EL COLEGIO DE MEXICO, A.C.

CENTRO DE ESTUDIOS INTERNACIONALES

LA SEGURIDAD INFORMATICA

EN LA

ADMINISTRACION PUBLICA FEDERAL

DE MEXICO

TESIS QUE PARA OPTAR POR EL TITULO DE
LICENCIADO EN ADMINISTRACION PUBLICA,

PRESENTA,

ALBERTO HERRERIAS FRANCO

MEXICO, D.F.

JUNIO DE 1990

A mis padres.	Con mucho amor y profundo agradecimiento. Por su enorme apoyo y ejemplo.
A Gonzalo.	Por su espiritu enorme. Con mucho amor.
A mis hermanos, Bertha Inés, Bernardo y Renata.	Por su amor y apoyo permanente.
A Leticia.	Por su motivación hacia la consumación de este trabajo. Por su solidaridad y amor. Por su trascendencia en mi vida y realización.
A mis abuelos, tíos, primos y amigos.	Siempre incondicionales. Por su apoyo y aliento a la consumación de este trabajo.

AGRADECIMIENTOS.

Para el desarrollo de este trabajo fue invaluable el apoyo y consejo del Prof. Manuel García y Griego, quien dirigió el desarrollo del estudio, y del Dr. Luis Aguilar Villanueva. Apoyaron técnicamente el estudio y ayudaron a definir el enfoque del trabajo, Jose Luis Arciga, Lic. Ramón Ocampo, M.en C. Mario Villalobos, el Ing. Ernesto Aguilar Aguilar, Lic. Armando Acevedo, Lic. Enrique Ampudia Mello, Lic. Cristian Zempóaltécatl, Act. Pedro García del Valle, Lic. Luis Vera Vallejo e Ing. Horacio Vidrio Amor.

En la comprensión del perfil del administrador, su ámbito de acción y técnicas, fueron importantes las ideas, conceptos y documentos proporcionados por Dr. Luis Aguilar Villanueva y Lic. Leticia Cabral Calvillo.

En la obtención de materiales bibliográficos y hemerográficos, agradezco la colaboración de Shirley Ainsworth y Micaela Chávez.

A los Ings. Enrique y Francisco Aristi Villalobos agradezco las facilidades para el desarrollo de este trabajo por computadora.

Expreso mi más sincero agradecimiento a los servidores públicos, profesores y especialistas que me concedieron su tiempo y facilitaron documentos durante la fase de entrevistas para el desarrollo de este estudio.

INDICE

Página

INDICE DE CUADROS Y FIGURAS

PROLOGO

Con el advenimiento y extensión del uso de nuevas tecnologías para el proceso de información --también conocidas como informática o computación--, se han manifiestado diversos problemas de seguridad, derivados del propio manejo automatizado de los datos. Entre ellos destaca la gran propensión de los sistemas computacionales a ser medios o fin de actos ilícitos o delictivos y de permitir enormes daños, perdidas o fugas de información, que afectan negativamente la operación y viabilidad de los organismos.

Dia a dia aparecen múltiples publicaciones impresas, que abordan los aspectos en que estas tecnologías favorecen la eficiencia y eficacia de las instituciones y liberan al hombre de tareas repetitivas o rutinarias. Sin embargo, los aspectos problemáticos que presenta la informática, y que se traducen en vulnerabilidad para el usuario computacional, han sido poco estudiados. La investigación, por su parte, se ha enfocado más a mejorar las tecnologías computacionales, en velocidad y volumen de proceso, que a asegurar el buen y correcto funcionamiento de los recursos informáticos ya existentes.

La Administración Pública Federal de México sigue esta misma linea. En los últimos años ha adquirido numerosos equipos de computación y ha desarrollado programas para el proceso de los datos. Ha buscado, asimismo, adoptar las

tecnologías más modernas en cada momento. Sin embargo, el aseguramiento del buen funcionamiento de estos recursos ha sido precario. Los daños ocurridos durante los sismos de 1985, en la Ciudad de México, lo hicieron evidente --y en la introducción se hace referencia a ello.

A pesar de la relevancia de la seguridad informática --concebida como el conjunto de medios que permiten garantizar el resguardo y buen uso de la información y otros activos computacionales--, poco se ha trabajado en México sobre ella. Este trabajo concibe la seguridad informática como un problema en la Administración Pública de México y que debe ser abordado por administradores públicos.

Por su propia naturaleza, la seguridad afecta uno de los medios más importantes para el funcionamiento de los organismos: la información y su proceso, que sustentan toda actividad y decisión administrativa y se constituyen en esencia de institucionalidad --la sección 3.5 habla sobre ello.

El interés del autor de trabajar el tema que ocupa este estudio surgió a partir de la vivencia de algunas experiencias negativas en el ámbito informático, ocurridas durante el desarrollo del servicio social. Ya en el programa de estudios de la licenciatura en administración pública, en El Colegio de México, A.C., había tenido lugar una aproximación propia hacia el mundo de la computación. El programa incluía una asignatura denominada "informática". Contemplaba temas como diseño de sistemas y programación en

diversos lenguajes computacionales. La seguridad no se mencionó en ningún momento.

Durante el segundo semestre de 1986 se desempeñó el servicio social. En la unidad administrativa en que éste tuvo lugar, se había iniciado, recientemente, la operación de sistemas de computación para el proceso y almacenamiento de información estadística. Había dos problemas que resaltaban por su frecuencia. Por una parte, se extraviaban discos flexibles magnéticos. Muchos de ellos contenían información, de la cual no existían respaldos. Aunque no se trataba de información confidencial, cuando ocurrían pérdidas de datos, la recuperación implicaba varias horas o jornadas de trabajo. Por otra parte, era común el daño o perdida de datos o programas, a causa de la inadecuada operación de los equipos.

De estos hechos surgió un incipiente interés propio por los aspectos del resguardo de la información y los activos informáticos en la administración pública. Al meditar sobre los efectos que traería la mala operación computacional o las pérdidas de datos vitales para algunas areas gubernamentales, incluyendo las instituciones bancarias, parecía evidente que la seguridad informática podía tratarse de una cuestión sumamente importante. A partir de ello, principió una fase larga de investigación, en la que dia a dia, la seguridad informàtica se fue presentando como un problema complejo y confuso. Se manifestaba en aspectos de administración de sistemas,

comunicación, manejo de personal, diseño de programas, operación y mantenimiento de equipos y programas, resguardo de los mismos, entre muchos. Ni los administradores de centros de cómputo ni los diseñadores de sistemas ni los programadores ni los operadores, tenían un conocimiento cabal de esta seguridad. Sus sugerencias verbales y documentales poco aclaraban o permitían entender el problema. Es más, muchos de ellos no reconocían el problema como tal.

Fue libro de David Hsiao el que ofreció un marco analítico para comprender la seguridad informática y, con base en él se desarrolló la investigación e integración del trabajo. El enfoque que se sigue para este estudio implica, en mucho, la visión de un administrador sobre un problema importante y complejo, y hacia el cual no existen soluciones únicas o fáciles. Se retoma la concepción del administrador como profesional al que le compéte conducir procesos decisorios para ser traducidos en acciónes que garanticen el logro de los objetivos propuestos. La seguridad informática se presenta como un problema vital para el funcionamiento de las instituciones y, por ello, de interés para el administrador público.

Por sus propia naturaleza, la seguridad informática es un tema confidencial para los organismos públicos. Por ello, no se hace mención en el trabajo de nombres de instituciones o personas entrevistadas. Muchos de ellos solicitaron confidencialidad en este aspecto, lo cual se respeta. Sin

embargo, cabe mencionar que en muchas instituciones fue posible "desnudar" la seguridad que prevalecía en ellas, debido a que los entrevistados no pusieron límite a proporcionar al autor toda la información solicitada. En otras, los interlocutores fueron reacios a brindar cualquier dato sobre el tema. El capitulo 7, presenta un panorama de la seguridad informática en la Administración Pública Federal de México, y se construyó con base en la información recabada en diferentes dependencias y entidades.

Dada la extensión del Ejecutivo Federal, no fue posible cubrir, ni por mucho, todo su àmbito informático. No obstante, la problemática en materia de seguridad se encontró muy similar en la mayoría de los organismos visitados y ello valida las conclusiones del trabajo.

ABREVIATURAS

A.M.A.I.	Asociación Mexicana de Auditores en Informática
A.P.F.	Administración Pública Federal.
AGN	Archivo General de la Nación.
Art.,Arts.	Artículo, Artículos.
C & C	Computadoras y comunicaciones.
CIA	*Central Intelligence Agency.*
CISA	*Certification on information systems audit.* Es una certificación de cualidades profesionales para ejercer la auditoría de sistemas de información, otorgada por la EDPAA.
D.O.	Diario Oficial de la Federación.
EEUU o USA	
E.U.A.o EUA	Estados Unidos de Norteamérica.
EDPAA	*Electronic Data Processiong Auditors Association.*
FBI	*Federal Bureau of Investigation.*
Fr.	Fracción.
I.L.O.	*International Labour Office* (Ginebra).
INAP	Instituto Nacional de Administración Pública.
INEGI	Instituto Nacional de Estadística, Geografía e informática.
MIT	*Masachussets Institute of Technology.*
NIP	Número de identificación personal. Se le conoce así al número que debe teclear un usuario de cajeros automáticos de los bancos.
O.I.T.	Oficina Internacional del Trabajo.
PC	*Personal Computer* o computadora personal.
PNB	Producto nacional bruto.
S.P.P.	Secretaría de Programación y Presupuesto.
UPIICSA	Unidad Profesional Interdisciplinaria de Ingeniería y ciencias sociales y administrativas. Integrante del Instituto Politécnico Nacional.

INTRODUCCION

La sociedad mexicana está inmersa en un proceso permanente de cambio y modernización. La propia dinámica del país, y la del mundo que le rodea, han impactado continuamente sus estructuras, funciones y valores. Bajo un enfoque sistémico, México ha buscado mantener su viabilidad como Estado-nación, estabilidad --en lo económico, político y social-- y una sana adaptación hacia los cambios que se le exigen en lo interno y en lo externo.

A lo largo de la historia, el hombre ha desarrollado tecnologías con objeto de facilitar su adaptación al mundo y la transformación del entorno. Se inventan o descubren nuevas técnicas que le permiten un mejor dominio sobre la naturaleza y mayor dinamismo en tareas cotidianas como trabajo, traslados, comunicaciones o esparcimiento.

Algunos cambios tecnológicos han alterado drásticamente la vida del hombre. Ejemplo de ellos son la aparición de la escritura, las máquinas, el ferrocarril, la energía eléctrica o el proceso electrónico de datos. Como sostiene Marshall McLuhan, éstos avances han acercado personas, cosas y conocimientos. Se constituyeron en "extensiones del hombre", que permitieron una mayor integración o interacción entre las sociedades. El mundo, así, se ha acercado gradualmente hacia la constitución de una "aldea global".(1) En muchos casos, el impacto de los grandes

---

1.- Para una exposición más amplia del impacto de las mencionadas tecnologías, ver McLuhan, Marshall:

cambios tecnológicos ha conllevado una reestructuración del medio ambiente humano, o la creación de otro completamente nuevo. (2) Al respecto, Nora y Minc afirman que las "revoluciones tecnológicas", en el pasado, provocaban una intensa reorganización de la economía y la sociedad.(3) 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 viabilidad 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. (4)

En general, los cambios sociales han sido menos ràpidos que la aparición y difusión de las nuevas tecnologías, que los provocan. Las sociedades son resistentes al cambio. Ello se manifiesta cuando intervienen afectaciónes en valores, tradiciones, culturas o intereses -- particulares, de grupos o de clases--; alteraciónes en modos de trabajar o de pensar; o alteraciones en las estructuras y prácticas de mando y

---

"Understanding media: the extensions of man".-- New York: Signet Books, 1964.

2.- V. Ibid. P. viii y 19. También, Ackoff, Russell: Rediseñando el futuro.-- México: Editorial Limusa, 1983. Pp. 4 y 5.

3.- Nora, Simon y Alain Minc: "La informatización de la sociedad".-- México: Fondo de Cultura Económica, 1980. P. 17.

4.- Ante ello, Ackoff afirma la necesidad urgente de incrementar la habilidad de la sociedad para aprender y adaptarse. Ibid. P.6.

organización de los seres humanos. 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. (5) Y ello, reconoce, es un problema crítico de la actualidad.

Después de la segunda mitad del siglo XX, en el mundo capitalista desarrollado, dio inicio la llamada "era de la información", como etapa sucesora de una era industrial. Se trata de una nueva fase en la evolución de la humanidad 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 del conocimiento. (6) La dinámica del mundo moderno gira, cada vez más, en torno a la capacidad de manejar y disponer de información.(7)

5.- Toffler citado por Ackoff, op. cit. P. 5.

6.- Para mayor profundidad ver capítulo 3, primeros párrafos. Naisbitt afirma que en los Estados Unidos de Norteamérica, la "era de la información" marcó su inicio en 1956, año en el cual el numero de empleados que ocupaban puestos técnicos, administrativos y de oficina, sobrepasó a en número a los de la clase obrera. V. Naisbitt, John: Macrotendencias.-- México: Edivisión, 1985. (Primera reimpresión). P. 22. Cabe también señalar que está en emergencia una nueva cultura: la 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 petroleo: nuevos ejes de poder y riqueza".-- México: Editorial Planeta,1985. P. 50.

7.- 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 constituído base para innumerables estudios posteriores y en él se

Esta "era de la información" tomó mayor fuerza, o se aceleró en su conformación, a través del desarrollo de 1) las telecomunicaciones, incluyendo el uso de 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 el manejo de mayores volúmenes de información y a velocidades crecientes.

De hecho, la informática tiene alcances insospechados. Facilita accesos, alteraciones, borrados, filtrado o procesamiento, almacenaje y distribución de datos; referentes a múltiples ámbitos de la vida del hombre. La computación permite un incremento importante en la productividad de las personas y las organizaciones. Facilita el proceso de la información que sustenta acciones o decisiones. Permite ejercer un mejor y más rápido control, y clasificación de los datos o archivos de las instituciones. Asimismo, los sistemas computacionales, que implican interconexión de diversos equipos de proceso o terminales, facilitan enormemente la interacción o coordinación de los trabajos de las diversas unidades administrativas de una institución.

La informática modifica, en suma, el tratamiento y conservación de la información, y en esa medida, afecta el

---

afirma el rol de las tecnologías mencionadas, en el funcionamiento de las sociedades. Nora, Simon y Alain Minc, op. cit.

"sistema nervioso" de las organizaciones y de la sociedad entera.(8) Asimismo, es parte de una revolución a nivel global, en la que se está gestando una forma de sociedad y de civilización basada en el proceso rápido y masivo de datos. La capacidad de disponer de mayor y mejor información para la toma de decisiones, es piedra angular de la nueva era. La computación se presenta como "revolución tecnológica" que, gradualmente, presiona hacia el cambio en las funciones y estructuras de la sociedad.(9)

El desarrollo de las tecnologías para el procesamiento electrónico de datos ha sido acelerado y está siendo, hoy por hoy, factor determinante de la supremacía entre las sociedades y las corporaciones. La difusión de la informática, asimismo, ha sido explosiva. Los fabricantes de equipos de computación, accesorios o programas, no han cesado de mejorar sus productos, perfeccionarlos y diversificarlos. Por su parte, las sociedades han

8.- Nora y Minc, op. cit. P. 17.

9.- La incorporación de la informática en las administraciones provoca cambios en multiples dimensiones. Entre otros, se pueden mencionar los siguientes. 1) Alteraciones en formas y canales de comunicación --que son esencia de una "organización". 2) Alteración de los métodos o procedimientos de registro o almacenamiento de datos. 3) Cambios en las funciones del personal institucional, en todos niveles --operativo, supervisor y directivo. 4) Creación de nuevos polos de poder o influencia, en las unidades administrativas que concentran servicios informáticos de los organismos. 5) Alteraciónes en las prácticas o funciones de supervisión. A este respecto, Herbert Simon afirma que "a medida que una cantidad cada vez menor de trabajo es regida por el hombre y cada vez más por la máquina, la naturaleza de la supervisión experimenta cambios". 6) Cambios en las tareas, hábitos y condiciones de trabajo del personal que ahora opera sistemas informáticos.

incorporado el uso de éstas tecnologías en casi todos los campos de actividad, al incorporarse en múltiples areas de la economía y la sociedad, en esferas de producción, distribución, consumo y administración. Nora y Minc afirman que la "revolución informática" está invadiendo toda la sociedad y que, sin ser la única innovación técnica de estos últimos años, constituye factor común que permite y acelera todos los demás progresos técnicos."(10)

Con base en ello, 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. En ese sentido, han surgido necesidades de definición y ejecución de políticas de utilización, educación e investigación, de las que se derive 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 informática, por su propia naturaleza, altera conceptos y el mismo ámbito la seguridad. Ésta se hace más crítica en

10.- Ibid. P. 31.

el campo computacional debido a que estas nuevas tecnologias magnifican los riesgos que puede presentar la información procesada y almacenada manualmente. La computación permite enormes concentraciones y volumenes de datos y facilita su transformación y emisión. El acceso a éstos ya no necesita efectuarse en la instalación física donde se almacenan los datos, sino que puede tener lugar en sitios o terminales remotas y ajenas a los organismos propietarios de los datos. Asi, con base en su enorme capacidad de manejo del recurso información, la computación es agente que incrementa la vulnerabilidad o propensión de las organizaciones hacia la intensidad y recurrencia de daños, pérdidas, desfalcos, sabotajes, fraudes o errores, si no es objeto de un adecuado control.

La seguridad informática encuentra aquí su campo de acción. Su esencia está en asegurar la continuidad, sana operación de un organismo y el control del buen uso de la información que le es propia. En otras palabras, su finalidad es el mantenimiento de la integridad y confidencialidad de los datos y otros activos informáticos. Con ella, se regula el qué, cómo, cuando, donde, quién y para qué accesa la información procesada electronicamente. Es controlar qué información se accesa; cómo debe de 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. La llave para el control de todo ello es la "autorización", que nace

en los altos niveles de mando político o administrativo y se ejerce de manera descendente en la organización. En un ambiente de seguridad computacional el esquema de actuación debe ser de "libertad negativa". Es decir, nada puede hacerse excepto lo está permitido para cada persona, en lugares, momentos y circunstancias predeterminadas.

La información, como se discutirá más adelante, es un recurso valioso en las administraciones. (11) Por una parte, permite que tenga lugar el funcionamiento correcto y esperado de las instituciones. Por otra, es factor de poder, al apoyar toma de decisiones y acciones en el ámbito del poder público. Con base en ello, el acceso, proceso y emisión de datos debe efectuarse por canales claramente predeterminados y reconocidos por todo usuario. El concepto de autorización será, entonces, función de la dirigencia organizacional, para habilitar personas en la operación de las fases o etapas del flujo de la información.

México, al igual que otras sociedades, se halla en proceso de informatización, es decir, en proceso de extensión del uso de tecnologías computacionales, de modo que cada dia apoyan más las operaciones y toma de decisiones en la sociedad. Los organismos públicos se hallan inmersos en este proceso. A medida que se extiende el uso de la informática, las instituciones se hacen más dependientes de su aplicación y a ellos condicionan la continuidad en su desempeño de labores.

11.- V. capitulo 3.

La seguridad informática se presenta como elemento que permite asegurar una aplicación o uso óptimo de los medios informáticos y garantiza el resguardo de la información, vital en el funcionamiento de todo organismo. Este trabajo aborda la seguridad informática y la enfoca hacia la Administración Pública Federal de México. Ello se hace importante debido a las siguientes consideraciones.

Primero. El aparato estatal se encuentra inmerso en un proceso de modernización y, con ello, de búsqueda de mayor racionalidad administrativa. Se pretende ser más eficiente, es decir optimizar la aplicación de los recursos y mejorar la disponibilidad y calidad de información para la toma de decisiones. Una de las herramientas básicas para este proceso es la informática y su uso es cada vez más extenso. Es, hoy por hoy, elemento constituyente del sistema nervioso de las instituciones públicas.

Segundo. La Administración Pública es el mayor usuario de la informática, a nivel nacional. Con ello, es también el más necesitado de contar con mecanismos de control y seguridad para ello.

Tercero. La Administración Pública Federal ejerce papel rector y regulador en la economía y la sociedad. El procesamiento electrónico de información coadyuva a esos fines y sustenta toma de decisiones importantes al interés nacional. En ese aspecto, el manejo no racional de los datos puede tener alcances insospechados en terrenos políticos, económicos o sociales, así como en el daño de los

derechos individuales y grupales. En la medida que la información es elemento constituyente del poder público, las fallas o eslabones débiles en el control de la información, pueden afectar o disociar ese poder, incluso ante entes extranjeros. De ese modo, la seguridad informática se convierte en elemento de consideración para la paz social y la seguridad nacional.

Una discusión frecuente a nivel internacional en el ámbito de la seguridad computacional, desde la década de los sesenta ha sido la referente 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 pósibilita grandemente el manejo, adquisición, cruce o intercambio de este tipo de datos. Algunas consideraciones sobre esta discusión se ofrecen en el cuarto capitulo, por ser un area importante en el tema que ocupa este trabajo, y por ser el aspecto dogmático (12) del que se deriva la legislación atañente a la protección de datos, con las consecuentes implicaciones sobre las instituciones.

Cuarto. La problemática de la seguridad computacional ha sido insuficientemente atendida en naciones desarrolladas. En México, salvo algunos casos aislados, su atención está practicamente ignorada. Muestra de ello es el

12.- Los aspectos dogmáticos de una ley fundamental o constitución son los referentes a las garantías individuales.

alcance de los daños, en muchas dependencias y entidades públicas, a causa de los sismos de 1985, en la Ciudad de México. No hubo institución pública alguna preparada para un siniestro de tal magnitud. Secretarías de Estado, instituciones bancarias y otros organismos descentralizados perdieron centros de cómputo y almacenes de datos, con volúmenes importantes de información no recuperable. Ello hizo notoria la ausencia de previsiones, para mantener la integridad de los datos y, simultaneamente, la falta de una cultura informática, de la que se desprendiera una adecuada administración computacional, que protegiera ante daños de esta magnitud.

Este trabajo tiene como objetivo analizar la seguridad informática como terreno de consideración importante en la Administración Pública Federal de México. Asimismo, la administración pública se concibe como disciplina que permite identificar y asegurar los medios para lograr fines previstos o deseados. Se pretende identificar los elementos que intervienen y garantizan esta seguridad. Los fines, que son el logro de la seguridad, y la seguridad como tal, no se discuten. Se les considera deseables y suficientes para todo organismo público que procesa información electrónicamente. Los medios, por su parte, si se discuten. Se trata de asegurar el logro efectivo de los fines de la seguridad. Así, los medios deben ser congruentes con ello.

El trabajo se constituye como un desarrollo analítico y lógico. Se llega a conclusiones lógicas, a partir de un

marco analítico. No se plantean hipótesis empíricas, para ser comprobadas o refutadas. Se presentan diferentes niveles y aspectos del problema de la seguridad informática y con base en ello, se generan conclusiones y proposiciones lógicas.

