SEGURIDAD INFORMATICA Y ADMINISTRACION PUBLICA

Alberto Herrerías Franco

La aparición de la informática ha impactado estructuras y funciones de la sociedad, como lo han hecho otros avances tecnológicos en la historia. Al permitir el manejo de grandes volúmenes de información -que sustenta acciones y decisiones- a grandes velocidades, se ha afectado el sistema nervioso de las organizaciones.

Las instituciones públicas han extendido el uso de tecnología computacional, sin embargo, ello no ha sido correspondido con un rediseño o cambio organizacional que propicie un desarrollo armónico entre organismos y tecnología. La sola incorporación de equipos informáticos no moderniza una administración y sí crea desadaptaciones que se revierten en problemas de seguridad.

Bajo estas consideraciones el trabajo pretende abordar la seguridad informática en esencia -su origen y sus manifestaciones- y exponer condiciones para su existencia. Esta seguridad equivale al mantenimiento permanente de la integridad y confidencialidad de la información, así como la garantía de la sana y contínua operación de los sistemas computacionales. Para la administración pública se trata de un asunto vital. De acuerdo con ello, el trabajo sustenta que los administradores públicos participen en el logro de los objetivos de seguridad. El administrador se concibe como profesional capaz de conducir procesos de decisión para ser transformados en acción y asegurar el cumplimiento de los fines propuestos. Con ello, se propone el desarrollo de una administración cabal sobre la seguridad informática. Se ofrece un marco analítico para comprender esta seguridad y lineamientos para el diseño de un esquema de administración adecuado.

A lo largo de la historia los grandes cambios tecnológicos han revolucionado la vida del hombre al permitirle mejor dominio sobre la naturaleza e imprimir mayor dinamismo en sus tareas cotidianas. Ejemplo de ello furon la escritura, la numeración, los calendarios, y, más recientemente, la electricidad, las comunicaciones alámbrica e inalámbrica, la aviación o la energía atómica. Todos ellos han

alterado drásticamente la vida del hombre.

Uno del los últimos grandes cambios tecnológicos es la "revolución informática" [1], la cual ha modificado el tratamiento y conservación de la información, y con ello ha afectado el "sistema nervioso" de las organizaciones y de la sociedad entera.[2] Así, se está gestando una forma de sociedad y de civilización basada en el proceso rápido y masivo de datos. La tecnología informática presiona gradualmente hacia el cambio o readaptación de funciones y estructuras de la sociedad. Proceso de cambio que se manifiesta en crisis o disfuncionalidades -frente a lo tradicional- que tienden a revertirse en inseguridad.

Este trabajo tiene como objetivo destacar la seguridad informática como terreno de consideración importante en la administración pública de México. Se pretende profundizar la esencia del problema de esta seguridad y resaltar su interés para el administrador público. Se busca identificar plenamente el problema de la seguridad informática, reconocerlo como tal y establecer lineamientos para resolverlo. No se plantean soluciones concretas a problemas particulares relacionados con este tema.

Se defiende una hipótesis: la seguridad informática tiene importancia vital para la administración pública y deberá ser administrada, es decir, ser objeto de un proceso de toma de decisiones racional. Este estudio se destina a afirmar esta hipótesis. El método que sigue consiste en un desarrollo analítico y lógico. Se llega a conclusiones lógicas, a partir del análisis del problema de la seguridad computacional. Con base en diferentes niveles y aspectos de este problema, se generan conclusiones y proposiciones lógicas.

El trabajo se presenta en cinco secciones. La primera refiere el impacto de la informática en la vida y dinámica humana. La segunda define y explica la seguridad informática. La tercera refiere un marco analítico de los aspectos vulnerables que representa la informática. La cuarta sección aborda un perfil del administrador público y la relevancia de su actuación ante el problema de la seguridad. La quinta presenta un marco analítico para la resolución de la seguridad informática y se ofrecen orientaciones hacia la integración de un esquema para su administración. Finalmente se ofrecen las conclusiones del trabajo.

La necesidad de garantizar el cumplimiento de los objetivos de los organismos públicos y de los fines que tienen sus sistemas computacionales, así como asegurar su correcto y buen funcionamiento, apoyan la importancia de este trabajo.[3]

[1] Término acuñado por Nora y Minc. V. Nora, Simon y Alain Minc: *La informatización de la sociedad*. México: Fondo de Cultura Económica, 1980.

[2] Nora y Minc, op. cit. P. 17.

[3] A lo largo del trabajo se hará referencia al término "información". Para los efectos del presente estudio, se le considera desde una perspectiva informática, es decir, destinada a la toma de decisiones o gestión organizacional. Hay también una perspectiva comunicacional, cuando hace referencia a mensajes, dirigidos a personas, que los reciben para saber, conocer, elegir, distraer, entre otros y reaccionan ante ellos modificándolos, aceptándolos o rechazándolos. Explicación de Téllez Valdés, Julio: *Derecho informático*. México: Universidad Nacional Autónoma de México, 1987. P.63.

EL IMPACTO DE LA INFORMATICA EN LA SOCIEDAD

Los grandes cambios tecnológicos, como sostiene Marshall McLuhan, son avances que han acercado personas, cosas y conocimientos. Se constituyen "extensiones del hombre", que permiten mayor integración o interacción entre las sociedades. El mundo, así, se ha acercado gradualmente hacia la constitución de una "aldea global".[4] En muchos casos, los grandes cambios tecnológicos han conllevado la reestructuración del medio ambiente humano, o la creación de otro completamente nuevo. [5] Al respecto, Nora y Minc afirman que las "revoluciones tecnológicas", en el pasado, provocaban una intensa reorganización de la economía y la sociedad. [6] Al aparecer tecnologías que implican mayor acercamiento entre los hombres, mejor comunicación, mayor facilidad de producción o distribución, las estructuras sociales se alteran -o deben hacerlo- para mantener su viablilidad y estabilidad. Las necesidades de cambio se manifiestan como etapas de crisis -de diversas magnitudes y orientaciones- que tarde o temprano, alteran las sociedades desde sus cimientos.

En general, los cambios sociales han sido menos rápidos que la aparición y difusión de las nuevas tecnologías que los provocan. Las sociedades son resistentes al cambio, al intervenir afectaciones en costumbres, valores, tradiciones, culturas o intereses; alteraciones en modos de trabajar, de pensar o alteraciones en las estructuras y prácticas de mando y organización. Alvin Toffler ha señalado que las sociedades han mostrado impericia en adaptarse a la "razón de cambio", independientemente del contenido o dirección del propio cambio". [7] Y ello, reconoce, es un problema crítico en la actualidad.

