Seguridad Pública

UnADM
Universidad Abierta y a Distancia de México

Nombre de la asignatura

Delincuencia tecnológica

5º semestre

Clave:

LIC. 01143526

Unidad 2

Delitos informáticos

División de Ciencias Sociales y Administrativas

Índice

Presentación

En esta unidad se analizará el marco jurídico internacional y nacional de los delitos tecnológicos, la tipificación de los delitos informáticos en el Código Penal Federal, las tecnologías que se deben normar para que los usuarios estén protegidos de acciones asociadas al uso de tecnologías, como: la corrupción de menores, pornografía infantil, robo de identidad, intromisión a la privacidad, derechos de autor y delincuencia organizada.

A través del análisis del marco legal se pretende proporcionar dos aspectos medulares para el profesional de seguridad pública: por un lado, que elabore propuestas de actualización del marco legal vigente (dada la aparición vertiginosa de nuevos delitos informáticos) y, por otro lado, ser consciente del marco legal para su actuación.

Se analizará el perfil criminológico de los delincuentes informáticos (hackers y crackers) y el *modus operandi* más común que los caracteriza, ya que existe una gran gama respecto a los delitos que se cometen y que han sido denominados “delitos informáticos”, “tecnológicos” o “cibernéticos”, como la intromisión a la privacidad o el robo de identidad. Se hablará también de sus efectos sociales y económicos en México y la clasificación de la delincuencia tecnológica.

Propósitos

Al final de la unidad, el (la) estudiante será capaz de:

- Identificar las principales leyes nacionales e internacionales que regulan los delitos informáticos.
- Analizar las características de la delincuencia tecnológica, así como el perfil criminológico y el *modus operandi* de losdelincuentes informáticos.
- Identificar las consecuencias de los delitos tecnológicos tanto sociales como económicos.

Competencia a desarrollar

- Analiza el marco jurídico que tipifica a la delincuencia tecnológica para identificar vacíos y duplicidades mediante la elaboración de propuestas de políticas públicas en materia de seguridad cibernética.

Marco jurídico de la delincuencia tecnológica

El surgimiento de Internet como herramienta de acceso a la comunidad cibernética ha dado paso a nuevos delitos en todo el mundo. La regulación y tipificación de las conductas denominadas delitos informáticos a nivel internacional y nacional para proteger a los usuarios de la red es una necesidad de la población, así como disminuir la impunidad y la corrupción en este ámbito. Los países que participaron en la elaboración de convenios y tratados internacionales **están obligados a armonizar sus leyes** para proteger a sus ciudadanos de los ataques de los delincuentes cibernéticos y establecer mecanismos de seguridad para los usuarios que utilizan la red. Los delincuentes aprovechan los vacíos legales para cometer los delitos que dejan indefensos a los usuarios de Internet, por lo que la seguridad informática es prioritaria y parte de la formación de nuevos profesionales de la seguridad pública.

Marco jurídico internacional

El *Convenio sobre la ciberdelincuencia* es el principal documento a nivel internacional para combatir lo que se denominó "ciberdelincuencia". Es el primero en definir una política penal en contra de la delincuencia informática, y promueve la participación de los estados europeos. En el artículo 1° se encuentran los conceptos medulares y los principales delitos informáticos:

1. Sistema informático	Todo aquel dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos sea el tratamiento automatizado de datos en ejecución de un programa.
2. Datos informáticos	Se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.
3. Proveedor de servicios	a) Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a travésde un sistema informático. b) Cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.
4. Datos relativos al tráfico	Se entenderán como los servicios relativos a una comunicación realizada por medio de un sistema informático, generados por este último y que indican el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de lacomunicación o el tipo de servicio subyacente.

Fuente: Council of Europe (2001, 4).

Los tipos penales que el *Convenio sobre la ciberdelincuencia* contiene son delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos, los propios delitos informáticos (falsificación de información y fraude informático), delitos relacionados con el contenido (como pornografía infantil), delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines y tentativa, complicidad y responsabilidad de las personas jurídicas. Al ser un convenio internacional, cada Estado suscrito a él tiene la facultad de tipificar las conductas mencionadas en él de acuerdo a su contexto derivado de su legislación.