La problemática de la seguridad computacional es comprendida como un conjunto de problemas, interrelacionados entre sí y cuya solución requiere la consideración de los diversos elementos que intervienen. Se afirma, que 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.

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. Se parte del supuesto que administrar significa tomar decisiones (13) y el proceso administrativo (14) equivale a un proceso de toma de decisiones, en el àmbito de una organización y con

13.- Herbert Simon es uno de los principales arquitectos de la noción de que administrar significa tomar decisiones y el administrador es un tomador de decisiones. V. Simon, Herbert A:"El comportamiento administrativo: un estudio de los procesos decisorios en la organización administrativa".-- Madrid: Aguilar, 1962.

14.- Por proceso administrativo se comprende como la definición de un conjunto de tareas secuenciales, que permiten asegurar el cumplimiento de objetivos deseados. En él, forman parte etapas de identificación de necesidades y objetivos, determinación de organización de trabajo y métodos, selección y participación de personas, dirección y control, entre otros.

base en la normatividad aplicable, para el cumplimiento de fines previstos y esperados.(15) La administración se concibe como arte de garantizar que las cosas se hagan. Con base en ello, la seguridad informatica deberá ser sujeta de toma 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 garantia de su funcionamiento. Ello implica que este profesional conozca el panorama del fenómeno informático, la problemática resultante y las caracteristicas 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 fisicos, 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

---

15.- Simon, Herbert A., op. cit., P.8.

protección sean como tales y no conlleven costos no deseados. (16)

En el desarrollo del trabajo subyacen dos hipótesis o supuestos normativos. Se trata de proposiciones, tomadas como verdaderas. No se discute su validez, aunque en algunas secciones del trabajo existen argumentos que los refuerzan.

El primer supuesto normativo sostiene que la informática solo puede ser agente modernizador, cuando su incorporación en las organizaciones se corresponda con un proceso de modernización administrativa o rediseño del ambiente donde se aplicaran las nuevas tecnologías. Ello se relaciona con la argumentación, presentada al inicio de esta introducción, en la que se sostiene que existen cambios tecnológicos importantes, que obligan a reestructurar el funcionamiento de la sociedad. Para las organizaciones, se afirma que su modernización, de modo estable, seguro, duradero y funcional con los objetivos propuestos, no se logra sólo con la incorporación de nuevos recursos tecnológicos. Es necesario que exista adaptación cabal entre institución y tecnologías, en ambos sentidos. Para ello se requiere rediseñar o modificar instalaciones o ambientes de trabajo, estructuras de comunicación, normatividad, actitudes y aptitudes de los servidores, métodos y procedimientos de trabajo, entre

---

16.- Por el alcance de la informàtica, su estudio debe ser de caràcter multidisciplinario. Tradicionalmente se le ha abordado sólo en sus aspectos de *hardware* y *software* y algunas implicaciones jurídicas y administrativas. No obstante, con el impacto a nivel de toda la sociedad, que está experimentando, debe ser tratada con mayor amplitud.

muchos. En otras palabras, bajo un enfoque sistémico, no es posible modernizar, o cambiar, un sistema u organización, de modo dinàmico, armónico y duradero, si no se moderniza el sistema en todos sus componentes, es decir, integralmente.

Como consecuencia, se sostiene que la discrepancias o incompatibilidades entre el uso de nuevas tecnologías de manejo de informaciòn y los ambientes sociales y organizacionales donde se insertan, son fuente primaria de riesgos y, por lo tanto, de problemas de seguridad --en este caso, de seguridad informàtica. En este sentido, en la medida en que las organizaciones apliquen la informàtica y no modernicen estructuras, funciones, comunicaciones y adiestren a sus servidores hacia nuevas aptitudes y actitudes, enfrentaràn problemas de seguridad informática. De acuerdo con Russell Ackoff, las instituciones deben buscar enfrentarse de manera efectiva con las problemáticas que surgen e interactùan en el medio ambiente, cada vez más complejo y dinámico, donde día a día aparecen nuevos recursos técnològicos. (17)

El segundo supuesto normativo, complementario del anterior, y mencionado como propuesta bàsica de este trabajo, sostiene que debe ejercerse administraciòn sobre

---

17.- Esta afirmaciòn 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 òptimo y moderno desempeño. este lo denomina problema de "humanizaciòn". V. Ackoff, Rusell, op. cit., capítulos 1 a 3.

la seguridad informàtica, como un modo adecuado de resolver ésta. Se trata de un problema complejo y polifacético, donde interactúan elementos físicos --equipos--, lógicos --programas de cómputo--, datos, estructuras organizacionales y personas, entre muchos. La administraciòn consistirá en conducir un proceso racional de toma de desiciones para garantizar el cumplimiento de los objetivos de la seguridad informática. Se destaca el rol del administrador público, como profesional capaz de tomar decisiones y traducirlas en acciones concretas. Como se mencionó antes, debe ser capaz de motivar y coordinar esfuerzos hacia el logro de las metas deseadas en las organizaciones. De ese modo, conduce el trabajo de especialistas en las diversas areas del conocimiento que intervienen en un ambiente informatizado. La formación del administrador de la seguridad se basará en el conocimiento de los mùltiples elementos que intervienen en la implantaciòn de una solución, ya sean tecnicos, humanos, politicos, económicos o de cualquier otro tipo.(18) En este terreno, cabe citar una afirmaciòn 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 lo rodea, que de sus métodos de soluciònar los problemas."(19)

La estructura del trabajo, es decir, la secuencia de los capitulos --y las secciones que los componen--, sigue un

18.- V. infra. Se abunda más acerca del administrador pùblico en la sección 2.2.
19.- Ackoff, Russell, op. cit., p.6.

orden lógico que va de lo general a lo particular, por una parte, y de lo contextual hacia el propio problema de la seguridad y su administración, por otro. Se busca que cada capítulo sea antecedente o fundamento de los subsiguientes. El desarrollo del trabajo, o su secuencia, tiene lugar de la siguiente manera. Después de la introducción, el capítulo 1 presenta conceptos preliminares o generales. Incluye definiciones y características de rubros presentes a lo largo del trabajo. Así, se abunda sobre conceptos de informática, información, privacia y seguridad informática.(20) El segundo capítulo presenta elementos de teoría administrativa y de admistración pública. Primero, se hace referencia a la modrnización del Gobierno Federal de México. Después, se discute el perfil del administrador público y las tareas que le corresponden. Por último, se habla de la incorporación de la computación en la Administración Pública Federal. Este capítulo se presenta como fundamento para el ejercicio de la administración sobre el problema que ocupa este trabajo.

El tercer capítulo inicia con la exposición del impacto de las nuevas tecnologías de proceso de datos en el mundo moderno. Estas tecnologías aceleran una revolución a nivel global, en la que la información cobra valor creciente. Las secciones subsiguientes de este capítulo, consideran diversos enfoques bajo los cuales se constata y fortalece el

20.- Para definición de otros términos de uso común en el trabajo o vocablos técnicos, ver glosario, después de las conclusiones del trabajo.

carácter de la información como activo esencial, o recurso importante en el mundo contemporáneo. Con base en ello, se desprende la necesidad de ejercer un adecuado resguardo sobre ella. El cuarto capitulo analiza uno de los orígenes del problema de seguridad informática: el reclamo por la salvaguarda de la privacià. Se hace mención de la polémica, en el plano internacional, que dió lugar a reforzar la consideración sobre la necesidad de ejercer mecanismos de control y protección de los datos, en diversos países.

El quinto capítulo introduce el lado menos abordado por la literatura de la computaciòn: sus aspectos vulnerables. Se aborda ya el problema de la seguridad como tal, a través de teorizar, de manera general, los aspectos de riesgo o problemática que presenta la informática. A partir de ello, se ofrece un cuadro tipológico de los daños, perdidas o delitos posibles, a los que se está expuesto, con la utilización de las tecnologías de proceso de datos.

El capitulo sexto presenta un marco analítico para comprender, de manera integral, la propia seguridad informática y el modo de resolverla. Se describen seis niveles de seguridad: 1) marco legal, 2) seguridad operacional o administrativa, 3) seguridad física, 4)seguridad en *hardware*, 5) seguridad en *software* y, por último, 6) seguridad en datos y transmisiones. Con base este marco analítico, se estructura el capitulo siete y, asimismo, se permite ubicar el marco legal (capitulo 8) y

la administración de la seguridad (capítulo 9), como los niveles 1 y 2 del problema de la seguridad.

El capítulo séptimo aborda, de manera amplia, la problemática de seguridad computacional, encontrada en la Administración Pública de México. Se expone con base en el marco analítico anterior. La investigación para ello se realizó mediante trabajo de campo, en el cual se visitaron dependencias, entidades, instituciones académicas y prestadores de servicios informáticos. Como consecuencia de la problemática encontrada, se refuerza la proposición del trabajo de enfrentar la seguridad informática mediante un proceso administrativo.

El capítulo 8 desarrolla el primer nivel de seguridad informática: el marco legal. Se resalta la falta de un derecho informático en nuestro país, se efectúa un recuento de la normatividad aplicable existente y se proponen elementos para una mejor regulación de la informática y su seguridad.

El capítulo 9 profundiza el siguiente nivel de seguridad: la seguridad administrativa. Se efectúa una división de ésta en cuatro fases: planeación, organización y ejecución, personal y evaluación; todas ellas como fases de un proceso administrativo. En cada una se exponen consideraciones relevantes para que la administración de la seguridad se optimice; sea, precisamente, racional; y apoye una modernización de los ambientes organizacionales donde se insertan los recursos informáticos, de modo que ambos se

desarrollen armonicamente. Este capítulo estructura medios administrativos para la solución de la seguridad informática, que deben ser considerados por el administrador público o la alta dirección institucional, en el abordaje del problema.

Después del cuerpo del trabajo, se presentan las conclusiones generales, en la que se recapitulan elementos importantes presentados a lo largo del trabajo. Se hace hincapié sobre los aspectos centrales del problema de la seguridad informática y se subrayan los medios de solución de ésta más relevantes. Asimismo, se mencionan orientaciones de estudios futuros sobre este tema.

Se incluyen cuatro anexos al estudio. Tres se refieren a elementos importantes de apoyo a la administración de la seguridad. El primero plantea los elementos para efectuar planeación de recuperación ante desastres computacionales. El segundo aporta elementos útiles para enfrentar el crimen computacional. El tercero expone una metodología para el desarrollo de análisis de riesgos, aplicado a la informática. Los tres constituyen rubros particulares acerca de la seguridad informática que, por su importancia, es conveniente ofrecer detalles sobre ellos. El cuarto anexo, por su parte, incluye el cuestionario bajo el cual se basó el trabajo de campo desarrollado para esta tesis.

El argumento del trabajo, en realidad, comprende tres areas generales. 1) Fundamentos para la seguridad

informática --origen del problema. 2) Análisis del problema. 3) Medios para resolverlo.

El area de los fundamentos u origen del problema de la seguridad se aborda en dos ángulos. A) La información se constituye como recurso valioso y por ello requiere protección y control (capitulo 3). B) Las personas y las organizaciones claman por el respeto a su privacía, a través del adecuado resguardo y control sobre el uso y distribución de la información (capítulo 4).

La segunda area corresponde al problema de la seguridad informática. En ello destaca la falta de reconocimiento del problema como tal y la propia existencia de la inseguridad informática. Se aborda en tres partes: la vulnerabilidad informática, en términos generales --capitulo 5--, la problemática que se presenta en la Administración Pública de México --capitulo 2, sección 2.3, y capitulo 7-- y la problemática, específica, en el terreno jurídico --capitulo 8, sección 8.1.

La tercer area, referente a los medios de resolver la seguridad informática, se aborda bajo los siguientes tópicos. Primero, se expone un marco analítico para resolver la seguridad --capitulo 6. Segundo, se exponen elementos teóricos que fundamentan el abordaje del problema bajo un enfoque administrativo --capítulo 2 y capitulo 3, sección 3.3. Tercero, se proponen elementos para un marco legal que norme la seguridad informática en México y en su Administración Pública --capitulo 8. Cuarto, se desarrolla

la propuesta de elementos para el proceso administrativo de la seguridad computacional --capitulo 9.

La intervención en el trabajo de las dos hipótesis o supuestos normativos tiene lugar de la siguiente manera. El primer supuesto normativo del trabajo refiere que la modernización, vía nuevas tecnologías, solo es posible si la adopción de éstas se corresponde armónicamente con una adecuación o rediseño del ambiente humano. Ello subyace, primero, la sección 2.3, que habla de la incorporación de la informática en la administración pública mexicana y se mencionan, en forma genérica, los desajustes resultantes. Segundo, en la sección 3.1, donde se habla del tránsito del mundo contemporáneo hacia una "era de la información", donde las nuevas tecnologías electrónicas de proceso de información y comunicaciones han impactado la dinámica de la sociedad y la han obligado a reestructurarse. Tercero, en la vulnerabilidad computacional -- expuesta en el capitulo 5-- y la problemática en México --presentada en el capitulo 7--, se ilustra la desadaptación entre las administraciones y las nuevas tecnologías informáticas, así como su manifestación en problemas de seguridad informática. Cuarto, en los capitulos 8 y 9, que proponen el rediseño en lo legal --capitulo 8, sección 8.2-- y en lo administrativo y organizativo --capitulo 9. Con ello se apunta hacia la modernización de las instituciones públicas, de modo que éstas tengan un desarrollo armónico, al incorporar y aplicar tecnologías informáticas.

Por su parte, la segunda hipòtesis o supuesto normativo, acerca de administrar la seguridad, tiene su desarrollo con base en las areas 2 y 3 del argumento del trabajo, descritos en los dos pàrrafos precedentes al anterior. El area 2 define o presenta el problema a resolver, de modo que se refleja su complejidad y magnitud. El area 3 presenta la administraciòn como medio de solución.

CAPITULO 1.- CONCEPTOS PRELIMINARES.

Debido a que la informática es de reciente aparición, algunos términos carecen de significado uniforme. Es necesario, por lo tanto, definir algunos conceptos que se mencionan con frecuencia en este estudio. Ellos son la informática, información, seguridad informática y privacia. Otras definiciones se hallan en el glosario de términos, anexo al trabajo.(1)

El vocablo "informatica" es un galicismo, acuñado al conjuntar sílabas de las palabras "Information Automatique", dando lugar a "Informatique". En su sentido más puro, se refiere a la "utilización de medios manuales, mecánicos, electromecánicos o electrónicos que permiten un manejo racional e idóneo de captación y proceso de datos, para la toma de decisiones". Para esta tesis, el término se referirá exclusivamente al ámbito de los datos procesados por medios electrónicos y los equipos y dispositivos implicados en ello.

La "información" (del latin *in-formare*, es decir, dar forma o poner en forma) es un concepto abstracto, pero la consideramos como elemento que refiere hechos o ideas y es susceptible de ser plasmado y transmitido por un signo o combinaciones de signos. En una perspectiva comunicacional,

1.- las definiciones ofrecidas se dan como adecuadas y válidas para todo el trabajo y pueden o no ser aplicables fuera de este estudio. Se determinaron con base en distintas fuentes. Entre ellas destacan diccionarios generales y especializados, definiciones de diversos tratadistas informáticos y conceptos de especialistas entrevistados durante la fase de investigación para este estudio.

la información hace referencia a mensajes, dirigidos a una o màs personas, que los reciben y reaccionan ante ellos modificàndolos, aceptándolos o rechazándolos. Los mensajes se emiten con alguna finalidad: saber, conocer, elegir, distraer, entre otros.(2) Desde una perspectiva informática, la informaciòn se destina a la toma de decisiones y, con base en su utilidad para ello, ostentará algún valor.(3) En la siguiente sección se ahondará sobre este aspecto.

La informaciòn es idónea para toma de decisiones en la medida que cumple los atributos enumerados en cuadro num. 1.(4)

2.- Explicación de Tellez Valdés, Julio: "Derecho informàtico".-- México: Universidad Nacional Autónoma de México, 1987. P. 63.
3.- Ibid, P. 65.
4.- Adaptado de apuntes del curso "Técnicas de investigación administrativa", que forma parte del programa de Licenciatura en Administración Pública, del Centro de Estudios Internacionales de El Colegio de México. Tomado en México, D.F., febrero a junio 1983, impartido por prof. Manuel Quijano.

CUADRO NUM. 1
ATRIBUTOS DE LA INFORMACION, COMO SOPORTE PARA LA TOMA DE DECISIONES.
1.- Considera sólo aspectos necesarios. 2.- Debe ser pura, no contaminada. 3.- Confiable, es decir que sus orígenes sean legitimos. 4.- Oportuna, en tiempo de respuesta como en acceso a ella. 5.- Util, a los fines propuestos. 6.- Actual. 7.- Su costo debe ser analizado con objeto de hacerla eficiente. Es necesario que no cueste más que los beneficios que va a generar. 8.- Racional, idónea para cumplir los fines por los cuales fue creada y procesada. 9.- Que tenga distribución por canales predeterminados y controlados.

La seguridad informática es el conjunto de acciones y previsiones que, en esencia, buscan que la información siempre mantenga presentes estos atributos, es decir, resguardar la integridad y confidencialidad de los datos. Con ello se garantiza la continuidad y el sano ejercicio de las operaciones o funciones de las organizaciones. La seguridad informática se relaciona de manera directa con los atributos 2,4, y 9, el resto atañen, de modo más amplio, a la administración general de los propios sistemas de información.

Respecto al segundo atributo, la seguridad busca garantizar que no habrá alteraciones no deseadas o no controladas, ni en los archivos de datos ni en los programas de computación. Para ello se prevee que la

información siga los cauces, las normas y los objetivos de las instituciones.

El cuarto atributo, la oportunidad, se relaciona con la seguridad informàtica en la medida que ésta procura medios para que no haya contingencia o daño o desastre que afecte la disponibilidad de los datos en el momento que se le requiere.

El noveno atributo está intimamente relacionado con el mantenimiento de la confidencialidad de los datos. Se procura que éstos se utilicen exclusivamente para los fines legítimos, por los cuales se posee y procesa determinada información. Se busca que no haya fugas de información incontroladas, de tal modo que pueda ser utilizada o poseída ilegalmente por personas o agrupaciones ajenas a los organismos propietarios.

La seguridad informàtica se constituye como elemento fundamental en la sana aplicación de nuevas tecnologías. Su objetivo es garantizar que el proceso de datos sea eficaz y eficiente a los fines que se tengan y no vulnerables. El campo de estudio de este trabajo, en consecuencia, afecta uno de los aspectos más vitales de los organismos públicos.

En el plano de los derechos individuales, el manejo ràpido y de grandes volúmenes de datos, afecta la vida privada del hombre. Se manejan datos de domicilio, fechas, lugares de nacimiento, estado civil, religión, cuentas bancarias, historias clínicas y antecedentes penales, entre

muchos, en las relaciones entre el individuo y los organismos públicos. Los centros de acopio son, por ejemplo, registros censales, civiles, parroquiales, médicos, académicos, deportivos, culturales, fiscales, bancarios, laborales o judiciales, entre otros. Al apoyarse con computadoras para su procesamiento, se da lugar a una sistematización y disponibilidad inmediata de datos para diversos fines. Las personas han reconocido este hecho y generado protesta contra el posible manejo no racional o incontrolado de los datos, que afecta privacía o intereses particulares. El temor se genera con base en la posibilidad de que se crucen datos entre diversas instituciones y se llegue a tener un estricto control o seguimiento de la vida de los individuos. Este fenómeno surgió en los países más desarrollados econòmicamente y está en proceso de extensión a todas las sociedades en proceso de informatización.

Es importante resaltar que la vulnerabilidad que presentan estos datos no es "per se", sino es el destino o uso que tengan, del que depende que se afecte o no intereses particulares. La variedad de supuestos de indefensión frente a la aplicación de los datos referidos puede provocar que las personas estén a merced de afectaciones como son la discriminación, manipulación, persecucion, chantaje, presión, asedio, entre muchos, y que pueden estar fuera de un control legal adecuado. (5)

5.- Ibid. Pp. 71-72.

La misma discusión, pero con respecto a organizaciones, se ha presentado en los países con mayor desarrollo. El derecho a la privacidad es reclamado por dependencias y entidades públicas, así como centros de educación, investigación o empresas privadas, con objeto de mantener secreto o confidencialidad de ciertas informaciones que les conciernen y que son de carácter interno para sus actividades.(6)

6.- La discusión sobre la privacidad, en general, se ha enfocado más hacia el lado de las personas, en el cual ha existido desarrollo importante en normatividad y políticas, a nivel internacional, como se mencionará al tratar más profundamente esta problemática, en el capítulo 4, y los aspectos jurídicos de la informática y su seguridad en México, en el capítulo 8. En el lado de la privacidad de las instituciones, el problema se presenta menos crítico: sus informaciones fluyen por canales predeterminados y establecidos en las estructuras propias y en las relaciones con otras organizaciones.

CAPITULO 2.- ADMINISTRACION PUBLICA, EL ADMINISTRADOR Y LA INFORMATICA

2.1 - LA ADMINISTRACION PUBLICA EN PROCESO DE MODERNIZACION.

El gobierno y la sociedad, por definición, conviven, se interpenetran y tienden a plasmar el uno en la otra sus caracteristicas más propias y profundas. En las relaciones entre aparato público y ciudadanía subyacen rasgos socioculturales o idiosicràticos, históricos y espirituales, que constituyen esencia de una sociedad o de una nación. Con base en ello, Caso afirma que "los problemas del cambio social se reflejan en los organismos públicos y éstos, si tienen suficiente flexibilidad y capacidad de adaptación, no solamente pueden acelerar los cambios, sino incluso promoverlos y dirigirlos"(1). En contraparte, si las instituciones pùblicas son rigidas y fallan en adaptarse a la realidad del país, se convierten en agentes de entorpecimiento del desarrollo. El rol del poder ejecutivo es, entonces, determinante del cambio social. Una administración mala o inadecuada o no evolucionada a la situación de la sociedad que dirige, obstruye o es limitante de transformaciones hacia el progreso. En otras palabras, se constituye lastre social, en merma de su propia viabilidad, supervivencia y legitimidad.

La Administración Pública mexicana está en proceso permanente de modernización y búsqueda de mayor racionalidad

---

1.- Caso Lombardo, Andrés: "Administración pública y desarrollo", en Revista de administración pública (México), febrero 1983. Pp.284. (Antología 1 - 54).

en el ejercicio de sus recursos.(2) Busca mejorar esquemas de organización y funcionamiento internos, así como su eficiencia en la administración de la economía, la sociedad y el desarrollo nacional. Está promoviendo, en suma, una reforma y modernización administrativa. Se busca la adecuación de las instituciones al desarrollo de una sociedad que evoluciona, ya sea por dinámica propia o por influencia del mundo exterior. Para un gobierno, Caso refiere que se trata de un problema de estrategia, que implica saber qué se desea hacer, cómo, cuándo y dónde y, todo ello, en armonía con los intereses de los individuos o grupos involucrados.(3) La reforma administrativa busca mejores niveles de eficiencia y eficacia en las tareas públicas, con base en objetivos y metas previa y claramente definidos, apoyados en los fines gubernamentales y en el marco jurídico aplicable.(4) En México, esta reforma se ha encauzado, basicamente, hacia los siguientes aspectos.

