Delitos Informáticos

Los delitos informáticos se definen como actitudes ilícitas que tienen a las computadoras como instrumento o las conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin.

Características:

- Son conductas criminales de cuello blanco, en tanto que sólo 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 aquellos que 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.

Clasificación:

Como instrumento.

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera).
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera).
- "Robo" de tiempo de computadora.
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- 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).

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

Como fin u objetivo.

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

Tipos de ataques contra los sistemas de información.

Acceso no autorizado a sistemas de información.

Esto incluye el concepto de "piratería informática", la cual consiste en tener acceso de manera no autorizada a una computadora o a una red de computadoras.

Perturbación de los sistemas de información.

Existen distintas maneras de perturbar los sistemas de información mediante ataques malintencionados.

Ejecución de programas informáticos perjudiciales que modifican o destruyen datos.

El tipo más conocido de programa informático malintencionado es el virus.

Intercepción de las comunicaciones.

La intercepción malintencionada de comunicaciones afecta los requisitos de confidencialidad e integridad de los usuarios y se denomina a menudo #sniffing (intromisión).

Clasificación de acuerdo con las naciones unidas

1. Fraudes cometidos mediante manipulación de computadoras.

   - Manipulación de los datos de entrada
   - Manipulación de programas
   - Manipulación de los datos de salida
   - Manipulación informática aprovechando retenciones automáticas de los procesos de cómputo.

2. Falsificaciones informáticas.

   Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada.

   Como instrumento: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

3. Daños o modificaciones de programas o datos computarizados.

   Sabotaje informático: Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Se usan técnicas como virus, gusanos o una bomba lógica o cronológica.

4. Acceso no autorizado a servicios y sistemas informáticos.

   Piratas informáticos o hackers: El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema.

   Reproducción no autorizada de programas informáticos de protección legal: Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos.

PORNOGRAFÍA INFANTIL EN INTERNET.

En 2000, el Protocolo Facultativo de la Convención sobre los Derechos del Niño define a la pornografía infantil en internet como toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales O simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales.

En la legislación mexicana, el Código Penal Federal se refiere la pornografía infantil como a los actos de exhibicionismo corporal, lascivos o sexuales con el objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro.

El uso masivo de internet ha propiciado un crecimiento exponencial de la pornografía infantil debido a la facilidad para dar visibilidad, publicidad y acceso a todo tipo de materiales.

internet hace factible la consulta de páginas web con material pornográfico, pero mantiene al usuario en el anonimato. Los programas peer to peer; hacen posible compartir el material ubicado en el disco duro de las computadoras, sin dejar rastro.

También el correo electrónico permite enviar fotografías o videos de una punta del mundo a la otra en cuestión de segundos, sin correr el riesgo de pasar por aduanas o controles policiales. Los chats, foros y páginas de comunidades facilitan la comunicación entre pedófilos e incluso el contacto directo con menores.

El uso más actual y novedoso es lo que se ha dado en llamar #pornografíaVirtual, que consiste en la creación de contenidos sexuales con imágenes no reales, como dibujos y animaciones de menores. Esto provoca problemas al perseguir la pornografía infantil legal y judicialmente porque no existen las personas ni las situaciones reproducidas; a pesar de ello, fomenta el consumo de otros materiales que sí lo hacen.

Con base en el Informe sobre Pornografía Infantil en Internet de ANESVAD, se estima que en el mundo existen más de 4 millones de sitios de internet que contienen material de sexo con menores y que cada día se crean 500 nuevos.

La mayoría de los sitios con pornografía infantil se encuentran en servidores de países de la antigua Unión Soviética y en algunos de América Latina, donde la legislación es mucho más permisiva con los menores.

CONVENCIONES INTERNACIONALES

En el ámbito internacional existen diversas convenciones internacionales que se refieren a los derechos de los niños y buscan prevenir la explotación y abuso:

- Declaración de Ginebra sobre los Derechos del Niño (1924).
- Declaración Universal de los Derechos Humanos (1948).
- Declaración de los Derechos del Niño (1959).
- Convención sobre los Derechos del Niño (1989).
- Declaración Mundial sobre la Supervivencia, la Protección y el
- Desarrollo del Niño (1990).

Entre esos instrumentos destaca la Convención sobre los Derechos del Niño, que define como niño a todo ser humano menor de dieciocho años de edad, excepto cuando, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad y, que como comentamos al analizar el concepto de pornografía infantil, establece como forma de abuso sexual la explotación del niño en espectáculos o materiales pornográficos.