A partir de los años 50, en algunos países desarrollados, inicia una "era de la información", como etapa sucesora de una era industrial. La sociedad se altera en una nueva fase en la que el concepto de valor económico o de activo se traslada gradualmente de bienes tangibles hacia la información. El trabajo humano se orienta crecientemente hacia el descubrimiento, invención, comunicación o proceso de conocimiento. [8] Así, la dinámica del mundo moderno gira, cada vez más, en torno a la capacidad de manejar y disponer de información. [9]

---

[4] Para una exposición más amplia del impacto de las mencionadas tecnologías, ver McLuhan, Marshall: *Understanding media: the extensions of man*. New York: Signet Books, 1964.

[5] V. Ibid. P. viii y 19. Y Ackoff, Russell: *Rediseñando el futuro*. México: Editorial Limusa, 1983. P. 4 y 5.

[6] Nora, Simon y Alain Minc: *La infomatización de la sociedad*. México: F.C.E., 1980. P. 17.

[7] Toffler citado por Ackoff, op. cit. P. 5.

[8] V. Naisbitt, John: *Macrotendencias*. México: Edivisión, 1985. (Primera reimpresión). P. 22. Cabe también señalar que está en emergencia una cultura informática. En ella, el concepto de valor se traslada de bienes físicos, tangibles, a espacios conceptuales, es decir, información. V. Nussbaum, Bruce: *El mundo tras la era del petróleo: nuevos ejes de poder y riqueza*. México: Editorial Planeta, 1985. P. 50.

[9] En diciembre de 1976, Simon Nora y Alain Minc presentaron al mandatario francés, Valery Giscard, un estudio pionero en el campo del impacto de las nuevas tecnologías de computación y comunicación en las estructuras de la sociedad y el gobierno. Su trabajo se ha constituido base para innumerables estudios posteriores y en él se afirma el rol de las tecnologías mencionadas, en la nueva sociedad. V. Nora, Simon y Alain Minc, op. cit.

Esta "era de la información" tomó mayor fuerza con el desarrollo de:

1) las telecomunicaciones, incluyendo los satélites artificiales, y

2) de las tecnologías para el procesamiento electrónico de datos, también conocidas como *informática o computación*. Con las primeras, se ha facilitado enormemente la transmisión de datos entre diversos puntos geográficos. Con las segundas, se ha permitido un manejo veloz de mayores volúmenes de información, que, de hecho, facilita accesos, alteraciones, filtrado o procesamiento, almacenaje y distribución de datos referentes a múltiples ámbitos de la vida del hombre. Así, permite incrementos importantes de productividad de personas y organizaciones, al facilitar el proceso de la información que sustenta acciones o decisiones.

La incorporación de la computación en nuestra administración pública, ha sido poco ordenada, al no responder a un proceso planeado y sistemáticamente fundamentado. Se adoptan recursos informáticos en momentos en que todavía no existía personal que evaluara acertadamente la viabilidad de las inversiones, cotejadas con necesidades y posibilidades reales de automatización de procesos de datos. Una causa directa de ello ha sido la falta de preparación técnica de los administradores o tomadores de decisiones respecto a la informática. La introducción de computadores ha partido de suposiciones erróneas acerca de los alcances, limitaciones y características de estas nuevas tecnologías. Se trata de una situación similar a la que ha tenido lugar en otro países. Russell Ackoff afirma al respecto que "a pesar de la enorme propaganda que se ha hecho a los sistemas de información administrativa, pocos satisfacen las necesidades de los administradores que los autorizan o utilizan." Aún más, se trata del problema referido por Nora y Minc, acerca de las crisis sociales desprendidas de la utilización de nuevas tecnologías.

A nivel organizacional, la informática ha inducido desajustes diversos, al alterar canales y formas de comunicación -que son esencia de organización-, métodos y procedimientos de manejo o tratamiento de información y funciones de personal. Este, acostumbrado a laborar de cierto modo, es obligado, repentinamente, a trabajar con equipos informáticos. Por otra parte, se crean nuevos polos de poder o influencia en las unidades administrativas que concentran servicios informáticos. El reconocimiento formal de ello ha sido escaso.[10]

Con el paso del tiempo se ha buscado ejercer mayor racionalidad en los recursos destinados a la informática y obtener mayores beneficios para el usuario. En el ámbito de la administración pública federal se creó el Instituto Nacional de Geografía, Estadística e Informática (INEGI), organismo desconcentrado de la Secretaría de Programación y Presupuesto. Entre sus atribuciones se encuentra la de "orientar de manera racional las adquisiciones de equipos de cómputo, cuidar la compatibilidad y propiciar la mejor aplicación de

[10] Los argumentos de este párrafo son adaptaciones de ideas de Herbert Simon, expuestas en, Simon, Herbert a.: *La nueva ciencia de la decisión gerencial*. México: Librería "El Ateneo" Editorial, 1982.

los cada vez más escasos recursos"[11]. Asimismo, tiene la atribución de promover el desarrollo informático nacional. Sus esfuerzos se han dirigido principalmente a dictaminar el gasto en materia de informática ejercido por las dependencias y entidades de la administración pública federal. Ello refleja, en cierta manera, que la preocupación en materia de regulación y control computacional ha sido más por la compra de equipos, dispositivos y programas, que por el aseguramiento de la viabilidad, buen uso y administración de los activos informáticos existentes. En materia legal, el marco jurídico en torno a la computación es escaso e inadecuado como para fundamentar políticas informáticas o regulación en los organismos públicos.

El terreno propio de la seguridad está aún menos trabajado y los problemas relacionados con ella han crecido tan rápido como la extensión de equipos y aplicaciones en las agencias públicas. Por su propia naturaleza, la informática altera conceptos y el mismo ámbito la seguridad. Ésta se hace más crítica en el campo computacional debido a que las nuevas tecnologías magnifican los riesgos que pueden presentar los datos procesados y almacenados manualmente. La información es recurso valioso en las administraciones para su funcionamiento y como sustento de decisiones. Por ello, la captura, tratamiento o salida de datos debe efectuarse por canales claramente predeterminados y reconocidos por todo usuario.

En suma, con base en sus capacidades, la computación incrementa la vulnerabilidad o propensión de las organizaciones hacia la intensidad y recurrencia de daños, pérdidas, desfalcos, sabotajes, fraudes o errores, cuando no es objeto de adecuado control.

