



**TECNOLÓGICO
NACIONAL DE MÉXICO**



**INSTITUTO TECNOLÓGICO DE
TLALNEPANTLA**

Tecnologías en seguridad de software

“Delitos informáticos en México, ¿qué dice la Ley?”

Docente: Hilda Díaz Rincón

Integrantes:

- **Espino Horta Maria Jose**
- **Calderón Hernández Miguel
Eduardo**
- **Alcántara Salazar Joel**

T92 09/09/21

Ante un **delito informático**, las **empresas afectadas** se pueden ver enfrentadas a la interrupción de la continuidad del negocio, pérdidas financieras y golpes a su reputación, pero las consecuencias legales también pueden ser profundas.

La **Organización para la Cooperación y el Desarrollo Económico (OCDE)** designó en París un comité de expertos para discutir los crímenes que tuvieran como centro a las computadoras y la necesidad de hacer cambios en los códigos penales. La **OCDE** recomendó a los países miembros modificar su legislación penal para integrar este tipo de delitos.

Ivonne Muñoz, abogada especializada en ciberseguridad y directora de IT Lawyers, despacho enfocado en temas de derecho informático, privacidad, pruebas digitales, propiedad intelectual y seguridad de la información, indica que en México a partir de 1999 existe **legislación a nivel federal que sanciona delitos informáticos**.

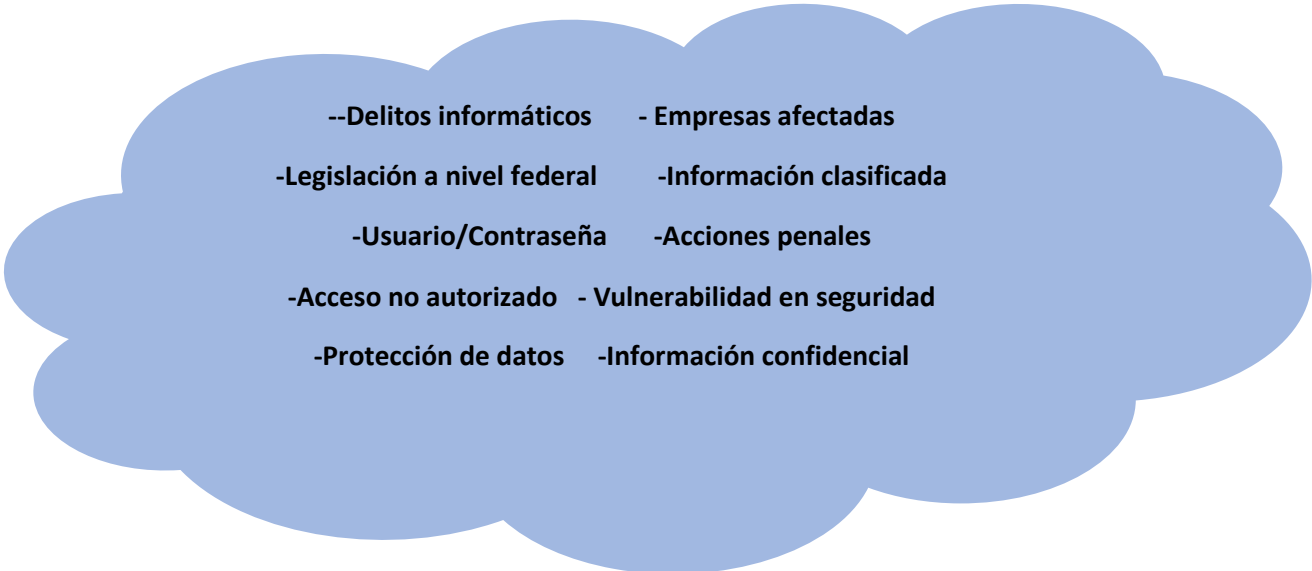
El fundamento legal para sancionar ese comportamiento es el **Artículo 112 Quáter y Quintus de la Ley de Instituciones de Crédito**. Lo establecido es una sanción de prisión de tres a nueve años y de 30,000 a 300,000 días de multa a quien sin causa legítima o sin consentimiento de quien esté facultado para ello acceda a equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.

Al hacer el análisis, Muñoz señala que hay que agotar variables: **«¿Hay descripciones de puesto en Banco de México? Si la respuesta es sí, vamos bien. ¿Está clasificada la información? ¿Hay mecanismos de seguridad? Esto es: si tienes toda la información en una red interna y yo trato de entrar a la carpeta de información de SPEI, ¿me deja entrar o me pide un usuario y contraseña? Se hace una lista para agotar todas las posibilidades con el fin de demostrar que todas las barreras necesarias para que un empleado de otra área no pudiera ver la información de SPEI fueron establecidas. Si el Banco de México cumple con todo esto, entonces sí se puede hablar de acceso no autorizado y hay que iniciar una acción penal»**.

