

DIPUTADO FAUSTO MANUEL ZAMORANO ESPARZA
PRESIDENTE DE LA MESA DIRECTIVA
DEL CONGRESO DE LA CIUDAD DE MÉXICO
II LEGISLATURA.
P R E S E N T E.

El suscrito, Diputado **Jhonatan Colmenares Rentería**, integrante del Grupo Parlamentario del Partido Revolucionario Institucional en este H. Congreso de la Ciudad de México, II Legislatura; con fundamento en lo dispuesto por los artículos 122 apartado A, fracción II de la Constitución Política de los Estados Unidos Mexicanos; 29 apartado A, numeral 1; apartado D, inciso a) y 30 numeral 1, inciso b) de la Constitución Política de la Ciudad de México; 12 fracción II de la Ley Orgánica del Congreso de la Ciudad de México; 5 fracción I, 82, 95 fracción II y 96 del Reglamento del Congreso de la Ciudad de México, someto a consideración de este Pleno, la presente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA UN CAPÍTULO III AL TÍTULO DÉCIMO TERCERO DEL CÓDIGO PENAL PARA EL DISTRITO FEDERAL, EN MATERIA DE DELITO INFORMÁTICO**, con base en la siguiente:

PLANTEAMIENTO DEL PROBLEMA

De acuerdo con la Oficina de las Naciones Unidas contra la Droga y el Delito “La ciberdelincuencia es un problema mundial creciente. Ya sea que usted dirija una pequeña empresa o una compañía de la lista Fortune 500, que esté adquiriendo su primer teléfono inteligente o esté por convertirse en experto en materia de ciberseguridad, debe ser consciente de la ciberdelincuencia. Internet ofrece oportunidades educativas y económicas que superan cualquier cosa antes vista. Esta misma herramienta, sin

embargo, da pie también a oportunidades sin precedentes de causar daños. Mediante el uso indebido de la tecnología, los delincuentes cibernéticos pueden llevar a las empresas a la ruina e incluso arruinar la vida a las personas. Muchos países y organizaciones de todo el mundo luchan para poner un alto a los delincuentes cibernéticos y contribuir a la seguridad de los sistemas. Sin embargo, uno de los mejores métodos de prevención es el que recurre a la educación.”¹

Así mismo el “Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente” señaló que En los años recientes las redes de computadoras han crecido de manera asombrosa. Hoy en día, el número de usuarios que se comunican, hacen sus compras, pagan sus cuentas, realizan negocios y hasta consultan con sus médicos online supera los 200 millones, comparado con 26 millones en 1995.

A medida que se va ampliando la Internet, asimismo va aumentando el uso indebido de la misma. Los denominados delincuentes cibernéticos se pasean a su aire por el mundo virtual, incurriendo en delitos tales como el acceso sin autorización o «piratería informática», el fraude, el sabotaje informático, el narcotráfico, la trata de niños con fines pornográficos y el acecho.

Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. En materia de delitos financieros como el fraude o el robo de información, la mayor categoría la forman los empleados de empresas, que son responsables del 90% de estos delitos, según el Manual de la Naciones

¹ <https://www.unodc.org/e4j/es/tertiary/cybercrime.html>

Unidas de 1997 sobre la prevención y la fiscalización de los delitos relacionados con las computadoras.²

De acuerdo con el Informe de Amenazas 2023 de la firma de ciberseguridad Sophos, el panorama ha alcanzado un nuevo nivel de comercialización, debido a la expansión de los delitos cibernéticos como servicio, facilitados por mercados clandestinos, como Genesis , en el que se puede comprar malware y donde también hay venta masiva de credenciales robadas.³

Que las principales características que revisten los Delitos informáticos son:

- a) Conductas criminógenas de cuello blanco.
- b) Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.
- c) Son acciones de oportunidad, en cuanto a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.
- e) Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.