LA SEGURIDAD INFORMATICA

Con fundamento en lo anterior, se ha hecho necesario establecer una adecuada administración de los recursos tecnológicos de proceso de datos, para que de ellos se derive un funcionamiento óptimo. La sola introducción de los computadores en la sociedad no garantiza su bueno o adecuado funcionamiento. Con ello, surgen necesidades de definición y ejecución de políticas de utilización, educación e investigación, de las que se deriva que los recursos computacionales sean funcionales a objetivos de mayor productividad y eficiencia y, en general, se adapten a los requerimientos del país y sus instituciones. Se trata, en realidad, que las organizaciones y los medios informáticos tengan un cabal desarrollo armónico.

Un elemento esencial para ello es el aseguramiento del buen uso y resguardo de los activos informáticos de las instituciones -equipos, accesorios, programas y datos-. La seguridad informática encuentra aquí un campo de acción. Su esencia está en asegurar la continuidad, sana operación de un organismo, el control del buen uso de la información y el mantenimiento de la integridad y confidencialidad de los datos y otros activos informáticos. Se trata de regular qué información se

[11] Tomado de Secretaría de Programación y Presupuesto: *Guía para la elaboración de programas de desarrollo informático*. México, Talleres Gráficos de la Nación, 1987. P. 1.

accesa; cómo debe hacerse; en qué momento; en qué instalación, sitio, equipo o terminal, quién está autorizado para hacerlo y qué fines debe tener la utilización de los datos o programas. Se trata de un problema complejo, que comprende un conjunto de problemas, interrelacionados entre sí y cuya solución requiere la consideración de los diversos elementos que intervienen, a saber, instalaciones; equipos; programas; comunicaciones; sistemas administrativos; aspectos jurídicos; personal operativo, supervisorio o directivo, entre otros. No existe solución única para atender los aspectos negativos o riesgosos, que presentan las nuevas tecnologías de proceso electrónico de datos. Se trata de un conjunto complejo de problemas que requiere cuidadosa atención.

La Administración Pública en México se auxilia cada día más de los recursos informáticos y su funcionamientos se ha hecho altamente dependiente de ellos. El ejercicio de la seguridad informática cobra relevancia especial y, adicionalmente, se apoya en las siguientes consideraciones.

Primero. El aparato estatal está en proceso de modernización y búsqueda de mayor racionalidad. La informática es herramienta básica para ello, al facilitar mejor información para la toma de decisiones.

Segundo. La administración pública ejerce papel rector en la economía y la sociedad. El manejo irracional o incontrolado de su información puede ser altamente nocivo en terrenos políticos, económicos o sociales, así como en el daño de los derechos individuales y grupales. Si la información sustenta poder, su falta de control, lo disocia, así, la seguridad informática se convierte en elemento de consideración para la paz social y la seguridad nacional.

Tercero. Una discusión frecuente a nivel internacional concierne a la merma en la privacía que provoca el manejo de información nominativa de personas físicas o morales. El Estado ha dispuesto de datos de éstos desde antes del advenimiento del cómputo. Pero con la capacidad actual de proceso y distribución de información, se posibilita grandemente el manejo, adquisición, cruce o intercambio de este tipo de datos, en perjuicio del individuo.

La seguridad informática, en suma, se constituye como elemento fundamental en la sana operación de la administración pública. Se trata de garantizar que el proceso de datos sea eficaz y eficiente a los fines que se tengan y no sean vulnerables.

LA VULNERABILIDAD INFORMATICA

El impacto negativo, desventajas o amenazas que conlleva el procesamiento electrónico de datos es menos reconocible que los beneficios que ha aportado. La informática permite eficiencia, pero también es campo potencial de errores, actos ilegales o delictivos. Con tecnología manual para proceso de datos, estos actos tienen también un alcance manual, pero con tecnología informática y grandes concentraciones y volúmenes de datos, los riesgos derivados son de dimensiones insospechadas.

El análisis de la vulnerabilidad informática se propone en cuatro vertientes:

1) Los errores y omisiones

2) Las pérdidas por desastres naturales

3) Los delitos informáticos y

4) Mal funcionamiento de equipos o dispositivos informáticos o de comunicación.

LAS PERDIDAS POR ERRORES Y OMISIONES

Los errores y omisiones constituyen el campo más frecuente de daños en sistemas de automatización de datos. Se originan, fundamentalmente, en el personal de las instituciones, el cual no está debidamente capacitado o entrenado acerca del funcionamiento de las nuevas tecnologías. Con el tiempo, las aplicaciones computacionales crecen en amplitud y complejidad, mientras los errores y omisiones del personal, se hacen cada vez más destructivos en potencia. Entre los casos comunes destaca el robo o extravío de discos o cintas conteniendo información valiosa; la pérdida de programas o archivos de datos -por haberse efectuado instrucciones equivocadas- que representaban muchas horas-hombres de captura y proceso, descuidos diversos en instalaciones o cuidado de equipos, dispositivos o datos.

Estos problemas, tienen origen, generalmente, en la ignorancia o negligencia del personal responsable por los recursos informáticos, de instrumentar normas o mecanismos de protección y darles seguimiento. Asimismo, se desprende la falta de capacitación y sensibilización del personal, sobre la aplicación de previsiones de control y seguridad.

LAS PERDIDAS POR DESASTRES NATURALES

Estas contingencias son menos frecuentes y las pérdidas se originan por falta de previsión. Pueden clasificarse en dos frentes. La primera es la de desastres naturales en tiempo corto. Ocurren durante lapsos reducidos de tiempo. Aparecen repentinamente y se les afronta con la planeación de ubicación de las instalaciones de cómputo, almacén de soportes magnéticos y con la existencia de planes para enfrentamiento de contingencias de esta índole. Ejemplo de ello son inundaciones, sismos, actividad volcánica o incendios. La segunda corresponde a los que ocurren en periodos prolongados y dañan los activos informáticos paulatinamente. Son casos como humedad incontrolada, presencia de partículas sólidas o sustancias corrosivas en el ambiente, radiaciones electromagnéticas o fauna nociva que penetra equipos computacionales.