Para saber más consulta el siguiente material	Recuperado de:
Council of Europe. (2001). *Convenio sobre la ciberdelincuencia*.	https://goo.su/Jr6u

Marco jurídico nacional

El marco jurídico nacional se conforma con los siguientes instrumentos jurídicos (se señalan aspectos relevantes):

Constitución Política de los Estados Unidos Mexicanos	**Artículo 133.** *Esta Constitución, las leyes del Congreso de la Unión que emanen de ella y todos los Tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión. Los jueces de cada Estado se arreglaráná dicha Constitución, leyes y tratados, a pesar de las disposiciones en contrario que pueda haber en las Constituciones o leyes de los Estados.*	**Artículo 104. Los tribunales de la Federación conocerán:** I" De los procedimientos relacionados con delitos del orden federal"	**Artículo 16 Constitucional Reformas DOF: 18/06/2008** *Por delincuencia organizada se entiende una organización de hecho de tres o más personas, para cometer delitos en forma permanente o reiterada, en los términos de la ley de la materia.* *"las comunicaciones privadas son inviolables.* *La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas"*
Ley Federal de Protección Datos Personales en Posesión de los Particulares	*Se establece que toda aquella persona física o moral que cuente con bases de datos que contengan datospersonales están obligadas a proteger en todo momento la privacidad de los mismos para garantizar este derecho humano y garantía individual que son fundamentales para el libre desarrollo de los ciudadanos.*		
La Ley Federal Contra la Delincuencia Organizada	*La presente Ley tiene por objeto establecer reglas para la investigación, persecución, procesamiento, sanción y ejecución de las penas, por los delitos cometidos por algún miembro de la delincuencia organizada. Sus disposiciones son de orden público y de aplicación en todo el territorio nacional.*		

Código Penal Federal	***Título noveno**: Revelación de secretos y acceso ilícito a sistemas y equipos de informática Artículos 210, 211, 211 Bis, 211 bis 2,211 bis 3, 211 bis 4, 211 bis 5.*	***Artículo 200.** Sobre la **corrupción de menores***	***Artículo 202.** Sobre la privacidad e integridad y los derechos humanos de los ciudadanos y niñas, niños y adolescentes, como es el caso de la **pornografía infantil***
Ley Federal de Derechos de autor	**Artículo 4°** *Protege las obras publicadas mediante el almacenamiento de medios electrónicos que permitan al público obtener ejemplares tangibles de las obras. Por lo que protege el contenido usado en la red por medio delos usuarios*		

De acuerdo con el artículo 21 de la Constitución Política de los Estados Unidos Mexicanos, se establece que “la investigación de los delitos corresponde al Ministerio Público y a las policías, las cuales actuarán bajo la conducción y mando de aquél en el ejercicio de esta función” (17), por lo que corresponde a la Fiscalía General de la República la persecución e investigación de delitos federales que establece la cooperación entre los niveles de gobierno para garantizar la seguridad nacional; para tales efectos se creó la **policía cibernética** perteneciente a la Policía Federal, que fue creada en 2001 y tiene la facultad para investigar los delitos cibernéticos.

Por lo tanto, los delitos informáticos son de competencia federal, por lo que el 28 de marzo de 2012, la Cámara de Diputados aprobó las reformas al Código Penal Federal para que se tipifiquen los delitos informáticos, por lo que se encuentran ya regulados, definidos y penados. Tratándose de competencia local, un ejemplo es el **Código Penal Federal** que establece:

Delito	Artículos
Usurpación de identidad	Artículo 211 bis: https://goo.su/wTFj8E
Revelación de secretos	Artículo 211 https://goo.su/M4bxY

Tipificación de los delitos informáticos

El Código Penal Federal, Título 9º, muestra los tipos penales de los delitos informáticos. En cuanto a **Revelación de Secretos**, postula lo siguiente:

Artículo 210	Artículo 211	Artículo 211 bis
Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que, sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.	*La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por personaque presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial*.	*Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sele impondrán de seis meses a dos años de prisión y de cien atrescientos 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 tresmeses a un año de prisión y de cincuenta a ciento cincuentadías multa.* *A quien revele, divulgue o utilice indebidamente o en perjuiciode otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días de multa.*

Respecto a **Acceso ilícito a sistemas y equipos de informática** postula:

211 bis 1 Sobre la revelación de secretos, el acceso ilícito a sistemas y equipos de informática	211 bis 2 Sobre la modificación, pérdida, destrucción, copia, utilización de información contenida en equipos o sistemas de informática del Estado o de seguridad pública.	211 bis 3 Sobre aquellos autorizados que modifiquen, destruyan, provoquen pérdida copieno utilicen de información de equipos de informáticadel Estado	211 bis 4 Sobre la modificación, destrucción, provocaciónde pérdida, copia de información contenida en sistemas o equipos del sistema financiero protegidos por algún sistema de seguridad	211 bis 5 Sobre aquellos autorizados que modifiquen, destruyan, provoquen pérdida copien o utilicen de información de sistemaso equipos del sistema financiero.

