es contraria a la sociedad.</p>	
<b>CAUSAS DE JUSTIFICACIÓN</b>	<p>{ No hay causas de justificación alguna que encuadre en este aspecto.</p>	
<b>IMPUTABILIDAD</b>	<p>{ La capacidad de querer y entender.</p>	
<b>INIMPUTABILIDAD</b>	<p>{ Se puede presentar que una persona no imputable realice la</p>	

AD	conducta, así como también sé de qué una persona lo realice de manera culposa.
CULPABILIDAD	{ Se puede dar de manera dolosa y culposa.
INCULPABILIDAD	{ Se podría presentar la <i>vis compulsiva o la obediencia jerárquica</i> .
CONDICIONES OBJETIVAS DE PUNIBILIDAD	{ Se persigue después de presentarse una demanda previa por la Secretaria de Hacienda.
PUNIBILIDAD	{ De seis meses a cuatro años de prisión y de cien a seiscientos días multa.
EXCUSAS ABSOLUTORIAS	{ <b>No cuenta con excusas absolutorias.</b>

Ahora bien, en cuanto a la segunda hipótesis ***“Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya [...]”***; con esta nueva parte integrada se nota directamente el verbo núcleo que en su caso sería “destruir”, pero para ser entendido es imperativo el que se complemente con “datos” pues queda especificado en el mismo párrafo que solo engloba los datos, no hardware o software.

Al ser esto una acción queda excluida la idea de una ausencia en la conducta pues no se puede presentar la vis mayor o vis absoluta pues es inconcebible que por causas ajenas al sujeto activo este mismo realice la acción de destruir información proveniente al sistema financiero.

En lo que respecta a la tipicidad se debe dar el exacto encuadramiento de la conducta al tipo, el cual contiene la conducta de destruir datos del sistema financiero, entendiéndose que los datos, sin importar la importancia de los mismos, están protegidos por el código protegiendo el derecho a la protección, valga la redundancia, de los datos propios o ajenos.

El tipo señalado consta de elementos objetivos, subjetivos y normativo, no estableciéndose ninguna modalidad de la conducta y en cuanto a la calidad

específica del sujeto activo se presenta el mismo caso que en la primera hipótesis, debe de contar con las siguientes características: **“son personas de un determinado nivel de inteligencia y educación, superior al común, mismos que pueden ser los programadores que violan o inutilizan controles protectores del programa o sistema, los analistas de sistemas que generalmente son los únicos que conocen la operación completa de ellos; los analistas de comunicaciones que diseñan la seguridad del sistema de comunicaciones, supervisores que tienen conocimiento integral de las operaciones y debilidades del sistema de seguridad; personal técnico y de mantenimiento, que suele tener libre acceso a los centros de cómputo y conoce los sistemas operativos y bases de datos; etcétera.”**; así también se entiende que son personas con autorización por lo que pueden ser cualquiera con acceso y con autorización con las capacidades antes mencionadas sería el sujeto activo.

También, en cuestión del sujeto pasivo pasa lo mismo, ya que como se entiende en el primer desarrollo de la hipótesis primera es que son aquellas instituciones dentro del sistema financiero mexicano.

La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar el verbo núcleo de la conducta o no cubrir el elemento subjetivo del ilícito.

Este delito es perseguido por la Secretaría de Hacienda y Crédito Público con una denuncia previa para después proceder legalmente ante el ámbito penal, esto de acuerdo con el artículo 211 Bis 6 y el artículo 400 Bis del CPF.

A continuación, se sintetiza lo presentado en los párrafos anteriores:

<b>CONDUCTA</b>	{	La conducta es de destruir los datos contenidos.
<b>AUSENCIA DE CONDUCTA</b>	{	No se puede dar ninguna de las formas de ausencia de conducta.
<b>TIPICIDAD</b>	{	La conducta está descrita en el artículo 211 Bis 5, párrafo primero del Código Penal Federal. El tipo consta de elementos subjetivos, objetivos y normativos.



		Se establece que debe ser una persona autorizada y al ser un delito de cuello
	<b>SUJETO ACTIVO</b>	{ blanco se entiende que hay características específicas del sujeto activo.
	<b>SUJETO PASIVO</b>	{ Solo se especifica que debe de ser una institución del sistema financiero mexicano.
	<b>BIEN JURÍDICO TUTELADO</b>	{ La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
	<b>OBJETO JURÍDICO</b>	{ La información.
	<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	{ Que tenga por objeto el sacar provecho del acto mediante el dolo.
<b>ATIPICIDAD</b>	{	Se puede presentar si llega a faltar algún elemento del tipo penal, por lo que podría existir la ausencia de los objetos jurídico y material, así como la del elemento subjetivo del ilícito.
<b>ANTI JURIDICIDAD</b>	{	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 Bis 5 fr. I del Código Penal Federal) y es contraria a la sociedad.
<b>CAUSAS DE JUSTIFICACIÓN</b>	{	No hay causas de justificación alguna que encuadre en este aspecto.
<b>IMPUTABILIDAD</b>	{	La capacidad de querer y entender.
<b>INIMPUTABILIDAD</b>	{	Se puede presentar que una persona no imputable realice la conducta, así como también sé de qué una persona lo realice de manera culposa.