LOS DELITOS INFORMATICOS

En forma paralela a la revolución informática, cobran importancia creciente los usos indebidos, o crímenes o delitos informáticos. La información es foco de criminalidad. Mientras las organizaciones y las sociedades más entrelazadas están, o más dependen de medios electrónicos, más vulnerables son ante actos destructivos. En lo económico y financiero, el potencial delictivo es evidente. Basta considerar la dependencia de las instituciones bancarias hacia los recursos informáticos para sus operaciones cotidianas. En aspectos humanos también ha cobrado relevancia la preocupación por la privacidad, que afecta los derechos de las personas, los

intereses de las corporaciones y la seguridad y soberanía nacionales.

En los países de mayor desarrollo hay antecedentes que confirman el potencial delictivo de la informática. El impacto más relevante se ha efectuado con intermedio de redes de teleproceso, para desfalcos bancarios y accesos ilegales a bancos de información. [12]

En criminalidad informática deben abordarse tres facetas:

1) Las instituciones

2) El defraudador informático y

3) El acto delictivo.

Las instituciones, por su parte, extienden los usos informáticos, pero no su armónica asimilación a la organización. El delito informático surge del mal manejo de concentraciones y volúmenes de datos, y de procesos complicados, a grandes velocidades, en conjunto con escasos medios de control y protección y normatividad aplicable.

Asimismo, las instituciones son propensas a actos delictivos al permitir la formación de élites que conocen en detalle los sistemas y los operan con total libertad.[13] También, como dice Bria, *los altos ejecutivos se preocupan más por la cantidad y velocidad para obtener la información, que en la calidad y seguridad de la misma.*[14]

A nivel del defraudador informático existen factores que le dan ventajas sobre los defraudadores tradicionales. Primero. Su nivel intelectual es alto y puede ocupar puestos altos. Segundo. No suele tener necesidad de actuar de prisa. Tercero. Hay pocos especialistas capaces de detectar actos ilícitos. Cuarto, y el más crítico: se puede delinquir sin dejar huella, dado que es factible borrar el programa o registro donde se asentó la transacción o alteración de la información.[15]

En cuanto al acto delictivo informático, dado su reciente desarrollo, es difícil detectarlo, con conocimiento de qué, cómo, dónde y cuándo ocurrió algo ilícito. Una operación fraudulenta se pierde en grandes volúmenes de información, y la detección, si ocurre, puede tomar semanas o hasta meses. A ello se añade el problema de la falta de expertos dedicados a este fin. Por otra parte, el marco jurídico es casi inexistente. El delito informático no está

[12] El teleproceso de datos consiste en procesamiento de información en que intervienen equipos ubicados en distintos puntos geográficos, interconectados mediante diversos medios o tecnologías de comunicación. Jesús Sotomayor afirma que a través del teleproceso se han efectuado los mayores desfalcos bancarios. V. Sotomayor, Jesús y A. Sánchez: *Planeación de la recuperación informática en casos de desastre*, ponencia en III Reunión de sistematización de bancos centrales americanos e ibéricos. (Santo Domingo, República Dominicana), 23 de noviembre a 1o. de diciembre de 1984. V. Introducción.

[13] González Castellanos, Herbin Amory: *Fraudes en sistemas de procesamiento electrónico de datos* (Tesis para obtener el título de contador público y auditor). Guatemala, Universidad de San Carlos (Facultad de Ciencias Económicas), 1978. p. 72 y ss.

[14] Bria, Ricardo: *Delitos en un ambiente informatizado*, en Actas: I Congreso Iberoamericano de Informática y Auditoría. (San Juan, Puerto Rico). 2 a 6 de noviembre de 1987. p. 121.

[15] Estos factores son mencionados por Téllez Valdés, Julio: *Derecho informático*. México, D.F.: Universidad Nacional Autónoma de México, 1987. P. 105., Krauss, Leonard & Aileen Mc Gaham: *Computer fraud and countermeasures*. New Jersey: Prentice Hall, 1979., Pp. XII y XII, V. González Castellanos, op. cit. P. 92

tipificado y los dispositivos electrónicos o magnéticos no constituyen elementos de prueba para efectos penales.[16] En consecuencia, se dan muchos ilícitos y pocas denuncias. El delito informático queda impune.

Bajo estas consideraciones, se puede elaborar un plan de fraude informático infalible, ya sea para malversación de fondos, chantaje, espionaje, o cualquier otro. El alcance del botín puede ser alto, y, ante esa expectativa, puede haber colusiones de personas con acceso a diversas fases de un flujo de datos, para la comisión del acto y el borrado de toda huella.

Adicionalmente, se destaca que los sistemas informatizados ofrecen facilidades en tiempo y espacio. El acto ilícito puede tener lugar en fracciones de segundo y, tal vez, sin necesidad de presencia física del defraudador.

EL MAL FUNCIONAMIENTO DE EQUIPOS O DISPOSITIVOS INFORMATICOS O DE COMUNICACION

Durante la operación informática pueden tener lugar fallas en los sistemas de información, que afectan, fundamentalmente, dos niveles: 1) los equipos de proceso, recuperación o almacenamiento de datos y 2) las líneas de comunicación. Las fallas de equipo se deben usualmente a desperfectos o a la presencia de algún agente de falla. El riesgo de ello se minimiza mediante la provisión de servicios periódicos de mantenimiento preventivo al equipo. Asimismo, pueden existir fallas al interrumpirse el suministro eléctrico normal, lo cual se evita por medio de la instalación de equipos tipo UPS. [17] Por su parte, las fallas de líneas de comunicación son más difíciles de controlar y se pueden deber a agentes atmosféricos o naturales diversos —ya mencionados en el apartado "Las pérdidas por desastres naturales"—, interrupciones de suministro eléctrico, sobrecargas de tráfico en las líneas de comunicación, acciones humanas accidentales o intencionales, entre otras.

La previsión y control de irregularidades computacionales, sólo puede lograrse, de manera óptima, con aplicación de un marco integral de medidas que incluyan los diversos elementos de la informática: personal, instalaciones, equipos, soportes magnéticos, programas y líneas de transmisión. En seguridad informática no hay solución única y total, pero existen mecanismos que contrarrestan riesgos múltiples.

EL ADMINISTRADOR PUBLICO Y LA SEGURIDAD INFORMATICA

En la década de los cincuenta, Herbert Simon publicó su obra *The administrative behavior*, en la que define la toma de decisiones como el corazón de la administración. [18] Estructura y analiza elementos

[16] Respecto a este punto, V. Téllez, op. cit., dedica un capítulo en su obra. V. Pp. 117 y 118.

[17] Iniciales correspondientes a *Uninterrupted Power Supply* (Equipo de suministro de fuerza ininterrumpido).