Para saber más consulta el siguiente material	**Recuperado de:**
Cámara de Diputados del H. Congreso de la Unión. *Código Penal Federal*	https://www.diputados.gob.mx/LeyesBiblio/ref/cpf.htm

Respecto a los delitos sobre la pornografía infantil y corrupción de menores, su tipificación es la siguiente:

Delitos	Tipo penal
Pornografía Infantil **Artículo 202**	Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto ***de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos dedatos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos***. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa…
Corrupción de menores. **Artículo 200**	***Al que comercie, distribuya, exponga, haga circular u oferte, a menores de dieciocho años de edad, libros, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes u objetos, de carácter pornográfico, reales o simulados, sea de manera física, o a través de cualquier medio***, se le impondrá de seis meses a cincoaños de prisión y de trescientos a quinientos días multa.

Fuente: Cámara de Diputados H. Congreso de la Unión (2021).

El análisis y conocimiento del marco legal proporciona herramientas para perseguir y sancionar los delitos informáticos, y que permanentemente debe actualizarse. También ofrece un marco de actuación a las acciones de seguridad pública, por ello es vital para los profesionales de seguridad pública.

Correspondencia entre el marco legal y el avance del uso de las tecnologías

Es necesario crear una nueva legislación respecto al uso de los servicios de redes sociales, las cuales están clasificadas en redes internas y externas. Dentro de las últimas están Myspace, Facebook, Twitter, así como aplicaciones que se han desarrollado respecto al tipo de mensajería, como WhatsApp, que es una de las más utilizadas.

Derivado del uso masivo de Twitter y Facebook, se han encontrado un sinnúmero de conductas antisociales que afectan los derechos y la privacidad de los usuarios. El uso de las tecnologías a través de equipos de cómputo, como tabletas y teléfonos inteligentes que utilizan el servicio de las redes sociales externas, constituye una problemática, por lo que falta en las legislaciones, tanto nacionales, como internacionales, regular y normar su uso, pues se han convertido en medios específicos utilizados por los usuarios y delincuentes informáticos para violar los derechos humanos, el libre desarrollo emocional y la privacidad de los usuarios de estas redes.

Delitos informáticos: perfil y conductas criminales

La delincuencia tecnológica comete delitos informáticos, que se pueden clasificar en dos tipos:

a. Como **instrumento** o **medio**. Están contempladas las conductas que utilizan las computadoras como método, medio o símbolo para la comisión del delito. Téllez (2008: 190) establece los siguientes ejemplos de lo que debe considerarse como instrumento o medios:

a)	Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera).
b)	Variación de los activos y pasivos en la situación contable de las empresas.
c)	Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera).
d)	"Robo" de tiempo de computadora.
e)	Lectura, sustracción o copiado de información confidencial.
f)	Modificación de datos tanto en la entrada como en la salida.
g)	Aprovechamiento indebido o violación de un código para penetrar a un sistema con instrucciones inapropiadas (esto se conoce en el medio como método del caballo de Troya).

h)	Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como técnica de salami.
i)	Uso no autorizado de programas de cómputo.
j)	Inclusión de instrucciones que provocan "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios.
k)	Alteración en el funcionamiento de los sistemas.
l)	Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.
m)	Acceso a áreas informatizadas en forma no autorizada.
n)	Intervención en las líneas de comunicación de datos o teleproceso.

b. **Como fin u objeto.** Aquí se encuentran las conductas dirigidas en contra de la computadora, accesorios o programas como entidades físicas. A continuación, se mencionan ejemplos establecidos por Téllez (2008: 190-191):

a)	Programación de instrucciones que producen un bloqueo total al sistema.
b)	Destrucción de programas por cualquier método.
c)	Daño a la memoria.
d)	Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera).
e)	Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
f)	Secuestro de soportes magnéticos en los que figure información valiosa (con fines de chantaje, pago de rescate, etcétera).