<b>CULPABILIDAD</b>	{ Se puede dar de manera dolosa y culposa.
<b>INCULPABILIDAD</b>	{ Se podría presentar la <i>vis compulsiva o la obediencia jerárquica</i> .
<b>CONDICIONES OBJETIVAS DE PUNIBILIDAD</b>	{ Se persigue después de presentarse una demanda previa por la Secretaria de Hacienda.
<b>PUNIBILIDAD</b>	{ De seis meses a cuatro años de prisión y de cien a seiscientos días multa.
<b>EXCUSAS ABSOLUTORIAS</b>	{ <b>No cuenta con excusas absolutorias.</b>

Por último, el presupuesto que se presenta a continuación: ***“Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información [...]”***; ahora bien, el verbo núcleo es “provocar”, pero por sí mismo no se entiende, por lo tanto es necesario agregar lo demás del supuesto que es “pérdida de información”; en esta caso sí se entiende el verbo que es “provocar la pérdida de información”.

Al ser esto una acción queda excluida la idea de una ausencia en la conducta pues no se puede presentar la *vis mayor* o *vis absoluta* pues es inconcebible que por causas ajenas al sujeto activo este mismo realice la acción de provocar la pérdida de información que sea proveniente al sistema financiero.

Como ya se mencionó anteriormente, en lo que respecta a la tipicidad se debe dar el exacto encuadramiento de la conducta al tipo, el cual contiene la conducta de provocar pérdida de información correspondiente al sistema financiero, entendiéndose que los datos, sin importar la importancia de los mismos, están protegidos por el código protegiendo el derecho a la protección, valga la redundancia, de los datos propios o ajenos.

El tipo señalado consta de elementos objetivos, subjetivos y normativo, no estableciéndose ninguna modalidad de la conducta y en cuanto a la calidad específica del sujeto activo se presenta las mismas características que en las

hipótesis anteriores, por lo que se entiende que debe de contar con las siguientes calidades: **“son personas de un determinado nivel de inteligencia y educación, superior al común, mismos que pueden ser los programadores que violan o inutilizan controles protectores del programa o sistema, los analistas de sistemas que generalmente son los únicos que conocen la operación completa de ellos; los analistas de comunicaciones que diseñan la seguridad del sistema de comunicaciones, supervisores que tienen conocimiento integral de las operaciones y debilidades del sistema de seguridad; personal técnico y de mantenimiento, que suele tener libre acceso a los centros de cómputo y conoce los sistemas operativos y bases de datos; etcétera.”**; así también se entiende que son personas con autorización por lo que pueden ser cualquiera con acceso y con autorización con las capacidades antes mencionadas sería el sujeto activo.

También, en cuestión del sujeto pasivo pasa lo mismo, son aquellas instituciones dentro del sistema financiero mexicano que son reguladas por la Secretaria de Hacienda y Crédito Público.

La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar el verbo núcleo de la conducta o no cubrir el elemento subjetivo del ilícito.

Este delito es perseguido por la Secretaria de Hacienda y Crédito Público con una denuncia previa para después proceder legalmente ante el ámbito penal, esto de acuerdo con el artículo 211 Bis 6 y el artículo 400 Bis del CPF.

Y para terminar con el estudio dogmático la sinterización de esta última hipótesis:

<b>CONDUCTA</b>	{ La conducta es de provocar la pérdida de la información contenida.
<b>AUSENCIA DE CONDUCTA</b>	{ No se puede dar ninguna de las formas de ausencia de conducta.

<b>TIPICIDAD</b>	{	La conducta está descrita en el artículo 211 Bis 5, párrafo primero del Código Penal Federal.	
		El tipo consta de elementos subjetivos, objetivos y normativos.	
		<b>SUJETO ACTIVO</b>	Se establece que debe ser una persona autorizada y al ser un delito de cuello blanco se entiende que hay características específicas del sujeto activo.
		<b>SUJETO PASIVO</b>	Solo se especifica que debe de ser una institución del sistema financiero mexicano.
		<b>BIEN JURÍDICO TUTELADO</b>	La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
		<b>OBJETO JURÍDICO</b>	{ La información.
		<b>ELEMENTO SUBJETIVO DEL ILÍCITO</b>	{ Que tenga por objeto el sacar provecho del acto mediante el dolo.
<b>ATIPICIDAD</b>	{	Se puede presentar si llega a faltar algún elemento del tipo penal, por lo que podría existir la ausencia de los objetos jurídico y material, así como la del elemento subjetivo del ilícito.	
<b>ANTI JURIDICIDAD</b>	{	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 Bis 5 fr. I del Código Penal Federal) y es contraria a la sociedad.	
<b>CAUSAS DE JUSTIFICACIÓN</b>	{	No hay causas de justificación alguna que encuadre en este aspecto.	
<b>IMPUTABILIDAD</b>	{	La capacidad de querer y entender.	
<b>INIMPUTABILIDAD</b>	{	Se puede presentar que una persona no imputable realice la	

AD	conducta, así como también sé de qué una persona lo realice de manera culposa.
CULPABILIDAD	{ Se puede dar de manera dolosa y culposa.
INCULPABILIDAD	{ Se podría presentar la <i>vis compulsiva o la obediencia jerárquica</i> .
CONDICIONES OBJETIVAS DE PUNIBILIDAD	{ Se persigue después de presentarse una demanda previa por la Secretaria de Hacienda.
PUNIBILIDAD	{ De seis meses a cuatro años de prisión y de cien a seiscientos días multa.
EXCUSAS ABSOLUTORIAS	{ <b>No cuenta con excusas absolutorias.</b>

#### **4.12 Estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan.**

El artículo 211 bis 5 párrafo segundo del Código Penal Federal establece lo siguiente:

“Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.”