2.- Para este trabajo, el concepto de racionalidad se fundamenta en las ideas de Herbert Simon. Atañe a un tipo de comportamiento o categoría de acción, que permite que las decisiones o acciones que se llevan a cabo, en una organización, permitan alcanzar ciertas metas o valores propuestos. La racionalidad no puede ser perfecta. Tiene límites. V. infra. Sección siguiente. V. Glosario: racionalidad.

3.- Adaptado de los argumentos de Caso. Ibid.

4.- La modernización o reforma administrativa es, en sus bases, un problema de cambio. No se trata de un cambio espectacular, sino, precisamente, de promover que los recursos públicos --incluyendo equipos, instalaciones y, ante todo personas--, se empleen con base en programas y objetivos predefinidos y acordes a los fines de la institución. Ibid.

1.- Responsabilizar instituciones y funcionarios de ejecutar con eficiencia y eficacia las acciones públicas que les competen, por medio de una aplicaciòn racional de recursos, basada en procesos de planeaciòn adecuados.

2.- Simplificar, agilizar y descentralizar mecanismos operativos o trámites.

3.- Promover que el servidor pùblico cuente con las habilidades que su puesto requiere, mediante aplicaciòn de programas adecuados de selecciòn, induccièn al puesto, capacitación en servicio, motivación y, en general, de fomentar actitudes y aptitudes de servicio, innovaciòn, responsabilidad y compromiso con las instituciones.(5)

El desarrollo administrativo y su propia reforma, se logran mediante la interacciòn de tres elementos, que destaca Wilburg Jimenez Castro.

1.- Las actitudes y aptitudes humanas.

2.- Los métodos y procedimientos administrativos.

3.- Las estructuras institucionales.

Estos tres, armonizados y dinamizados hacia el desarrollo, permiten el progreso. Están intimamente relacionados con factores educativos, sociales, culturales, econòmicos y morales del hombre, entre otros, y determinan la calidad de vida de cada país y su evolución.(6) El primero de los tres

5.- Ideas tomadas de García Cárdenas, Luis: "Las innovaciones administrativas en el sector pùblico mexicano y su importancia en el campo", en Revista de Administraciòn Pública (México), feb. 1983. Pp. 156-157. (Antologia 1-54)

6.- Jimenez Castro, Wilburg: Administración pública para el desarrollo integral.— México: Fondo de Cultura Econòmica, 1973. 1971. Pp. 14. Los tres elementos los reconoce como

elementos, se refiere a la calidad de los recursos humanos con que se cuenta. Jimenez Castro define la aptitud como potencia y la actitud como acto.(/) La aptitud es efecto directo de la educación, ya sea escolaridad, capacitación o experiencia y constituye el herramental técnico y propensión del personal a desempeñar con eficacia sus funciones. La actitud es un elemento más subjetivo. Se desenvuelve en el espíritu de compromiso, honestidad y servicio del trabajador público. Para el mismo Jimenez Castro, el funcionamiento eficiente de cualquier institución depende, en último término, de la calidad de los seres que la integran.

El segundo elemento, los métodos y procedimientos corresponden a los modos institucionalizados de llevar a la práctica los objetivos de la organización. El método es el camino para llegar al fin propuesto. Los procedimientos son cada uno de los pasos que se ordenan en secuencia dentro del camino trazado.

El tercer elemento se refiere a las estructuras institucionales, es decir, a los modos en que está organizada y jerarquizada la dependencia o entidad. Ello incluye la definición de canales para ejercicio del mando y flujos de información. Se establecen las vías más adecuadas para que el desempeño de las organizaciones sea con apego

---

integrantes de la administración púlica para el desarrollo integral y los reitera a todo lo largo de su obra. (texto a insertar después) competencia misma del Estado asumir el cumplimiento de los objetivos del País y elegir los medios de llegar a ellos, estimulando, al mismo tiempo, todas las fuerzas agrupadas para ello.

/.- Jimenez Castro, op. cit. P. 109.

estricto a los fines institucionales y a la normatividad aplicable.

Los tres elementos, propuestos por Jimenez Castro, deben dinamizarse hacia el desarrollo de la politica, la economia y la sociedad, y asi responder y ser funcionales al desarrollo nacional.

La modernización administrativa implica trabajo conjunto de servidores públicos responsables de toma de decisiones con especialistas técnicos en cada una de las materias que se abordarán y con servidores encargados de llevar a la práctica las decisiones tomadas. Esto tiene como fin promordial que las decisiones, planes o programas desarrollados sean racionales hacia los objetivos planteados y se eviten cambios o innovaciones ideales que los tornen imprácticos u obsoletos. A este respecto, Caso Lombardo afirma que las decisiones deberán ser "tecnicamente viables y politicamente realizables"(8). Asimismo, la realización de una decisión y su viabilidad dependen de los recursos con que se disponga. En un ambiente de desarrollo administrativo se debe buscar el mejor aprovechamiento de los recursos existentes, de tal manera que su empleo se adecúe dinámicamente a mejorar su rendimiento a través de incrementar productividad.

En México, a raíz del crecimiento en el tamaño del aparato público y de una mayor cobertura de funciones sobre

8.- Caso Lombardo, op. cit. P. 284. Esta afirmación es idealista si se confronta con los límites de la racionalidad expuestos en el siguiente apartado del trabajo.

la economía y la sociedad, se hizo necesario buscar medios para adecuar la administración a nuevas realidades. Los esquemas tradicionales de organización y los métodos y procedimientos se vieron cada vez más rebasados por la problemática y dinámica que se daba en las instituciones públicas y en la sociedad misma. El Estado mexicano creció en gran medida y tuvo que enfrentar problemas de irracionalidad administrativa, ineficiencia y obsolescencia en sus esquemas de funcionamiento. (9)

Entre los elementos que han dinamizado la modernización administrativa, destaca uno de los actores más característicos de las sociedades contemporáneas: la informática y la revolución consecuente, en el tratamiento, generación y disposición de información. Las nuevas tecnologías para el proceso de datos son adoptadas crecientemente en las dependencias y entidades de nuestro país. Su enorme capacidad de manejo de grandes volúmenes de información, a velocidades antes insospechadas, abre

9.- Acerca del crecimiento del aparato estatal mexicano y problemas de irracionalidad administrativa v. Gil Villegas, Francisco: "la crisis de legitimidad en la última etapa del sexenio de López Portillo", en Foro Internacional (México) No.98 , octubre-diciembre 1984. En la teoría en torno al Estado capitalista contemporáneo, se presentan elementos conceptuales aplicables a la evolución reciente del Estado mexicano y permiten visualizar su crecimiento e ineficiencia en concordancia con los fenómenos de las sociedades capitalistas modernas. V. Wolfe, Alan: "Los límites de la legitimidad.-- México: Siglo XXI, 1980. Claus Offe introduce el concepto de "ingobernabilidad" de la sociedad contemporánea, debido a la desadaptación del Estado a la dinámica de evolución de la sociedad. V. Offe, Claus: "Ingobernabilidad: el renacimiento de las teorías conservadoras", en Revista Mexicana de Sociología, (México), No. 81, 1981.

perspectivas hacia un mejor desempeño de las gestiones públicas. El complemento esencial, para este mejor desempeño, es la aplicación de políticas adecuadas de desarrollo, utilización y control de la aplicación de estas tecnologías.

En general, la informática ha otorgado apoyo definitivo a la toma de decisiones públicas y, de ese modo, se integra en la tarea más esencial de los administradores públicos: precisamente, la toma de decisiones.

El creciente rol, que el elemento informático ha jugado en la gestión pública, lo ha convertido en recurso crítico para el funcionamiento de las instituciones gubernamentales. De manera casi simultánea a la aparición de la informática, nació la administración de centros de cómputo y la administración de los servicios que le son relativos. Se pretendió, con ello, racionalizar la adquisición y uso de tiempo, equipos y dispositivos computacionales.

La informatización creciente del gobierno y la sociedad han demandado mayor calidad en la administración computacional. Como una especialización de ella y, con base en los problemas y vulnerabilidad que conllevan las tecnologías de procesamiento electrónico de datos, se ha propuesto un nuevo terreno de estudio y consideración: la administración de la seguridad informática. Ello significa integrar conocimientos que soporten 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 asi un nuevo terreno de toma de decisiones racional y ordenada, que deberà atender el administrador público.

2.2.- EL ADMINISTRADOR PUBLICO Y LA TOMA DE DECISIONES.

En la década de los 50, Herbert Simon publicó su obra "The administrative behavior", en la que define la toma de decisiones como el corazón de la administración.(10) Fue obra pionera en su género. Estructura y analiza los diversos elementos que intervienen en la toma de decisiones racional, de modo que de ésta se deriven efectos óptimos, que coadyuven a que las instituciones logren los fines que se proponen. Habla de la administración como el arte de asegurar que las cosas se hagan. (11) Y 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, el cual consiste en segregar ciertos elementos decisorios entre los miembros de la organización. Se establecen métodos y procedimientos regulares para seleccionar y determinar esos elementos y comunicarlos a las personas implicadas.(12) Define la toma de decisiones como el esfuerzo de estrechar las diversas alternativas de acción a una que, de hecho, se llevará a cabo, y ello con base en principios o requerimientos

10.- Simon, Herbert A:"El comportamiento administrativo: un estudio de los procesos decisorios en la organización administrativa".-- Madrid: Aguilar, 1962. P. xviii.
11.- Ibid. P. 1
12.- Ibid. P. 8

derivados del propósito y objetivos generales de la institución.(13)

En la determinación del perfil del tomador de decisiones, en un contexto organizativo, es interesante la visión de Herbert Simon, en la que confronta al llamado "hombre economico" y "hombre administrativo" --o social. El primero se deriva de la teoria económica y supone un comportamiento apegado al mundo real, a los hechos y a los números. Dispone de un sistema completo y consistente de preferencias, que le permiten elegir entre alternativas expresadas de la manera más cuantitativa posible. Según este modelo, el hombre económico "optimiza" con sus decisiones. Simon afirma que esto tiene escasa relación con el comportamiento real o posible de los seres humanos.(14) Asimismo, sostiene que el comportamiento del administrador como hombre económico, no es tan racional como lo dice la teoria económica. El desempeño real se desvia de esta teoria y el papel del medio organizativo -- incluyendo los aspectos psicológicos del hombre --, juega un papel importante.

Como alternativa, Simon presenta al "hombre administrativo". Lo define como aquel que toma decisiones en consideración de aspectos humanos, psicológicos y sociales. Percibe un modelo simplificado de la "confusión" que constituye el mundo real y sòlo considera factores que, a su juicio, son los màs notables o importantes, para

---

13.- Ibid. P. 3.
14.- Ibid. Pp. xxi y xxii.

enfrentar una situación dada. La decisión busca ser aplicable en el contexto organizativo y ser aceptada por el personal. Al intervenir el elemento humano, y otras limitaciones del medio ambiente, las soluciones ya no son óptimas, sino "satisfactorias". (15)

En toda organización tienen lugar decisiones con mayor o menor grado de especialización e importancia. Simon afirma que así como la división del trabajo horizontal permite mayor nivel de pericia en el desempeño de tareas operativas, es absolutamente esencial la división del trabajo vertical, entre los niveles operativos, supervisorios y directivos, para llevar a cabo los procesos decisorios institucionales. Reconoce que el administrador —-ejecutivo o gerente-— es un decididor.(16) Tiene ante sí cuatro procesos para decidir. 1) Investigar ambientes para hallar las condiciones que exigen una decisión. 2) Diseño, es decir, invención o desarrollo y análisis de posibles cursos de acción. 3) Elección o selección de un curso determinado para actuar, a partir de cursos de los cuales se dispone. 4) Evaluación o revisión de la elección tomada y conocimiento sobre el logro de resultados. (17)

En un proceso de modernización administrativa, el papel del administrador público, como profesional en la toma de decisiones gubernamentales es cada vez más crítico. En

---

15.- Ibid. Pp. xxiii y xxiv.
16.- Simon, Herbert A.:"La nueva ciencia de la decisión gerencial".-- México: Librería "El Ateneo" Editorial, 1982. P. 36.
17.- Ibid. P. 37.

tiempos recientes, el cambio social ha sido cada vez más rápido. Es precisamente este profesional el arquitecto del desarrollo administrativo. Como tomador de decisiones, debe integrar en su conocimiento muchas disciplinas. Como dice Octavio Rodriguez Araujo,"... el saber histórico le es indispensable como la sociologia, la politica y la economia. Le es imprescindible conocer técnicas referentes a la planeación, a la programación y al uso óptimo de los recursos, de todo tipo, que integran la acción pública" (18). Más adelante dice,

"debe ser capaz de estudiar las estructuras de la Administración Pública, así como las funciones de cada una de ellas, en términos de su idoneidad con los ojetivos y las metas del régimen politico en cada momento... A través del estudio, análisis y desarrollo de técnicas administrativas, coadyuvará en que se haga posible la acción gubernamental en la sociedad "(19).

El trabajo práctico de este profesional se desenvuelve entre las siguientes modalidades.

1.- Como asesor o proporcionador de elementos de apoyo a la toma de decisiones. Ello supone capacidad de anticiparse a los acontecimientos sociales. En consecuencia, elabora planes o diseña estructuras y provee elementos para su correcta evaluación.

2.- Como investigador administrativo. Estudia la composición y funcionamiento de la Administración Pública, en busca de congruencia con su misión social. En este

---

18.- Rodriguez Araujo, Octavio: "El perfil profesional del administrador público", en Revista de Administración Pública (México), Febrero 1983. (Antología 1-54). P. 503.
19.- Ibid.

aspecto, analiza el rendimiento del personal público y prepara mecanismos de formación, especialización y actualización para mejorar su ejercicio profesional. A su vez, estudia las técnicas para mejor aplicación de recursos materiales, financieros y tecnológicos.

3.- Como directivo, tomador de decisiones en los organismos públicos. Debe procurar que la institución o un sector de la que dirige, opere de manera eficaz. Elabora planes y programas de trabajo. Lleva control de gestión de la unidad administrativa bajo su responsabilidad. Inclusive, prevee las decisiones subordinadas, que se fundamentan en las suyas propias.(20) Le compete, asimismo, efectuar un manejo racional de los recursos para obtención de resultados en al calidad, tiempo y cantidad requeridos.(21)

El administrador público tiene como rol fundamental, en suma, la toma de decisiones racional, que permita instrumentar acciones hacia el cumplimiento de los fines de las organizaciones y a la satisfacción de las demandas y necesidades de la sociedad.

En la organización, el comportamiento de los individuos está orientado hacia metas u objetivos. Estos traen, como consecuencia, la integración de modelos de comportamiento hacia los fines deseados. La finalidad se constituye en primer criterio para determinar cúales son las cosas que hay que hacer. La decision comprende la selección

20.- Cf. Simon, Ibid. P.41.
21.- Las tres funciones del administrador público, se tomaron y adaptaron de Rodriguez Araujo. Ibid. P. 505.

de una meta y un comportamiento relacionado con la misma. Simon sostiene que en la selección de la meta intervienen 1.- proposiciones "éticas", que también llama "juicios de valor" y 2.- proposiciones fácticas o "juicios de hecho".(22) Las proposiciones éticas se refieren a la determinación de objetivos, metas, políticas y normas de la organización, es decir, a las decisiones institucionales y legales, que son común denominador en el desempeño de todo miembro o servidor. Equivale a la determinación de deberes o funciones imperativas en la organización , --es decir proposiciones que implican un alto contenido ético, por lo que no es posible afirmar su verdad o falsedad.

La determinación de los "juicios de valor" es tarea de la alta dirección institucional. Se toman en cuenta los aspectos institucionales, como son objetivos, fines, base legal, normatividad interna, políticas, idearios de trabajo y otros valores. Para que la proposición ética sea útil en la decisión racional, según Simon, 1) los valores u objetivos de la organización deben ser definidos de tal manera que se pueda determinar su grado de realización en cualquier momento y 2) debe ser posible evaluar las acciones que hacen realizables los objetivos.

Las proposiciones fácticas, o "juicios de hecho", son afirmaciones acerca de aspectos visibles u operativos.

22.- En una nota de pie de página, Simon clarifica estos dos tipos de juicios. Llama juicio de valor al que se refiere al "debe" y, juicio de hecho al aludir los "es". Simon. ibid. P. 6.

Requieren información, como materia prima esencial, y son efectuados en todos los niveles organizacionales. El empleado operativo, así como el directivo medio, efectúan "juicios de hecho", con base en los conocimientos o capacitación, que los forman hacia aptitudes y actitudes ventajosas para la organización. Asimismo, reciben información que delimita, norma y da bases a sus procesos decisorios subordinados.(23)

Las proposiciones fácticas, en algunas ocasiones, pueden ponerse a prueba para determinar si son verdaderas o falsas. En otras, es necesario elegir continuamente premisas cuya verdad o falsedad no se conoce definitivamente ni puede determinarse con certidumbre, ante la información y tiempo que se disponen. De los "juicios de hecho" se deriva la definición de métodos, procedimientos o tareas para alcanzar los fines. En ello, se busca descubrir qué factores son importantes y qué factores no lo son, para efectuar una correcta elección, ante una situación dada y se basa en el conocimiento empírico del comportamiento de diversas alternativas de acción. La elección racional será factible en la medida que la serie limitada de factores en que se

---

23.- Simon, ibid. P.53. La distinción entre "juicios de hecho" y "juicios de valor" tiene relación con la distinción tradicional entre política y administración. Política suele ser entendida como decisión. Administración, como acción. No obstante, en la realidad la frontera no es clara. La acción también implica elementos decisorios. A primera vista, la administración implica decisiones que no que no requieren control exterior porque poseen un criterio interno de corrección. V. Simon, ibid., p.44.

basa la decisión, corresponda a un sistema cerrado de variables.(24)

Con base en los dos tipos de proposiciones o juicios anteriores, las decisiones no pueden ser valoradas como correctas o incorrectas, sino unicamente su relación, de hecho, con los fines que se persiguen. (25) Lo fáctico se valida por su conformidad con los hechos. Lo ético, por principio de autoridad. Una decisión es más que una relación de hechos. Describe un estado futuro de cosas, que se selecciona con preferencia sobre otros y el comportamiento se dirige hacia la alternativa elegida. (26)

Simon, adicionalmente, presenta un esquema de clasificaciòin de las decisiones organizacionales: las programadas y las no programadas. Las primeras son aquellas que enfrentan problemas frecuentes, repetitivos y se abordan con procesos rutinarios. Se trata de decisiones rutinarias que se canalizan a través de una secuencia de respuestas claramente estructurada dentro de la organización y que cuentan con canales de información bién definidos. Para ellas, se desarrollan estàndares de operación, con base en los objetivos, politicas, normas y estructura institucional. Por su parte, las decisiones no programadas son novedosas, no estructuradas o muy importantes. Su atención exige el

---

24.- Simon, ibid. P. 79.
25.- Simon: "El comportamiento...". P. 45.
26.- Simon, ibid. P. 55. V. Discusión acerca de los limites para la separación real entre las proposiciones fácticas y éticas. Simon, ibid., Pp. 56 y 57.

criterio del administrador, su experiencia, motivación y perspicacia. Para ellas no se cuenta con una colección de reglas en secuencia. (27) En general, las instituciones buscan que las actividades programadas tiendan a desplazar las no programadas. A medida que se toman previsiones para enfrentar las segundas, se delimitan responsabilidades especificas, en la organización y sus unidades administrativas y se van convirtiendo en programadas. (28)

Es factible, como ejercicio lógico, trasponer las dos clasificaciones de decisión a un contexto organizacional (1.- juicios de valor y juicios de hecho y 2.- decisiones programadas y decisiones no programadas). La organización puede comprenderse como estructura de tres cuerpos superpuestos. En el inferior operan, basicamente, las decisiones programadas y juicios de hecho. El superior toma decisiones no programadas y juicios de valor, que consisten, entre otros aspectos, en procesos para diseñar o rediseñar todo el sistema, suministrarle metas, objetivos y evaluar su desempeño. El nivel intermedio se ocupará de tareas supervisorias, fundamentalmente, en las que tiene ante si la elaboración de juicios de hecho, de decisiones programadas

---

27.- Simon: "La nueva ciencia...". P. 45. Y Simon:"El comportamiento...". Pp. 43 a 47.

28.- Simon reconoce la investigación de operaciones como instrumento moderno que permiten llevar las decisiones no programadas a ser programadas. Simon:" La nueva ciencia...". Pp.77,79 y ss. V. También, Simon: "El comportamiento...". P. 85.

y, ocasionalmente, no programadas que se subordinan a lineamientos emitidos por el nivel superior.(29)

La eficiencia que alcanza una organización administrativa es correspondiente al nivel de eficiencia alcanzado por las decisiones y acciones de los miembros que la componen, en todos los niveles de mando o responsabilidad.

John Forrester, con base en supuestos de Simon y otros, indica que para una toma de decisiones ideal se requiere que el problema esté bien definido, se cuente con un conjunto completo de alternativas para considerar, completa información de apoyo --inclusive acerca de los valores y preferencias de los afectados--, tiempo suficiente para tomar la decisión, recursos y capacitación en el decisor.(30)

Lo real, es que la toma de decisiones cuenta con éstos de manera fragmentaria o imperfecta y se aleja de este "idealismo racional". Los trabajos de Simon ven al tomador de desiciones como un "racionalista limitado", que busca soluciones satisfactorias, no óptimas, en los contextos organizativos. Según él mismo, la capacidad de la mente humana para formular y resolver problemas complejos es muy

---

29.- Basado en Simon: "La nueva ciencia...". P. 123.
30.- Forrester, John: "Bounded racionality and the politics of muddling through", en Public Administration Review (E.U.A.), vol. 44, num. 1. P. 25.

pequeña, en comparación con la magnitud de los problemas cuya solución se requiere. (31)

El individuo, como tomador de decisiones, está limitado en los siguientes aspectos.

1) Se limita por su destreza manual, tiempo de reacción y fuerza.

2) Por otro lado, se limita por la extensión de su conocimiento de las cosas relacionadas con su tarea. Inciden aquí cuestiones como cantidad de información que la mente puede retener y aplicar, rapidez de asimilación, cómo se comunica la información hacia los centros decisorios, etc. (32)

3) Se limita por sus valores y por los conceptos de finalidad que influyen en él al tomar decisiones --las proposiciones éticas que debe considerar. (33)

Forrester profundiza las limitaciones que reviste el proceso decisorio y las conceptualiza como límites a la racionalidad. Presenta cinco niveles de limitaciónes.

1o. Los límites debidos a un conocimiento imperfecto o insuficiente. (34)

31.- Holsti, Ole R.: "Modelos de relaciones internacionales y politica exterior", en Foro Internacional. (México), vol. xxix, num. 4 (abril-junio de 1989). P. 548.
32.- Simon:"El comportamiento...". P. 40.
33.- Simon, ibid, p. 39.
34.- Simon afirma que es imposible que el comportamiento de un individuo solo y aislado alcance un grado alto de racionalidad. Es tan grande el número de alternativas que necesita explorar y tan escasa la información que tendría que valorar, que resulta difícil concebir, siquiera una aproximación a la realidad objetiva.