[18] Simon, Herbert a.: *El comportamiento administrativo: un estudio de los procesos decisorios en la organización administrativa*. Madrid, Aguilar, 1962.P. xviii.

decisorios, de modo que de ellos se deriven efectos óptimos y las instituciones logren sus fines. Habla de la administración como el arte de asegurar que las cosas se hagan. [19] El problema central de su trabajo es abordar los procesos de decisión que se transforman en acción. Para él, el proceso administrativo es un proceso de toma de decisiones. Define la toma de decisiones como el esfuerzo de estrechar alternativas de acción a una que, de hecho, se llevará a cabo, y ello con base en principios o requerimientos derivados del propósito y objetivos generales de la institución.[20] Reconoce que el administrador - ejecutivo o gerente- es un decididor. [21] Tiene como rol fundamental, en suma, la toma de decisiones racionales, que permita instrumentar acciones y coordinar esfuerzos hacia el cumplimiento de los fines de las organizaciones y la satisfacción de las demandas y necesidades de la sociedad.

El presente trabajo propone que la seguridad informática puede resolverse adecuadamente si es administrada. En otras palabras, se propone el desarrollo de una administración de la seguridad informática. Si la administración se concibe como arte de garantizar que las cosas se hagan, la seguridad informática deberá ser objeto de una toma racional de decisiones. Se profundizará en los ámbitos de esta seguridad que se propone sean abordados por el administrador público.

Se trata de un campo de acción, hasta ahora, no atribuido a este profesional, ni en la práctica ni en la literatura. Se infiere que al administrador corresponde, no la ejecución técnica u operación de los medios de seguridad, sino la conducción y garantía de su funcionamiento. Ello implica que este profesional conozca el panorama del fenómeno informático, la problemática resultante y las características de los activos informáticos de la institución a la que sirve. Debe ser activo en un proceso integral de administración informática. Ello significa que deberá considerar los elementos físicos, lógicos, humanos y organizacionales, que intervienen en el problema y conducir fases de planeación, organización, dirección y control, constituyentes del proceso administrativo. Asimismo, deberá estudiar los impactos organizacionales en estructuras y personas, que tienen las políticas, normas y mecanismos de seguridad, con objeto de asegurar que los beneficios que aportan los recursos de protección sean como tales y no conlleven costos no deseados.

La formación del administrador de la seguridad se basará en el conocimiento de los múltiples elementos que intervienen en la implantación de una solución, ya sean técnicos, humanos, políticos, económicos o de cualquier otro tipo. En este terreno, cabe citar una afirmación de Ackoff: "La habilidad de una persona de administrar sus asuntos o los de la sociedad, depende más de su comprensión y actitud hacia el mundo que la rodea, que de sus métodos de solucionar los problemas."[22]

[19] Ibid. P. 1.

[20] Ibid. P. 3.

[21] Simon, Hebert: *La nueva ciencia de la decisión gerencial*. México, Librería "El Ateneo" editorial, 1982. P. 36.

[22] Ackoff, Russell. op. cit., p.6.

HACIA UNA ADMINISTRACION DE LA SEGURIDAD INFORMATICA

Se sostiene que la informática sólo puede ser agente modernizador cuando se armonizan tecnología y organización, donde ésta se rediseñe, adapte y se superen las crisis resultantes del choque tecnología vs. tradición. Así, la sola adopción de equipos no moderniza de modo estable, seguro, duradero y funcional con los objetivos propuestos. Deben cambiar instalaciones o ambientes de trabajo, modos de comunicación, normatividad, actitudes y aptitudes de los servidores, métodos y procedimientos de trabajo, entre muchos. De acuerdo con Russell Ackoff, las instituciones deben buscar enfrentarse de manera efectiva con las problemáticas que surgen e interactúan en el medio ambiente, cada vez más complejo y dinámico, donde día a día aparecen nuevos recursos tecnológicos. [23]

De manera casi simultánea a la aparición de la informática, nació la administración de centros de cómputo y sus servicios. Se pretendió, con ello, racionalizar las adquisiciones y uso de tiempo de recursos computacionales. Como especialización de ella se ha propuesto un nuevo terreno de estudio y consideración: la administración de la seguridad informática. Ello significa integrar conocimientos que apoyen una toma de decisiones que aborde de manera integral los aspectos de protección de los datos, su integridad y confidencialidad, así como el resguardo de los activos informacionales en general. Se constituye así un nuevo terreno de toma de decisiones racionales y ordenadas, que deberá atender el administrador público.

La problemática de la seguridad informática es amplia. Involucra muchos aspectos, como se ha visto.

Un marco analítico adecuado a una concepción amplia del problema de la seguridad informática es el propuesto por David Hsiao, en su obra *Computer Security* [24]. Propone un marco en el que diferencia, niveles de seguridad e identifica los recursos que posibilitan su solución. El modelo de Hsiao se esquematiza en la figura 1.

En este modelo subyacen algunos supuestos. La seguridad se logra al resolver todos los niveles. Cada uno cuenta con medios para proveer seguridad. Los niveles interactúan entre sí de manera concéntrica. La seguridad en un nivel dado es condición de seguridad para los niveles inscritos en él. El desarrollo de cada uno de los niveles se presenta a continuación.

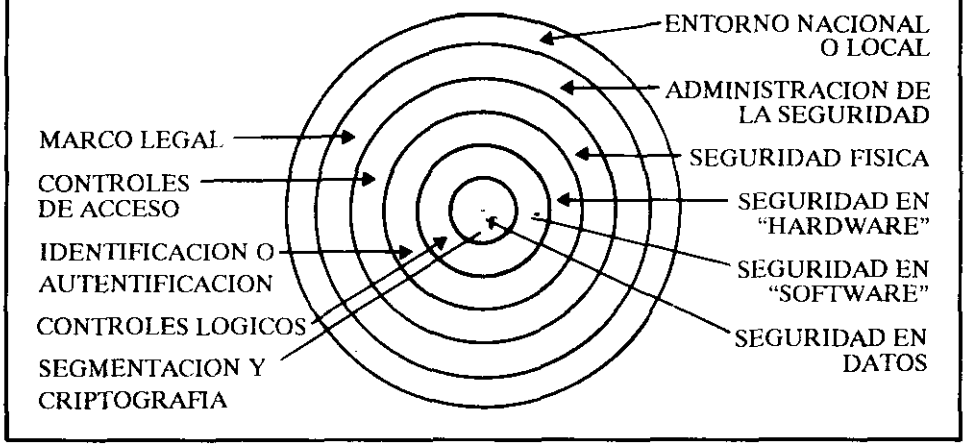
El primer nivel, referente al entorno nacional, provee un marco legal aplicable a la informática, con base en la situación económica, social, política o cultural prevaleciente en un lugar.