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

<b>Conducta</b>	La conducta es de acción, y es el copiar indebidamente información que contengan los sistema y equipos de las instituciones que integren el sistema financiero	
<b>Ausencia de conducta</b>	No se puede dar ninguna de las formas de ausencia de conducta.	
<b>Tipicidad</b>	La conducta está descrita en el artículo 211 bis 5 del Código Penal Federal	
	<b>Sujeto activo</b>	El tipo establece la calidad específica "La persona autorizada para acceder a los sistemas y equipos".
	<b>Sujeto pasivo</b>	Las instituciones que integran el sistema financiero
	<b>Bien Jurídico Tutelado</b>	La información privada de las instituciones que integran el sistema financiero .
	<b>Objeto jurídico</b>	Protección de datos personales
	<b>Elemento subjetivo del ilícito</b>	Que tenga por objeto anular su derecho a intimidad y protección y uso de sus datos .
	<b>Elemento normativo</b>	Copiar indebidamente información
<b>Atipicidad</b>	Se puede presentar si llega a faltar algún elemento del tipo penal, por lo que podría existir la ausencia de los objetos jurídico y material, así como la del elemento subjetivo del ilícito.	

<b>Antijuridicidad</b>	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 bis 5 del Código Penal Federal)
<b>Causas de justificación</b>	No se puede aplicar ninguna.
<b>Imputabilidad</b>	La capacidad de querer y entender.
<b>Inimputabilidad</b>	Se puede presentar que una persona no imputable realice la conducta.
<b>Culpabilidad</b>	Se puede dar únicamente de manera dolosa.
<b>Inculpabilidad</b>	ERROR DE HECHO ESENCIAL En el error esencial de hecho, actúa antijurídicamente, creyendo que se actúa jurídicamente, es decir hay un desconocimiento de la antijuridicidad de su conducta.
<b>Condiciones objetivas de</b>	Se persigue de oficio .
<b>Punibilidad</b>	Se le impondrán de 3 meses a 2 años de prisión y de 50 a 300 días multa.  Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.
<b>Excusas absolutorias</b>	No existen

solo compete el primer párrafo por lo que el estudio será solo de:

Calidad específica del sujeto pasivo	Hipótesis	
Institución del sistema financiero	<ul style="list-style-type: none"> <li>• <b>Modificar.</b></li> <li>• <b>Destruir.</b></li> <li>• <b>Provocar perdida.</b></li> </ul>	
	Total de hipótesis previstas en el artículo 211 Bis 5, Párrafo Primero del Código Penal Federal.	<b>3</b>

Como se logra apreciar, en el párrafo correspondiente y a su vez resaltado, sólo se pueden identificar un sujeto pasivo, tres hipótesis correspondientes y las características del sujeto activo, por lo tanto, es imperativo el detenerse a desarrollar las hipótesis; siguiendo el orden correspondiente se dividirá en párrafo por partes y así obtener de mejor manera cada punto tocado en la redacción del artículo.

1. El antes mencionado se desarrolla de la siguiente manera: *“Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique [...]”*; desde este apartado se puede retomar tanto al sujeto pasivo como el primer verbo núcleo.

En el párrafo del artículo se encuentra el verbo núcleo “modificar”, esto no alcanza por sí mismo para entender el ilícito, por lo que va acompañado de “datos”, ahora bien, si se juntan ambos quedaría “modificar los datos contenidos” que sería el



primer supuesto ilícito al que se refiere el párrafo y una vez con el primer verbo núcleo bien delimitado se pueden llegar a las siguientes conclusiones; en primera no puede haber ausencia de conducta ya que se trata de un hecho de acción para ser concebido; después, no hay cabida al apercibimiento de los movimientos reflejo pues para llevar a cabo el hecho es necesario estar consiente del acto, así mismo, no se puede pensar en que el hecho es resultado de una fuerza física superior e irresistible proveniente de la naturaleza o de otro ser humano.

En cuanto a la tipicidad, se debe de hacer un perfecto encuadramiento en la acción precisa que es el “modificar”, y a su vez, se le podría encuadrar en las modalidades de la conducta que son el dolo y la preterintencionalidad, exceptuando la culpa puesto que este no permite la culpa por las cualidades que debe de tener el sujeto activo. Con respecto a las cualidades del sujeto activo me basare a lo que expresa el licenciado Lucerito Ludmila Flores Salgado en su libro sobre Derecho Informático en el cual se plantea lo siguiente:

“Tocante al sujeto activo de los delitos informáticos se ha observado que por lo general son personas de un determinado nivel de inteligencia y educación, superior al común, mismos que pueden ser los programadores que violan o inutilizan controles protectores del programa o sistema, los analistas de sistemas que generalmente son los únicos que conocen la operación completa de ellos; los analistas de comunicaciones que diseñan la seguridad del sistema de comunicaciones, supervisores que tienen conocimiento integral de las operaciones y debilidades del sistema de seguridad; personal técnico y de mantenimiento, que suele tener libre acceso a los centros de cómputo y conoce los sistemas operativos y bases de datos; etcétera.”

