**H. CONGRESO DEL ESTADO DE YUCATAN**
**PRESENTE.**

El Suscrito diputado Luis Enrique Borjas Romero, integrante de la LXII Legislatura del Congreso del Estado, con fundamento en los artículos 35 fracción I de la Constitución Política; 16 y 22 fracción VI de la Ley de Gobierno del Poder Legislativo, así como los artículos 68 y 69 del Reglamento de la Ley del Poder Legislativo, todos del Estado de Yucatán, someto a consideración de esta Honorable Asamblea la siguiente iniciativa de reformas al Código Penal, en materia de Delitos Informáticos. Por lo cual me permito manifestar la siguiente:

## EXPOSICION DE MOTIVOS

La revolución informática ha originado que no exista área que no se encuentre afectada por el fenómeno. Ante dicha situación, varios países han tomado las previsiones jurídicas que impone el caso, y México no es la excepción.

Así es como se ha desarrollado lo que en la actualidad se conoce como derecho informático. Se puede definir al derecho informático como el conjunto de normas jurídicas tendientes a regular la propiedad, uso y abusos de los equipos de cómputo y de los datos que se transmiten en forma electromagnética.

Los delitos informáticos, llamados también delitos cibernéticos, delitos electrónicos, delitos relacionados con las computadoras, delincuencia relacionada con el ordenador, Computer related crimes, etc. se han definido por la Organización para la Cooperación Económica y el Desarrollo, como:

*"Cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automatizado de datos y/o la transmisión de datos".*

En esta definición podemos encontrar elementos de valoración ética que son trascendentes para el derecho penal. En nuestro país ya existe legislación que regula las novedosas relaciones y realidades que se vinculan con la computación.

La problemática de los delitos informáticos requiere un estudio especial con vistas a determinar la medida en que la legislación penal (códigos penales y leyes especiales) deba prever la incidencia en los citados ilícitos.

Una de las peculiaridades de este tipo de delitos es que desafortunadamente no conllevan una problemática local; la existencia de redes internacionales como Internet abre la posibilidad de transgresiones a nivel mundial y con gran impunidad.

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurtos, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera.

Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

Es evidente que el objeto de todos los estudios, es la regulación penal de aquellas actitudes antijurídicas estimadas graves, como último recurso para evitar su impunidad.

Por lo que deberemos reconocer como "Delito electrónico", en un sentido amplio a

- Conexiones falsas o evil twin: Son redes inalámbricas Wi-Fi que aparentan ofrecer conexiones a Internet con el mismo aspecto que el de decenas de miles de redes públicas inalámbricas, pero es sólo una fachada que para robar cualquier número de tarjeta de crédito y contraseñas que se digite usando la conexión.

- Pharming: Cuando un criminal informático desvía a un consumidor hacía una página electrónica apócrifa, de igual manera, es una forma para robar información confidencial con fines fraudulentos.

- Spam: También llamado correo basura, consiste en el envío masivo de información no solicitada por medio del correo electrónico. Generalmente la información que se difunde tiene fines publicitarios, pero también puede dañar el software, sistema o equipo sin consentimiento.

- Ciber terrorismo: Se refiere a la posibilidad de que los sistemas de información como las redes de datos sean atacados o que estos sean utilizados por y para perpetrar actos terroristas.

- Malware: Proveniente de los términos MALicious y softWARE, se constituye por programas, documentos o mensajes que pueden causar daños a los equipos de los usuarios.

- Pop ups y Adware: Se caracterizan por ser programas que se instalan con o sin el consentimiento de los usuarios informáticos, se despliegan en intervalos de tiempo anuncios y mensajes publicitarios que se sobreponen a la aplicación informática que se tenga en ese momento en uso.

cualquier conducta criminal que en su realización hace uso de la tecnología electrónica, ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel, ya sea como método, medio o fin".

En México por ejemplo, se reconoce la copia ilegal de programas de cómputo como un delito en la Ley de Derechos de Autor, así como la copia ilegal de topografías (como diseños industriales) en la Ley de Propiedad Industrial.

Pero en el extranjero ya se han reconocido como modalidades de delitos informáticos, los siguientes: Manipulaciones, el espionaje, el sabotaje y el hurto de tiempo, entre algunas de las acciones ilícitas penalmente hablando.

Sin embargo las conductas más conocidas utilizadas se destacan las siguientes:

- Hacking: Es una conducta criminógenas de acceso no autorizado a un equipo o sistema informático.