2o. Los limites debidos a la diferenciación social. En este nivel, las decisiones implican la intervenciòn de muchas personas, en diversas unidades administrativas. La información ya no sólo es imperfecta, sino que tiene calidades distintas, està en lugares distintos y menos accesibles de manera directa.

3o. Limites por conflictos pluralistas, que se presentan cuando hay confrontaciòn, oposición, resistencia, intransigencia, entre los diversos actores. Intervienen lealtades, intereses creados o alianzas. La toma de decisiones se haca màs compleja. La información se conviente en recurso politico y puede estar distorsionada o ser objeto de manipulaciones.

4o. Distorsiones estructurales. Éstas se basan en que la sociedad està estructurada en redes sociales y económicas. La ciudadania no està atomizada, sino organizada, en grupos de distinta finalidad, nivel de recursos y facilidades. No se puede satisfacer las demandas de todos en la misma proporción y calidad. (35)

La toma de decisiones se hace màs compleja. hay actores jugando diversos roles en una estructura de poder, problemas ambiguos, diferentes ideologias, tiempos limitados para diseño de decisiones y, a su vez, informaciòn insuficiente y, posiblemente, contaminada o inaccesible.

35.- Forrester, op. cit. A lo largo del articulo expone los cuatro niveles de limitaciones a la racionalidad.

Las soluciones prácticas dependen de las peculiaridades de cada contexto, que definen un problema dado. Ser práctico implica responder a demandas dadas en una situación, con todas sus inestabilidades. Como afirma Forrester, los administradores hacen lo que pueden. Buscan satisfacer, no optimizar o maximizar.(36) Los contextos para las decisiones son dificilmente dados de forma clara y diferenciada. Para enfrentar eso, el rol de la teoria administrativa no será predecir --¿ qué pasaría si...?--, sino dirigir al tomador de decisiones ante qué variables significativas o importantes, actores, eventos y señales, deberá alertarse.

2.3.- LA INFORMATICA EN LA ADMINISTRACION PUBLICA.

La incorporación de nuevas tecnologías para el procesamiento de datos, en nuestra Administración Pública, se ha desarrollado de manera desordenada, más que como respuesta a un proceso planeado y sistematicamente fundamentado. Los equipos de cómputo parecen haber entrado en servicio en las dependencias públicas en momentos en que todavia no existia personal público que evaluara acertadamente la viabilidad de las inversiones, cotejadas con necesidades y posibilidades reales de automatización de procesos de datos. Menos, aún, se estaba preparado para la operación adecuada de los equipos, para la programación dirigida a desarrollar aplicaciones óptimas que satisfacieran necesidades concretas de automatización. Una de las causas más directas de ello ha sido la falta de

---

36.- Forrester, op. cit. P. 29.

conocimientos o de preparación técnica de los administradores o tomadores de decisiones. El proceso de introduccion de los computadores en las agencias públicas ha partido de suposiciones erróneas acerca de los alcances, limitaciones y caracteristicas de estas nuevas tecnologias.

Se trata de una situación no distinta de la que ha tenido lugar en otros paises. 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." Él mismo reconoce que "Muchos errores y decepciones se hubieran evitado si no se hubiera partido de suposiciones falsas generalmente implícitas al desarrollar el diseño."(37) Aún más, se puede añadir que en realidad se trata, en el fondo, de un problema ampliamente abordado en tiempos modernos. Como se refirió en la introducción de este trabajo, citando a Nora y Minc, se argumenta que la utilización de nuevas tecnologias da lugar a problemáticas personales, sociales, organizacionales o nacionales, por los conflictos que se generan entre los valores y costumbres tradicionales y los requerimientos o implicaciones de la modernidad. Ackoff Russell retoma para diversas obras la tesis central de los trabajos de Alvin Toffler, a saber, la impericia de la sociedad para adaptarse a la "...razón creciente de cambio -- no a su contenido o

---

37.- Ackoff, Russell: "Planificación de la empresa del futuro".-- México: Editorial Limusa, 1983. P. 172.

dirección." La reconoce como uno de los problemas más críticos de nuestro tiempo.(38) Y es argumento en la hipótesis central de esta tesis.(39)

Esta desadaptación ante los cambios, tiene lugar en el terreno de la informática desde que ésta aparece en México. La entrada de las nuevas tecnologías de tratamiento de datos, para captura, proceso, generación y reproducción de información, ha sido sumamente rápida, en busca de eficientar la gestión pública y responder mejor ante las demandas sociales. Sin embargo, los cambios tecnológicos trajeron consigo alteraciones en líneas y residencia de poder, en los métodos y procedimientos de trabajo, en el desempeño de los servidores públicos y en otros múltiples aspectos, como se reflejará en el capitulo 7. La respuesta hacia esta problemática ha sido menos rápida que la misma adquisición de equipos y la extensión de sus aplicaciones. Ahora, el elemento informàtico participa como actor fundamental en la operación y viabilidad de los organismos gubernamentales. Es a la vez antídoto ante problemas administrativos, como efecto o causa de disfuncionalidades en administraciones que se desempeñan bajo esquemas tradicionales o inadecuados de trabajo y organización. En todos los casos, la incorporación y aprovechamiento de los recursos informáticos se ha insertado en ambientes organizacionales no adecuados a los cambios que conlleva el

38.- Ackoff, Russell: "Rediseñando el futuro".-- México: Editorial Limusa, 1983. P. 5
39.- V. Introducción.

utilizar nuevas tecnologías para manejo de información. Y esta última es, tal vez, el componente más importante de toda institucionalidad, es decir de la continuidad, permanencia o viabilidad de las organizaciones. (40) Por ilustrar estas afirmaciones, basta mencionar que las unidades de informática de los organismos se han convertido en puntos críticos de líneas de poder y responsabilidad debido a las enormes concentraciones y disponibilidad de información que implican. El reconocimiento formal de ello ha sido escaso y es frecuente que estas unidades se establezcan en niveles jerárquico-organizacionales inferiores.

Con el paso del tiempo se ha avanzado en ejercer con mayor racionalidad en los recursos destinados a la computación y obtener los mayores beneficios para los usuarios. El personal de mando en las unidades de informática de las diversas dependencias y entidades reconoce que el desarrollo computacional está todavía en etapa inicial. La adquisición de equipos y programas y el desarrollo de aplicaciones específicas, idóneas para cada institución, son aspectos que aún no han logrado optimizarse, pero se trabaja continuamente en ello. Estamos

---

40.- Sobre la relación que existe entre la información y las instituciones y la propia institucionalidad, v. Ampudia, Mello, Jose Enrique: "Institucionalidad y gobierno: un ensayo sobre la dimensión archivística de la Administración Pública".-- México: AGN-INAP, 1988. P. 46 y sr.

en un proceso, todavía inconcluso, de incorporación de los recursos informáticos en nuestro gobierno. (41)

En el seno 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 los cada vez más escasos recursos"(42). Asimismo, tiene como atribución de promover el desarrollo informático nacional. Esta última ha sido la menos abordada en la gestión del INEGI. De hecho, las acciones que ha realizado se han dirigido, en lo fundamental, 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 procupación 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

41.- Esta afirmación se sustentará en el capítulo 7, que aborda la problemática en torno a la computación y su seguridad en la Administración Pública Federal.
42.- Tomado de México, Secretaría de Programación y Presupuesto: "Guía para la elaboración de programas de desarrollo informático".-- Talleres Gráficos de la Nación, 1987. P. 1.

regulación en los organismos públicos. El capitulo 8 abordará con extensión la situación jurídica de la informática y su seguridad en México.

El terreno propio de la seguridad está aùn menos trabajado y los problemas relacionados con ella han crecido tan rápido como la extensión de equipos y aplicaciones en las agenciae públicas. Se puede afirmar que es difícil, hoy por hoy, encontrar unidades administrativas que no se auxilien de dispositivos computacionales para sus operaciones.

La informática se presenta, cada vez más, como objeto de administración, es decir, exige imperiosamente que se le aborde con la extensiòn e intensidad que su papel en la administración pública implica. Se convierte en materia de una racional toma de decisiones, de la que se consideren requerimientos de automatización; alternativas de solución; programas de trabajo para investigación, desarrollo y operación de los sistemas; impacto organizacional; impacto en el desempeño del personal; revisión de condiciones generales de trabajo; seguridad y auditoría a las aplicaciones computacionales, entre muchas. En otras palabras, sostenemos que se hace fundamental ejercer una adecuada administración sobre la computación y, con ello, la participación del administrador público en la toma de decisiones idóneas, hacia el contexto y el elemento informático, cada véz más críticos e indispensables en la función pública. En adición, Ackoff reconoce que es

necesario que los administradores no sòlo sepan cómo utilizar los sistemas de información, sino que conozcan en detalle su funcionamiento con objeto de poder evaluarlos.(43) Lo usual es que los diseñadores de sistemas o los programadores se encarguen de la mayor parte del problema informático y los administradores participen marginalmente en el desarrollo computacional, recibiedo indicaciones de los primeros y utilizando sistemas de información sin estar planemante seguros de su funcionamiento correcto. De ese modo, el tomador de decisiones, se halla incapacitado para controlar y evaluar el sistema de informaciòn, como un todo. Delega esa función al mismo diseñador, que rara vez es un administrador capacitado. Russell Ackoff afirma que un sistema de información no debe ponerse en funcionamiento, a menos que los administradores hayan comprobado su eficacia y su rendimiento hacia los objetivos perseguidos. " Los administradores deben controlar los sistemas de informaciòn, no éstos a los administradores"(44).

El control en la computación tiene muchas facetas. Implica asegurar los sistemas de información, incluyendo sus componentes físicos y lógicos, al menos en los siguientes tres aspectos.

43.- Ackoff, Russell: "Planificaciòn...". P. 179.
44.- Las últimas lineas de este parrafo son adaptadas de los argumentos de Ackoff. V. Ackoff, Russell; ibid. Pp. 180 y 181.

1.- Que su diseño y adquisición se fundamenten en necesidades predefinidas y en objetivos viables.

2.- Que en el desarrollo de aplicaciones se evalúen continuamente los métodos y procedimientos que se siguen. Asimismo, que los programas sean eficaces y eficientes para los fines que se determinaron y no deberan ser puestos en operación, a menos de que se halla probado totalmente su buen funcionamiento.

3.- La operación de los sistemas de información se debe conllevar con programas de evaluación permanente de su correcto uso, funcionamiento, mantenimiento (equipos, accesorios, conexiones, programas y datos) y resguardo de la integridad y confidencialidad de la información.

El control en los sistemas de información electrónica, en general, es requisito para el ejercicio de la seguridad. Un gerente de informática de una importante institución bancaria aseveró que "no se puede lograr la seguridad si no se tiene control sobre el elemento a asegurar" (45). La seguridad informática implica, en consecuencia, que ya se tiene algun nivel de control sobre los sistemas computacionales y los propios datos. En la medida que ocurre esto último, se facilita lo primero. La seguridad, de hecho, interviene en los tres aspectos referidos. Los administradores públicos ya participan, de alguna forma, en la administración informática y, en consecuencia, en el

---

45.- Entrevista del autor, en la Ciudad de México, en abril de 1989.

control. No obstante, el tema de la seguridad es aún poco conocido por ellos. Inclusive, lo es para los mismos analistas de sistemas, y programadores.

La seguridad, así como la administración informática, ha sido escasamente abordada, no sólo en nuestro País, sino en el medio internacional. Como se sostendrá más adelante, los esfuerzos en la investigación computacional se han canalizado más hacia el desarrollo de equipos y aplicaciones más modernas, que hacia la búsqueda de medios de administrar o controlar esos recursos y la información que manejan.

Se hace necesario reforzar la consideración y concepción de la seguridad en los administradores públicos y este estudio se dirige a ello. La actuación de estos profesionales en el terreno de la aplicación y buen uso de nuevas tecnologías será cada día más indispensable.

Se resalta la participación del administrador público como profesional en la toma de decisiones y que tiene frente a sí un aspecto fundamental de la administración moderna: el aseguramiento del resguardo y buen uso de los recursos computacionales, que garanticen la integridad y confidencialidad de la información. Resaltamos la opinión de Wilson respecto a que la mejor manera de llevar a cabo una administración, o la toma de decisiones, es que sea llevada a cabo por administradores de carrera, de los que se requiere una "multi-percepción" de la problemática a abordar. Este concepto es identificado por el mismo autor

como la "Weltanschauung", es decir, visión global, o visión de mundo, que habilita al observador a atribuir significado a lo que está observando.(46) El mismo Simon dice que cuando se presenta un problema al administrador, a menos que le sea de un tipo totalmente familiar, debe, en primer término conocerlo con amplitud, comprenderlo plenamente y encontrar alguna forma de representárselo, antes de poder encarar el trabajo de solución.(47)

En adelante, este estudio busca la dotación de elementos de juicio, al administrador público, para tomar decisiones, concretamente, con respecto a la seguridad informática, en consideración de su contexto. La linea de trabajo que se sigue va desde aspectos generales de la informática, que se tratan en el siguiente capitulo, para avanzar hacia problemas concretos en la administración de su seguridad.

46.- Wilson es discipulo de un famoso investigador en materia de Teoria General de Sistemas, en la Gran Bretaña, Peter Checkland. Las comillas son de Wilson y sus argumentos se extractan de su obra, Wilson, Brian: "Systems: concepts, methodologies and applications.-- U.K.: John Wiley & Sons, 1984. Pp. 29 a 31.

47.- Simon:"La nueva ciencia...". P.41.

CAPITULO 3.- LA INFORMACION COMO RECURSO.

3.1.- HACIA UNA SOCIEDAD DE INFORMACION.

Hace unos treinta años, comenzó una nueva revolución mundial: el tránsito de una sociedad industrial al de una sociedad de la información. Nora y Minc lo definen como la informatización de la sociedad. (1) Para Russell Ackoff es el paso de una "edad industrial" a una "edad de los sistemas".(2) Nussbaum teoriza la nueva sociedad de la información y de las "C & C" (o sea, de las computadoras y comunicaciones) (3). Estos, y otros muchos autores, reconocen la mayor integración o acercamiento de las sociedades y la mayor racionalidad que experimenta su propia dinámica. (4) En la racionalidad subyace un elemento fundamental: la información.(5) Peter Drucker, al respecto

---

1.- V. Nora, Simon y Alain Minc: "La informatización de la sociedad".-- México, D.F,: Fondo de Cultura Económica, 1981.
2.- Ackoff, Russell L.: "Rediseñando el futuro".-- México: Editorial Limusa, 1984. V. Introducción.
3.- Nussbaum, Bruce: "El mundo tras la era del petroleo: los nuevos ejes de poder y riqueza".-- México, D.F.: Editorial Planeta, 1985.
4.- Esta racionalidad, bajo las ideas de Simon, significa el ejercicio de los recursos correctos para maximizar unos valores dados en una situación dada. En el contexto organizacional, un acto es racional si se orienta hacia las finalidades de la propia organización. De Simon, Herbert A.:"El comportamiento administrativo: un estudio de los procesos decisorios en la organización administrativa".-- Madrid: Aguilar, 1962. Pp. 73 y 74.
5.- A este respecto, se puede citar a David Bell, que afirma que en la sociedad agricola el hombre se enfrentaba directamente a la naturaleza. En la sociedad industrial, el hombre se enfrenta a la naturaleza fabricada. En la sociedad de la información, por primera vez en la civilización, el juego es de gente interactuando con otra gente. "Eso hace crecer el número de transacciones personales de una manera geométrica, es decir en todas las formas de comunicación interactiva: en llamadas telefónicas, en cheques expedidos,

de ésta, afirma que "la productividad del conocimiento ya se ha convertido en la clave para el progreso y el logro económico".(6) La informática, en la medida que es más eficiente y rápida, permite disponer mejor información. Los equipos de cómputo, y sus programas, son capaces de captar, procesar y emitir información a grandes velocidades. Así se constituyen como piedra angular en la sociedad y civilización modernas.

En el siglo XX los cambios tecnológicos han producido más riqueza, más consumo, más educación y más comunicación, que en cualquier otro momento de la historia. En otra época, los ferrocarriles unieron puntos geográficos distantes, facilitando nuevos e importantes mercados. Ahora, las computadoras han sido recurso para enormes posibilidades de proceso y disposición de datos, de modo que la información cobra un valor estratégico creciente. El procesamiento más eficiente de los datos permite mejorar de manera importante los atributos de la información en confiabilidad, costo de producirla, actualidad, oportunidad, entre otros, y ello facilita las tareas de toma de decisiones.(7) Asimismo, con intermedio de las telecomunicaciones, para envíos e intercambio de información, las economías y sociedades se integran más y se teje un mercado global.

---

en memos, mensajes, etc.". David Bell, citado por Naisbitt, John: "Macrotendencias".-- México: Edivisión, 1985. P. 29.
6.- Drucker, citado por Naisbitt, op. cit. P. 25.
7.- Para los atributos de la información, ver supra. P.2.

En la década de los 90 será común la operación y programación de computadoras, para el trabajo de las personas, en muchas areas. Maestros, empleados de oficina, secretarias, contadores, administradores, agentes de bolsa, empleados de seguros, banqueros, burócratas; además de muchos tipos de profesionales como abogados, ingenieros, programadores de cómputo, médicos, arquitectos, bibliotecarios, reporteros o cientificos sociales, se cuentan como trabajadores de información y, por lo tanto, de la informática.(8) Todavía hasta mediados de los setenta, la computación era cara y estaba al alcance tan sólo de una élite. Solo un grupo restringido de organizaciones la utilizaban. A partir de la década de los 80, se impone una informática de masas, que invade, cada vez más, todos los sectores sociales. Nora y Minc dicen.

> "Antes sólo existian grandes computadores, hoy hay multitud de maquinitas, potentes y baratas y no están aisladas, sino muchas de ellas unidas entre si en redes". (9)

En paises industrializados, la utilización de computadores está más difundida. En los Estados Unidos, toda empresa cuenta con ellos y por lo menos, para 1990, un 25% de los hogares cuenta con equipos de computación. (10) Este uso creciente ha motivado, a algunos, a llamar la época

---

8.- Esta enumeración de trabajadores de la información, la menciona y amplia Naisbitt, op. cit. Pp. 24 y 25.
9.- Nora y Minc, op. cit. P. 17.
9.- Naisbitt, op. cit. Este autor explica ampliamente la difusión de la computación en los Estados Unidos en su capitulo I y se apoya con muchas cifras.

actual como "era de la computación". En el caso de México, el desarrollo es aún incipiente, no obstante la Administración Pública, las grandes y medianas empresas, asi como instituciones de educación superior, entre muchas, han instalado y aplicado progresivamente los recursos informáticos.

En la "revolución informática" de Nora y Minc,(11) se modifica el sistema nervioso de las organizaciones y, por ello, la sociedad entera que está en evolución hacia la informatización. Aparece un nuevo escenario.(12) La computación es liberadora de enormes cargas de trabajo manual e intelectual para los individuos y está permitiendo eficiencia y productividad, como nunca antes en la historia.(13) En el pasado, la velocidad del progreso llegaba hasta donde la capacidad manual y mental del hombre lo permitia. Ahora esa velocidad llega hasta donde los cerebros electrónicos lo permiten. No es la computación la única innovación tecnológica de los últimos años, pero si ha permitido y acelerado las demás.

11.- Nora y Minc, op. cit. P. 17. Los autores llaman "revolución informática" a la incorporación de las nuevas tecnologias en el manejo de la información.
12.- Nora Minc, op. cit. P. 14.
13.- Este punto de vista se basa en el de Tellez, Julio: "Derecho Informático".-- México: Universidad Nacional Autónoma de México, 1987. P. 19.

3.2.- LA INFORMACION, SEGUN LA TEORIA GENERAL DE SISTEMAS.

Un enfoque menos usual de conceptualizar los cambios contemporáneos, es el que sostienen autores como Russell Ackoff y Ludwig von Bertalanffy: la revolución de los "sistemas". El elemento esencial es la noción misma de "sistema". Se pretende ver el mundo como una organización. (14) Es una tendencia señalada con el surgimiento de disciplinas como la cibernética, la teoría de la información, la teoría general de sistemas. Y con aplicaciones prácticas, el análisis de sistemas, la investigación de operaciones y la ingeniería de sistemas. Estas tienen características distintas, --- en sus bases, metas y las técnicas --, pero coinciden en ocuparse, de una u otra forma, del estudio de "sistemas totalizadores" y "organización", que dejan entrever el nuevo enfoque.(15) En este contexto, se han desarrollado corrientes de racionalización organizacional para solución de problemáticas de diverso tipo y en busca de mejor comprensión y predicción.

En el campo de ciencias sociales, la teoría sociológica consiste, en gran medida, en intentos de definir sistemas socioculturales y en entender los fenómenos sociales con respecto a un "todo" que los comprende. Ese "todo" es el

---

14.- Bertalanffy, Ludwig von: "Teoría general de los sistemas".-- México: Fondo de Cultura Económica, 1982. P. 146.

15.- Ibid. P. 197. Para un conocimiento a manera de esquema de los avances en la Teoría General de Sistemas, ver pp. 93 y 94, del mismo.

sistema sociocultural, "causal-lògico-significativo, en niveles biológico, simbólico y de valor", como explica Bertalanffy.(16) El trabajo de autores como Parsons y Merton, se inscribe en los desarrollos en este campo.

Claude Shannon y Weaver, en 1949, se constituyeron padres de la "Teoría de la Información". Ésta se basa en conceptualizar la informaciòn como expresión "isomorfa con la teoria de la entropía negativa de la termodinámica".(17) La entropía es una medida de desorden y atañe a la probabilidad de ocurrencia de un arreglo molecular de las partículas de gas. Traspuesto a la información, estos autores generan un modelo conceptual. La entropia se refiere a la cantidad de variedad en un sistema, donde ésta variedad se interpreta como la cantidad de incertidumbre que existe en una situaciòn de elección entre muchas alternativas distinguibles. Un sistema --en este caso un problema de una organización--, se comporta dentro de una dualidad entre dos extremos. Por un lado està la entropía, es decir, la variedad o incertidumbre o desorden. Por el otro està lo contrario: orden y certidumbre. La entropia negativa es el movimiento del primer extremo hacia el otro. Reducir la entropía es reducir la cantidad de incertidumbre que prevalece. Y esto ocurre al obtenerse informaciòn. De ese modo, la informaciòn es significativa, según las alternativas, en un momento determinado. Las aportaciones de

---

16.- Ibid. P. 206
17.- Ibid. P. 21

Shannon y Weaver se dieron en el establecimiento de la equivalencia de la entropía (incertidumbre), con la cantidad y calidad de la información.(18) El siguiente cuadro es ilustrativo en este respecto.

CUADRO 2. REDUCCION DE LA ENTROPIA.