²

<https://www.un.org/es/conf/xcongreso/prensa/2088hs.shtml#:~:text=Los%20denominados%20delincuentes%20cibern%C3%A9ticos%20se,fines%20pornogr%C3%A1ficos%20y%20el%20acecho.>

³ <https://expansion.mx/tecnologia/2022/12/30/que-espera-2023-en-ciberataques#:~:text=Los%20da%C3%B1os%20a%20la%20ciberseguridad%20crecen%20144%25%20cada%20a%C3%B1o%20y,la%20proliferaci%C3%B3n%20de%20grupos%20maliciosos.&text=El%202022%20fue%20un%20a%C3%B1o,sigui%C3%B3%20dando%20de%20qu%C3%A9%20hablar.>

- h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- i) En su mayoría son imprudenciales y no necesariamente se cometen con intención.
- j) Ofrecen facilidades para su comisión a los menores de edad.
- k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
- l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

México ha sido una de las naciones que mayormente ha tenido una tendencia al alza en ciberataques, lo cual indica la necesidad de impulsar estrategias de ciberseguridad en las distintas órdenes de gobierno, así como crear estrategias y/o políticas empresariales para prevenir ser vulnerados desde el exterior. Asimismo, IDC mencionó que, como parte de una política empresarial, es crear 3 pilares: seguridad, consolidación y simplicidad que permiten mayor protección y mejores políticas de estado para nuestro país, así como para el sector empresarial.⁴

ARGUMENTOS QUE LA SUSTENTAN

- Que el Estado tiene la obligación de modernizar las leyes, las técnicas de investigación, la asesoría jurídica y en general las estrategias en materia de ciberdelitos.

4

<https://www.idc.com/getdoc.jsp?containerId=prLA49766122#:~:text=M%C3%A9xico%20tiene%20el%20primer%20lugar,lugar%20con%206.3%20mil%20millones.>

- México se encuentra entre los países más vulnerables en delitos informáticos de acuerdo con el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones, agencia de la Organización de las Naciones Unidas.
- Tanto las personas físicas como las personas morales enfrentan amenazas en su patrimonio.
- El delito cibernético se ha convertido en un negocio que supera el billón de dólares anual producto del fraude cibernético, el robo de identidad y la pérdida de propiedad intelectual.
- La ONU declaró la seguridad cibernética como un problema mundial que demanda un enfoque mundial.
- Que las amenazas del delito informático han aumentado desmedidamente perjudicando a un aproximado de 431 millones de víctimas adultas en todo el mundo, lo que equivale a catorce víctimas adultas por segundo y a un millón de víctimas de delitos cibernéticos por día.
- México tiene el primer lugar con 85 mil millones de intentos de ciberataque en el primer semestre de 2022, lo que representa un aumento del 40% en cifras anuales. Le sigue Brasil con 31,5 mil millones de ciberataques durante el mismo periodo de tiempo y Colombia en tercer lugar con 6,3 mil millones.

- Que entre los delitos cibernéticos más comunes se encuentra el robo de identidad y fraudes por correo electrónico y plataformas digitales, como facebook, instagram y twitter.
- En 2022, se registraron 80,000 millones de intentos de ciberataques.

La presente iniciativa plantea adicionar un capítulo al Código Penal para el Distrito Federal, enfocado a los delitos informáticos.

FUNDAMENTO LEGAL, CONSTITUCIONAL Y CONVENCIONAL

El Convenio de que México es parte, sobre ciberdelincuencia, firmado en Budapest Hungría el 23 de noviembre de 2001 y entrando en vigor el 01 de julio de 2004, es el primer tratado internacional que busca abordar los delitos informáticos y de Internet para armonizar las leyes nacionales, mejorar las técnicas de investigación y aumentar la cooperación entre las naciones.

El párrafo noveno del artículo 21 de la Constitución Política de los Estados Unidos Mexicanos, prevé que:

La seguridad pública es una función del Estado a cargo de la Federación, las entidades federativas y los Municipios, cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como contribuir a la generación y preservación del orden público y la paz social, de conformidad con lo previsto en esta Constitución y las leyes en la materia. La

seguridad pública comprende la prevención, investigación y persecución de los delitos, así como la sanción de las infracciones administrativas, en los términos de la ley, en las respectivas competencias que esta Constitución señala. La actuación de las instituciones de seguridad pública se regirá por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos reconocidos en esta Constitución.

El derecho a la seguridad ciudadana y a la prevención de la violencia y del delito se encuentra contemplado en el apartado B del artículo 14 "Ciudad segura" de la Constitución Política de la Ciudad de México, el cual a la letra versa:

"Artículo 14 Ciudad segura

A. (...)

(...)

B. Derecho a la seguridad ciudadana y a la prevención de la violencia y del delito Toda persona tiene derecho a la convivencia pacífica y solidaria, a la seguridad ciudadana y a vivir libre de amenazas generadas por el ejercicio de las violencias y los delitos. Las autoridades elaborarán políticas públicas de prevención y no violencia, así como de una cultura de paz, para brindar protección y seguridad a las personas frente a riesgos y amenazas."