Por otro lado, existen dos clasificaciones más de los delitos informáticos que no están especificadas en las tablas anteriores, como los ligados directamente con acciones efectuadas contra los sistemas:

a) **Acceso no autorizado:** uso ilegítimo de *passwords* y la entrada de un sistema informático sin autorización del propietario.
b) **Destrucción de datos:** los daños causados en la red mediante la introducción de virus, bombas lógicas, etcétera.
c) **Infracción a los derechos de autor de bases de datos:** uso no autorizado de información almacenada en una base de datos.
d) **Intercepción de e-mail:** lectura de un mensaje electrónico ajeno.
e) **Fraudes electrónicos:** mediante compras realizadas al usar la red.
f) **Transferencias de fondos:** engaños en la realización de este tipo de transacciones.

La segunda clasificación es la concerniente al uso de Internet que permite la comisión de los siguientes delitos:

1. **Espionaje:** acceso no autorizado a sistemas informáticos gubernamentales y grandes empresas, e intercepción de correos electrónicos.
2. **Terrorismo:** mensajes anónimos aprovechados por grupos terroristas para remitir consignas y planes de actuación a nivel internacional.
3. **Narcotráfico:** transmisión de fórmulas para la fabricación de estupefacientes, para el lavado de dinero y para la coordinación de entregas y recogidas.
4. **Otros delitos:** las mismas ventajas que encuentran en Internet los narcotraficantes pueden ser aprovechadas para planificar otros delitos, como tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas y cualquier otro que pueda ser trasladado de lavida real al ciberespacio o viceversa (Téllez, 2008: 204).

Los delitos informáticos son muy específicos y tienen características que los hacen diferentes a otros, de acuerdo con Téllez (2008).

- Son conductas criminales de cuello blanco, *white collar crimes*, en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden cometerlas.
- Son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto está trabajando.
- Son acciones de oportunidad porque se aprovecha una ocasión creada o altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a quienes los realizan.
- Ofrecen facilidades de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física.
- Son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica a nivel internacional.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.

- Presentan grandes dificultades para su comprobación, por su carácter técnico.
- En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales.
- Ofrecen a los menores de edad facilidades para su comisión.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional. Presentan grandes dificultades para su comprobación por su carácter técnico (188).

Las características indican que el **sujeto activo del delito** debe tener un conocimiento específico sobre el manejo de sistemas informáticos; generalmente, busca ubicarse laboralmente en un ambiente en el que le sea posible el acceso a la información. Suele estar al tanto de las modificaciones de las leyes para cometer sus "conductas" y que no se le imponga una sanción. Al tratarse de delitos "de cuello blanco", las ganancias que obtiene le permiten tener acceso a las tecnologías necesarias para burlar los sistemas de seguridad y no ser identificado, por lo tanto es indispensable establecer su perfil criminológico para identificarlo y tratar de establecer un perfil de búsqueda que permita a los cuerpos de seguridad identificar a estos sujetos socialmente nocivos para la sociedad, por lo que en el siguiente tema se analizará y establecerá el perfil general de estos delincuentes.

Perfil criminológico

Profiling es un perfil criminal o criminológico. Garrido (2012) define al perfil de los delincuentes desconocidos como "la disciplina de la ciencia forense que se ocupa de analizar las huellas del comportamiento en una escena del crimen con el objeto de proveer información útil a la policía para la captura de un delincuente desconocido".

Para saber más consulta el siguiente material	Recuperado de:
Rivera, S. (2009). Los delitos informáticos. *Boletín Criminolóxico*, 2009(11), 10-12.	http://goo.gl/PkVGTz

Perfil genérico de los hackers

En general, los hackers son expertos en el manejo de una o varias ramas técnicas relacionadas con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, por lo que buscan el descuido de los usuarios para obtener los datos necesarios. Generalmente por requerimientos del ambiente en que se desenvuelven, usan seudónimos; sin embargo, cabe recalcar que no siempre son antisociales o disociales, o que no son poseedores de un perfil criminal necesario, sino que por lo general tienen una vasta diversidad de motivos por los cuales realizan las actividades. Generalmente tienen un alto coeficiente intelectual y se sienten estimulados con las novedades de este tipo. No se puede estandarizar como un solo perfil, lo cual los hace más difíciles de ser detectados.

Como verás, derivado del perfil se llega a la conclusión de que el tipo de personalidad correspondiente a los delincuentes informáticos es muy específico, lo que permite a su vez poder delimitar la investigación respecto a los delitos informáticos.