El segundo nivel atañe a la administración de los servicios informáticos en las

[23] Esta afirmación se basa en Ackoff, que la define como problema de "autocontrol". El mismo autor también afirma que se deben satisfacer los propósitos institucionales, de manera que se satisfagan los propósitos de cada uno de sus componentes, como requisito de un óptimo y moderno desempeño; éste lo denomina problema de "humanización". V. Ackoff, Russell, op. cit., capítulos 1 a 3.

[24] Hsiao, David; Douglas Kerr y Stuart Madnick: *Computer security*. San Francisco, Academic Press, 1979.

FIGURA 1 LOS NIVELES DE LA SEGURIDAD INFORMATICA



Fuente: Basado en, Hsiao, David; Douglas Kerr y Stuart Madnick: *Computer security*. San Francisco: Academic Press, 1979. P.2.

organizaciones. En ella se adoptan políticas de operación, que se derivan en métodos y procedimientos de trabajo y se atiende el flujo de la información, desde su origen hasta su destino final. Se busca, en general, garantizar la sana operación de los recursos computacionales y los datos que estos manejan. Se estudian causas, efectos y nivel de vulnerabilidad de los diversos elementos informáticos. Con conocimiento de ello, se establecen prioridades de protección. Medios más complejos para estos estudios son los análisis de riesgos, estudios de viabilidad, clasificación de datos según niveles de vitalidad para la institución o confidencialidad.

Los aspectos relativos al personal informático son también materia de cobertura de la seguridad operacional. En esencia, toda medida de protección y control se aplica a individuos. Se debe prever que éstos conozcan los medios o mecanismos de seguridad y estén sensibilizados sobre la vitalidad que representan los datos para la institución. Además, le concierne vigilar que se tenga un ambiente de trabajo idóneo para óptimo desempeño del personal.

Al tercer nivel, la seguridad física, le conciernen dos aspectos básicos:

1) El control de acceso de personas a instalaciones de cómputo o a sitios que albergan terminales u otros dispositivos. Se apoya en los controles administrativos, emitidos en el nivel de seguridad operacional.

2) La protección de equipos, instalaciones y dispositivos magnéticos - en lo físico- contra desastres naturales o acciones maliciosas de destrucción.

El cuarto nivel corresponde al *hardware* o equipos y dispositivos. En este nivel y los siguientes, los controles son más técnicos que administrativos. Se atienden cuestiones de identificación y autentificación del usuario. [25]

El quinto nivel se refiere a la seguridad en el *software*. Comprende todo tipo de programas de cómputo para efectuar procesos de datos. El principal agente de seguridad en este nivel es el adecuado desarrollo de los programas, en todas sus fases: diseño, programación, pruebas, puesta en función y documentación.

El sexto nivel corresponde a los datos. Para ello se deben atacar dos aspectos: "el ocultar el uso de ciertos datos a los equipos que los pueden accesar y la determinación de quién puede hacer qué tipo de operaciones con qué datos" a través de controles de acceso al usuario. [26] En el primer aspecto existe la criptografía como medio de protección, con la cual los datos se codifican y la hacen ilegible en accesos no autorizados. En el segundo aspecto, en la determinación del usuario y, las funciones que pueden efectuar, se requiere que el sistema provea de adecuada identificación al usuario, que a su vez lleve a determinar qué agregado de información se autoriza a utilizar y qué operaciones pueden efectuar con ella.

Para el desarrollo de un esquema adecuado de administración de la seguridad informática es necesario profundizar los dos primeros niveles referidos: El entorno nacional y local, desde el cual se emite una legislación aplicable y la seguridad operacional o administrativa.

En el primer nivel, cabe destacar que la informática abre perspectivas de desarrollo. No obstante, se trata de tecnologías generadas en otras sociedades y, por ello, su asimilación debe establecerse en un marco jurídico adecuado a la realidad mexicana y de definición de políticas para su óptima utilización. Se busca establecer leyes y disposiciones que otorguen "seguridad jurídica" a la utilización de herramientas informáticas. [27] Es el Estado quien debe promover esta seguridad y, para ello, generar normatividad aplicable, con la garantía de su poder coactivo.

En nuestro país, por ahora, no existe un marco jurídico integral a la informática. Existen ordenamientos dispersos que de una u otra forma se relacionan con el tema computacional. Ello tiene razón de ser: el fenómeno informático es de aparición reciente y su asimilación en la sociedad está en una etapa inicial. De esta situación no es posible que se derive un orden jurídico sistemático ni integral.

En México no existe ley alguna que se dirija a la informática y menos a su seguridad. El marco jurídico aplicable proviene de normas que se refieren, primordialmente, a otros ámbitos y hacen alguna alusión a la computación, o de instrumentos jurídicos cuya interpretación se relaciona con el terreno de las nuevas tecno-

[25] El usuario establece su identidad, se autentifica que es él mismo y que está operando su terminal autorizada.

[26] Ibid.

[27] Término de Vera Vallejo, Luis: *Algunos aspectos legales de la seguridad en informática*. S.P.I., mimeo (1988) (Ponencia presentada en diversos seminarios organizados por la Asociación Mexicana de Bancos). P.2.

logías para proceso de datos. Mientras las actividades públicas incrementan el uso, y dependencia, de los computadores crece la propensión a situaciones indeseables. Lo cual es cada vez más incongruente con una administración moderna o en vías de serlo.

Respecto al segundo nivel de seguridad, el diseño de un marco de administración de la seguridad informática, reviste dificultades, dadas las características de cada organismo usuario. Sin embargo, se pueden ofrecer algunos lineamientos generales para ello, que se presentan en cuatro campos, a saber:

A) planeación

B) organización

C) personal informático y

D) evaluación de la seguridad.

La planeación consiste en fijar el curso de acción a seguir, estableciendo principios orientadores, el orden a seguir en las operaciones y la asignación de recursos. Comprende, fundamentalmente, las siguientes tareas:

— Conocimiento cabal de los sistemas informáticos a controlar y proteger, incluyendo equipos, informaciones, programas, comunicaciones, etcétera.

— Determinación de necesidades de seguridad.