De acuerdo a lo antes planteado se entiende que la calidad del sujeto activo no es general pues debe de contar con características específicas como lo son la “educación superior”, “inteligencia”, ser un “programador”, “analista de sistemas”, “supervisores”, etcétera; sin embargo, se entiende por la formula del artículo que cualquier persona “autorizada” por lo que se caracterizaría por ser un delito de cuello blanco y esto determina que no puede ser cualquier persona.

Ahora bien, en cuanto al sujeto pasivo se entiende que es aquella institución que cuente con la característica de ser parte del sistema financiero, esto delimita la calidad específica del sujeto a todas aquellas instituciones que están reguladas por la secretaria de Hacienda y Crédito Público de acuerdo con el artículo 400 Bis. La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar el verbo núcleo de la conducta o no cubrir el elemento subjetivo del ilícito.

Con respecto a la antijuricidad se entiende que cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 Bis 5 fr. I del Código Penal Federal) y es contraria a la sociedad.

Así también en cuanto a las causas de justificación no hay alguna forma de que se presente puesto que no hay forma alguna de que mediante el cumplimiento de un deber o el ejercicio de un derecho se realice el acto, así como tampoco se podría dar el consentimiento del titular, siendo específico ya que en el artículo se menciona que el sujeto cuenta con el consentimiento para tener acceso, sin embargo, no puede disponer del bien jurídico que en este aspecto es la información pues no está legitimado por no ser dueño del bien y mucho menos tiene la capacidad jurídica como lo plantea el artículo 29 del Código Penal Federal. Este delito es perseguido por la Secretaría de Hacienda y Crédito Público con una denuncia previa para después proceder legalmente ante el ámbito penal, esto de acuerdo con el artículo.

### **211 Bis 6 y el artículo 400 Bis del Código Penal Federal.**

Todo lo explicado queda sintetizado de la siguiente manera.

<b>Conducta</b>	La conducta es de modificar los datos contenidos.
<b>Ausencia de conducta</b>	No se puede dar ninguna de las formas de ausencia de conducta.
<b>Tipicidad</b>	La conducta está descrita en el artículo 211 Bis 5, párrafo primero del Código Penal Federal. El tipo consta de elementos subjetivos, objetivos

	y normativos.	
	<b>Sujeto activo</b>	Se establece que debe ser una persona autorizada y al ser un delito de cuello blanco se entiende que hay características específicas del sujeto activo.
	<b>Sujeto pasivo</b>	Solo se especifica que debe de ser una institución del sistema financiero mexicano.
	<b>Bien Jurídico Tutelado</b>	La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
	<b>Objeto jurídico</b>	La información.
	<b>Elemento subjetivo del ilícito</b>	Que tenga por objeto el sacar provecho del acto mediante el dolo.
<b>Atipicidad</b>	Se puede presentar si llega a faltar algún elemento del tipo penal, por lo que podría existir la ausencia de los objetos jurídico y material, así como la del elemento subjetivo del ilícito.	
<b>Antijuridicidad</b>	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 Bis 5 fr. I del Código Penal Federal) y es contraria a la sociedad.	

<b>Causas de justificación</b>	No hay causas de justificación alguna que encuadre en este aspecto.
<b>Imputabilidad</b>	La capacidad de querer y entender.
<b>Inimputabilidad</b>	Se puede presentar que una persona no imputable realice la conducta, así como también sé de qué una persona lo realice de manera culposa.
<b>Culpabilidad</b>	Se puede dar de manera dolosa y culposa.
<b>Inculpabilidad</b>	Se podría presentar la <i>vis compulsiva</i> o la <i>obediencia jerárquica</i> .
<b>Condiciones objetivas de punibilidad</b>	Se persigue después de presentarse una demanda previa por la Secretaria de Hacienda.
<b>Punibilidad</b>	De seis meses a cuatro años de prisión y de cien a seiscientos días multa.
<b>Excusas absolutorias</b>	<b>No cuenta con excusas absolutorias.</b>

1. Ahora bien, en cuanto a la segunda hipótesis “Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya [...]”; con esta nueva parte integrada se nota directamente el verbo núcleo que en su caso sería “destruir”, pero para ser entendido es imperativo el que se complemente con “datos” pues queda especificado en el mismo párrafo que solo engloba los datos, no hardware o software.

Al ser esto una acción queda excluida la idea de una ausencia en la conducta pues no se puede presentar la *vis mayor* o *vis absoluta* pues es inconcebible que por causas ajenas al sujeto activo este mismo realice la acción de destruir información proveniente al sistema financiero.

En lo que respecta a la tipicidad se debe dar el exacto encuadramiento de la conducta al tipo, el cual contiene la conducta de destruir datos del sistema financiero, entendiéndose que los datos, sin importar la importancia de los mismos, están protegidos por el código protegiendo el derecho a la protección, valga la redundancia, de los datos propios o ajenos.