Elevado -----Desorden----- Bajo
Elevado -----Variedad----- Bajo
Elevado ---Incertidumbre-- Bajo
Elevado -----Entropía----- Bajo
Extenso --# alternativas-- Pequeño
Pequeño --Probabilidad de- Evento
----un evento----
Extenso --Probabilidad de- Pequeño
-un estado total--
Bajo ---Regulación y --- Elevado
-----Control------
La información debe obtenerse y procesarse para mover el sistema de izquierda a derecha.(19)

La información tiene función de combatir la variedad, consistente en el número de posibilidades o elementos en un conjunto. Gigch señala: "a mayor variedad, mayor número de alternativas y menores probabilidades para cada alternativa"(20) El control de un sistema está, entonces, en función del contenido y disponibilidad de la información. ésta se constituye elemento fundamental de administración,

---

18.- Esta explicación de la "Teoría de la información", se extractó de la que presenta Gigch, John P. van: "Teoría general de sistemas".-- México: Editorial Trillas, 1987. Pp. 53 y 54. Norbert Wiener define la dualidad entropía-información de este modo. "Justo como la cantidad de información en un sistema es una medida de su grado de organización, de la misma manera la entropía de un sistema es una medida de su grado de desorganización; y una es simplemente lo negativo de la otra." Wiener,Norbert: "Cybernetics".-- Cambridge, Mass.: MIT Press, 1961. P. 11
19.- Ibid p. 53.
20.- Gigch, op. cit. P. 480.

es decir, de toma de decisiones para funciones de regulación, organización y control. Así, toma el papel de activo para las instituciones que buscan enfrentarse con éxito a su problemática interna y al medio o sistemas que le rodean.

3.3.- LA INFORMACION Y LA TEORIA DE LA ADMINISTRACION.

La información o conocimiento ocupa un lugar central en la teoria de la administración y acerca de ello, en esta sección se retoman conceptos relevantes de trabajos de Herbert Simon.

Una de sus aportaciones en las teorías de la administración, y de la organización, es precisamente el rol que desempeñan la información y su dinámica en las instituciones. Esto se aborda en dos secciones. 3.3.1) La información como sustento en la toma de decisiones. 3.3.2) La comunicación administrativa.

3.3.1.- LA INFORMACION COMO SUSTENTO EN LA TOMA DE DECISIONES.

La información o conocimiento tiene un papel esencial en todo proceso decisorio. Interviene en los siguientes aspectos.

1) Permite descubrir las situaciones en las que debe ejercerse un proceso de decisión, que se traducirá en acción.

2) Apoya la definición de los propios problemas. o situaciones. En la medida que éstos son precisados o clarificados, se facilita abordarlos.

3.- Permite seleccionar diversas alternativas de solución.

4.- La información es valioso auxiliar para conocer las posibles consecuencias de las alternativas de acción seleccionadas y, con base en ello, diseñar o escoger la vía más satisfactoria para resolver situaciones.

5.- Cuando se cuenta con información acerca de los valores y preferencias de las personas afectadas por las decisiones, se facilita la selección de alternativas y la implementación práctica de la decisión, de modo que sea aceptada o acatada.

6.- Los conocimientos con que cuenta el decisor, o su nivel de capacitación, afectan la calidad o racionalidad de las decisiones.

En estos seis aspectos, la información tiene rol vital para que los individuos estimen una situación dada. Es tarea suya seleccionar, a partir de toda clase de posibles consecuencias, una subclase más limitada o incluso una serie única de consecuencias relacionadas con cada alternativa. En general, el curso de las decisiones tomadas está influido por el comportamiento humano y otras limitantes del medio ambiente. El decisor genera expectativas de las consecuencias futuras basadas en relaciones empíritas conocidas y en la información acerca de la situación existente. (21)

21.- Simon, op. cit. P. 66.

Simon afirma que el aumento de conocimientos humanos es el factor primordial que señala a un sistema su dirección, en especial el que fijará los limites de lo que es tecnológicamente factible.(22) En el dominio de lo tecnológicamente factible se determinará lo que es económico. En la actualidad, afirma, la tarea crítica no consiste en generar, almacenar o distribuir información, sino en filtrarla de modo que se cuente con mejores soportes para la toma de decisiones, hacia los objetivos de las instituciones. Asi, el recurso escaso, hoy en dia, no es la información como tal, sino la capacidad de procesarla.(23)

3.3.2.- LA COMUNICACION ADMINISTRATIVA.

La información es buscada continuamente, a lo largo de las operaciones de una institución y es necesaria para que todas las unidades administrativas que la componen, operen con éxito. (24) La sola presencia de información no permite el funcionamiento de las organizaciones. ésta debe ser comunicada o transmitida de modo que los puntos de decisión cuenten con ella en la cantidad y calidad adecuados y en el momento apropiado.(25) A este respecto, Deutsh afirma que

22.- Simon, Herbert A.:"La nueva ciencia de la decisión gerencial".-- México: Libreria "El Ateneo" Editorial, 1982. ibid. P. 12.
23.- Simon, ibid. P. 104.
24.- Simon, Herbert: "El comportamiento...", p.149. Para una exposición de diversos problemas de comunicación administrativa. V. ibid. Pp. 155 a 157.
25.- V. Supra. Capítulo 1, sección sobre los atributos de la información, como sustento de la toma de decisiones.

las instituciones se componen de partes que se comunican entre sí. Reciben mensajes del mundo exterior y almacenan información. El problema práctico en la administraciónes es el de asegurar una organizaciòn del proceso decisorio, que lleve los conocimientos importantes al punto en que se toma la decisión.(26) Este problema se enfrenta con el diseño de sistemas de comunicaciòn o de información administrativa. La comunicaciòn es mecanismo que une segmentos de un sistema entre sí, de modo sincronizado.(27) Asimismo, es método por el que se evoca la acciòn y se controla y coordina las partes del sistema.

Los sistemas de comunicación administrativa son, formalmente, procesos mediante los cuales las premisas decisorias se transmiten de un miembro de la organización a otro. En ellos debe resolverse qué tipos de informaciòn deben canalizarse de un modo màs o menos controlado, de acuerdo con su nivel de importancia o confidencialidad y cómo debe intercambiarse la información, para apoyar diversas decisiones o unidades administrativas.(28)

La comunicación es indispensable en la organización, para influir en el comportamiento del individuo, ademàs de asegurar que el trabajo de éste se integre a la dinàmica y finalidad institucional.

26.- Deutsh, citado por Scott, William G.:"Organization theory", en Journal of the Academy of Management. (E.U.A.), vol. 4, num. 1 (abril 1961), Pp. 22.
27.- Scott, ibid.
28.- Basado en Simon, ibid., pp. 39 y 40.

De la disponibilidad de técnicas de comunicaciòn, se determinará la manera en que las funciones decisorias se distribuyan en el organismo. Como se mencionò en el apartado anterior, los individuos podràn tomar decisiones concretas si cuentan con la informaciòn para ello y con medios de transmitir las decisiones a los demàs miembros.

En las instituciones, la informaciòn fluye hacia arriba -- se filtra para sustentar decisiones supervisorias o estratégicas --, hacia abajo -- para normar la gestión de los mandos intermedios y los niveles operativos -- y hacia los lados -- para coordinar o secuenciar fases de supervisión u operación.(29) Asimismo, la comunicación administrativa tiene lugar en dos direcciones. 1) La información hacia el centro decisorio (órdenes, información, consejo) y 2) las decisiones transmitidas hacia otros puntos de la organización.

Por otra parte, la informaciòn que se relaciona con la decisión tiene diversos orígenes, a saber.

1) De órganos que reciben información exterior al organismo.

2) De los individuos, cuyo reclutamiento supone que poseen conocimientos o formación previa. Por ejemplo, los abogados que sirven en unidades jurídicas.

3.- De las operaciones o funcionamiento del propio organismo.

29.- Simon, ibid., p. 147.

4.- De las "memorias artificiales"(30) de la organizaciòn, como son los manuales y sistemas de registro como archivos, bibliotecas o unidades de documentación. (31)

La informaciòn necesaria para una decisión rara vez se halla en posesiòn de un sólo individuo o unidad admiistrativa. En lo práctico, las decisiones suelen dividen en premisas componentes, desde centros separados, hasta el punto donde pueden ser combinadas y transmitidas. Para Simon, ésto es la esencia de la organización, (32) cuya estructura corresponde, generalmente, a la especificaciòn de un sistema formal de comunicaciones. Este se completa con la red de comunicaciones no formales, basada en la red de relaciones sociales dentro de la organización. (33)

3.4.- LA INFORMACION EN LA ECONOMIA.

La información también rebasa los ámbitos politico, jurídico o ideológico y penetra en esferas de producción, circulación y consumo. Es, además, recurso básico para procesos productivos y administrativos. Repercute en la productividad y el empleo y, por lo tanto, en el producto

---

30.- Simon describe las "memorias artificiales" como medios no humanos de retenciòn de información. V. Infra. Sección 3.5, en la que se habla de los archivos como sustento de la institucionalidad.
31.- Entre los manuales màs frecuentes en las instituciones públicas destacan los manuales de organización, los de descripción de puestos, los de descripción de métodos o procedimientos haca fines especificos, los de inducción al puesto, entre otros.
32.- Simon, ibid., p. 148.
33.- Simon, ibid., p. 163.

nacional bruto. (34) La informàtica, por su parte, ha sido auxiliar esencial de las instituciones modernas, dada su capacidad de almacenamiento, tratamiento, transmision y utilizacion de datos para toma de decisiones con impacto económico.

La información no es valiosa "per se", sino sólo cuando está organizada, controlada, ostenta los atributos referidos en el capítulo 1 y es útil, en consecuencia, en la toma de decisiones, en la productividad, en la innovaciòn y en la competencia. La informàtica es gran impulsor económico en varios frentes.

Primero, acelera cambios tecnológicos y organizacionales y las transacciones entre instituciones o personas al "derrumbar la flotación de la información"(35). El efecto neto es el flujo màs rápido de datos, que permite interacciones instantáneas entre personas y équipos. El tiempo de respuesta se vuelve inmediato y el proceso de toma de decisiones se acelera.

Segundo, los costos de los equipos de computación van en decremento. De ese modo, se vislumbra un panorama próximo en el que los métodos de trabajo, de compras, de inversiones y de bùsqueda de información, en un amplio espectro del conocimiento y actividades, cambiarán

---

34.- Tellez, op. cit. p. 67. Ver. cifras sobre el impacto de la información en el PNB de los EEUU en Nussbaum, Bruce, op.cit. P. 32.
35.- Ibid. P. 37. Naisbitt explica la flotación de la información como el tiempo que ésta permanece en el medio de transmisión, entre el emisor y el receptor.

dramaticamente. En términos prácticos, las nuevas tecnologías para proceso y transmisión de datos desplazan envíos de personas y cosas a través de espacios físicos urbanos o a través del aire. Nussbaum afirma que "los hombres de negocios y los profesionistas prefieren las computadoras y comunicaciones para desempeñar sus trabajos, que moverse físicamente".(36) Esto conlleva importantes ahorros en tiempo, en dinero y en desgaste personal.

Tercero, la informática asume cargas de trabajo rutinarias e impulsa la creatividad y desempeño del hombre, en extensión y calidad. La velocidad de disposición de nueva información es inmensa, que permite mejor toma de decisiones y, contundentemente, mayor productividad. Asimismo, la informática ofrece soluciones adaptables a toda forma de administración y legislación. Permite descentralización e incluso autonomía de unidades administrativas periféricas. Ello aligera la estructura de las administraciones, mejora su eficacia y relaciones con los administrados. En suma, las organizaciones se ponen en mejores condiciones de respuesta ante necesidades de competitividad y abren nuevos cauces de desarrollo.

Cuarto, la información presenta un valor económico definitivo. El principio, por el lado de la oferta, la información vale por sus costos de producción, en horas-equipo y en horas-hombre. En esta producción intervienen personas con distintos niveles de capacitación y con

36.- Nussbaum, op. cit. P. 47.

especialidad en diversas disciplinas. En el lado de la demanda, el valor de la información se hace presente en el momento en que los usuarios, a través de medios prácticos, pueden localizar el agregado de datos que necesitan para satisfacer sus necesidades y están dispuestos a pagar por ello. Naisbitt afirma que "... aunque una economía basada en torno a la información parezca menos real que otra basada en bienes tangibles primarios o manufacturados, eso no importa mientras la gente pague por la información o el conocimiento.(37)

Quinto, las organizaciones de todo tipo se han hecho altamente dependientes de la tecnología para el proceso rápido de la información. Nussbaum reconoce que "sin datos, las comunicaciones, las labores de venta, la ingeniería, los seguros, la contabilidad, la sanidad, los gobiernos, el turismo y los viajes, llegarían a pararse".(38) El mismo, afirma que la tecnología industrial del mundo fue inventada durante el siglo pasado. El progreso posterior ha sido, practicamente, refinamiento y no cambios drásticos.(39) Ejemplos de ello son la industria química, de teléfonos y telégrafos, maquinaria pesada y transportes terrestres. La mayor y mejor información ha sido determinante en ese refinamiento de las industrias, en la medida que se ha dispuesto de alta calidad en los datos. En las fabricas

37.- V. Naisbitt, op. cit. P. 35.
38.- Nussbaum, op. cit. P. 146.
39.- Ibid. P. 146. El autor exceptúa, obviamente, para este argumento los casos de la industria aerea y la nuclear, pero ello no demerita sus afirmaciones.

del futuro, las computadoras tomaran lugar en el diseño y control de las lineas de fabricación.

Los procesos y comunicación de información toman fuerza económica al ser activos en la generación de riqueza. Esta fuerza se complementa del impacto informàtico en las interrelaciones entre el Estado y la sociedad y entre esta en sí misma, que se abordan a continuación.

3.5.- LA INFORMACION EN LA ADMINISTRACION PUBLICA, LA SOCIEDAD Y LA POLITICA.

Los gobiernos son redes de instituciones que tienden a constituirse en agregados formales y estables. Definen espacio de acción propia, alrededor del cual se establecen y organizan los espacios de actividad de las personas fisicas y morales de una determinada sociedad civil. Es, en otras palabras, factor ordenador de la vida social. La autoridad estatal tiene tiempo más duradero que el de las personas que la conforman. Integra mecanismos de jerarquia y estructura, es decir, de organizaciòn. Su razón de ser y funciones se enmarcan en leyes y reglamentaciones, emanadas de realidades sociales, culturales y de fines públicos. Nora y Minc aseveran "El modelo cultural de una sociedad descansa sobre su memoria, cuyo dominio condiciona, en gran medida, la jerarquia de los poderes".(40) Esta memoria es, precisamente, presencia de información y es factor de durabilidad o permanencia cultural. Para los gobiernos, éste es un concepto fundamental. Crean documentos y archivos como

40.- Nora y Minc, op. cit. P.182

"garantia de subsistencia y operación". (41) Ampudia afirma que éstos son la "expresiòn más clara y firme sustento de la naturaleza institucional de la Administraciòn Pública"(42). La información, entonces, como esencia de institucionalidad, es patrimonio de la funciòn pública eficaz y eficiente. Es agente que permite la citada durabilidad y prevalencia sobre intereses particulares, para darle un enfoque social o público. Fluye por canales formales, preestablecidos, y asi cubre la organización, en todas sus partes, como un sistema nervioso que inerva cada célula del organismo vivo.(43) Ello hace interactuar todos los componentes de una entidad, de manera ordenada y crea coordinaciòn estricta que fortalece, aùn más, la institucionalidad.

En el contexto de la modernizaciòn administrativa, el mismo Ampudia asevera:

"Si el entramado permanente de las instituciones está constituido por los sistemas que permiten a sus componentes intercambiar y conservar ordenadamente información, consiguiendo asi la estabilidad y coherencia que le es propia a las organizaciones pùblicas, entonces la adaptación y mejoramiento de estos sistemas de informaciòn, son requisitos del mejoramiento integral de las entidades públicas"(44).

En el campo de la politica, el control de la información, es fuente de poder. En la "revolución informática", el que tiene la información tiene el

41.- De Ampudia Mello, Enrique: "Institucionalidad y Gobierno: un ensayo sobre la dimensiòn archivìstica de la Administración Pública".-- México: Instituto Nacional de Administración Pública - Archivo General de la Nación, 1988.
42.- Ibid. P. 40.
43.- Karl Deutsch es el autor de esta analogìa. Citado por Ampudia, op. cit. P. 13.
44.- Ibid. P. 46.

poder.(45) Es por ello que ha constituido preocupación de los gobiernos, al ser elemento esencial en el mantenimiento de la seguridad y soberanía nacional. "Vivimos en una sociedad moderna compuesta por múltiples organizaciones formales. Según sociólogos, son sistemas para copar con la incertidumbre en sus medios ambientes" (46) En su afán por mantener un rumbo predecible, las organizaciones buscan reducir la incertidumbre conociendo mejor sus competidores, opositores; personas y agrupaciones. Para ello requieren y procesan mayor y mejor información. Buscan reducir la incertidumbre y conocer mejor el comportamiento humano, individual y social.

Los sistemas de información burocráticos, computarizados, son nueva forma de desarrollo del control social. Ello equivale a ejercer patrones de influencia por organizaciones sobre el comportamiento de las personas, que pueden ser benignos o coercitivos. El "mass surveillance and control" (47), es decir la vigilancia y control de masas, es un aspecto sociológico distintivo de las sociedades avanzadas, según Hircsham.

La "razón instrumental" de Horkheimer, es decir el proceso de razonamiento lógico y analítico que se efectúa en las organizaciones, es el medio más aceptado para llegar a un proceso de toma de decisiones, más eficaz y eficiente en

45.- Nora, Minc, op.cit. P.18.
46.- Rule, citado por Hirscham, R.A.: "Computers and privacy", en "Computer Bulletin", March 1983 P.7.
47.- Termino acuñado, definido y utilizado por Hircsham, ibid.

la dinámica del medio ambiente. Es lo que Rule llama "fine grained decision making", es decir decisiones depuradas en respuesta a problemáticas especificas. (48)

Es factible que el control social, por parte de las burocracias, derive en un declinamiento a largo plazo de la autonomia del individuo, familias o comunidades, al contarse con más y mejor información disponible de las personas. Puede ocurrir una fuerte centralizaciòn de este control, en grandes unidades burocràticas, o como reconoce Hircsham, la regulación de la sociedad podria ser inefectiva.(49)

Cuando la tecnologia en el proceso de datos es en pequeña escala, el efecto de control social no puede ser muy grande, pero cuando la tecnologia es grande y poderosa los efectos pueden ser de cualquier magnitud. Y es en este punto donde nace la discusión sobre la protección de la esfera del individuo o la agrupaciòn frente a las grandes organizaciones privadas o pùblicas. En otras palabras, el concepto de "privacia".

48.- Rule citado por Hircsham, op. cit. P.8
49.- Ibid.

CAPITULO 4.- LA PRIVACIA DE LA INFORMACION.

La afectación de la privacia que resultaba de la aplicación de nuevas tecnologías para el proceso de datos, fue uno de los detonantes que motivó la aparición de las discusiones acerca de la seguridad informática.(1) Hacia un análisis más riguroso acerca del concepto de privacia, se puede citar la definición de Hirscham. Afirma que es, "...la expectativa social de la extensión de un individuo o colectividad a tener influencia sobre la información propia, en su utilización y comunicación hacia otros". Con base en ello, se busca evitar usos no autorizados de los datos, el aseguramiento de su confidencialidad y la protección contra información no deseada, impropia o negativa.(2) En este aspecto hay dos grandes corrientes de opinión a nivel internacional, que

---

1.- V. supra. P.4. Una explicación para mejor comprensión de este aspecto es la siguiente. "Imaginemos una caja de comunicaciones electrónicas a través de la cual usted efectúe sus transacciones bancarias, despache su correspondencia, haga sus compras de bebidas espirituosas, solicite billetes de avión y sus reservas de hoteles y realice sus envios de flores, amén de contemplar los programas de entretenimiento. Todas estas gestiones, extremadamente privadas, se encuentran ahora en un solo sistema electrónico, centralizado y muy accesible. Hacienda puede querer echar un vistazo y también pueden desearlo vendedores y acreedores de todas clases. Cabe que a su jefe le agrade saber qué hace usted fuera de la oficina, y también su propia esposa puede mostrarse curiosa. La nueva tecnologia de comunicaciones planteará nuevas e importantes cuestiones sociales en el àmbito de la intimidad y la seguridad". De Nussbaum, Bruce: "El mundo tras la era del petroleo: los nuevos ejes de poder y riqueza".-- México, D.F.: Editorial Planeta, 1985. P.55.

2.- Hirscham, R.A.: "Computers and privacy", en "Computer Bulletin" (U.S.A.), Marzo 1983. P.7.

sintetiza adecuadamente Alan Westin.(3) 1.- Los optimistas, que resaltan los beneficios del cómputo en el progreso de la humanidad, control de la naturaleza, toma de decisiones racionales y comprensión de problemas. Adicionalmente, ayuda a la confección de servicios a los individuos, comunidades o grupos, de muchas actividades y especialidades. En el otro lado, se encuentran 2.- Los "orwellianos", que ven la informática como pesadilla. Contemplan las computadoras y las tecnologias de comunicación como medios para control social por parte de las agencias pùblicas o empleadores, para obtener datos sobre los individuos o agrupaciones y ejercer un rígido control. El anonimato, la espontaneidad y la capacidad de evadir vigilancia y espionaje es anulada.

En tiempos previos al computo ya existían previsiones hacia la privacia y libertades individuales. El "Bill of Rights", de la Constitución de los Estados Unidos de América, La "Declaración Universal de los derechos del Hombre", las garantias individuales, en las constituciones de diversos países, entre otros, estatuyen la libertad de expresión, de pensamiento, de religión, y otras, para limitar abuso de poder. Se buscò, en realidad, balancear demandas de libertad y la necesidad de orden por parte de las autoridades.(4)

3.- Westin, Alan: "Privacy, technology and regulation", en Donnelly, D. (ed): "The computer culture".-- London & Toronto, Associated University Press, 1985. P.136.
4.- Westin, Alan, ibid. P. 138

En el pasado, el concepto de privacia se construyó alrededor de la no violación de propiedades, ya sea no entrar fisicamente al lugar privado o acercarse a su estructura y ver o escuchar asuntos ajenos. La legislación derivada se basó en la tecnología de ese momento. La privacía implicaba la idea que la gente no podía introducirse fisicamente en lugares protegidos, a menos que satisfaciera la garantía de que la intrusión tenia motivos razonables. Las cuestiones de respeto a la privacia se fortalecen en regímenes democráticos, rebeldes contra prácticas monárquicas o totalitarias.(5)

Entre las décadas del 60 y del 70, algunos observadores sociales afirmaron que las nuevas tecnologías eran amenaza al equilibrio entre los valores sociales, la ley y la tecnología.(6) Si antes, traspasar límites físicos era el fundamento del concepto de privacia, ello se viene abajo ante las potencialidades de los sistemas de vigilancia a control remoto con cámaras, micrófonos, teléfonos, etc. Después, lo que es más importante, la capacidad de capturar, guardar, procesar y distribuir información, alentó las discusiones que se centraban en argumentar que, en adelante, la tecnología sería la única limitante en atentar más y más

5.- El aspecto, tal vez más critico en la combinación entre el modo de vida y la disponibilidad de tecnología limitada, se constituyó con base en los registros de datos sobre personas.