Regulaciones jurídicas a nivel internacional.

A finales de la década de 1970 y comienzos de la de 1980 comenzó el impulso de medidas legislativas, centradas en la prohibición de la producción, venta y distribución de la pornografía infantil.

En Estados Unidos los intentos por regular y proscribir la pornografía eran frecuentemente criticados como censura y violación de la Primera Enmienda. El Congreso aprobó en 1984 el Acta de Protección Infantil, que brindaba restricciones más severas contra la pornografía infantil.

En 1968 Dinamarca emitió una ley con disposiciones referentes a acciones contra la obscenidad en la palabra escrita. En 1988 la pornografía infantil se volvió ilegal en Gran Bretaña. Otros países empezaron a legislar más recientemente: Noruega en 1992, Alemania, Francia y Canadá en 1993, Austria en 1994 y Dinamarca, España y Bélgica en 1995.

Por lo que se refiere a pornografía infantil en internet, las legislaciones difieren considerablemente de un país a otro. Algunos no tienen referencias específicas al uso de internet, aunque se puede enjuiciar a los autores en virtud de la legislación general sobre pornografía infantil o explotación o abusos sexuales de niños.

Respecto a la edad para ser sujeto de pornografía infantil, se establece en general de menos de 18 años, pero hay países que consideran una edad menor, por ejemplo: Australia, Portugal, Polonia y Suecia. A este respecto también existen contradicciones con la edad de consentimiento para la actividad sexual, como es el caso de Suiza. También existen diferencias en las legislaciones en relación con las sanciones impuestas. Algunos países establecen penas máximas de 5 años y otros llegan a 10 o 12.

Regulaciones jurídicas a nivel nacional.

En México existen varios instrumentos jurídicos que establecen disposiciones para la protección de los niños, en general, y contra el delito de la pornografía infantil, en particular. La reforma al artículo 4 de la Constitución Política, elevó a rango constitucional el derecho de niñas y niños a satisfacer sus necesidades de alimentación, salud, educación y sano esparcimiento.

La Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, emitida el 29 de mayo de 2000, contiene un capítulo específico para el tema de la protección en la integridad y la libertad, así como contra el maltrato y el abuso sexual.

Artículo 21. Niñas, niños y adolescentes tienen el derecho a ser protegidos contra actos u omisiones que puedan afectar su salud física o mental, su normal desarrollo o su derecho a la educación en los términos establecidos en el artículo 30 constitucional. Las normas establecerán las formas de prever y evitar estas conductas. Enunciativamente, se les protegerá cuando se vean afectados por:

A. El descuido, la negligencia, el abandono, el abuso emocional, físico y sexual.

B. La explotación, el uso de drogas y enervantes, el secuestro y la trata de personas.

C. Conflictos armados, desastres naturales, situaciones de refugio desplazamiento, y acciones de reclutamiento para que participen en conflictos armados.

OTRAS CLASIFICACIONES:

Por otra parte, existen diversos tipos de delito que pueden cometerse y que se encuentran ligados directamente con acciones efectuadas contra los sistemas, como los siguientes:

1. Acceso no autorizado: uso ilegítimo de passwords y la entrada de un sistema informático sin autorización del propietario.

2. Destrucción de datos: los daños causados en la red mediante la introducción de virus, bombas lógicas, etcétera.

3. Infracción a los derechos de autor de bases de datos: uso no autorizado de información almacenada en una base de datos.

4. Intercepcion de e-mail: lectura de un mensaje electrónico ajeno.

5. Fraudes electrónicos: mediante compras realizadas al usar la red.

6. Transferencias de fondos: engaños en la realización de este tipo de transacciones.

Por otro lado, internet permite dar soporte para la comisión de otro tipo de delitos, a saber:

1. Espionaje: acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

2. Terrorismo: mensajes anónimos aprovechados por grupos terroristas para remitirse 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 la internet los narcotraficantes pueden ser aprovechadas para planificar otros delitos, como tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

Naturaleza del riesgo

Las autoridades encargadas de hacer cumplir la ley suelen adaptarse con lentitud a las nuevas tendencias, mientras que los grupos delictivos organizados tienden a adaptarse rápidamente y a aprovechar los adelantos tecnológicos debido a los inmensos beneficios que producen sus actividades ilícitas.

Los adelantos en la tecnología de las comunicaciones han determinado que surgieran nuevas oportunidades para la comisión de delitos sumamente complejos, en particular un aumento significativo del fraude en la Internet, y esas oportunidades han sido explotadas por los grupos delictivos organizados.