- Cracking o Copia de programas: A diferencia del hacker, el cracker se limita a la vulneración del software o conductas de piratería informática.

- Phishing: Se trata de correos electrónicos y portales de Internet falsos, que se hacen pasar por una institución con la que se está acreditado, y piden al usuario que actualice sus datos. Sin embargo, el usuario estará proporcionándoselos a la delincuencia informática.

- Snifers: Los rastreadores o sniffers, "...suelen ser usados para penetrar en el disco duro de los ordenadores conectados a la red, buscando cierto tipo de información.

- El Spyware y el software espía: son aplicaciones informáticas cuyo objetivo es la recopilación de información personal sin consentimiento, para ser transmitida a terceros interesados y para vigilar silenciosamente las conductas, actividades e información de una persona, con ello se puede obtener passwords, estados de cuenta bancarios, conocimiento de su correspondencia electrónica, etcétera.

Cualquiera de estas conductas, a través de las formas antes señaladas, tiene que ver con la carencia de una ética tecnológica, originada por la rapidez con que la misma tecnología gana espacios en las sociedades, y el estupor con que se enfrenta la problemática, que incita paradójicamente a que en esta novedosa forma de procesamiento de información se identifiquen nuevas vulnerabilidades de las cuales se aprovechan delincuentes conocedores de la tecnología.

En virtud de lo anterior y en ejercicio de la facultad que me confiere el artículo 35 fracción I, de la Constitución Política del Estado de Yucatán, someto a su consideración la siguiente:

Propuesta con proyecto de Decreto por el que se adicionan los artículos 243 Bis 5, 243 Bis 6, 243 Bis 7, 243 Bis 8, 243 Bis 9, 243 Bis 10 y un nuevo Capítulo al Título Decimoprimero denominado "Delitos Informáticos", todos del Código Penal del Estado de Yucatán, en materia de Delitos Informáticos:

**Decreto por el que se Modifica el Código Penal del Estado de Yucatán en Materia de Delitos Informáticos**

**Artículo Primero**.- Se adicionan los artículos 243 Bis 5, 243 Bis 6, 243 Bis 7, 243 Bis 8, 243 Bis 9, 243 Bis 10; se adiciona un nuevo Capítulo VI al TÍTULO DECIMOPRIMERO denominado "Delitos Informáticos" y se recorre el actual capítulo VI para pasar a ser el Capítulo VII, todos del Código Penal del Estado de Yucatán, para quedar como sigue:

**Artículo 243 Bis 5**.- Al que sin autorización, para beneficio propio o ajeno, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos informáticos protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de mil a dos mil unidades de medida y actualización.

**Artículo 243 Bis 6**.- Al que sin autorización, para beneficio propio o ajeno, se introduzca por cualquier medio a un sistema o equipo de informática protegido por algún mecanismo de seguridad para sustraer, eliminar o cambiar información contenida en él, con la intensión de provocar un desperfecto en su funcionamiento que lo deje total o parcialmente inoperable o intercepte comunicaciones privadas con la intensión recabar información personal o financiera, se le impondrán de 1 a 3 años de prisión y de mil a dos mil unidades de medida y actualización.

**Artículo 243 Bis 7.**- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente sustraiga información para beneficio personal o ajeno, se le impondrán de uno a cuatro años de prisión y de mil a dos mil unidades de medida y actualización.

**Artículo 243 Bis 8.**- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique o destruya información para beneficio personal o ajeno, se le impondrán de uno a cuatro años de prisión y de mil a dos mil unidades de medida y actualización.

**Artículo 243 Bis 9.**- Al que estando autorizado para acceder a sistemas y equipos de informática, indebidamente modifique o provoque pérdida de información que contengan, se le impondrán de dos a cuatro años de prisión y de mil a dos mil unidades de medida y actualización.

**Artículo 243 Bis 10.**- Las sanciones contenidas en los artículos 243 Bis 7 y 243 Bis 8 de este código, se duplicarán cuando la conducta tenga la intención de obstruir, entorpecer, obstaculizar, limitar o imposibilitar la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

## TRANSITORIOS

**Artículo Primero.-** El presente decreto entrará en vigor al día siguiente al de su publicación en el Diario Oficial del Gobierno del Estado.