6.- V. Nora, Simon y Alain Minc: "La informatización de la sociedad".-- México, D.F,: Fondo de Cultura Económica, 1981. P. 24., Hsiao, David; Douglas Kerr y Stuart Madnick:"Computer security".-- San Francisco: Academic Press, 1979. Pp. 17 y 18.

contra la esfera personal. De repente fue posible recabar mucha información de individuos, analizarla, distribuirla, intercambiarla y vigilar las transacciones de la persona, conociendo qué hace, dónde y cuándo. Parece como si la antigua protección de la información se basara en las limitaciones de la tecnología manual para procesar datos en forma rápida y eficiente, haciendo al gobierno incapaz de contar con datos sobre amplios sectores de la población. La información personal, antes separada entre escuelas, médicos, trabajo, bancos, aseguradores, etc., ahora está en la posibilidad de integrarse con amenaza a la privacía.(7)

Desde principios de los 60, en países capitalistas desarrollados, surgieron discusiones, en los medios masivos de comunicación y parlamentos, sobre la nueva privacía de los individuos. Se establecieron comisiones de expertos y de gobierno para analizar el tema. Se debatía entre lo que serían hechos y lo que sería fantasía, con base en las capacidades de la tecnología y de los sistemas de información. En los Estados Unidos, surge en 1970 el primer documento regulatorio para los datos informatizados: el llamado "*Fair credit reporting act*", acerca del uso de los reportes bancarios que afectan el crédito individual y oportunidades de seguros y empleo.(8)

7.- V. 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. P. 27.

8.- Estos aspectos los refieren Westin, Alan, op. cit. P.140., y Hsiao, David, op. cit. P.17.

La aproximación más inmediata para defender las amenazas a la privacia es la existencia de medios para que los individuos accesen registros de datos que les conciernen y permitir que validen su exactitud e integridad. Con ello se genera el derecho de revisión, rectificación, eliminación de datos y prohibición de interconexión, lo que significa la habilitación del derecho de las personas para conocer y verificar la información en circulación acerca de ellos.(9)

Es también en Estados Unidos donde aparece el primer documento legal a este respecto: el "Federal Privacy Act of 1974".(10) El Acta cubre todas las agencias y departamentos federales y los obliga a listar publicamente los registros de información acerca de individuos ya se trate de licencias, beneficiarios de programas de gobierno, contribuyentes o veteranos. Cada vez que se hacen altas en archivos con registros de personas se deben listar éstas y se habilita a los individuos involucrados a conocer los

---

9.- De Tellez, Julio: "Derecho informàtico".-- México, D.F.: Universidad Nacional Autònoma de Méxio,1987. P. 73.

10.- El presidente, entonces, Richard Nixon, es su promotor. La raiz de ello fue un hecho esencial en la historia de la seguridad en la información: el escándalo "Watergate". El público lo percibió como un hecho basado fundamentalmente en información. Es el esfuerzo del Presidente y sus seguidores y subordinados de adquirir información por medios ilegitimos, entrando a las oficinas de siquiatras para obtener datos sobre Daniel Ellsburg, o usar archivos especiales para castigar enemigos y circularla por todo el gobierno o Watergate como tal o la entrada a las oficinas centrales del Partido Demócrata para instalar aparatos de espionaje telefónico y, además, los esfuerzos de cubrir los hechos. Todo ello hizo emerger con fuerza nunca antes vista, en el mundo occidental, la cuestión del uso ilegítimo de información por gente en el poder. Este relato está extractado de Westin, Alan, op. cit. P.143.

datos acerca de ellos. Se establecen algunas excepciones para los archivos de inteligencia o ejercicio de la ley.(11)

En general, esta acta es una garantia para defender la privacia del individuo. Inclusive, se enuncia que, a menos que el Congreso lo autorice especificamente, ninguna información puede recabarse acerca de las libertades de prensa, expresión, asociación, religión, entre otras muchas. En ésta, que es la base del enfoque norteamericano, quedan legalmente establecidos los derechos de acceso, rectificación y eliminación de información, si lo desea la persona interesada, asi como el derecho de prohibir o controlar la interconexiòn de archivos entre distintos organismos. De la no observancia de la norma se derivan sanciones y ello fortalece su posibilidad de vigencia. Hay algunas excepciones al ejercicio del acta, como son los aspectos de equilibriio del Estado, seguridad nacional, persecución de delitos, aspectos monetarios o de salud pública.

Un segundo enfoque, en el balance entre tecnologia y privacia, es el modelo europeo, impulsado principalmente en Suecia, República Federal Alemana, Francia y Holanda. Su aproximación al tema viene de la tradición del Código Napoleónico y refleja la cultura politica de los estados del viejo continente.(12) Su postura fundamental es la de

---

11.- El Acta está reproducida en Tellez, Julio, op. cit, pp. 175 a 197, Anexo V. Un resumen de sus puntos más importantes lo ofrece Hsiao, op. cit. Pp. 19 y 20.
12.- De Westin, Alan, op. cit. P. 147.

controlar, desde el gobierno, la creación de archivos de datos personales, a través de comisiones especializadas. Las leyes de protección de datos indican que antes que cualquier institución o agencia pública o privada efectúe la creación de sistemas de información que contengan datos personales, deben solicitar una licencia por parte de las mencionadas comisiones. Éstas, a su vez, definen los estándares generales de seguridad, confidencialidad, acceso y transferencia de datos en el interior o al exterior. Se examinan las necesidades del solicitante, la razonabilidad de la solicitud y se emite un documento de aceptación o rechazo. Paralelamente, los individuos pueden acudir a las mismas comisiones para quejarse de la falta de acceso a datos sobre ellos mismos o de atentados contra la privacía.(13)

En Europa, la discusión se ocupa del control del gobierno sobre el uso de la tecnología computacional en la sociedad. En especial, en Suecia hay puritanismo al

---

13.- Como ejemplos de leyes de protección de datos europeas destacan las siguientes, reproducidas en Tellez, op. cit. "Ley de Protección de datos de Hesse" de 1970 (Estado de Land Hessen ,Alemania Federal) y "Ley Federal de Protección de Datos"de 1977 (Alemania Federal). "Ley de datos de Suecia" de 1973. "Ley sobre Procesamiento de Datos, Archivos y las Libertades Individuales" de 1978 y "Loi No. 85-660 du 3 Juillet 1985" (Francia). México, SPP, INEGI, op. cit. P. 30., cita las siguientes "Ley referente al Registro de Datos Personales", de 1978 (Noruega). Leyes referentes a los registros privados y públicos, de 1978 (Dinamarca), entre otros. V. Tambièn, International Labour Office: "New technologies: their impact on employment and working environment.-- Geneva: I.L.O., 1982. Pp. 34 a 39.

respecto.(14) Su actitud se basa en precaverse sobre la creación de información peligrosa a los derechos de las personas. En contraste, los americanos consideran la generación y procesamiento de información como consecuencia de la libre empresa. Si hay abusos o ilícitos, se acusan como crímenes. Otra diferencia fundamental entre ambos, la refiere David Hsiao. En Europa se proveen instancias institucionales. En los Estados Unidos, el individuo debe perseguir su propio caso personalmente. (15)

Como resolución a la discusión acerca de la privacía, el mismo Alan Westin ofrece dos consideraciones fundamentales. Primero. El propio mercado es un regulador. Al menos en Estados Unidos, las aplicaciones computacionales se realizan si alguien está dispuesto a pagar por ellas y le va a reportar beneficios monetarios. Por ejemplo, en los 60 se pensaba que en la década actual todas las operaciones de compraventa se realizarían vía tarjetas plásticas. En este momento surge el cuestionamiento: ¿quién lo desea y quién paga por ello?. Por otro lado, el recurso de la información es una fuente de poder que nadie obtiene sin costo. Y existen muchos medios

---

14.- V. México, SPP, INEGI, ibid. Tellez, op. cit. Pp.132 a 141, Anexo III., reproduce la Ley de Datos de Suecia, que presenta múltiples restricciones para el acopio, proceso, utilización, difusión y exportación de datos nominativos. V. Nussbaum, Bruce: "El mundo tras la era del petroleo: los nuevos ejes del poder y la riqueza".-- México: Editorial Planeta, 1985. P.149.
15.- Hsiao, David, op. cit. P. 21.

efectivos para controlar y establecer limites en accesos y usos de la información.(16)

Segundo. En las sociedades democráticas, o en las que aspiran serlo, se debe decidir cuánto, cómo y porqué intervenir en el uso y circulación de datos. Ello con base en criterios de servir propósitos sociales.

Las cuestiones de la privacia, en general, han sido motivo de polémica en las sociedades que se informatizan. A medida que se avanza en las deliberaciones sobre la materia, aparecen normas que con implicaciones técnicas para la operación de las organizaciones. Del marco legal, se derivan derechos y obligaciones, y de éstas, politicas, métodos y procedimientos para garantizar que las instituciones operen de acuerdo con principios de observancia de la privacia. La mayor implicación, de la problemática de la privacia, sobre los archivos de datos, es que primero debe controlarse el acceso a los dispositivos informáticos; segundo, a los archivos de información; tercero, dentro de esos archivos, a los datos que el usuario o consultante estará autorizado a accesar. De ahi nace la necesidad de clasificar adecuadamente la información y segmentarla en diversos niveles de confidencialidad. (17) Sobre ello se profundizará en el capitulo 6, al referir el marco analitico para la seguridad informática y al abordar la administración de esta seguridad, en el capitulo 9.

16.- Westin, Alan, ibid.
17.- V. Hsiao, op. cit. Pp. 23 y 24.

CAPITULO 5.- LA VULNERABILIDAD INFORMATICA.

El impacto negativo, desventajas o amenazas que conlleva el procesamiento electrònico de datos es menos reconocible que los beneficios que ha aportado. La informática ha permitido mayor eficiencia administrativa y productiva. No obstantye, es también nuevo campo potencial de errores, actos ilegales o delictivos. Con tecnologìa manual para proceso de datos, estos actos tienen alcance limitado a las capacidades humanas. Pero, con grandes concentraciones y volùmenes de datos, los riesgos derivados son de dimensiones insospechadas.(1)

El análisis de la vulnerabilidad informática se propone en tres frentes: 1) los errores y omisiones, 2) las pérdidas por desastres naturales y 3) los delitos informáticos.

5.1.- LAS PERDIDAS POR ERRORES Y OMISIONES.

Los errores y omisiones constituyen el campo màs frecuente de daños en sistemas de automatizaciòn de datos. Se originan, fundamentalmente, en el personal de las instituciones. Por lo general, los procesos de

1.- Sendrow establece una analogìa. Dice que el impacto negativo de la informàtica tiene ahora el mismo comportamiento que el saber leer y escribir con la emisiòn de cheques malos. Hace 100 años, pocas personas estaban alfabetizadas. Conforme hubo más y más gente preparada, creció el número de cuentas bancarias y el número de cheques malos. En el desarrollo reciente, al crecer los niveles de operación y programación por parte de los usuarios de los sistemas de computo, la vulnerabilidad ante usos no autorizados de la información y el valor esperado de las pérdidas crece. Sendrow, Marvin: "Impact of rapidly changing computer technology on computer crime: advance computer security concepts", S.P.I., mimeo, 1980. Pp. 11 y 12.

informatización han ocurrido con incorporación de equipos, sin corresponderse con programas adecuados de entrenamiento, capacitación y sensibilización del personal, cuyas labores se relacionan con la computación. Los proveedores ofrecen cursos, como complemento del suministro de computadores. Estos son tomados por un número reducido de personas que, a la larga, no transmiten los conocimientos a otros, de manera adecuada, o abandonan la institución.

Ello da lugar, con el tiempo, a que las aplicaciones computacionales crezcan en amplitud y complejidad, mientras los errores y omisiones del personal, se hacen, cada vez, más destructivos, potencialmente. 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-hombre de captura y proceso. Un caso particular, ilustrativo, es el del centro de proceso de datos de una importante dependencia. Su diseño e instalación fueron cuidadosos. En materia de seguridad se consideraron medidas para la protección de datos, programas, equipos e instalaciones. Se instaló un sistema de alimentación eléctrica de emergencia para garantizar la continuidad en las operaciones al ocurrir interrupciones de energía. El día que hubo un corte en la energía de la red pública, no funcionó el sistema de emergencia: faltaba diesel en la planta eléctrica.

Este tipo de problemas, se deriva, en general, de la ignorancia o negligencia del personal responsable de los recursos informàticos 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.

5.2.- LAS PERDIDAS POR DESASTRES NATURALES.

Este tipo de contingencias es menos frecuente y las pérdidas se originan por falta de previsiòn. Pueden clasificarse en dos vertientes. La primera es la de desastres naturales en tiempo corto. Ocurren durante lapsos reducidos de tiempo. Ejemplo de ello son inundaciones, sismos, actividad volcánica o incendios. La segunda corresponde a los ocurren en periodos prolongados y dañan los activos informàticos paulatinamente. Son los casos de humedad incontrolada, presencia de particulas sólidas o de sustancias corrosivas en el ambiente, radiaciones electromagnéticas, entre otros.

Los desastres naturales de tiempo corto 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.(2)

2.- En el anexo 1 de este trabajo, se aborda con detalle este tipo de planes. Por otra parte, cabe señalar que los sismos ocurridos en la Ciudad de México, en septiembre de 1985, fueron gran detonante para iniciar en nuestro pais el ejercicio de previsiones de seguridad. Cuatro sociedades nacionales de crédito y múltiples dependencias y entidades perdieron sus centros de cómputo. Algunas de ellas no

Los desastres naturales de tiempo prolongado obedecen, en todos los casos, a diseño deficiente de instalaciones de cómputo. En la investigación realizada para este trabajo, se conocieron casos de equipos dañados por humedad en zonas tropicales o de lluvias frecuentes y casos de presencia de animales, en el interior de los equipos de procesamiento.

5.3.- LOS DELITOS INFORMATICOS.

En forma paralela a la revolución informática, está cobrando importancia creciente la cuestión de los usos indebidos de los recursos computacionales, que se constituyen en crímenes o delitos informáticos.

Una de sus manifestaciones, la "piratería", comenzó hace varios años en el mundo de la información y de las telecomunicaciones. Principió con las antenas para interceptar programas de televisión, transmitidos via satélite. Se extendió después a la intercepción de teleconferencias y de teleproceso de datos. (3)

La información, como activo valioso, es foco de criminalidad. Mientras más dependen las organizaciones y las sociedades de medios electrónicos, y más entrelazados están, más vulnerables son. En terreno económico y financiero, el potencial delictivo es evidente. Para ello, basta considerar la dependencia que las instituciones bancarias tienen hacia

---

contaban con respaldos de datos y no pudieron recuperar informaciónes que representaban incontables horas-hombre de estudio, captura y proceso.

3.- Nussbaum, Bruce: "El mundo tras la era del petroleo: los nuevos ejes de poder y riqueza".-- México, D.F.: Editorial Planeta, 1985. P. 47.

los recursos informáticos para sus operaciones cotidianas. En aspectos humanos también ha cobrado relevancia la procupación por la privacidad, que afecta los derechos de las personas, los intereses de las corporaciones y la seguridad y soberanía nacionales.

En los paises 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.(4)

El crimen relacionado con las nuevas tecnologías tienen caracteristicas particulares en tres facetas: 1)la institución, 2) el defraudador informático y 3) el acto delictivo. En relación con la primera, la informática ha tenido crecimiento explosivo en extensión y calidad de aprovechamiento. Crecimiento no correspondido por conocimiento y asimilación del impacto computacional sobre la organización, el personal y los métodos de trabajo, entre muchos. Menos, todavia, se han abordado los posibles efectos

---

4.- El teleproceso de datos consiste en captura, transformación y transmisión de información entre equipos o dispositivos computacionales, ubicados en diferentes instalaciones en un mismo centro urbano o en localizaciones distantes. La transmisión se efectúa a través de microondas, via satélite o via redes pùblicas o privadas de telefonía alámbrica o inalámbrica. Jesús Sotomayor afirma que a través del teleproceso se han efectuado los mayores desfalcos bancarios. V. Sotomayor, Jesus y A. Sanchez: "Planeación de la recuperación informática en casos de desastres", ponencia en "III Reunión de sistematización de bancos centrales americanos e ibéricos". (Santo Domingo, Repùblica Dominicana), 25 de noviembre a 1o. de diciembre de 1984. V. Introducción.

negativos que conlleva la automatización de datos. En general, los eventos irregulares con intermedio del cómputo, surgen de mal o inadecuado manejo de las concentraciones y volúmenes de datos, así como de los procesos complicados, a grandes velocidades. Ello, en conjunto con escasos medios de control y protección.

A nivel organizacional, la propensión a actos ilícitos se destaca en varios aspectos.(5)

Primero. Existen instituciones con sistemas de información complejos, que solo son conocidos en detalle por una élite de analistas o expertos, y que pueden ejecutar cualquier proceso con los datos a su alcance.

Segundo. Se deposita excesiva confianza en estos expertos. Manejan indistintamente información confidencial o no. Este hecho va paralelo a la confianza de los analistas de sistemas sobre la ignorancia de sus superiores hacia los riesgos informáticos.

Tercero. Se carece de un marco normativo que contrarreste o limite la comisión de actos ilegales.

Cuarto. El personal directivo o administrativo descuida la protección informática. Es usual que, en los sistemas de cómputo del gobierno federal, se observe la seguridad unicamente en aspectos físicos de los equipos y se desatiendan otros ámbitos de protección.

5.- Tomados de González Castellanos, Herbin Amory:"Fraudes en sistemas de procesamiento electrónico de datos" (Tesis para obtener el titulo de contador público y auditor).-- Guatemala: Universidad de San Carlos (Facultad de Ciencias Económicas), 1978. P.72 y ss.

En general, 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. Ello hace, en cierto modo, pequen de negligencia involuntaria." (6)

A nivel del defraudador informático existen factores que le dan ventajas sobre los defraudadores tradicionales.

-- Primero. Tiene mayor nivel intelectual y puede desempeñar cargos de alta jerarquia o importancia para la organización.

-- Segundo. Por lo general, no tiene limitaciones econòmicas que lo obliguen a actuar de prisa.

-- Tercero. Hay pocos especialistas capaces de detectar actos ilicitos.

-- Cuarto. Y el más critico, 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. (7)

-- Quinto. Debido al escaso tratamiento legal del delito informático, el delincuente piensa que, en el peor de los casos, la sentencia serà benigna. Incluso, si se descubre un

---

6.- Bria, Ricardo: "Delitos en un ambiente informatizado", en Actas: I Congreso iberoamericano de informàtica y auditoria. (San Juan, Puerto Rico). 2 a 6 de noviembre de 1987. P. 121.

7.- Estos factores son mencionados por Tellez Valdés, Julio: "Derecho informático".-- México, D.F.: Universidad Nacional Autónoma de Méxio,1987. P.105., Krauss, Leonard & Aileen Mc Gaham: "Computer fraud and countermeasures".-- New Jersey: Prentice Hall,1979., Pp. xii y xii. V. Gonzalez Castellanos, op. cit. P.92

hecho ilicito, probarlo es dificil, ya que se basa en medios intangibles, como es la informaciòn.

En cuanto al acto delictivo informàtico, dado su reciente desarrollo, es dificil enfrentarlo. La tecnologia de concentraciòn y proceso rápido de los datos ha avanzado más que el estudio sobre la vulnerabilidad computacional y la investigaciòn de los actos ilegales derivados de ella. Al respecto hay tres consideraciones importantes. Por un lado, la detecciòn y estudio de estos actos, es decir el conocimiento de qué, còmo, dónde y cuándo ocurrió algo ilicito, es sumamente dificil. En grandes volúmenes de informaciòn y procesos, una operaciòn o transacciòn fraudulenta escapa de un control eficiente e inmediato. Pueden pasar semanas,. o hasta meses, para la detecciòn, si es que ésta ocurre. Y a ello se añade el problema de que pocas veces se cuenta con expertos dedicados a este fin.

El segundo problema en este rubro es, una vez màs, la falta de un marco juridico a nivel nacional, local y organizacional, que cuente con previsiones para delitos computacionales. En realidad, éstos no están tipificados. Los materiales electrònicos y magnéticos no constituyen elementos de prueba para efectos penales.(8) Las cuestiones

8.- Respecto a este punto, v. Tellez, op. cit., dedica un capitulo en su obra De ahi resaltan los siguientes aspectos. El desarrollo moderno ha dado nueva orientaciòn a los sistemas probatorios. La prueba, como tal, constituye un hecho, que surge de la realidad extrajurídica y del orden natural de las cosas, y se toma como medio para la actuaciòn judicial. Como principales medios de prueba destaca la confesion, documental, pericial -- dictamen de perito --, testimonial, inspecciòn judicial y presunciones --a partir

de culpabilidad o tentativa y complicidad tienen un carácter menos concreto que en la criminalidad clàsica. (9). En consecuencia, se dan muchos ilicitos y pocas denuncias. El delito informático queda inpune.

Bajo estas consideraciones, es posible la elaboración de un plan de fraude informàtico infalible, ya sea para malversación de fondos, chantaje, espionaje, o cualquier otro. El alcance del daño puede ser alto, y, ante la expectativa de grandes beneficios, se pueden coludir personas con acceso autorizado a diversas fases de un flujo de datos, para la comisión del acto y el borrado de toda huella.

Como tercer problema, se destaca que los sistemas informatizados ofrecen facilidades en tiempo y espacio. En fracciones de segundo puede cometerse un acto ilícito y sin necesidad, en muchos casos, de presencia fisica del

---

de un hecho conocido, se concluye la operación lògica de otro hecho. Aunque la mayoria de éstos puede tener relación con el uso de computadoras, la prueba documental es la màs cercana a los soportes magnéticos de registro de datos.

El documento es toda representación material destinada e idónea para reproducir manifestaciones del pensamiento, en forma escrita, fotográfica, copia fotostática, entre otras. Al crecer volumen y complejidad de actividades organizacionales , los documentos escritos han sido sustituidos, debido a razones prácticas, por los medios derivados de las nuevas tecnologias: microfilmes, discos, cintas o tarjetas magnéticas. No obstante, éstos carecen, en la mayoría de los países, de disposiciones jurídicas que incluyan previsiones especificas para su respaldo legal. V. Pp. 117 y 118.

9.- México. Secretaría de Programación y Presupuesto, Instituto nacional de Geografia, Estadistica e Informática: La informática y el derecho: informática jurídica y derecho informático para México.-- México, D.F.: Talleres Gráficos de la Nación, 1983. P. 25.

defraudador. En sistemas de transmisión de datos a sitios alejados, es factible interceptar información durante su traslado o hacer uso ilegal de terminales remotas. (10)

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

10.- Por ejemplo, es el caso de accesos a cajeros automáticos bancarios con tarjetas de crédito o débito robadas o falsificadas.

5.4.- TIPOLOGIA DE LOS RIESGOS INFORMATICOS.

