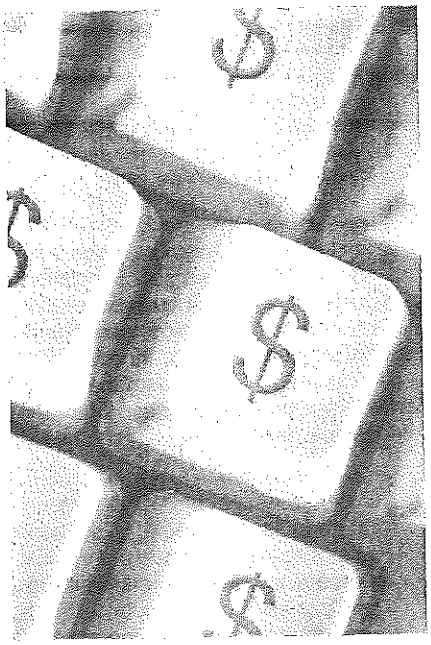
Los delitos informáticos

Juan Guillermo Madrid Mejía
Analista y Auditor de Procesos e Informática
Estudiante 2º semestre Contaduría Pública
Email: juangmomadrid@hispavista.com



Los delitos informáticos afectan directa o indirectamente la labor de procesamiento electrónico de datos. En el área contable se deben tener presentes en todo momento, ya que no hay total certidumbre sobre si los datos procesados serán confiables o no para la emisión de informes; en la actualidad existen riesgos para un fácil contagio o daño a la información, bien sea por intervención de delincuentes informáticos o el uso inapropiado de los medios y tecnología electrónica disponibles (por ejemplo Internet).

A continuación se exponen algunos de los métodos más comunes de delitos informáticos en el ámbito internacional.

1. Manipulación de datos de entrada y de salida: Uso de la computadora como instrumento para planificar y controlar un delito, usando técnicas de simulación y modelos. El hecho se tipifica con la manipulación de datos antes o durante su entrada a la computadora. Implica un delito contra la propiedad y, en ese orden, podría considerarse como una forma específica de estafa.

2. Fraude efectuado por manipulación informática (Filtración de datos): Sustracción de datos o copias de datos de un sistema, como por ejemplo, duplicación de una cinta magnética u óptica.

3. Sabotaje informático (Caballo de troya): Introducción de un grupo de sentencias en la codificación de un programa para realizar una función no autorizada. Es el método más común de sabotaje, implica tener acceso a cualquier archivo usado normalmente por el programa que permita alternar su funcionamiento lógico.

4. Daños o modificación de Programas (Puertas con trampas):

Utilización de "interrupciones" dentro de la lógica de un programa informático cuando está en su fase de desarrollo, para su depuración y uso posterior con fines delictivos. Muy pocos sistemas son lo suficientemente seguros para evitar este tipo de delito o alteración de los programas o archivos externos.

5. Introducción de virus informático (Bombas lógicas):

Consiste en introducir algún tipo de virus informático que pueda causar algún daño. También pueden ser software maligno que se ejecuta en un momento específico o previamente programado, cuando se cumplan determinadas condiciones, tales como fechas, horas, etc. Cuando la condición o estado se presenta entonces una rutina realiza una acción no autorizada. Por ejemplo el caso de los virus "Viernes 13" o "Sábado 14" que se activan en dichas fechas si la máquina está infectada con dichos virus.

6. Reproducción no autorizada de programas (Superzapping): Se conoce popularmente como piratería, es un uso no autorizado de programas. Es uno de los delitos más comunes en la actualidad y del cual pocos se "salvan". ¡Quien esté a libre de este delito que tire la primera piedra¡

7. Utilización ilícita de datos, acceso no autorizado a sistemas o servicios informáticos (Suplantaciones, trasiego e imitación): Acceso sin autorización a áreas controladas, sea por medios electrónicos o mecánicos, usando técnicas o claves de acceso.

8. Falsificación de documentos a través de máquinas electrónicas: También es común la falsificación física de cualquier tipo de documentos utilizando la computadora o cualquier hardware y software.

9. Obtención de datos y residuos: Obtención de información "residual" de la memoria después de la ejecución de un trabajo o labor, sea impresa en papel o cinta magnética; tales como copias en carbón, papeles de copias terceras, etc. En auditoría informática hay un uso lícito que es cuando se arma un "rompecabezas" de papel picado para elaborar pruebas físicas de un delito cuyo soporte pudo haber sido el papel impreso u otros medios.

10. Redondeo (Rounding Down = Técnica de salami o embutido): Sustracción de pequeñas cantidades de "activos", a través de los registros en programas de numerosas procedencias, por ejemplo redondeo de cuentas. Los fondos así obtenidos se aplican a una cuenta especial.

CONCLUSIONES Y RECOMENDACIONES

Es importante comprender que hoy en día se manejan muchos conceptos en el área de la informática y que dada la facilidad y acceso de todo tipo de personas a estas herramientas es difícil estar totalmente a salvo de esta variedad de delitos; son riesgos inherentes y las organizaciones empresariales deberían tener pólizas de seguros que cubran siniestros por la ejecución de alguna de estas modalidades. Como medidas detectivas, preventivas y correctivas se recomiendan las siguientes acciones:

- Mantener instalado en la computadora un sistema antivirus confiable y original.
- Estar al tanto de los boletines relacionados sobre los últimos virus y antivirus que aparecen permanentemente y actualizar su sistema de antivirus.
- Usar programas instalados de procedencia confiable y vacunados previamente a su instalación.
- No leer correos electrónicos y de origen desconocido y alternar el uso de al menos dos cuentas de correo.
- Evitar la copia frecuente de programas a través de cd-rom, disquetes o desde la Internet, especialmente si se trata de experimentar gran variedad de programas.
- Borrar periódicamente la basura del sistema y archivos no utilizados. Desinstalar programas y eliminar archivos temporales que con frecuencia quedan residentes cada vez que se ingresa a la Internet.
- Procurar que la computadora sea usada como herramienta personal y no multipersonal. Si es necesario se pueden configurar varios perfiles de usuario con sus respectivas claves de acceso y cambiar con frecuencia sus clave de acceso personal.
- Si la máquina sufre de bloqueos, reseteos o caídas de programas con frecuencia es posible que tenga problemas con el Hardware o que el Software esté infectado, por lo que debería hacerse una revisión técnica.
- Mantener doble copia de la información a través de medios magnéticos y ópticos como son lo backup (copias de seguridad), a fin de volver a restaurar la información en caso de un daño severo.