En el contexto penal mexicano se pueden encontrar, dos tipos de ilícitos básicos en el mundo y en **primer lugar se encuentran los que tienen la finalidad de destruir alterar o extraer información no autorizada de los sistemas informáticos en segundo los delitos del orden común que se cometen a través de nuevas tecnologías**, en este último rubro encontramos por ejemplo el popular facing jurídicamente son varios ilícitos que se cometen en un mismo momento.

Una de las primeras condenas por cometer **delitos informáticos** sucedió en 1983 contra cuando fue sentenciado a 24 meses de libertad condicional por **acceso no autorizado** a diversos sistemas de entidades financieras de eeuu. Después una de las condenas más famosas fue la que se impuso a Kevin Mitnick un **hacker** que logró **vulnerar la seguridad** de los sistemas operativos de digital midnight fue considerado por las autoridades federales de eeuu como uno de los individuos más peligrosos durante el juicio los abogados en su contra convencieron al juez de al jurado de que Mitnick tenía la capacidad de comenzar una guerra nuclear a través del sistema telefónico. Las empresas tampoco se salvan del juicio, en julio de este año la oficina del comisionado de información del reino unido informó a marista internacional que le impondría una sanción de 124 millones de dólares por incumplir el reglamento general de **protección de datos** europeos al no almacenar con suficiente **seguridad** los datos de sus clientes.

En México de acuerdo con la abogada, asistente a solistas, socia del léxico y especialista en legislación informática, el país ha avanzado en materia de **delitos informáticos** en los últimos años desde el 2000 se han realizado una serie de **reformas legislativas** a nivel del código penal federal y desde el 2008 se han incorporado en los códigos penales de diferentes estados como Querétaro, Yucatán Chihuahua y Baja California, entre otros ilícitos que son considerados como delitos informáticos. Si revisamos la legislación mexicana veremos que a quien acceda sin consentimiento a medios electrónicos para obtener **información confidencial** u obtener recursos económicos se le aplicará una **sanción** de hasta nueve años en prisión y 300.000 días de salario mínimo en multas que equivaldrían más o menos a un millón y medio de dólares el reto que tiene la legislación mexicana es crear nuevos tipos penales con nuevas figuras delictivas para poder aplicar las sanciones adecuadas.



- Delitos informáticos
- Empresas afectadas
- Legislación a nivel federal
- Información clasificada
- Usuario/Contraseña
- Acciones penales
- Acceso no autorizado
- Vulnerabilidad en seguridad
- Protección de datos
- Información confidencial

Algunos delitos informáticos actualizan los del orden común

Hay dos tipos de **delitos** de este tipo: aquellos que tienen como **finalidad destruir, alterar, modificar o extraer información de manera no autorizada** de los sistemas informáticos; y los delitos del **orden común que se cometen a través de nuevas tecnologías**. En la segunda clasificación entra el **phishing**. Jurídicamente es un concurso de delitos, son diferentes **ilícitos** que se cometen en un mismo momento.

El hecho de **copiar o clonar la apariencia de una página web ya es un delito** en materia de derechos de autor, pero lo que se busca realmente es cometer el delito de fraude: apoderarse de un bien a través del engaño o aprovechando el error de la persona. El fraude se puede cometer a través de **medios electrónicos o físicos**. Ese es un **delito federal del orden común**.

Del 2000 para acá ha habido **reformas legislativas** a nivel del Código Penal Federal, como los artículos **210, 211, 211 bis** y subsecuentes que incorporaron por primera vez tipos penales que hablan de sistemas de cómputo. Desde el 2008 se han incorporado en los **Códigos penales de diferentes estados** (como Querétaro, Yucatán, Chihuahua y Baja California, entre otros) ilícitos que son considerados **delitos informáticos**.

Se ha observado el aumento en casos **phishing** y de **ransomware** que han sufrido compañías de todos los tamaños, desde las chiquitas hasta paraestatales como Pemex, SE o Mapfre. A nivel global, en 2020 han crecido **715%** los reportes de **ataques por ransomware** de un año a otro, de acuerdo con el Reporte de amenazas de mediado de año del 2020, de **Bitdefender**.