Por lo anteriormente expuesto, someto a consideración de este H. Congreso de la Ciudad de México la siguiente iniciativa por el **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA UN CAPÍTULO III AL TÍTULO DÉCIMO TERCERO DEL CÓDIGO PENAL PARA EL DISTRITO FEDERAL, EN MATERIA DE DELITO INFORMÁTICO**, para quedar de la siguiente manera:

TEXTO VIGENTE	TEXTO PROPUESTO
TÍTULO DÉCIMO TERCERO INVOLABILIDAD DEL SECRETO	TÍTULO DÉCIMO TERCERO INVOLABILIDAD DEL SECRETO
CAPÍTULO I VIOLACIÓN DE LA INTIMIDAD PERSONAL 212. ...	CAPÍTULO I VIOLACIÓN DE LA INTIMIDAD PERSONAL 212. ...
CAPÍTULO II REVELACIÓN DE SECRETOS 213. ...	CAPÍTULO II REVELACIÓN DE SECRETOS 213. ...
(SIN CORRELATIVO)	CAPÍTULO III DELITO INFORMÁTICO
(SIN CORRELATIVO)	ARTÍCULO 214. COMETE EL DELITO INFORMÁTICO: I. QUIEN REVELE, DIVULGUE O UTILICE INDEBIDAMENTE O EN PERJUICIO DE OTRO, INFORMACIÓN, CONVERSACIONES O MENSAJES DE TEXTO, IMÁGENES O ARCHIVOS DE VOZ, CONTENIDOS EN SISTEMAS O EQUIPOS INFORMÁTICOS;

	<p>OBTENIDOS A TRAVÉS DE MECANISMOS DISTINTOS A LA INTERVENCIÓN DE COMUNICACIÓN PRIVADA, MEDIANTE EL EMPLEO DE APARATOS O DISPOSITIVOS ELECTRÓNICOS FIJOS O MÓVILES O A TRAVÉS DE LA SUPLANTACIÓN DE IDENTIDAD, CON EL FIN DE DEFRAUDAR, OBTENER DINERO, BIENES O INFORMACION.</p> <p>II. QUIEN SIN AUTORIZACIÓN ACCESA, MODIFIQUE, DESTRUYA O PROVOQUE PÉRDIDA DE INFORMACIÓN CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMÁTICA QUE ESTÉN O NO PROTEGIDOS POR ALGÚN MECANISMO DE SEGURIDAD, O TAMBIÉN SIN AUTORIZACIÓN ACCEDA A DICHOS SISTEMAS O EQUIPOS DE INFORMÁTICA O MEDIANTE CUALQUIER MECANISMO QUE DE MANERA DIRECTA O REMOTA LES CAUSE DAÑO.</p> <p>III. QUIEN, CON O SIN AUTORIZACIÓN CONOZCA, COPIE, MODIFIQUE, DESTRUYA O PROVOQUE PÉRDIDA DE INFORMACIÓN</p>
--	--

	<p>CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMÁTICA QUE PERTENEZCAN AL ALGUNA INSTITUCIÓN GUBERNAMENTAL, PROTEGIDOS POR ALGÚN MECANISMO DE SEGURIDAD.</p> <p>IV. QUIEN CON O SIN AUTORIZACIÓN CONOZCA, COPIE, MODIFIQUE, DESTRUYA O PROVOQUE PÉRDIDA DE INFORMACIÓN CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMÁTICA DE LAS INSTITUCIONES QUE INTEGRAN EL SISTEMA FINANCIERO, PROTEGIDO POR ALGÚN MECANISMO DE SEGURIDAD.</p> <p>AL RESPONSABLE DE ESTE DELITO, SE LE IMPONDRÁ UNA PENA DE SEIS MESES A DOS AÑOS DE PRISIÓN Y DE NOVENTA A DOSCIENTOS CINCUENTA DÍAS MULTA UNIDADES DE MEDIDA Y ACTUALIZACIÓN VIGENTES.</p> <p>CUANDO EL AGENTE SEA SERVIDOR PÚBLICO, SE LE IMPONDRÁ, ADEMÁS, DESTITUCIÓN E INHABILITACIÓN DE SEIS MESES A TRES AÑOS.</p>
--	---

DENOMINACIÓN DE LA LEY O EL DECRETO.

SE ADICIONA UN CAPÍTULO III AL TÍTULO DÉCIMO TERCERO DEL CÓDIGO PENAL PARA EL DISTRITO FEDERAL, EN MATERIA DE DELITO INFORMÁTICO.