Tipología de los delincuentes informáticos

La más común de las tipologías de los delincuentes tecnológicos es:

Piratas informáticos	Denominación general usada para hackers y crackers. Este tipo de sujeto se dedica a copiar software sin permiso del autor para, posteriormente, venderlo o liberarlo en la red.
Phreaker	Estos sujetos son expertos en el uso de la telefonía, la cual pueden manipular para su propia conveniencia. En la actualidad, los *phreaker* se han especializado en teléfonos celulares
Lammers	Estos sujetos no poseen las capacidades y habilidades de un hacker o un cracker, sino que con el poco conocimiento que poseen se hacen pasar como por uno de ellos.

Sin embargo, con el avance de las tecnologías, se encontrará nuevas tipologías delincuenciales respecto a los delitos informáticos, que pueden ser realizados por varios sujetos activos que, en conjunto, realizan una sola conducta delictiva, por eso es importante determinar el grado de participación y culpabilidad del sujeto. Así, se ha establecido una serie de conductas que son las más comunes dentro de los delitos informáticos, como el fraude y el robo a personas y empresas. De acuerdo con el Manual de las Naciones Unidas para la prevención y control de los delitos informáticos, se determinó que el 90% de estos delitos son cometidos por personas que laboran dentro de la misma empresa víctima del delito.

Dentro de los delitos informáticos hay que especificar bien la conducta que se está cometiendo y que se encuentra tipificada como delito, ya que, si se lleva a cabo una conducta, pero ésta no se cometió tal como lo establece el Código Penal, se estará frente a una conducta que lesiona el bien común, pero por las variantes que presenta, no sería considerada como un delito.

Por ejemplo:

Karla utilizó Facebook en un café Internet y, al terminar la conversación, no cerró la sesión; sólo cerró la página. El siguiente usuario que llegó a la computadora abrió Facebook y encontró la sesión de Karla activa; copió sus contactos y conversaciones y, haciendo uso de la información, molestó a todos los contactos de Karla e intentó extorsionarla para que deje de molestar a sus contactos.

En este caso, el sujeto invadió la privacidad de Karla y de sus contactos, pero no hay delito, ya que la conducta no se adecua al siguiente tipo penal del Código Penal Federal:

Artículo 211 bis. A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Dado que en ningún momento el sujeto intervino la comunicación de Karla, no hackeó su cuenta, sino que ella la dejó abierta a disposición de cualquiera, el tipo penal no se adecua al hecho.

Modus operandi

Los *modus operandi* más comúnmente utilizados por los delincuentes informáticos son:

Introducción de datos falsos (*data diddling*). Es la manipulación fraudulenta de las transacciones de entrada a un sistema informático al introducir movimientos falsos o eliminar la entrada de operaciones reales

Caballo de Troya (*Trojan horse*). En un programa normal se incluye una serie de instrucciones no autorizadas que actúan, en ciertos casos, de forma diferente a aquello que había sido previsto; evidentemente, en beneficio del autor o para sabotear al usuario.

Técnica del salami (*salami technique*). Consiste en pequeñas manipulaciones que, sumadas, hacen un gran fraude. Es habitual citar en este punto el no demostrado y casi mítico caso de la desviación fraudulenta de centavos en transacciones bancarias o de nóminas.

Uso no autorizado de programas especiales (*superzapping*). Hace referencia a la utilización no autorizada de cualquier programa para alterar datos y resultados, u obtener información. El nombre en inglés de este tipo de fraude deriva de un conocido programa de servicio de ciertos sistemas de IBM: "*superzap*".

Puertas falsas (*trap doors*). Consiste en hacer "agujeros" y defectos en la seguridad de los sistemas y las "entradas especiales" que, generalmente, con aspecto de provisionalidad, poseen los programas para hacer más ágil su proceso de prueba y depuración, y permitir que la instalación de la versión definitiva sea exitosa.

Bombas lógicas (*logic bombs*). Permiten realizar un tipo distinto de sabotaje, utilizando rutinas ocultas (la bomba lógica). En cada ejecución de un programa, por ejemplo, al llegar a un cierto valor, se ejecuta una operación destructiva. Es un procedimiento que, regulado por una computadora o por un dato clave, se convierte en el más habitual de los virus informáticos.