El tipo señalado consta de elementos objetivos, subjetivos y normativo, no estableciéndose ninguna modalidad de la conducta y en cuanto a la calidad específica del sujeto activo se presenta el mismo caso que en la primera hipótesis, debe de contar con las siguientes características: “son personas de un determinado nivel de inteligencia y educación, superior al común, mismos que pueden ser los programadores que violan o inutilizan controles protectores del programa o sistema, los analistas de sistemas que generalmente son los únicos que conocen la operación completa de ellos; los analistas de comunicaciones que diseñan la seguridad del sistema de comunicaciones, supervisores que tienen conocimiento integral de las operaciones y debilidades del sistema de seguridad; personal técnico y de mantenimiento, que suele tener libre acceso a los centros de cómputo y conoce los sistemas operativos y bases de datos; etcétera.”; así también se entiende que son personas con autorización por lo que pueden ser cualquiera con acceso y con autorización con las capacidades antes mencionadas sería el sujeto activo.

También, en cuestión del sujeto pasivo pasa lo mismo, ya que como se entiende en el primer desarrollo de la hipótesis primera es que son aquellas instituciones dentro del sistema financiero mexicano.

La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar el verbo núcleo de la conducta o no cubrir el elemento subjetivo del ilícito.

Este delito es perseguido por la Secretaria de Hacienda y Crédito Público con una denuncia previa para después proceder legalmente ante el ámbito penal, esto de acuerdo con el artículo

### 211 Bis 6 y el artículo 400 Bis del CPF.

A continuación, se sintetiza lo presentado en los párrafos anteriores:

<b>Conducta</b>	La conducta es de destruir los datos contenidos.	
<b>Ausencia de conducta</b>	No se puede dar ninguna de las formas de ausencia de conducta.	
<b>Tipicidad</b>	La conducta está descrita en el artículo 211 Bis 5, párrafo primero del Código Penal Federal. El tipo consta de elementos subjetivos, objetivos y normativos.	
	<b>Sujeto activo</b>	Se establece que debe ser una persona autorizada y al ser un delito de cuello blanco se entiende que hay características específicas del sujeto activo.
	<b>Sujeto pasivo</b>	Solo se especifica que debe de ser una institución del sistema financiero mexicano.
	<b>Bien Jurídico Tutelado</b>	La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
	<b>Objeto jurídico</b>	La información.
	<b>Elemento subjetivo del ilícito</b>	Que tenga por objeto el sacar provecho del acto mediante el dolo.

<b>Atipicidad</b>	Se puede presentar si llega a faltar algún elemento del tipo penal, por lo que podría existir la ausencia de los objetos jurídico y material, así como la del elemento subjetivo del ilícito.
<b>Antijuridicidad</b>	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 Bis 5 fr. I del Código Penal Federal) y es contraria a la sociedad.
<b>Causas de justificación</b>	No hay causas de justificación alguna que encuadre en este aspecto.
<b>Imputabilidad</b>	La capacidad de querer y entender.
<b>Inimputabilidad</b>	Se puede presentar que una persona no imputable realice la conducta, así como también sé de qué una persona lo realice de manera culposa.
<b>Culpabilidad</b>	Se puede dar de manera dolosa y culposa.
<b>Inculpabilidad</b>	Se podría presentar la <i>vis compulsiva o la obediencia jerárquica</i> .
<b>Condiciones objetivas de punibilidad</b>	Se persigue después de presentarse una demanda previa por la Secretaria de Hacienda.
<b>Punibilidad</b>	De seis meses a cuatro años de prisión y de cien a seiscientos días multa.
<b>Excusas absolutorias</b>	<b>No cuenta con excusas absolutorias.</b>

Por último, el presupuesto que se presenta a continuación; : “Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información [...]”; ahora bien, el verbo núcleo es “provocar”, pero por sí

mismo no se entiende, por lo tanto es necesario agregar lo demás del supuesto que es “perdida de información”; en esta caso sí se entiende el verbo que es “provocar la pérdida de información”.

Al ser esto una acción queda excluida la idea de una ausencia en la conducta pues no se puede presentar la vis mayor o vis absoluta pues es inconcebible que por causas ajenas al sujeto activo este mismo realice la acción de provocar la pérdida de información que sea proveniente al sistema financiero.

Como ya se mencionó anteriormente, en lo que respecta a la tipicidad se debe dar el exacto encuadramiento de la conducta al tipo, el cual contiene la conducta de provocar pérdida de información correspondiente al sistema financiero, entendiéndose que los datos, sin importar la importancia de los mismos, están protegidos por el código protegiendo el derecho a la protección, valga la redundancia, de los datos propios o ajenos.

El tipo señalado consta de elementos objetivos, subjetivos y normativo, no estableciéndose ninguna modalidad de la conducta y en cuanto a la calidad específica del sujeto activo se presenta las mismas características que en las hipótesis anteriores, por lo que se entiende que debe de contar con las siguientes calidades: “son personas de un determinado nivel de inteligencia y educación, superior al común, mismos que pueden ser los programadores que violan o inutilizan controles protectores del programa o sistema, los analistas de sistemas que generalmente son los únicos que conocen la operación completa de ellos; los analistas de comunicaciones que diseñan la seguridad del sistema de comunicaciones, supervisores que tienen conocimiento integral de las operaciones y debilidades del sistema de seguridad; personal técnico y de mantenimiento, que suele tener libre acceso a los centros de cómputo y conoce los sistemas operativos y bases de datos; etcétera.”; así también se entiende que son personas con autorización por lo que pueden ser cualquiera con acceso y con autorización con las capacidades antes mencionadas sería el sujeto activo.



También, en cuestión del sujeto pasivo pasa lo mismo, son aquellas instituciones dentro del sistema financiero mexicano que son reguladas por la Secretaria de Hacienda y Crédito Público.