— Análisis de riesgo informático, que consiste en evaluar niveles de riesgo y costos de pérdidas, cotejados con costos de proveer seguridad y con las magnitudes en que el riesgo se reduce al aplicar medios de protección o control.

— Definición de objetivos de seguridad a alcanzar.

— Identificación de los elementos informáticos a proteger (equipos, informaciones, dipositivos, instalaciones, personas, etcétera).

— Determinación de programas y presupuestos para la seguridad.

El segundo campo, la organización, incluirá la definición de categorías funcionales, rediseño de estructuras organizacionales, documentación de la seguridad y desarrollo de métodos, procedimientos y medidas específicas. Entre las categorías funcionales se propone crear la administración de la seguridad informática, que se concreta en persona(s) o en unidades administrativas, dentro de la jerarquía organizacional. Dependerá y reportará a los mandos más altos de la organización. Sus funciones serán de sensibilización del alto mando acerca de la seguridad; coordinación de capacitación del personal; administración de la recuperación en caso de desastres; elaboración de estudios de análisis de riesgo informático; proponer estrategias, objetivos, programas, métodos o procedimientos de seguridad; ejercer control y auxiliar la evaluación de la seguridad; ser responsable que los recursos de seguridad estén debidamente documentados, entre otros.

Las funciones y responsabilidades del ejercicio de la seguridad deberán conferirse a cada servidor público usuario, que deberá asumir su papel plenamente y ser capaz de responder por el buen o mal desempeño de sus labores, ante los superiores indicados.

También, en la fase de organización se determinan los métodos y procedimientos

para la seguridad. Se pretende establecer un esquema de seguridad integral para una dependencia, entidad o unidad administrativa. Esto se logra al formar un sistema de protección y control en el que los procedimientos o medios estén debidamente definidos, estandarizados, obedezcan políticas institucionales de informática, atiendan metodologías de trabajo y documentación completa, aceptada y plasmada en manuales institucionales (manuales de organización, de procedimientos, de descripción de puestos, entre otros).

El campo del personal, se refiere a la administración de recursos humanos, orientada a la seguridad. Se tratan políticas generales de personal, selección e inducción, capacitación y desarrollo, responsabilidades directivas e impacto de la informática en las condiciones de trabajo.

Los aspectos de personal constituyen el principal asunto de la seguridad computacional. El éxito o fracaso de todo plan de seguridad está condicionado al desempeño del personal.

Los aspectos mínimos a considerar en materia de personal para un adecuado plan de seguridad son los siguientes:

— Adopción de políticas, estandarizadas y documentadas, que fomenten actitudes cooperativas y sean conocidas por el personal.

— Adecuada selección, inducción y capacitación del personal que operará sistemas de información.

— Se deberá extender una "cultura informática", como visión global del mundo informacional de la que se desprenden aptitudes y actitudes encauzadas a adecuarse a nuevas formas prácticas, métodos y mentalidad y mística de trabajo.

La evaluación de la seguridad se plantea con base en la función de auditoría informática, de la que derivan opiniones profesionales para medir la eficacia y eficiencia del ejercicio de la seguridad, así como la propuesta de medidas correctivas. Esta auditoría se ha difundido cada vez más entre los grandes usuarios de tecnología computacional y cuenta con bases y metodologías propias.

El punto de equilibrio del ejercicio de la seguridad consiste en atender el problema hasta el punto en que las organizaciones requieran y estén dispuestas a protegerse y pagar por ello. La disposición de abordar el problema debe partir de la premisa de que se conoce cabalmente la vulnerabilidad del ambiente informatizado y que se cubrirán los aspectos de mayor a menor riesgo, dejando, finalmente, un riesgo residual, con proporciones que la institución esté dispuesta a absorber en caso de siniestros.

CONCLUSION

La seguridad informática se concibió, en suma, como la garantía del resguardo de la integridad y confidencialidad de la información, y el mantenimiento de la continuidad y sana operación de las organizaciones. Con base en ello, se sustenta que la informática y su seguridad deben ser administrados, es decir, ser objeto de toma racional e integral de decisiones, donde es esencial la participación del administrador público, quien deberá ser capaz de determinar prioridades, objetivos, costos, beneficios, impactos organizaciona-

les, medios de control, evaluación y retroalimentación. Coordina esfuerzos y, en materia de recursos humanos, puede aportar elementos para la formación de personal sensibilizado, responsable y motivado, capaz de integrarse en esfuerzos colectivos.

Ackoff reconoce que es necesario que los administradores no sólo sepan utilizar los sistemas de información, sino que conozcan en detalle su funcionamiento con objeto de poder evaluarlos.[28] "Los administradores deben controlar los sistemas de información, no éstos a los administradores"[29]

Con base en lo anterior, se considera cumplido el objetivo del trabajo, que fue mostrar la seguridad informática como problema y terreno de consideración importante en la administración pública, y subrayar que el uso de técnicas administrativas es esencial en la solución de este problema. Asimismo, con apoyo del conocimiento del impacto informático en la sociedad, la variedad de manifestaciones que tiene la vulnerabilidad, los niveles que intervienen en la seguridad, el perfil del administrador y la esencia de la administración, se considera confirmada la hipótesis central de estudio.

Se destacó la desadaptación tecnología-organización, como fuente de inseguridad informática, por lo cual se requiere un cabal desarrollo armónico entre ambos.

La administración pública mexicana ha sido cada vez más dependiente de la aplicación de los recursos informáticos y por ello se recomienda enfocar la seguridad de modo preventivo y no correctivo. Corregir resultará más costoso que prevenir, lo cual es más crítico mientras se involucran masas importantes de información que significan dinero o poder y ponen en peligro los sistemas nerviosos publiadministrativos.[30] El nivel de sencillez o complejidad a que se llegue en el ejercicio de la seguridad informática, es decisión de cada organismo, según sus necesidades y recursos. En cualquier caso, ya sea grande o pequeña la institución, la seguridad deberá administrarse y abordarse en todos sus niveles, es decir, de manera integral. La seguridad deberá estar estandarizada y documentada, asentada en manuales de organización, de procedimientos, de descripción de puestos, así como en documentación específica de la seguridad [31] y

[28] Ackoff, Russell: *Planificación...* . P. 179.

[29] Las últimas líneas de este párrafo son adaptaciones de Ackoff. V. Ackoff, Russell: ibid. Pp. 180 y 181.

[30] Afirmaciones de Sendrow, Martin: *Impact of rapid changing computer technology on computer crime: advance computer securiy concepts*. S.P.I., mimeo, 1980. P.16.