Ataques asíncronos (*asynchronous attacks*). Se aprovecha la posibilidad que tiene el sistema operativo de volver a inicializar el sistema en condiciones diferentes a las autorizadas, por ejemplo, en ciertos puntos de recuperación del sistema. Un ejemplo de un ataque asíncrono sería un programa que reproduzca la pantalla de entrada en un sistema. Cuando el usuario proporciona su clave, se almacena ésta en un archivo de la persona que realiza el fraude. De esta manera logra el acceso que le estaba prohibido.

Recogida de información residual (*scavenging*). Consiste en aprovechar todo tipo de desechos, como listados y manuales tirados en la papelera, que no han sido destruidos; emplear el estado final de la memoria al finalizar la ejecución de un programa, etcétera, para obtener información reservada y sensible.

Divulgación no autorizada de datos reservados (*data leakage*). Incluye la divulgación no autorizada de información secreta, datos obtenidos por espionaje o adquiridos de manera fraudulenta. Suele ser información producida con otra finalidad, como el censo electoral, información médica, etcétera.

Entrada a caballo (*piggybacking and impersonation*). Conocido también como "ingeniería social", consiste, por ejemplo, en hacerse pasar por otra persona para conseguir información reservada.

Intervención de líneas (*wiretapping*). Se intervienen las líneas de comunicación informática para acceder o manipular los datos que circulan a través de ellas.

Simulación y modelado de delitos (*simulation and modeling*). Se utiliza una computadora para planear y controlar un delito mediante técnicas de simulación que permiten ver qué pasaría si realmente se realiza el delito.

Exploración (*scanning*). Consiste en hacer una exploración secuencial para encontrar números telefónicos o claves de usuario que permiten el acceso a la computadora o a los sistemas informáticos reservados.

Mirar sobre el hombro (*shoulder surfing*). Como su nombre lo indica, se trata de mirar sobre el hombro de un operador autorizado para seguir el movimiento de sus dedos sobre el teclado cuando escribe su clave con el fin de robarla.

Buscar en la basura (*dumpster diving*). Se buscan en la basura documentos que no fueron destruidos y que contienen información sensible.

Mistificación (*spoofing*). Es la nueva denominación que se da a la anteriormente llamada "ingeniería social", que permite obtener información con engaños y simulación de personas.

Fuente: Albizuri (2002).

Los medios por los cuales los delincuentes informáticos cometen los delitos cambian de forma vertiginosa, lo que da como resultado un sinnúmero de *modus operandi*; por ello, la intervención e investigación es crucial para detectarlos a tiempo.

Consecuencias del delito tecnológico

Las consecuencias que provocan los delitos tecnológicos son: la intromisión a la privacidad de las personas que ponen en riesgo su integridad personal; el robo de identidad (ha provocado un sinnúmero de fraudes y delitos contra el patrimonio de personas a nivel mundial); por ello, es importante conocer las consecuencias, así como la clasificación de los delitos informáticos.

Intromisión a la privacidad

El derecho a la privacidad, contenido en el artículo 16, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, establece: Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Así, la privacidad es un derecho consagrado como garantía individual y derecho humano que, si se viola, deja desprotegida a la víctima. En la legislación se encuentran estos derechos protegidos por la Ley Federal de Protección de Datos y el Aviso de Privacidad, en donde se establece cuáles son los datos privados:

1. Nombre completo 2. Dirección 3. Números telefónicos (casa o celular)	4. Clave Única de Registro de Población 5. Registro Federal de Contribuyentes 6. Estado civil	7. Preferencia sexual 8. Firma electrónica avanzada 9. Tipo de sangre

Este tipo de delito comprende conductas que afectan dicha privacidad y la divulgación indebida de los datos, ya sea a través de la red o con fines de lucro indebido o, en su caso, para extorsionar a la víctima.

Se necesita elaborar un tipo penal que contemple, por lo menos, los principales *modus operandi* por los cuales se viola este derecho. Por ello ha quedado establecido y tipificado este delito, por lo que se requiere que se regulen tres aspectos importantes:

Interceptación del e-mail	Interceptación de telecomunicaciones: con el uso de tecnología para escuchar transmitir, grabar o reproducir sonidos o imágenes sin autorización.	Divulgación no autorizada de datos: dicha información puede estar contenida en una computadora que está clasificada como confidencial.