-Delito federal de orden común

- Destruir/Alterar/Modificar/Extraer Información

-Lícitos

- phishing

--Ataques

- Ransomware

-Copiar/Clonar apariencia de páginas web

-Reformas legislativas

-Medios electrónicos y físicos

La estrategia nacional es comparable con la de otros países

Aún cuando México ha sido criticado por no incorporar más delitos relacionados con tecnología, sigue la tendencia de países como Francia, que ha tenido un gran avance. En EE.UU., mientras tanto, existe el mismo modelo que en México: no hay como tal un catálogo especializado de delitos, **no hay una ley de delitos informáticos**, pero en la práctica se **incorporan o se adecuan** algunos tipos penales comunes al **entorno informático**.

Un tema especialmente delicado en materia de **legislación informática** es el de la **violencia digital**, que puede comenzar con la difusión sin consentimiento de imágenes, videos o audios personales. El 3 de diciembre de 2019 se aprobó en el Congreso de la Ciudad de México la llamada “**Ley Olimpia**”, un conjunto de reformas a Códigos Penales de las entidades federativas, así como a la Ley general de Acceso de las mujeres a una vida libre de violencia.

Estas reformas reconocen la **violencia digital** como un tipo de **delito** que consiste en actos de acoso, hostigamiento, amenazas, vulneración de datos e información privada, así como la difusión de contenido sexual (ya sean fotos, videos o audios), sin el consentimiento o mediante engaños a una persona.

Alessandra Rojo de la Vega, diputada local por la Ciudad de México, comentó que ya se presentó la iniciativa en el Congreso de la Unión para que esta ley tenga **aplicación en todo el país**.

-Ley de delitos informáticos

-Incorporan/adecuan

-Entorno informático

- Legislación informática

-Violencia digital

-"Ley Olimpia"

-Acoso/Hostigamiento/Amenazas/Etc

-Aplicación en todo el país

Hay gran riesgo de que la legislación quede rezagada

Solís, quien desde agosto de este año es **coordinadora** de la Comisión de Protección de **datos personales y transparencia** de la Barra Mexicana de Abogados, BMA, considera que **México** va por buen camino en **legislación de delitos informáticos**, hay ocasiones que las **actualizaciones no se hacen adecuadamente y es fácil que la legislación se rezague**.

Artículos que se introdujeron en esa ocasión está el **269E**, acerca del uso de **software malicioso**, que indica que “El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1,000 salarios mínimos legales mensuales vigentes”.

Se estableció el delito de **phishing** como tal, refiriéndose a la **suplantación de sitios web para capturar datos personales (Artículo 269G)**; pero solamente lo enfocaron a páginas web y dejaron fuera el phishing que se comete a través de redes sociales, filtros, incluso el propio **SMiShing**.