Como complemento de las tres secciones anteriores, de este capítulo, a manera de ilustración, se presenta una tipologia de los riesgos o amenazas que presenta un ambiente informatizado. Se trata de ejemplificar los conceptos de vulnerabilidad, con situaciones prácticas posibles.

Los riesgos informáticos son la variedad de actos disfuncionales que pueden tener lugar en torno a la computación, ya sea ésta medio o fin. El panorama de los riesgos mencionados se presenta con base en fuentes bibliográficas, hemerográficas y casos narrados por diversos expertos o servidores pùblicos entevistados. No se pretende ser exhaustivo a todas las posibilidades. La problemática computacional es extensa y variada. Se busca abordar malos usos y disfunciones, asi como las técnicas para ello, de modo sistemàtico y ofrecer una visión amplia de la vulnerabilidad computacional.

No existe consenso, entre los tratadistas informáticos, acerca de la clasificaciòn de riesgos en un ambiente informatizado. Algunos abordan el tema en trabajos de carácter general y los, pocos, que lo hacen especificamente difieren en sus criterios. Es un area en la que falta mucho por investigar, tipificar y estandarizar. El esquema propuesto en este trabajo toma elementos, en forma selectiva, de varias fuentes.(1)

1.- Se toman elementos de clasificaciones ofrecidas por Tellez, Bria, INEGI, Gonzàlez Castellanos, Sendrow, Vera Vallejo y Van Eck.

Se clasifican los riesgos informáticos en dos grandes apartados. 1) Los riesgos de origen intencional y 2) los riesgos de origen no intencional, o errores y omisiones.

5.4.1.- RIESGOS DE ORIGEN INTENCIONAL.

Esta categoría alude la gama de amenazas de daño o fraude, que puede presentar un ambiente computarizado, por acciones deliberadas de personal de la organización, para

---

De Tellez, op. cit. P.106, clasifica los delitos informáticos en dos criterios: el uso del computador como medio y como fin. No obstante, su apreciación es poco clara al presentar los delitos, como tales, mezclados con las técnicas para ellos. Bria, op. cit. P. 123., utiliza un esquema similar al de Tellez, pero de manera más superficial y simplista. México, SPP, INEGI, op. cit. P.25., tipifica el delito informático tomando como referencia a tratadistas franceses, que utilizan cuatro categorías: robo de tiempo de computadora, manipulaciones diversas de información, sabotaje y divulgación o apropiación de datos confidenciales. González Castellanos, op. cit., presenta cuatro rubros de clasificación: manipulaciones para el delito, clasificación por número de ejecutantes, por naturaleza del delito y errores. Ofrece muchos ejemplos, ilustrativos a sus clasificaciones. No obstante, no vincula sus rubros para ofrecer una visión integral y global del problema. Sendrow, Marvin, op. cit., se centra en el universo de las amenazas que puede tener un sistema de transmisión electrónica de fondos. Divide éstas en amenazas internas en la organización y amenazas externas. Sin embargo, al desarrollar su clasificación, confunde aspectos de muy diverso tipo en el universo informático, al mezclarlos unos con otros: la organización, las instalaciones, los equipos y los soportes magnéticos de almacén de datos. Vera Vallejo, Luis, entrevistado por Morales, Jorge: "Los fabricantes opinan sobre la piratería", en "Computerworld"-(México), año 7, num. 138, abril 13, 1987. Clasifica unicamente los tipos de "piratería" de programas o *software*. Van Eck: "Las radiaciones electromagnéticas han de ser revisadas nuevamente", en "Data Processing Digest" (U.S.A.), vol 15, num. 2, feb. 1987. Se enfoca a los riesgos que presentan para el cómputo las radiaciones electromagnéticas y atañen principalmente a la transmisión de información a sitios remotos.

fines distintos a los que tienen los sistemas de información.

5.4.1.1.- NATURALEZA DE LOS RIESGOS INTENCIONALES.

En primera instancia, estas amenazas pueden ser de diversa naturaleza, según los objetivos de quien los comete. En forma genérica se denominan fraudes. Para efectos analíticos, se determinaron tres esquemas de clasificación, expuestos en el mismo número de cuadros. El cuadro 3 refiere impactos de daño computacional según las funciones sustantivas de las instituciones. El cuadro 4, clasifica también naturaleza de daños informáticos, pero en niveles funciones de apoyo institucional: recursos humanos, finanzas, recursos materiales y servicios de cómputo. El cuadro 5, analiza riesgos o daños posibles, según se afectan derechos de privacia o patrimonio de personas físicas y morales.

La gama de posibilidades de actos maliciosos con la informática supera, con mucho, los ejemplos anotados estos cuadros. En la medida que crece la utilizaciòn de las nuevas tecnologias, crecen las alternativas de uso ilícito de los datos. La computaciòn simplifica procesos y elimina personas en el flujo de los datos. Al no contemplar la posible vulnerabilida de los nuevos sistemas informáticos en operaciòn, estará presente el riesgo. Cuando éste existe, el daño o pérdida o fraude ocurrirá, en algún momento y en algún lugar.

C U A D R O 3

RIESGOS INFORMATICOS DE ORIGEN INTENCIONAL
Clasificacion segun la naturaleza de la institucion
(Algunos ejemplos)

TIPO DE INSTITUCION	EJEMPLOS
Bancaria	Reduccion de saldos de cuentas sin movimientos. Aplicacion de tasas de interes ilegales. Sustraccion de excedentes de operaciones de redondeo. Ingreso ilegal de transacciones. Otorgamiento de creditos ilegales.
Comercial	Otorgamiento de descuentos o bonificaciones no permitidas. Salida de mercancia sin facturar. Venta a precios no autorizados. Venta ilegal de directorios de clientes.
Industrial	Manipulacion de secretos o formulas o procedimientos de fabricacion. Divulgacion de informacion sobre nuevos productos.
Dependencia publica	Circulacion ilegal de informacion confidencial sobre aspectos internos a favor de intereses ajenos. Manipulacion de informacion relevante a la seguridad nacional. Manipulacion de informacion en sistemas de servicios al publico, licencias, ejercicio de derechos, etc.
Organismo electoral	Manipulacion de padrones electorales. Manipulacion de computo de votos.
Academico	Aprobacion ilegal de materias. Aprobacion ilegal de examenes de admision. Emision de documentos de certificacion falsos.
Militar	Espionaje.

C U A D R O 4

RIESGOS INFORMATICOS DE ORIGEN INTENCIONAL
Clasificacion segun funciones de apoyo institucional.

FUNCION	EJEMPLOS
Administracion de Recursos Humanos.	Alta de servidores inexistentes. Ex-empleados o fallecidos no dados de baja. Alteracion de computo de horas trabajadas. Alteracion de monto de compensaciones.
Administracion de Recursos Financieros.	Manipulacion de pagos a proveedores o acreedores. Malversacion de fondos institucionales.
Administracion de Recursos Materiales.	Alteracion del registro de inventarios.
Administracion de Servicios de Computo.	Utilizacion de tiempo de computadora para beneficio personal. Destruccion o alteracion de programas o datos.

C U A D R O 5

RIESGOS INFORMATICOS DE ORIGEN INTENCIONAL.
Clasificacion segun afectacion de derechos o patrimonio de las personas fisicas o morales.

DERECHO AFECTADO	EJEMPLO
Danos a la propiedad informatica.	Afectacion de derechos de autor por circulacion ilegal o pirateo de programas. Destruccion o sabotaje a datos o programas.
Danos a la privacia del individuo.	Trafico ilegal de directorios. Transferencia de informacion sobre vida privada del individuo. Manipulacion de datos para chantaje, presion o intimidacion.
Danos a la privacia de los institutos.	Sustraccion de informacion institucional para negociar con terceros. Espionaje.

5.4.1.2.- INTERVENCION DE LA COMPUTACION EN LA COMISION DE ACTOS ILICITOS.

En el análisis del papel que juega la computación, para llevar a cabo un acto dañino intencional, se hace distinción de dos categorías: 1) cuando la computación es el medio para el delito y 2) cuando la computación es el fin del delito.

5.4.1.2.1.- USO DE LA INFORMATICA COMO MEDIO DE COMISION DE ACTOS ILICITOS.

En ésta categoría se inscriben los actos maliciosos que se valen de la informática como método o medio. Medio que puede estar a disposición de dos tipos de personas: personas ajenas a la organización o personal propio de ella.

5.4.1.2.1.1.- MEDIOS DE PERSONAS AJENAS A LA ORGANIZACION.

En este apartado se hace referencia a diversos medios o manipulaciones que pueden efectuar personas ajenas a una institución para cometer daños o fraudes contra ésta, según ejemplifica el cuadro 6.(2)

2.- Para la intercepción en teleproceso de datos. V. Bria, op. cit. P.122. Ello con el fin de captar mensajes de terceros o ingresar información para desvirtuar comunicaciones o alterar archivos. Este ha sido el medio que más daño ha causado en los Estados Unidos de América, en cuanto a montos de pérdidas en sistemas de transferencia electrónica de fondos.

Van Eck, op. cit. Pp. 85 a 92. El autor describe experimentos efectuados en la intercepción de información radiada en las tres formas indicadas. Menciona que las disposiciones legales existentes, (se refiere, por supuesto a los paises más desarrollados) hacen alusión al mal uso de la informática con presencia física en las instalaciones de cómputo o las terminales del usuario legítimo. Pero no hay alusióna la recepción remota de datos por personas no autorizadas. Refiere que los requerimientos técnicos para estas intercepciones pueden ser dispositivos cuyo valor de

C U A D R O 6

MEDIOS AL ALCANCE DE PERSONAS AJENAS A LAS INSTITUCIONES PARA LA COMISION DE ACTOS ILEGALES

MEDIO	CASOS EJEMPLO
A traves de mecanismos de acceso a los sistemas computacionales.	Trajetas plasticas extraviadas o robadas o falsificadas. No actualizada de terminales o dispositivos informaticos.
En teleproceso de datos.	Intercepcion, acceso y/o captura de datos en puntos intermedios de transmision electronica.
Acceso a informacion radiada.	Captacion en telecomunicacion sin hilos, a traves de antenas. Captacion de ondas propagadas por hilos telefonicos mal protegidos o mal aislados. Captacion de emisiones electromagneticas de monitores o pantallas.

5.4.1.2.1.2.- MEDIOS DEL PERSONAL INTERNO.

En el ámbito de los medios para la comisión de actos ilicitos, destaca la conducta del personal de las areas informatizadas. Es tal vez, el eslabòn màs débil en un sistema informàtico y de la seguridad propia. De la conciencia y responsabilidad, en el ejercicio de las funciones, que tiene asignadas el personal, depende el éxito o fracaso de la aplicaciòn de la operación de las computadoras y los mecanismos de seguridad previstos, ya sean de tipo técnico o de tipo administrativo.

---

mercado oscila entre los 35 y los 50 dólares. Por lo tanto constituye un medio accesible y seguro ante el mal uso en la informática. Se trata de uno de los aspectos más recientes que se han atendido en el campo de la seguridad informática y, a su vez, el más desprotegido legalmente, a nivel mundial.

Todo sistema de información presenta vulnerabilidad *per se* ante el desempeño del personal operativo, directivo y, en su caso, de la honestidad y capacidad técnica de quien inspeccione la seguridad o efectúe auditoría. Ello ya se constata con los ejemplos mencionados en los cuadros ofrecidos en este capítulo. Algunas de las conductas riesgosas, que puede tener el personal son las siguientes.

- Indiferencia o apatía ante las medidas de protección y control.

- Exponer los medios de seuridad internos, a personas ajenas a la organización, que podría derivarse en accesos activos o accesos pasivos a los datos. (3)

- Duplicación de archivos o cintas magnéticas que contengan información crítica o confidencial, sin control. Por ejemplo, en una institución bancaria se podrían emitir copias de archivos con números de cuenta y NIP's, para usos fraudulentos.

Una tipología de medios prácticos para la comisión de actos ilícitos, por parte del personal interno de las organizaciones, se presenta en el cuadro 7.

3.- El acceso activo se refiere a alterar, borrar o introducir datos. El acceso pasivo consiste sólo en leer información.

C U A D R O 7

MEDIOS AL ALCANCE DEL PERSONAL INTERNO DE LAS INSTITUCIONES PARA LA COMISION DE ACTOS ILEGALES

NIVEL O FASES DE SISTEMAS	TECNICAS	EJEMPLOS
a) En captura de datos	Ingreso de datos o mensajes desvirtuados.	Emision o alteracion de captura de transacciones.
b) En proceso de datos	Aprobacion y proceso fraudulento de operaciones o transacciones.	No deduccion o aplicacion a cuentas. Aplicacion a cuentas falsas. Transacciones con cuentas inexistentes. Autorizacion fraudulenta de emision de tarjetas de credito o tarjetas de acceso.
c) En software o programas	Cambios clandestinos en programas.	Generacion de programas "parche" para manipulaciones ilicitas de datos.
	Tecnica "caballo de troya"	Variante del anterior. Consiste en correr ciertos programas al cumplirse una condicion predeterminada.
	Tecnica "puertas trampa"	Introduccion de puntos debiles en un sistema, con objeto de eludir controles normales y facilitar accesos.
d) En los archivos de datos	Cambios de datos en bancos de informacion por personal que tiene acceso a ellos y conoce su estructura.	Cambios de titular de cuentas o beneficiarios. Malversacion de fondos de cuentas abandonadas.

Un aspecto que merece especial atenciòn, es el referente a la reproducciòn y circulación ilegal de programas --también conocida como "pirateria de *software*"--, merece atención especial. Vera Vallejo reconoce tres niveles en los que se desarrolla ésta. (4)

4.- Morales, Jorge, op. cit.

1) El vendedor ofrece al cliente copias de programas, con objeto de incentivar el cierre del negocio.

2) A nivel organizacional, la dirección permite que de un paquete original se obtengan copias para todos los usuarios bajo su responsabilidad. Ello con la intención de ahorrar dinero.

3) Intercambios entre instituciones o entre éstas y particulares o entre particulares mismos.

La "piratería" de programas atenta contra la seguridad informática de diversos modos.

a) Se pierde el control sobre qué equipos utilizan qué *software* y para qué.

b) Se desconoce si los paquetes están completos, son auténticos, si están adulterados o no y si están contaminados con "virus" informático. (5)

c) Se carece de documentación adecuada para los programas.

d) Las copias ilegales carecen de todo respaldo y garantía por parte del fabricante.

e) El *software* obtenido ilegalmente, así como las aplicaciones que se desarollen con base en éste, carecen de toda seguridad jurídica. En el caso de éstas, no podrán inscribirse en el Registro Nacional de Derechos de Autor, al provenir de lenguajes o programas de dudosa autenticidad.

f) Se fomenta la proliferación de "virus" computacional.

5.- V. infra. Los "virus" se tratan más detalladamente en la sección 5.4.1.2.2.

5.4.1.2.2.- LA INFORMATICA COMO FIN DE ACTOS ILICITOS.

Esta categoría se refiere a las conductas maliciosas que se dirigen contra las instalaciones, los equipos y los accesorios, como entidades físicas y contra los programas o información, en su integridad. En éste caso, la computación ya no es medio criminógeno, sino fin en sí mismo. Corresponde a los fraudes o daños contra la propiedad informática. (6)

La categoría del daño informático como fin en sí mismo no atañe exclusivamente a la destrucción de recursos informáticos por la simple razón de destruirlos. Por lo general, al afectar un sistema o ambiente computarizado, se hace con otros fines, (políticos, terroristas, etc.) pero el daño es directamente en lo físico o en la integridad o confidencialidad de los datos. Los tratadistas franceses denominan "sabotaje" este aspecto. Se refieren a afectar sistemas de información de tal modo que una organización se dañe, paralice o desaparezca.(7) El cuadro 8 ofrece una clasificación del sabotaje, según nivel de afectación.

El resultado del impacto, tiene lugar en dos frentes: a nivel físico y a nivel lógico. Lo ilustra el cuadro 9. (8)

6.- V.supra., en el apartado de la naturaleza de los actos intencionales de riesgo informático. Sección 5.4.1.1.
7.- México, SPP, INEGI, ibid.
8.-Un medio para la programación de instrucciones que provocan bloqueo de sistema es la técnica "Caballo de Troya" arriba referido, pero en este caso se programa para afectaciones definitivas.

C U A D R O 8		
NIVELES DE AFECTACION DE SISTEMAS DE INFORMACION: SABOTAJE		
Sabotaje:	Secuestro	Toma temporal de centros de compu para presion politica, economica, chantaje o pago de rescate.
	Dano parcial	Afectaciones en sistemas, reparab en tiempo previsible.
	Destruccion Total	Poner fin a instalaciones, equipo o dispositivos.

C U A D R O 9	
TIPOS DE IMPACTO EN SISTEMAS DE INFORMACION CUANDO SON FIN DE ACTOS ILICITOS	
Nivel fisico:	- Atentado contra instalaciones que alojan equipos. - Dano a equipos de proceso. - Danos a accesorios perifericos (conexiones, lineas de transmision, terminales, impresoras). - Destruccion, robo o secuestro de medios magneticos de almacenamiento.
Nivel logico:	- Programacion de instrucciones que provocan bloqueo parcial o definitivo en un sistema. - Destruccion de archivos de datos sin destruir el medio natural que los soporta. - Introduccion de virus informatico.

Por su creciente importancia, vale prestar atenciòn con mayor profundidad a este último. Los "virus" o "programas virus" son conjunto de instrucciones que penetran ilegalmente los sistemas de cómputo. En esencia de los "virus" informàticos consisten en pequeños programas diseñados para autorreproducirse y propagarse rapidamente. Alunos de ellos lo hacen a grandes velocidades, destruyendo toda información a su paso. En los medios magnéticos se esconden en los sitios menos accesibles y entran en acciòn al darse una determinada condiciòn. Esta puede ser una fecha, una instrucciòn de copiado, o, simplemente, el encendido de un equipo o la carga de un disco. Lo hacen de dos formas: a través de discos o medios magnéticos, "contaminados" con esos "virus" o a través de las lineas de teleproceso de datos. En el primer caso, los "virus" son introducidos para efectos terroristas, vandalicos o para protección contra la "piratería" de programas.(9) En el caso de las lineas de comunicaciòn, el "virus" sale del equipo de cómputo de su creador y se propaga por las redes públicas de telefonia o de teleproceso hasta penetrar en los equipos adscritos a ellas. Para penetrar en las victimas, se violan los controles de acceso a través de diversos medios

9.-Algunos productores de *software* han creado los "virus" para evitar la circulaciòn ilegal de éste. Estos se activan al intentar efectuar copias no permitidas. En general, esta clase de "virus" se propaga según circulan los discos que los contienen.

técnicos.(10) La diferencia màs importante, con la transferencia a través de las lineas de comunicación es que por medio de este último se han provocado impactos masivos en cuestión de horas o dias, en los Estados Unidos, principalmente, y su control se ha hecho sumamente dificil.

No todos todos los "virus" conocidos son totalmente destructivos.(11) Algunos son relativamente benignos: interrumpen el trabajo en una microcomputadora o terminal para desplegar mensajes de algún tipo -- casi siempre

---

10.- El más usual es el de los "virus" que generan aleatoriamente, sin detenerse, diversos tipos de claves, hasta que aciertan el adecuado y penetran.

En los Estados Unidos se calcula que en los primeros 9 meses de 1988 fueron afectados, alrededor de, 250,000 computadores, de todos los tamaños, por los "virus". Y se reconoce que, una vez que surge una "enfermedad electrónica", alcanza rapidamente proporciones epidémicas. En los Estados Unidos, al menos, existen millones de puntos de entrada y salida de datos en grandes redes. Eventualmente, se pueden afectar seriamente los sistemas màs vitales. Hasta ahora éstos han estado exentos de "virus". Ni los sistemas de transferencia electrónica de fondos, esenciales para el sector financiero, ni las bolsas de valores ni las instituciones de seguros ni los sistemas de tráfico aereo ni los militares han sido dañados. No es el caso, por ejemplo de la CIA o el FBI (Central Intelligence Agency y Federal Bureau of Investigation), que ya sufrieron ataques. Eso lo refiere Elmer-De Witt, Philip: "A virus epidemic strikes terror in the computer world",en "Time" (U.S.A.), Vol. 132, No. 13, 26 sept. 1988. Pp. 30 a 32.

11.- Hasta ahora no se puede hablar de la creación de estos programas por organizaciones terroristas. El único caso, ampliamente difundido, es el del "virus" diseñado para destruir toda la información en la "Jerusalem Hebrew University", en los Estados Unidos de Norteamérica. El "virus" fue destruido a tiempo y se le erradicó antes de atacar. El dia que se conmemoraba el 40 aniversario de la fundación del Estado de Israel, el "virus" atacaría. Este caso lo mencionan Elmer de Witt, op. cit. P. 31 y Mc Lellan, Vin: "Computer systems under siege", en "EDP Audit Journal", Vol. III, 1988. P. 31.

pacifistas -- (12) o despliegan figuras en movimiento, (13) por ejemplo, sin dañar información. Otros causan bloqueos en los sistemas, parciales o temporales.(14)

La problemática que presenta esta tipo de programas es relativamente nueva. Aparecieron alrededor de 1986, pero fue en 1988 cuando se presentó su extensión masiva. Se han desarrollado programas "antivirus", mejor conocidos como "vacunas", pero ninguna de ellas cubre todo el espectro de posibilidades tecnológicas de "virus", por mucho. La investigación para un adecuado control de éstos constituye un importante reto a corto plazo.

5.4.2) RIESGOS DE ORIGEN NO INTENCIONAL O ERRORES Y OMISIONES.

Se trata de los daños en un medio omputarizado provocados de manera involuntaria. Sus causas primarias son la falta de conciencia informática, sensibilidad y responsabilidad por parte del personal que labora en las distintas fases del procesamiento electrónico de datos. Ellas fomentan actitudes de descuido, falta de comunicación, falta de precaución, apatía e indiferencia hacia la búsqueda

12.- Ejemplo de ello es el "Peace Virus", difundido en los Estados Unidos. V. Elmer-De Witt, Philip, op. cit. P. 34.
13.- Por ejemplo el virus "ping-pong", que consiste en una pequeña pelota que barre los monitores, pero sin dañar información.
14.- Para una mayor comprensión de la problemática de los "virus" informáticos v. los siguientes. Merino, Marco Antonio: "Virus informático", s.p.i., mimeo, 1988. (presenta una clasificación de los "virus" conocidos). Buerger, David J.: "Detecting and combating computer viral infections" en "Infoworld" (U.S.A.), March 21, 1988. P. 14. En la misma, v. Johnston, Stuart: "Computer virus spreads to commercial software".

de seguridad, eficiencia y productividad, en los sistemas de información.

Los daños involuntarios pueden clasificarse en diversas categorías, según el cuadro 8. (15)

Del panorama presentado, de los riesgos informáticos, se desprende la seguridad computacional como problemática que no se resuelve con medidas de protección y control aisladas. Es materia de consideración plena por parte de la administración de las organizaciones y su solución requiere trabajo conjunto de especialistas en recursos humanos, en ingeniería de cómputo, en leyes, entre muchos otros. El siguiente capitulo se destinará a exponer un marco analítico para comprender y abordar la seguridad informática de manera integral y fundamentar el esquema de administración de la seguridad propuesto, en la parte complementaria de este trabajo.