La atipicidad se puede dar cuando falte alguno de los elementos mencionados, pudiéndose no agotar el verbo núcleo de la conducta o no cubrir el elemento subjetivo del ilícito.

Este delito es perseguido por la Secretaria de Hacienda y Crédito Público con una denuncia previa para después proceder legalmente ante el ámbito penal, esto de acuerdo con el artículo 211 Bis 6 y el artículo 400 Bis del CPF.

Y para terminar con el estudio dogmático la sinterización de esta última hipótesis:

<b>Conducta</b>	La conducta es de provocar la perdida de la información contenida.	
<b>Ausencia de conducta</b>	No se puede dar ninguna de las formas de ausencia de conducta.	
<b>Tipicidad</b>	La conducta está descrita en el artículo 211 Bis 5, párrafo primero del Código Penal Federal. El tipo consta de elementos subjetivos, objetivos y normativos.	
	<b>Sujeto activo</b>	Se establece que debe ser una persona autorizada y al ser un delito de cuello blanco se entiende que hay características específicas del sujeto activo.
	<b>Sujeto pasivo</b>	Solo se especifica que debe de ser una institución del sistema financiero mexicano.

	<b>Bien Jurídico Tutelado</b>	La pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica.
	<b>Objeto jurídico</b>	La información.
	<b>Elemento subjetivo del ilícito</b>	Que tenga por objeto el sacar provecho del acto mediante el dolo.
<b>Atipicidad</b>	Se puede presentar si llega a faltar algún elemento del tipo penal, por lo que podría existir la ausencia de los objetos jurídico y material, así como la del elemento subjetivo del ilícito.	
<b>Antijuridicidad</b>	Cuenta con la formal y material, ya que la conducta transgrede una norma dictada por el Estado (art. 211 Bis 5 fr. I del Código Penal Federal) y es contraria a la sociedad.	
<b>Causas de justificación</b>	No hay causas de justificación alguna que encuadre en este aspecto.	
<b>Imputabilidad</b>	La capacidad de querer y entender.	
<b>Inimputabilidad</b>	Se puede presentar que una persona no imputable realice la conducta, así como también sé de qué una persona lo realice de manera culposa.	
<b>Culpabilidad</b>	Se puede dar de manera dolosa y culposa.	
<b>Inculpabilidad</b>	Se podría presentar la <i>vis compulsiva</i> o la <i>obediencia jerárquica</i> .	

<b>Condiciones objetivas de punibilidad</b>	Se persigue después de presentarse una demanda previa por la Secretaria de Hacienda.
<b>Punibilidad</b>	De seis meses a cuatro años de prisión y de cien a seiscientos días multa.
<b>Excusas absolutorias</b>	<b>No cuenta con excusas absolutorias.</b>

### **Agravantes de los delitos informáticos.**

Las agravantes que se pueden percibir en el TÍTULO NOVENO “Revelación de secretos y acceso ilícito a sistemas y equipos de informática”, CAPÍTULO II “Acceso ilícito a sistemas y equipos de informática”, del Código Penal Federal, son las siguientes:

“ARTÍCULO 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto,

cargo o comisión pública. Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.”

En azul se encuentran las agravantes que se lograron localizar, al final del párrafo tercero y el párrafo cuarto, las cuales e ilustran de la siguiente manera:

**PÁRRAFO CUARTO:**

<b>Conducta</b>	<b>Agravante</b>
Obstruya la procuración o impartición de justicia	· Las sanciones que se señalaron en el artículo se duplicaran.
Entorpezca la procuración o impartición de justicia	· Las sanciones que se señalaron en el artículo se duplicaran.
Obstaculice la procuración o impartición de justicia	· Las sanciones que se señalaron en el artículo se duplicaran.
Limite la procuración o impartición de justicia	· Las sanciones que se señalaron en el artículo se duplicaran.
Imposibilite la procuración o impartición de justicia	· Las sanciones que se señalaron en el artículo se duplicaran.
Provoque que recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes	· Las sanciones que se señalaron en el artículo se duplicaran.

**Párrafo cuarto:**

Como se puede observar, la conducta en este párrafo denota que es de acción, cuyos verbos núcleos son “obstruir”, “entorpecer”, “obstaculizar”, “limitar” o “imposibilitar” la procuración o impartición de justicia, “provocar” que recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes, no pudiéndose presentar alguna forma de ausencia de la conducta, no se puede pensar en que por una fuerza física superior e irresistible proveniente de la naturaleza o de otro ser humano o por medio de movimientos reflejos se obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, así como provocar que recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

**Artículo 211 bis 5:**

En su párrafo tercero encontramos esta agravante “Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.” En este se establece que si las conductas, las cuales se mencionan en los párrafos anteriores llegasen a ser realizadas por funcionarios o empleados de

instituciones las cuales estén dentro del sistema financiero. Por lo cual nos deja claro que hay una calidad específica del sujeto activo, siendo este aquel funcionario o empleado que estuviera relacionado en alguna institución del sistema financiero.

Artículo 211 bis-6:

En este artículo se hace menciona los numerales de los artículos 211 bis-4 y 211 bis-5 en estos mismos se mencionan las instituciones que integran el sistema financiero, entendiéndose estas con base al artículo 400 bis del mismo código donde se determina que son todas aquellas donde la secretaria de hacienda y crédito público ejerza sus facultades

Artículo 211 bis-7

Este artículo tiene un carácter agravante de hasta una mitad cuando la información obtenida en cuestión se utilice en provecho propio o ajeno.