-Datos personales y transparencia inadecuadas

-Actualizaciones

-Rezago de legislación

-Artículo 269E

-Software malicioso

-Phishing

- Suplantación de sitios web

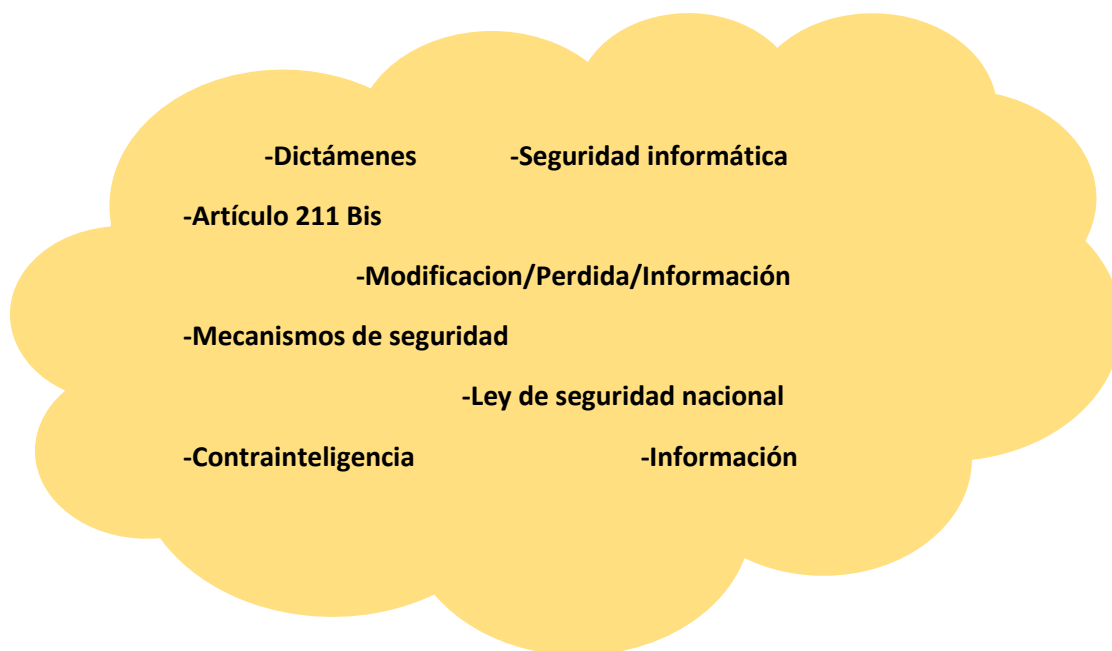
- Datos personales

Reformas relativas a delitos informáticos

En septiembre del 2019, la Comisión de Seguridad Pública de la Cámara de Diputados **aprobó dos dictámenes** para reformar las leyes General del Sistema Nacional de Seguridad Pública relativa a **seguridad cibernética** y de Seguridad Nacional en materia de inteligencia.

Se trata de una reforma al **Artículo 211 Bis 1** del Código Penal Federal para que quede como sigue: **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 dos a cinco años de prisión y de trescientos a seiscientos días multa. 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 seis meses a tres años de prisión y de ciento cincuenta a doscientos cincuenta días multa.

El segundo dictamen modifica el **artículo 32 de la Ley de Seguridad Nacional**, e indica que para los efectos de esta normatividad se entiende por **contrainteligencia a la generación de información** y a las actividades dirigidas a la detección, localización y protección contra actividades de inteligencia, espionaje y sabotaje realizados o planificados por gobiernos extranjeros, individuos u organizaciones del exterior, o por el crimen organizado, con pretensiones de vulnerar la estabilidad interior.



Protección de datos personales

Las organizaciones también tienen una responsabilidad de **protección sobre los datos personas que guardan**. En México también existe la **La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPP)**, que establece un tratamiento especial para información que, de divulgarse de manera indebida, afectarían la esfera más íntima del ser humano. **La Ley y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) garantizan el derecho de protección de datos personales.**

En la página web del INAI se listan varias categorías de datos personales:

- De identificación: nombre, domicilio, teléfono, correo electrónico, firma, RFC, CURP, fecha de nacimiento, edad, nacionalidad, estado civil, etcétera.
- Laborales: puesto, domicilio, correo electrónico y teléfono del trabajo.
- Patrimoniales: información fiscal, historial crediticio, cuentas bancarias, ingresos y egresos, etcétera.
- Académicos: trayectoria educativa, título, número de cédula, certificados, etcétera.
- Ideológicos: creencias religiosas, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas; de salud (estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico).
- Características personales: tipo de sangre, ADN, huella digital o similares.
- Características físicas: color de piel, iris y cabellos, señales particulares, entre otras.
- Vida y hábitos sexuales, además de origen étnico y racial.

En la **LFPDPP** se establece que “los poseedores de los datos deben dar a conocer a los titulares, la información que de ellos se recaba y los fines para los cuales serán utilizados sus datos, a través del **aviso de privacidad**”.

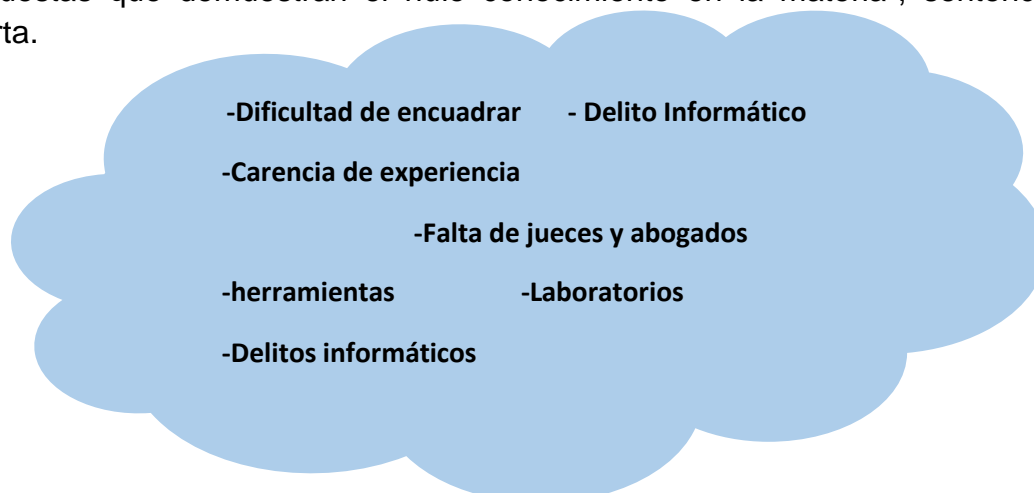
En caso de **incumplimiento** se podrán imponer **sanciones** desde 100 a 320,000 días de multa y/o de tres meses a tres años de cárcel a cualquier persona autorizada para **procesar datos personales que, con fines de lucro, provoque una violación de seguridad que afecte a las bases de datos**; de seis meses a cinco años de cárcel a cualquier persona que, con el **objetivo de obtener ganancias ilegales**, procese los datos personales engañosamente.