[31] Se consideran documentos específicos de seguridad los siguientes.

— Documentación derivada del proceso administrativo de la seguridad informática.

— Manuales para métodos y procedimientos en materia de seguridad.

— Planes de recuperación informática ante casos de desastre.

— Manuales técnicos y manuales de usuario para mecanismos técnicos de protección.

— Documentos sobre normas de instalación de centros de cómputo, en materia de seguridad, ya sea para enfrentar o prevenir daños por siniestros naturales o intencionales.

— Manuales para el desempeño de la función auditora.

— Manuales de enfrentamiento o respuesta ante el crimen computacional, entre otros.

documentos de carácter jurídico. Las políticas y normas que se definan deben ser adaptables a la rápida evolución que se tiene en el uso de las nuevas tecnologías.[32]

Es claro que el éxito o fracaso de todo plan de seguridad, depende del personal. Por ello se requiere una adecuada política de administración de recursos humanos que coadyuve a los objetivos propuestos. Asimismo, se deberá fomentar la formación de especialistas en seguridad y auditoría, donde las instituciones de educación superior tendrán un papel relevante. Se extiende la informática, pero se adolece de expertos en su control. Esto es incongruente con la realidad de un país en proceso de informatización.

La seguridad informática es relevante, pero no es el factor primordial a considerar en un sistema de información ni el que más debe atender el personal. [33] Es importante que forme parte de un conjunto de actividades de las instituciones y se supedite a los objetivos que las constituyeron, así como a los fines de los sistemas de información como tales. Si no cumple éstos, no es racional priorizar las consideraciones sobre seguridad. La administración de la seguridad, incluyendo los planes, programas, métodos, procedimientos y mecanismos técnicos se integran en forma armónica en las tareas fundamentales del organismo y de cada uno de sus servidores. La seguridad, de ese modo, es medio de fortalecimiento de los organismos.

No se espera que por causa de la seguridad informática, provengan problemas fatales para las organizaciones o el propio país. Tarde o temprano se tendrá que afrontar el lado oscuro de la informática. Nora y Minc afirman, "en realidad, ninguna tecnología, por innovadora que sea, acarrea consecuencias fatales. Sus efectos son dominados por la evolución de la sociedad, más de lo que la constriñen. El reto es la dificultad de construir la red de lazos que haga progresar conjuntamente la información y la organización."[34]

Se sugiere que futuros estudios, en materia de seguridad informática o áreas afines, se orienten hacia un mejor conocimiento de:

1) el personal que labora en ambientes informatizados, como aspecto esencial de seguridad,

2) reorganización organizacional, al alterarse líneas, formas o prácticas de comunicación en los organismos y

3) análisis integral de la vulnerabilidad informática.

Las tecnologías de información juegan cada vez un papel más importante en el proceso de modernización publiadministrativo. Las computadoras deben ofrecer alta rentabilidad en lo político, administrativo, económico y social. Esto equivale a ser plenamente funcional a los objetivos del Estado mexicano. La importancia de contar con una visión estratégica, que

[32] Se recomienda, más que crear nuevas políticas, obtener mayor provecho de las ya existentes y conocidas por el personal, pero adaptadas al fenómeno informático.

[33] Excepto en sistemas de información de alta confidencialidad o críticos para la seguridad económica o política o social de la Nación.

[34] Nora, Simon y Alain Minc, op. cit. P. 25.

aborde la problemática de la seguridad informática para la administración pública en un futuro cercano, será crítica.

BIBLIOGRAFIA

Ackoff, Russell: *Rediseñando el futuro.* México: Editorial Limusa, 1983.

Ackoff, Russell: *Planificación de la empresa del futuro.* México: Editorial Limusa, 1983.

Bria, Ricardo: "Delitos en un ambiente informatizado", en *Actas: I Congreso Iberoamericano de Informática y auditoría.*

(San Juan, Puerto Rico). 2 a 6 de noviembre de 1987.

González Castellanos, Herbin Amory: *Fraudes en sistema de procesamiento electrónico de datos* (Tesis para obtener el título de contador público y auditor). Guatemala: Universidad de San Carlos (Facultad de Ciencias Económicas), 1978.

Hsiao, David; Douglas Kerr y Stuart Madnick: *Computer security.* San Francisco: Academic Press, 1979.

Krauss, Leonard & Aileen McGaham: *Computer fraud and countermeasures.* New Jersey: Prentice Hall, 1979.

McLuhan, Marshall: *Understanding media: the extensions of man.* New York: Signet Books, 1964.

México, Secretaría de Programación y Presupuesto: *Guía para la elaboración de programas de desarrollo informático.* Talleres Gráficos de la Nación, 1987.

México, Secretaría de Programación y Presupuesto, Instituto Nacional de Geografía, Estadística e Informática: *La Informática y el derecho: informática jurídica y derecho informático para México.* México, D.F.: Talleres Gráficos de la Nación, 1983

Naisbitt, John: *Macrotendencias.* México, Edivisión, 1985. (Primera reimpresión).

Nora, Simon y Alain Minc: *La informatización de la sociedad.* México: Fondo de Cultura Económica, 1980.

Nussbaum, Bruce: *El mundo tras la era del petróleo: nuevos ejes de poder y riqueza.* México, Editorial Planeta, 1985.

Sendrow, Marvin: *Impact of rapidly changing computer technology on computer crime: advance computer security concepts*, S.P.I., mimeo, 1980.

Simon, Herbert A.: *La nueva ciencia de la decisión gerencial.* México, Librería "El Ateneo" Editorial, 1982.

Simon, Herbert A: *El comportamiento administrativo: un estudio de los procesos decisorios en la organización administrativa.* Madrid, Aguilar, 1962.

Sotomayor, Jesús y A. Sánchez: *Planeación de la recuperación informática en casos de desastres*, ponencia en "III reunión de sistematización de bancos centrales americanos e ibéricos". (Santo Domingo República Dominicana), 25 de noviembre a 1o. de diciembre de 1984.

Téllez Valdés, Julio: *Derecho informático.* México, Universidad Nacional Autónoma de México, 1987.

Vera Vallejo, Luis. *Algunos Aspectos Legales de la seguridad en informática.* S.P.I., mimeo. (1988) (Ponencia presentada en diversos seminarios organizados por la Asociación Mexicana de Bancos).

Wilson, Brian: *Systems: concepts, methodologies and applications.* U.K., John Wiley & Sons, 1984.