La Organización para la Cooperación y el Desarrollo Económico (OCDE) propone ocho principios para proteger la privacidad:

1. Límite de obtención	✓ Consiste en la imposición de límites para la obtención de datos personales a través de medios apropiados y legales, haciéndolo del conocimiento y obteniendo el conocimiento
2. Calidad de los datos	✓ Consiste en la importancia de asegurar la exactitud, totalidad y actualización de los datos.
3. Propósito de descripción	✓ Consiste en especificar el propósito de recabar información en el momento en que se lleva a cabo la recolección y el subsecuente uso limitado del cumplimiento de dichos propósitos u otros que no seanincompatibles con aquellos especificados en cada ocasión.
4. Límite de uso	✓ Consiste en no divulgar los datos personales o los utilizados para propósitos distintos a los contemplados en el principio anterior.
5. Protección a la seguridad	✓ Tiene la función de proteger datos personales mediante mecanismos razonables de seguridad en contra de riesgos, tales como: pérdida, acceso no autorizado, destrucción, utilización, modificación o divulgación dedatos.
6. Parcialidad	✓ Consiste en establecer políticas generales de imparcialidad sobre desarrollos, prácticas y políticas con respecto a datos personales, asegurando la transparencia en el proceso de obtención de información yestableciendo propósitos para su utilización.
7. Participación individual	✓ Consiste en el derecho que tiene un individuo de obtener del controlador de datos la confirmación de tener o no los datos del individuo, ya que el controlador de datos se lo haya comunicado en un tiempo y forma.
8. Responsabilidad	✓ Consiste en la responsabilidad del controlador de datos de cumplir efectivamente con medidas suficientes para implementar los siete principios anteriores.

La privacidad es un derecho fundamental de todo ser humano, pero por medio del uso de Internet, es el más violado por los delincuentes, ya que se usa la información privada de las personas para lucrar. A pesar de las múltiples recomendaciones y medidas de seguridad adoptadas, aún no se ha podido controlar esta conducta que afecta a los usuarios de las tecnologías.

Robo de identidad

De acuerdo con el Centro de Seguridad y Protección de Microsoft, el robo de identidad "es cualquier clase de fraude que dé como resultado la pérdida de datos personales, como por ejemplo contraseñas, nombres de usuarios, información bancaria o números de tarjetas de crédito". A este delito se le conoce también como suplantación de identidad o con el término anglosajón: *phishing*, que es el más adecuado para referirse al robo de identidad en línea. Dos ejemplos comunes y actuales son:

Correos electrónicos o páginas de Internet diseñadas para robar contraseñas: Un correo electrónico de una cuenta que proporciona la información de un contacto con una liga a una página web y solicita la contraseña personal.	Correo de la Secretaría de Hacienda y Crédito Público donde se informa que el destinatario no ha cumplido con sus declaraciones fiscales, por lo que se solicita acceder a la liga del contribuyente.

Actualmente, la Cámara de Diputados trabaja para que esta conducta sea tipificada de manera correcta y se pueda imponer una sanción a los delincuentes que cometen este delito. Este delito va en aumento; según datos de la empresa CCP de México, este país ocupa el octavo lugar a nivel mundial en cuanto a robo de identidad.

Efectos sociales y económicos

Los dispositivos electrónicos, como computadoras, teléfonos inteligentes, tabletas y otras tecnologías con acceso Internet, se están masificando y con ello los delitos de pornografía infantil, pedofilia, explotación sexual infantil, corrupción de menores y trata de personas.

La pornografía infantil y pedofilia, en México (2010-2011), ha ocupado el primer lugar mundial de acuerdo con datos recabados por la Fiscalía General de la República. El documento de la Policía Federal. División Científica. (2013). *Pornografía infantil en México*, destaca que:

- En 2011 fueron contabilizados cerca de **16,700** sitios web con imágenes y videos de pornografía infantil alojados en 196 países, de los cuales sólo 46 cuentan con una legislación para combatir el abuso infantil.
- En 2010, **España y México tuvieron el mayor intercambio de archivos P2P sobre pornografía infantil** alrededor del mundo.
- En 2011, **México ocupó el tercer lugar a nivel mundial en delitos cibernéticos relacionados con pornografía infantil**. Datos de Google Trends señalan que, durante 2012, **México fue uno de los países que registró mayores búsquedas relacionadas con pornografía infantil.**

Como respuesta a los altos índices de delitos contra niños, niñas y adolescentes relacionados con la pornografía infantil a través de la tecnología, se crea la Coordinación para la Prevención de Delitos Electrónicos, en la División Científica de la Policía Federal.