Retos por delante

No obstante, en la práctica, la especialista se ha enfrentado a casos donde el juez no entiende cómo se lleva a cabo la conducta y le es **muy difícil encuadrar el delito informático en un tipo penal existente**. En derecho penal es requisito que la ley específica describa la conducta, luego tienes que comprobar que cada punto se cumplió. «Entonces, si la conducta no está descrita como tal, a detalle y con la redacción que está prevista en el Código, no puedes hacer nada. » .

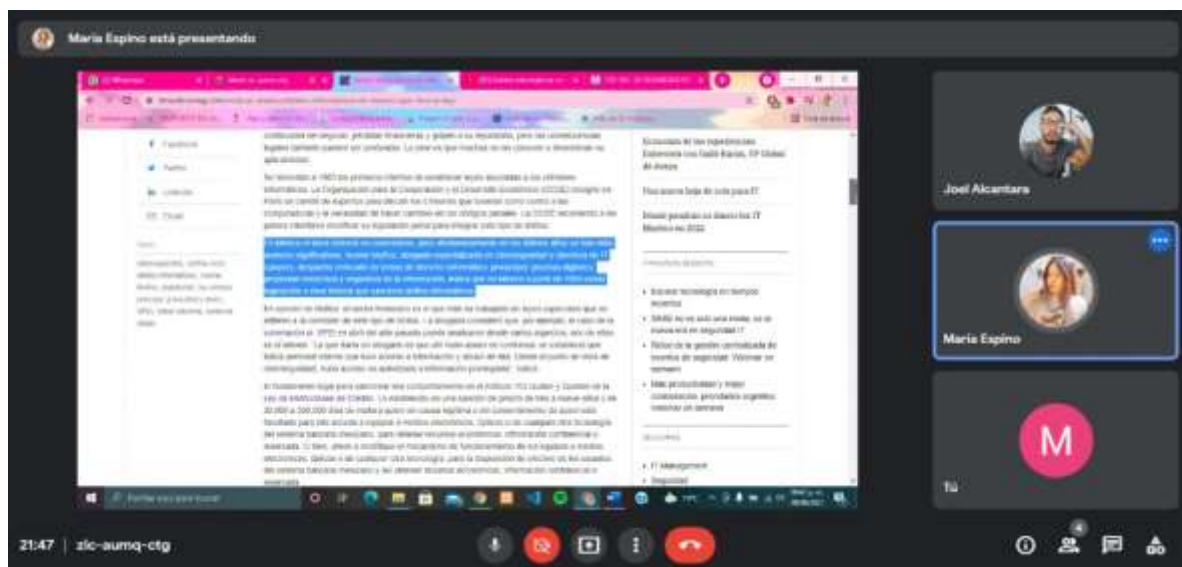
Para Muñoz, el panorama es bastante gris, porque la autoridad investigadora suele **carecer de experiencia, a pesar de contar con laboratorios y herramientas que investigan los delitos informáticos** como cualquier otro. Además hay muy **pocos abogados y jueces especializados**, y la actual legislatura ha presentado "propuestas que demuestran el nulo conocimiento en la materia", sentencia la experta.



Referencias:

- Ferrer, J., & Quiceno, I. (2021, February 18). Confianza Cero. Vmware.com. <https://blogs.vmware.com/latam/2021/02/confianza-cero.html>
- inicio - PNT. (n.d.). Org.Mx. Retrieved September 8, 2021, from <https://www.plataformadetransparencia.org.mx/web/guest/inicio>
- Nueva Ley Publicada en el Diario Oficial, de la F. el 18 de J. de. (n.d.). LEY DE INSTITUCIONES DE CRÉDITO. Gob.Mx. Retrieved September 8, 2021, from https://www.senado.gob.mx/comisiones/finanzas_publicas/docs/LIC.pdf
- (N.d.). Gov.Co. Retrieved September 8, 2021, from https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf
- Delitos informáticos en México, ¿qué dice la Ley? (2019, October 4).

Evidencia de trabajo en equipo



21:48 | zic-aumq-ctg