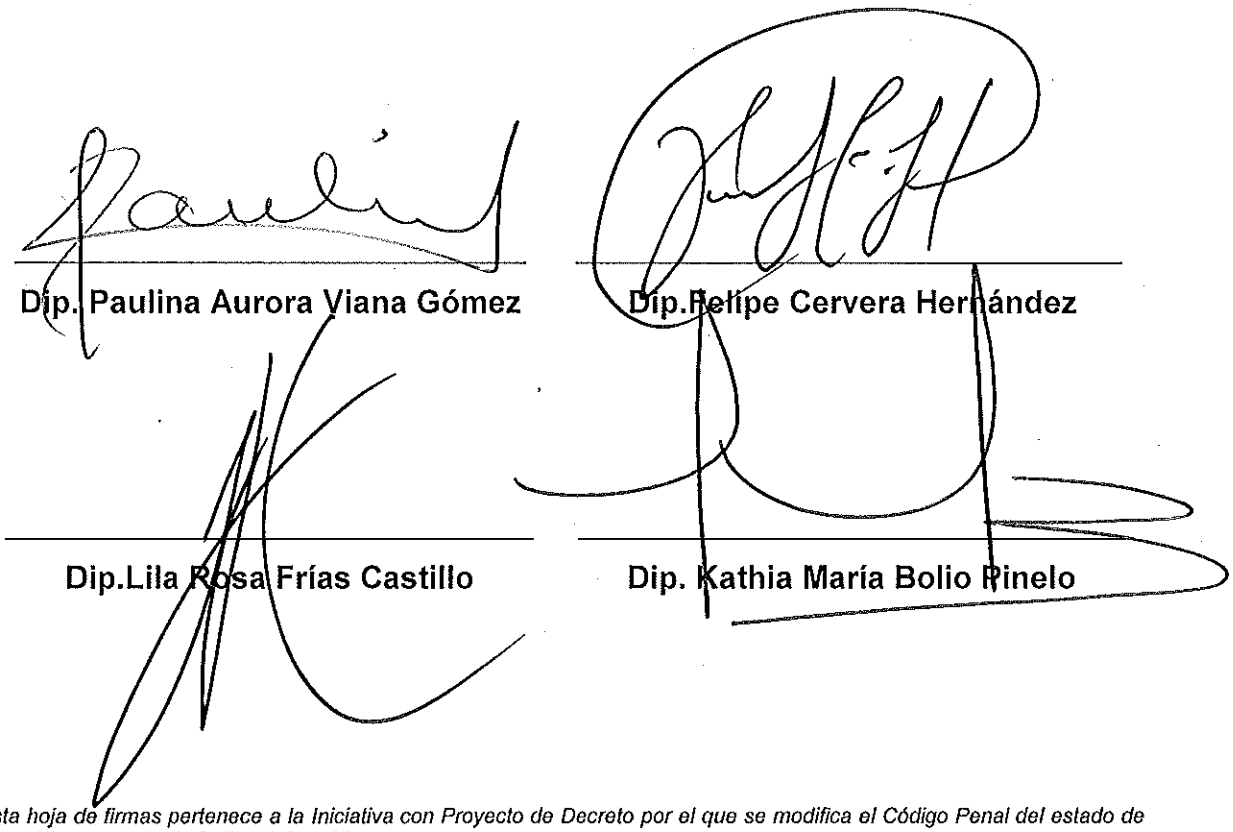
**Artículo segundo.** Se derogan todas las disposiciones que se opongan a lo dispuesto en este decreto.

**Protesto lo necesario en la ciudad de Mérida, Yucatán, a los veinte días del mes de febrero del año dos mil diecinueve.**

**Luis Enrique Borjas Romero**

**integrante de la LXII Legislatura del Congreso del Estado**

En sesión plenaria de fecha 20 de febrero del presente año, el diputado Luis Enrique Borjas Romero presentó durante los Asuntos Generales la Iniciativa con Proyecto de Decreto por el que se modifica el Código Penal del estado de Yucatán en materia de Delitos Informáticos; los diputados Paulina Aurora Viana Gómez, Felipe Cervera Hernández, Lila Rosa Frías Castillo y Kathia María Bolio Pinelo, solicitaron suscribirse a la misma, lo cual fue aceptado por su autor para formar parte de la citada iniciativa.



**Dip. Paulina Aurora Viana Gómez** **Dip. Felipe Cervera Hernández**

**Dip. Lila Rosa Frías Castillo** **Dip. Kathia María Bolio Pinelo**

*Esta hoja de firmas pertenece a la Iniciativa con Proyecto de Decreto por el que se modifica el Código Penal del estado de Yucatán en materia de Delitos Informáticos.*