Las consecuencias económicas de los delitos informáticos a nivel económico, de acuerdo con la Interpol (2013):

> "Se estima que en 2007 y 2008 la ciberdelincuencia tuvo un coste a escala mundial de unos 8,000 millones de USD. Por lo que toca al espionaje informático, en todo el planeta los delincuentes informáticos han robado a diversas empresas propiedad intelectual valorada en un billón de USD" (Interpol, 2013).

Estos delitos denominados "de cuello blanco" dejan millones de ganancias a los delincuentes, millones de pérdidas a las víctimas y cuesta millones al mundo para combatirla.

Cierre

Las competencias desarrolladas en esta unidad sirven para proponer nuevas y creativas acciones de prevención, seguimiento y combate a los delitos informáticos, siempre dentro del marco jurídico vigente a nivel nacional e internacional, por ello es importante identificar la concepción de estos, sus características, el perfil y los tipos de *modus operandi* de los delincuentes; la clasificación delincuencial y las conductas más comunes realizadas por estos sujetos; las consecuencias sociales y económicas que están provocando los delitos informáticos, así como las técnicas que utilizan los delincuentes para cometer el delito de intromisión a la privacidad y robo de identidad.

Uno de los aspectos relevantes de la unidad es reconocer las consecuencias de los delitos informáticos asociados a otras conductas de la delincuencia organizada, como: la pornografía infantil, la trata de personas o la intromisión a la privacidad. Sin embargo, el conocimiento del marco jurídico también provee al nuevo servidor de seguridad pública un marco de actuación legal para que no cometa los mismos delitos en aras de prevenir, dar seguimiento y combatir a la delincuencia tecnológica; es decir, que reconozca los derechos humanos a la privacidad y a una vida libre de violencia como eje normativo y ético de su quehacer.

Para saber más consulta el siguiente material	Recuperado de:
Sullivan, R. (2009). ¿Pueden las tarjetas inteligentes reducir el fraude de pagos y elrobo de identidad? *Boletín del CEMLA,* LV (1), 34–50.	http://goo.gl/Moxm90
Saldaña, N. (2007). La protección de la privacidad en la sociedad tecnológica: elderecho constitucional a la privacidad de la información personal en los Estados Unidos. *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades,* 9(18), 85-115.	http://goo.gl/AF8v3i

Fuentes de consulta

- Acurio, S. (s. f.). Delitos informáticos: Generalidades. Recuperado de http://goo.gl/C5V6Qx
- Albizuri, B. (2002). El fraude y la delincuencia informática: un problema jurídico y ético. *Revista de la Universidad Nacional Autónoma de México*, 3(2), 1-13. Recuperado de http://goo.gl/L4Ua4N
- Council of Europe (2001). Convenio sobre la ciberdelincuencia. Recuperado de https://goo.su/Jr6u
- Europa Press (2012, 28 de diciembre). Los delitos por amenazas y acoso crecen en Twitter y en Facebook en 2012. Recuperado de http://goo.gl/CzTolp
- Garrido, V. (2012). *Perfiles criminales: Un recorrido por el lado oscuro del ser humano*. España: Ariel.
- Interpol (2013). Ciberdelincuencia. Recuperado de https://www.interpol.int/es/Delitos/Ciberdelincuencia
- Notimex (2013, junio 8). Proponen tipificar como delito el robo de identidad. El Financiero Digital. Recuperado de http://goo.gl/qkhKsE
- RAE (2001). *Diccionario de la Real Academia de la Lengua*. Recuperado de http://goo.gl/wtMw2f
- Rivera, S. (2009). Los delitos informáticos. *Boletín Criminolóxico*, *2009*(11), 10-12. Recuperado de http://goo.gl/9WNjJ6
- Téllez, J. (2008). *Derecho informático* (4ª ed.). México: McGraw-Hill.
- Vega, E. *et al*. (2009). *El uso de sistemas cibernéticos de pago en el lavado de dinero.* LexJuris de Puerto Rico. Recuperado de http://goo.gl/vRR02h

Legislación

- Código Penal Federal.
- Constitución Política de los Estados Unidos Mexicanos.
- Ley Federal Contra la Delincuencia Organizada.
- Ley Federal de Protección Datos Personales en Posesión de los Particulares.
- Ley Federal del Derecho de Autor.