## CONCLUSIONES

1. El derecho informático, como una nueva rama del conocimiento jurídico, es una disciplina en constante desarrollo, que tiene hasta la fecha nuevos antecedentes a nivel histórico, podemos decir que las alusiones más específicas sobre esta interrelación existen a partir de 1949 con la obra de Norbert Wiener, en cuyo capítulo 4, dedicado al derecho y las comunicaciones, expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico.
2. Desde hace varios años, la información jurídica ha permitido un mejor conocimiento de los fenómenos jurídicos, por lo que muchos juristas, anteriormente escépticos e indiferentes, han encontrado en la computadora un instrumento eficaz para mejorar sus actividades.
3. Es evidente que el avance tecnológico impacta a la regulación penal, por lo que es menester que se cuente con una tutela actualizada y acorde a los bienes jurídicos en juego, con el consecuente dinamismo implícito en el desarrollo de las tecnologías informáticas.
4. Se han generado serios problemas en relación con el uso y abuso de tal producto tecnológico, la incorporación del Internet al mundo real fue avasallador de tal manera que los sistemas jurídicos de las naciones no se encontraban preparados con los mecanismos legales necesarios para afrontar dicha problemática.
5. La informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial.
6. Por delito informático, suele entenderse toda aquella conducta ilícita susceptible de ser sancionada por el derecho penal, consistente en el uso indebido de cualquier medio informático.

7. En el ámbito internacional encontramos que existe una ingente preocupación por este fenómeno, la Organización de las Naciones Unidas contiene un llamamiento a los estados miembros para que armonicen sus legislaciones a fin de sancionar penalmente el uso indebido de tecnología de la información, al tiempo que los exhorta a garantizar la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos frente a los accesos no consentidos.
8. El Código Penal Federal recoge una serie de figuras delictivas que ponderan diversos bienes jurídicos tutelados, los mismos se encuentran definidos a partir de cada artículo, teniendo como base al acceso ilícito a sistemas y equipos de informática, en diversas modalidades, por lo que en esta investigación se ha ofrecido un análisis pormenorizado de cada hipótesis prevista en los numerales correlativos del código punitivo.
9. Algunas legislaciones en México han recogido una parte de los tipos penales que nos ocupan pero en contrapartida, en la mayoría de los casos han dejado la cuestión probatoria en materia de pruebas electrónicas sin modificaciones que permitan una correcta persecución de estas conductas
10. .El marco jurídico con el que cuenta México en materia de delitos informáticos ha crecido de manera importante, pero por la propia naturaleza de la materia tutelada, resulta complicado y difícil estar a la vanguardia.



## FUENTES CONSULTADAS

### BIBLIOGRAFÍA

- AGUILAR LÓPEZ, Miguel Ángel. *El delito y la responsabilidad penal*. Editorial Porrúa, 2010.
- ALAMILLA VILLEDA, Erasmo Palemón. *Interpretación a la Teoría del Delito*, México D.F., Editorial Instituto Nacional de Desarrollo Jurídico, 2007.
- AMUCHATEGUI REQUENA, Griselda. *Derecho Penal*, México, Oxford, 2010.
- AZAOLA CALDERÓN Luis, *Delitos Informáticos y Derecho Penal*, Ubijus, Investigación y ciencias penales, México, 2010.
- CAMPOLI Andres, *Delitos Informáticos en la legislación Mexicana*, INACIPE Mex.2007
- CARRANCA Y TRUJILLO, Raúl, CARRANCA Y RIVAS, Raúl. *Derecho Penal Mexicano, Parte General*, México, Editorial Porrúa, 2007.
- CARRANCA Y TRUJILLO, RAÚL. *Derecho Penal, Parte General*, México, editorial Porrúa, 2001.
- CARRARA, Francesco. *Derecho Penal*, México, Oxford Editor, 2000.
- CARRILLO AHUMADA, Faustino. *Teoría del Delito, Sistema Jurídico Penal Legal*, México, Flores editor y distribuidor, S.A. de C.V, 2010-
- CASTELLANOS TENA, Fernando. *Lineamientos Elementales de Derecho Penal*, México D.F., Editorial Porrúa, 2010.
- DE PINA VARA, Rafael. *Diccionario de Derecho*. México, Editorial Porrúa, 1999.
- DÍAZ-ARANDA Enrique, *Derecho Penal, parte general*, 3ª. Edición, México, Editorial Porrúa, 2008.
- FLORES PRADA, Ignacio, *Criminalidad Informática*, Tirant lo Blanch, México 2012
- FLORES SALGADO, Lucerito, *Derecho Informático*, Patria, México 2009.
- GARCIA RAMÍREZ, Sergio. *Imputabilidad en el Derecho Penal Mexicano*, México, Universidad Nacional Autónoma de México, 1981.
- GONZÁLEZ BONNESIO, Alejandro. *Codificación de Derecho Penal*, Milán, Editorial Oxford, 1991.