PROYECTO DE DECRETO

ÚNICO.- Se adiciona un Capítulo III al Título Décimo Tercero del Código Penal para el Distrito Federal, en materia de delito informático, para quedar de la siguiente manera:

CÓDIGO PENAL PARA EL DISTRITO FEDERAL

TÍTULO DÉCIMO TERCERO INVOLABILIDAD DEL SECRETO

CAPÍTULO I

VIOLACIÓN DE LA INTIMIDAD PERSONAL

212. ...

CAPÍTULO II REVELACIÓN DE SECRETOS

213. ...

CAPÍTULO III

DELITO INFORMÁTICO

ARTÍCULO 214. COMETE EL DELITO INFORMÁTICO:

I. QUIEN REVELE, DIVULGUE O UTILICE INDEBIDAMENTE O EN PERJUICIO DE OTRO, INFORMACIÓN, CONVERSACIONES O MENSAJES DE TEXTO, IMÁGENES O ARCHIVOS DE VOZ, CONTENIDOS EN SISTEMAS O

EQUIPOS INFORMÁTICOS; OBTENIDOS A TRAVÉS DE MECANISMOS DISTINTOS A LA INTERVENCIÓN DE COMUNICACIÓN PRIVADA, MEDIANTE EL EMPLEO DE APARATOS O DISPOSITIVOS ELECTRÓNICOS FIJOS O MÓVILES O A TRAVÉS DE LA SUPLANTACIÓN DE IDENTIDAD, CON EL FIN DE DEFRAUDAR, OBTENER DINERO, BIENES O INFORMACION.

II. QUIEN SIN AUTORIZACIÓN ACCESA, MODIFIQUE, DESTRUYA O PROVOQUE PÉRDIDA DE INFORMACIÓN CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMÁTICA QUE ESTÉN O NO PROTEGIDOS POR ALGÚN MECANISMO DE SEGURIDAD, O TAMBIÉN SIN AUTORIZACIÓN ACCEDA A DICHOS SISTEMAS O EQUIPOS DE INFORMÁTICA O MEDIANTE CUALQUIER MECANISMO QUE DE MANERA DIRECTA O REMOTA LES CAUSE DAÑO.

III. QUIEN, CON O SIN AUTORIZACIÓN CONOZCA, COPIE, MODIFIQUE, DESTRUYA O PROVOQUE PÉRDIDA DE INFORMACIÓN CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMÁTICA QUE PERTENEZCAN AL ALGUNA INSTITUCIÓN GUBERNAMENTAL, PROTEGIDOS POR ALGÚN MECANISMO DE SEGURIDAD.

IV. QUIEN CON O SIN AUTORIZACIÓN CONOZCA, COPIE, MODIFIQUE, DESTRUYA O PROVOQUE PÉRDIDA DE INFORMACIÓN CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMÁTICA DE LAS INSTITUCIONES QUE INTEGRAN EL SISTEMA FINANCIERO, PROTEGIDO POR ALGÚN MECANISMO DE SEGURIDAD.

AL RESPONSABLE DE ESTE DELITO, SE LE IMPONDRÁ UNA PENA DE SEIS MESES A DOS AÑOS DE PRISIÓN Y DE NOVENTA A DOSCIENTOS CINCUENTA DÍAS MULTA UNIDADES DE MEDIDA Y ACTUALIZACIÓN VIGENTES.

CUANDO EL AGENTE SEA SERVIDOR PÚBLICO, SE LE IMPONDRÁ, ADEMÁS, DESTITUCIÓN E INHABILITACIÓN DE SEIS MESES A TRES AÑOS.

TRANSITORIOS

PRIMERO. Publíquese el presente decreto en la Gaceta Oficial de la Ciudad de México y para su mayor difusión publíquese en el Diario Oficial de la Federación.

SEGUNDO. El presente decreto entrará en vigor al día siguiente de su publicación en la Gaceta Oficial de la Ciudad de México.

TERCERO. Todas las disposiciones legales que contravengan esta reforma, se entienden como derogadas.

Dado en el Recinto Legislativo de Donceles, sede oficial del H. Congreso de la Ciudad de México, a los 16 días del mes de mayo del año dos mil veintitrés.

A T E N T A M E N T E



DIPUTADO JHONATAN COLMENARES RENTERIA
INTEGRANTE DEL GRUPO PARLAMENTARIO
DEL PARTIDO REVOLUCIONARIO INSTITUCIONAL
DEL CONGRESO DE LA CIUDAD DE MÉXICO
II LEGISLATURA