- GRANADOS ATLACO, Miguel Ángel. *Derecho Penal Electoral Mexicano*. Editorial Porrúa, 2012.
- JIMENEZ DE ASÚA, Luis. *Lecciones de Derecho Penal*, México, Oxford Editor, 2000
- JIMÉNEZ DE ASÚA, Luis. *Tratado de Derecho Penal*. Tomo II. *Filosofía y Ley Penal*. Editorial Losada, S.A. Buenos Aires. 5ª Edición Actualizada. 1992.
- JIMÉNEZ HUERTA, Mariano. *Derecho Penal Mexicano*. Tomo I, México, Editorial Porrúa, 1983.
- JIMÉNEZ HUERTA, Mariano. *La Antijuricidad*. Imprenta Universitaria. México. 1952.
- JIMÉNEZ HUERTA, Mariano. *La Tipicidad*, Editorial Porrúa, México, 1955.
- LASCUARAIN SÁNCHEZ, Juan Antonio. *Solo penas legales y previas: el derecho a la legalidad penal en la jurisprudencia constitucional*. España, Tribunal Constitucional, 2009.
- LÓPEZ BETANCOURT, Eduardo. *Imputabilidad y Culpabilidad*, México D.F., Editorial Porrúa, 2002.
- LÓPEZ BETANCOURT, Eduardo. *Teoría del Delito*, México, Editorial Porrúa, 2007.
- MEZGER, Edmundo. *Derecho Penal*, México, Cárdenas Editor y Distribuidor, 1985.
- MONARQUE UREÑA, Rodolfo. *Lineamientos Elementales de la Teoría General del Delito*, México, editorial Porrúa, 2002.
- MUÑOZ CONDE, Francisco. *Teoría General del Delito*, Bogotá, Editorial Temis, S.A, 1990.
- PAVÓN VASCONCELOS, Francisco. *Derecho Penal Mexicano*, México, Editorial Porrúa, 2010.
- PLASCENCIA VILLANUEVA, RAÚL. *Teoría del delito*, México, Editorial UNAM, 2004.
- REYES ECHANDIA, Alfonso. *Antijuricidad*, 4ª Edición, Temis, Bogotá, Colombia, 1989, p. 218.
- REYNOSO DÁVILA, Roberto. *Teoría General del Delito*, México, editorial Porrúa, 2003.

- RIQUERT, Marcelo A. *Informática y derecho penal argentino*, Ad Hoc, Buenos Aires, 1999.
- SALT, Marcos, “Delitos informáticos de carácter económico”, en delitos no convencionales, Julio B.J. Maier (comp.), Editores de Puerto, Buenos Aires, 1994.
- SOLER, Sebastián. *Derecho Penal Argentino*, Argentina, Tipografía Editora Argentina, 1999.
- TÉLLEZ VALDÉS, Julio, *Derecho Informativo* Mc Graw hill, México 2000.
- UROSA RAMÍREZ, Gerardo Armando, *Teoría de la Ley Penal del Delito*, México, Editorial Porrúa, 2006.
- VELA TREVIÑO, Sergio. *Culpabilidad e Inculpabilidad*, México D.F., Editorial Trillas, 2007.
- VILLARREAL PALOS, Arturo. *Culpabilidad y Pena*, Naucalpan, Edo. de México, Editorial Porrúa, 2001.
- ZAFFARONI, Eugenio Raúl. *Teoría del delito*, Sociedad Anónima Editora, Comercial, Industrial y Financiera, Ediar, 1973.

#### LEYES DE CONSULTA

Constitución Política de los Estados Unidos Mexicanos. Versión electrónica.

Cámara de Diputados. [www.diputados.gob.mx](http://www.diputados.gob.mx).

Código Penal del Distrito Federal. Versión electrónica. Cámara de Diputados.  
[www.diputados.gob.mx](http://www.diputados.gob.mx)..

Código Penal para el Estado de Nuevo León, H. Congreso del Estado de Nuevo León. Versión electrónica. Cámara de Diputados. [www.hcnl.gob.mx](http://www.hcnl.gob.mx).

Código Penal para el Estado Chiapas, H. Congreso del Estado de Chiapas. Versión electrónica. Cámara de Diputados. [www.congresochiapas.gob.mx](http://www.congresochiapas.gob.mx).

## PROPUESTA

Con el fin de evitar las repeticiones innecesarias y darle mayor claridad al texto penal, nos permitimos proponer la siguiente redacción de los artículos analizados en la presente investigación.

### Capítulo II

#### Acceso ilícito a sistemas y equipos de informática

**Artículo 211 Bis 1.-** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática particulares, o que pertenezcan al Estado, o bien al sistema financiero, y que además se encuentren protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática particulares, o que pertenezcan al Estado, o bien al sistema financiero, se le impondrán de tres meses a dos años de prisión y de cincuenta a seiscientos días multa.

**Artículo 211 Bis 2.-** Al que estando autorizado para acceder a sistemas y equipos de informática del Estado o de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a ocho años de prisión y cien a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado o de las instituciones que integran al sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a cuatro años de prisión y de cincuenta a cuatrocientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados del Estado o de instituciones que integran al sistema financiero.

**Artículo 211 bis 3.-** A quien sin autorización conozca, obtenga, copie o utilice información contenida en contenida en cualquier sistema, equipo o medio de

almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal.

Si el responsable, en cualquiera de los supuestos antes señalados, es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

**Artículo 211 Bis 4.-** Para los efectos de estos artículos, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

**Artículo 211 Bis 5.-** Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.