15.- Gonzalez Castellanos, op. cit. Pp. 50 a 53. El autor presenta esta clasificación, que damos por válida, pero la descripción de cada categoría es propia.
Para consulta de los atributos de la información, V. Supra. Capitulo 1.

C U A D R O 10

CLASIFICACION DE DANOS INVOLUNTARIOS EN SISTEMAS DE INFORMATICA (ERRORES U OMISIONES)

DANOS GENERICOS	CASOS	EJEMPLOS
Errores administrativos. Conciernen a inadecuada toma de decisiones.	En las politicas hacia el personal.	- Cuando este maneja inadecuadamente informacion confidencial y hay fugas de datos.
	En la Jerarquizacion de la informacion.	- Cuando no se valora la importancia o confidencialidad de los datos y se les desprotege.
	En la seleccion de personal.	- Se reclutan servidores no aptos para operar o disenar sistemas.
	En la asignacion de responsabilidades.	- No se obliga a nadie a velar por el cuidado y respaldo de datos.
Errores en las instalaciones.	Imprevision de localizacion de centros de computo.	- Vulnerabilidad de danos por agentes naturales o artificiales.
	Descuido de instalar sistemas de proteccion.	- Se omite instalar equipo de deteccion y control de fuego, humedad, temperatura u otros.
	Descuido en diseno de controles de acceso de personas a las instalaciones.	
	Errores en el proceso de instalacion de equipos.	- Malas conexiones electricas o protecciones inadecuadas en lo electrico.
Errores en el "hardware". Conciernen al funcionamiento de los equipos y accesorios.	En la ingenieria de los equipos. Son poco frecuentes y se detectan tan pronto se pone en marcha un computador o accesorio. Las correcciones corresponden al fabricante.	
	Errores de operacion.	- Bloqueos de comunicacion por mala sincronizacion entre emisor y receptor.
Errores en el "software". Conciernen a paquetes o lenguajes con los cuales se desarrollan programas de aplicacion.	Operacion de lenguajes o paquetes sin control de calidad adecuado.	- Desvirtuacion o dano de informacion al ser manejada por software inadecuado.
	Operacion de paquetes sin capacitacion suficiente al usuario.	- Dano al mismo paquete o a los datos por mala capacitacion al usuario.
Errores en programas de aplicacion.	Mal diseno o desarrollo de programas.	- Programas creados y puestos en operacion con presion de tiempo e imprevision. Hay fallas en planeacion, diseno o liberacion del sistema o programa. Provoca su mal funcionamiento, obsolescencia y no cumple objetivos requeridos. Se desvirtuan los datos.

DAÑOS GENERICOS	CASOS	EJEMPLOS
Errores de operacion. Metodos y procedimientos erroneos en las rutinas de trabajo.	Borrados accidentales.	- En programas. - En archivos de datos.
	Duplicacion u omision de captura de datos.	
	Carga de cintas o discos, erroneos.	- Se usan soportes magneticos inadecuados o equivocados por estar mal almacenados o etiquetados
	Uso de archivos de datos no actualizados.	- Se desvirtua la informacion.
	Descuido o negligencia de respaldar informacion.	
	Errores u omisiones en el seguimiento de las rutinas de trabajo por mala comunicacion al ocurrir rotacion de personal.	

CAPITULO 6.- MARCO ANALITICO PARA LA SEGURIDAD INFORMATICA INTEGRAL.

Las bases teóricas para la seguridad informática son escasas. A nivel mundial, pocos investigadores han abordado el problema de manera integral. No obstante, son más frecuentes los articulos, ponencias o secciones en obras de carácter más general, que abordan aspectos específicos de la salvaguarda de los datos. Casi siempre, estos trabajos se desprenden de experiencias adversas que han tenido todo tipo de organizaciones en los paises màs desarrollados.

En concepción amplia, la seguridad computacional procura la protección de los activos informáticos y la integridad y confidencialidad de los datos. La problemática derivada, como se ha reflejado de las secciones anteriores, es sumamente amplia. Involucra practicamente todos los aspectos relacionados con las tecnologias modernas de proceso de datos: marco juridico, normas y políticas institucionales, métodos y procedimientos administrativos, estudios de viabilidad de equipos y programas, los equipos y el soporte lógico mismos, la información, instalaciones, entre muchos otros.

La seguridad informática puede concebirse desde varias categorias de análisis. (1) La de uso más frecuente, divide en dos grandes campos esta materia: seguridad fisica y seguridad lógica. La primera se ocupa de la protección de

---

1.- Recogidos durante las entrevistas con expertos en informática. Fueron descritos verbalmente por ellos.

locales, equipos e instalaciones, tanto en la prevención de desastres naturales -- fuego, sismos, humedad, etc. --, como el control de acceso a los mismos, las terminales y los medios magnéticos de almacenamiento. La segunda se refiere a la seguridad en operación de programas y de información en fases de captura, procesamiento, accesos de consulta, alteraciones duplicaciones o borrados.

Otro enfoque, es un planteamiento en doble vertiente: la seguridad desde el punto de vista de las instituciones y la seguridad desde el punto de vista de las personas. Las instituciones buscan en la seguridad la garantía de valores de integridad y confidencialidad de la información, así como la continuidad en sus operaciones computacionales. Se buscan medios para que la información no sea manipulada erróneamente o ilegalmente. Las personas, por su parte, buscan la salvaguarda de sus derechos de privacía, en las informaciones que les conciernen y que poseen las instituciones.

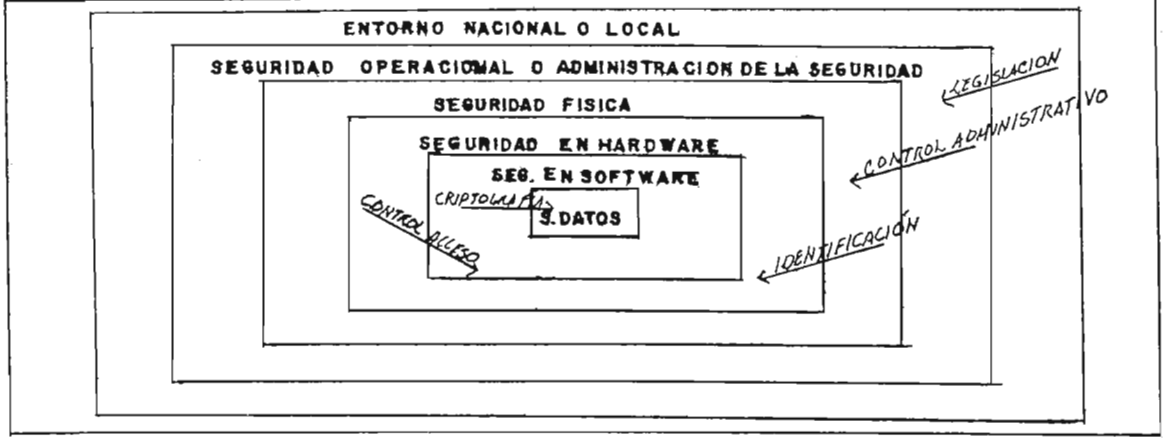
El modelo teórico, seleccionado para fundamentar este estudio es el propuesto por David Hsiao, en su obra "Computer Security" (2). Este autor reconoce que la seguridad informática es un problema cuya solucion implica la atención de todos los elementos que intervienen en la

2.- Hsiao, David; Douglas Kerr y Stuart Madnick: "Computer security".-- San Francisco: Academic Press, 1979. Es la única obra encontrada, durante la fase de investigación bibliográfica, que se extiende sobre todos los ámbitos en que está inmersa la seguridad informática. Presenta un marco teórico que describe la problemática integral en esta materia, a pesar de ser publicada en 1979.

aplicación de la computación. Es decir, que para una correcta solución de la problemática de la seguridad es necesario considerar aspectos jurídicos, de administración informática, de operación de equipo, de instalaciones, de programas y de los propios archivos de datos, todos ellos como problemas específicos a resolver. Propone un marco en el que diferencia, como niveles, los aspectos anteriores y busca identificar los recursos que posibilitan la seguridad para cada nivel.

El modelo de Hsiao se presenta esquematizado, en la figura 1.

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.

Este modelo implica los siguientes supuestos.

-- La seguridad informática se logra de manera óptima cuando se resuelve el problema en todos los niveles.

-- Para cada uno de los niveles se tienen recursos específicos para proveer seguridad.
-- Los niveles son interactuantes entre sí, en el sentido de que la seguridad en un determinado nivel es requisito para el óptimo funcionamiento de los recursos de protección y control de los niveles concéntricos inscritos en él. En otras palabras, en la medida que existe seguridad en un determinado circulo, o nivel, es viable que exista en los niveles inscritos en él. Es importante señalar que de cada uno de los niveles no solo se apoya la seguridad del nivel inmediato concentrico, sino de todos los inscritos en él.

De modo más ilustrativo, el modelo supone que una adecuada seguridad en el nivel de entorno nacional o local facilita la existencia de la seguridad operacional. De este nivel se desprenden medidas legislativas hacia la operación informática de las organizaciones. Esto apoya y norma la seguridad operacional o la administración de la seguridad. De ésta emanan controles administrativos que regulan la seguridad física -- y la seguridad sobre los niveles concéntricos a éste -- y asi sucesivamente. El desarrollo de cada uno de los niveles se presenta en las siguientes secciones de este capítulo.

Es necesario señalar que el trabajo de Hsiao es el más adecuado que se encontró para comprender con amplitud el problema de la seguridad informàtica. No obstante, desde la óptica de los objetivos de este trabajo, presenta algunos puntos débiles. Estos radican en la falta de mayor

consideración hacia los aspectos de administración de la seguridad. El capitulo al respecto, en ese trabajo, aborda diversos rubros que son importantes en la gestión de planeación, organización, dirección y control. Pero no los vincula sistematicamente para ofrecer un esquema administrativo, aplicable a todo el entorno informático. Asimismo, no considera suficientemente la auditoria informática --instrumento fundamental de evaluación de operación computacional y su seguridad-- y omite el tema de la planeación de recuperación para casos de desastres mayores o menores en un ambiente informatizado.

6.1.- ENTORNO NACIONAL O LOCAL.

Con base en la situación económica, social, política y cultural de un pais o localidad, las aplicaciones computacionales ejercen impacto sobre la vida de las personas y el funcionamiento de los organismos. El instrumento para apoyar el adecuado desarrollo informático de la sociedad es el establecimiento de un marco legal, aplicable a las nuevas tecnologías y su utilización. Ello da como resultado la normatividad para recabación y diseminación de datos, derechos de los individuos y de las personas morales, tipificación de actos delictivos y penalidades. Todo ello, proporciona las bases para determinar políticas de utilización de computadoras, comunicaciones y el desarrollo informático nacional.

6.2.- LA SEGURIDAD OPERACIONAL O ADMINISTRACION DE LA SEGURIDAD.

La legislación fundamenta y da seguridad jurídica a las aplicaciones computacionales. Ello permite que la administración de las organizaciones ejerza control y sea responsable por el funcionamiento de las unidades de informática a su cargo. La administración de la seguridad o seguridad operacional, adopta politicas de operación, que se derivan en métodos y procedimientos aplicables al desarrollo de sistemas o programas; al flujo de la información, desde su origen hasta su destino final; a las rutinas de respaldo; al almacenamiento de la información y, en general, a 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 base en el conocimiento de los grados de exposición a amenazas de utilización ilegal de los datos, se establecen prioridades de protección. Medios más sofisticados 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 preveer 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.

La gestión de la seguridad operacional se completa con la integración de soportes documentales, que plasman las prevenciones de protección y control en manuales de organización, manuales de procedimientos, manuales de descripción de puestos, manuales de usuario o manuales técnicos de los sistemas de cómputo y de los mecanismos de seguridad y los planes de recuperación informática en casos de desastres. El trabajo, en los siguientes capitulos, se destina a profundizar la seguridad operacional o administración de la seguridad.

6.3.- SEGURIDAD FISICA.

A la seguridad física le conciernen dos aspectos basicos. 1) El control de acceso de personas a instalaciones de cómputo o a sitios que albergan terminales u otros dispositivos. Se apoya de los controles administrativos, emitidos en el nivel de seguridad operacional. 2) La protección de equipos, instalaciones y dispositivos magnéticos --en lo fisico-- contra desastres naturales o acciones maliciosas de destrucción. Se preveen aspectos técnicos de ubicación, instalación, prevención y detección de fuego, protección contra humedad o inundaciones, controles de temperatura, iluminación, salidas de emergencia, entre otros.

6.4.- SEGURIDAD EN *HARDWARE*

El *hardware* consiste en los equipos de procesamiento de datos o los computadores como tales, con todos sus dispositivos de comunicación, almacenamiento de datos, visualización, impresión, etc. La primera cuestión, en este ámbito, es el acceso al equipo de cómputo. Este se efectúa mediante mecanismos de identificación o autentificación. El usuario establece su identidad, se autentifica que es él mismo y que está operando una terminal autorizada para él. Según Hsiao, los mecanismos de control pueden ser por: 1) algo que el usuario sabe (claves de acceso o preguntas de tipo personal, que hace el equipo, por ejemplo), 2) algo que el usuario lleva consigo (tarjetas magnéticas, llaves, etc.), 3) vía características físicas (huellas digitales, identificación de la geometría facial o de la mano, configuración de la retina del ojo) y 4) por algo que el usuario puede hacer (autentificación de su firma).(3) Los dos primeros son los más usuales y extendidos en el mercado. Los dos últimos son de mayor sofisticación, de alto costo y uso en sistemas muy críticos o confidenciales.

Para el nivel de seguridad en *hardware* y los dos siguientes --seguridad en *software* y en los datos-- la protección se proveé en la operación de los propios sistemas de información. Una vez ganado el acceso físico, entran en juego controles más técnicos que administrativos.

3.- Este no es mencionado por Hsiao.

En el nivel *hardware*, se cuenta, entre otros, con los siguientes recursos de protección.

1) Protecciones en la memoria del equipo. Se controla el acceso del usuario a las areas de memoria, a través de claves que permiten la utilización de unos o varios segmentos de la información grabada.

2) Rutinas de ejecución múltiple. Permiten que ciertos programas corran simultáneamente a nivel usuario y a nivel supervisión -- ésto tiene lugar cuando personal, que cuenta con privilegios de acceso, audita el desarrollo de ciertas funciones o programas o cuando los mismos programas cuentan con jerarquias en sus rutinas para que programas de mayor nivel tengan prioridad sobre los de menor nivel.

3) Microprocesadores -- que son dispositivos para efectuar los procesos de datos. En materia de seguridad, se pueden ubicar entre los canales de entrada y salida de datos y la memoria principal, para controlar accesos a ésta. Se programan de tal modo que operen como procesadores especializados, que permitan un post-procesamiento de datos para regular su salida o acceso a los dispositivos de memoria.

4) Los minicomputadores, que pueden constituirse como equipos de control y rastreo de transacciones o procesos en general.

6.5.- SEGURIDAD EN *SOFTWARE*.

El *software* es todo tipo de programas de computo para efectuar procesos de datos. Se pueden distinguir dos tipos principales: programas fuente y programas de aplicación. Los primeros son los conocidos como lenguajes o paquetes de programación. Ellos constituyen una serie de instrucciones, bién integradas, para facilitar la comunicación entre el programador y los elementos electrónicos de las computadoras. En esta categoria se pueden incluir lenguajes como "pascal", "cobol", "fortran", "C", entre otros; y paquetes como bases de datos y hojas electrónicas. Los programas de aplicación se desarrollan para efectuar procesos especificos con archivos de datos. Ellos son, por ejemplo, los programas para manejo de nóminas, contabilidad, estadistica, etc.

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. En el caso de los programas fuente, el problema lo resuelven los fabricantes. En los programas de aplicación, corresponde a los propios analistas o programadores de la institución.(4) Un *software* seguro es

4.-La excepción a ello es cuando en esta última se programan aplicaciones en lenguaje de màquina, o lenguaje ensamblador. Ahi se borra la frontera entre los dos tipos de programa citados. Se pueden citar varios pasos para un adecuado desarrollo de sistemas. Primero, se necesita establecer un método de diseño, con objeto de que los programas sean seguros en sus resultados. Esto requiere el trabajo en equipo de los futuros usuarios, con el personal informático de programación y los administradores. Se

esencial para la operación de mecanismos técnicos de seguridad, entre los que podemos citar dos tipos: los que se basan en vigilancia y control -- como son las claves y controles de acceso -- y los que se basan en aislamiento -- para ciertas aplicaciones o procesos se definen y aislan ciertos equipos o terminales. (5)

---

establecen requerimientos para los usos y procesos de datos, los controles y las prioridades. Segundo, se verifica y prueba que los programas desarrollados son, en realidad, los proyectados. (4) Tercero. Se ponen en marcha los sistemas y se efectuan evaluaciones periódicas para retroalimentación en la instrumentación de mejores y más eficientes procesos y controles.

5.- Vigilancia y control, así como aislamiento son terminos traducidos literalmente de los conceptos de Hsiao: "surveillance", el primero y "isolation", el segundo. V.Ibid. P.4.

6.6.- SEGURIDAD EN LOS DATOS.

La esencia de esta categoría es que en la medida que se requiere integridad y mayor confidencialidad, debe proveerse seguridad. 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 y con qué datos" -- a través de controles de acceso al usuario. (6)

En el primer aspecto existe la criptografía como medio de protección. Esta consiste en técnicas de codificación de la información con objeto de hacerla ilegible a los accesos no autorizados. Las formas más usuales son la trasposición de caracteres y las sustituciones. Trasposición se refiere a intercambiar de lugar. Sustitución es cambiar unos caracteres por otros. Para este proceso de determina una tabla de referencia, para efectuar la operación de codificación de un modo controlado. En la tabla se precisa una secuencia de intercambios o sustituciones para un agregado de datos. La traducción a la forma original de los datos, o decodificación, se hace tomando la misma tabla como referencia. Las claves de codificación son guardadas y controladas por los usuarios autorizados de la información, bajo diversas formas: tarjetas con banda magnética que contiene la tabla o discos flexibles, por ejemplo. Las mismas claves son modificadas con regularidad predeterminada para un mayor aseguramiento. Estas deben ser lo

6.- Ibid.

suficientemente confiables, de tal modo que los mensajes o la información no sufra daño o alteracion alguna, al ser decodificada. (7) Esto es importante, particularmente, en la información numérica o financiera. Un error en un dígito puede causar daños importantes.

En el segundo aspecto, en la determinación del usuario y las funciones que puede 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. Otro requisito es que el sistema de información sea capaz de delimitar, dentro de los datos permitidos a cada usuario, qué tipo de operación éste puede hacer con ellos: lectura, captura, modificación, borrado o listado.

La adecuada organización en los almacenes de memoria de los computadores es fundamental para ejercer controles. Al dar formato a los datos con cadenas de caracteres, campos, tablas, registros, archivos y bases de datos, es decir, en unidades lógicas de guardado de información, se facilita el proceso de segmentación y protección de cadenas. (8) El uso de éstas unidades lógicas permite la definición de los distintos niveles o tipos de información, según su

---

7.- En 1977, el gobierno federal de los Estados Unidos de América aprobó el "Data Encription Standard" (DES), para la protección de información confidencial, no militar. Su uso se ha extendido, por el mundo, de tal modo que en la actualidad es la norma de criptografía más utilizada.

8.- Segmentación significa identificación y separación de los agregados de datos, autorizados para cada usuario o tipo de usuario.

confidencialidad. La determinación de estos niveles parte de las politicas establecidas en la institución. En la medida que haya mayor claridad en este aspecto, puede ponerse en práctica una gama de controles idónea a las necesidades de la organización.

Una última consideración en la seguridad de datos jerarquizados reside en su almacenamiento físico. Idóneamente, las informaciones con similar nivel de importancia o sensitividad se deben guardar en el mismo dispositivo magnético -- cinta, disco o tarjeta. El acceso a datos con un determinado requerimiento de privacia no debe envolver acceso a datos con otros requerimientos.

CAPITULO 7.- LA PROBLEMATICA DE LA SEGURIDAD INFORMATICA EN LA ADMINISTRACION PUBLICA FEDERAL DE MEXICO.

La seguridad informática está poco atendida en la Administración Pública Federal de México, tanto en dependencias como en entidades. Varios factores lo explican. Primero, la utilización de computadores continúa en etapa de introducción. Si bien muchos organismos cuentan con equipos informáticos, desde hace más de una década, ante los cambios tecnológicos y extensión de aplicaciones, el parque computacional ha aumentado continuamente y se han sustituido equipos obsoletos. Segundo, la sociedad mexicana está lejos de alcanzar un nivel cultural, que se preocupe por la salvaguarda de privacidad en manejo de información y vele por la utilización y control racional de los recursos informáticos. Tercero, los administradores de centros de cómputo, asi como el personal de operación y desarrollo de sistemas, desconoce la dimensión de la seguridad informática. Cuarto, el personal público rara vez asume el buen uso y control de la información que dispone. Prevalecen actitudes de indiferencia, insensibilidad, irracionalidad, pereza, falta de previsión y de responsabilidad con la ciudadania e instituciones a las que sirven.

Estas son las conclusiones generales de una investigación exploratoria desarrollada en muchos organismos públicos. Se efectuó con base en 50 entrevistas, con personal que administra o participa en unidades de informática o en areas que cuentan con recursos computacionales para su operación,

y con responsables de auditoria o seguridad --en los organismos que contaron con unidades administrativas para estos fines.(1) Adicionalmente, se escuchó a especialistas que sirven en despachos privados, instituciones de educación superior y empresas prestadoras de servicios informáticos. La finalidad de la investigación fue conocer apreciaciones sobre las siguientes preguntas generales.

7.1.- ¿Qué es la seguridad informática? Con ésta se buscó conocer la apreciación acerca de la seguridad informática en los entrevistados.

7.2.- ¿Que informaciones se procesan electronicamente en los organismos públicos? Dirigida a conocer tipos de informacion procesados por medios electrónicos.

7.3.- ¿Qué importancia tiene la seguridad para los organismos públicos? Complemento de la primera, se dirigió a conocer el nivel de preocupación institucional por la seguridad en cuestión y la sensibilidad hacia la vulnerabilidad que presentan los datos o las irregularidades en el desarrollo u operación de sistemas.

7.4.- ¿Qué problemática se ha presentado en el organismo en cuestión y qué problemática conoce que se ha presentado en la Administración Pública mexicana, en general? Este aspecto se abordó, cuando el interlocutor lo permitió, y se hizo con base en un cuestionario que cubrià los diversos niveles de

---

1.- Fundamentalmente las sociedades nacionales de crédito.

seguridad computacional, con objeto de conocer el tipo y dimensión de los problemas que han tenido lugar.(2)

7.5.- ¿Cómo se ha atacado ésta? Recogió información sobre los recursos de seguridad, que operan en los organismos visitados.

7.6.- ¿De que manera se puede mejorar la seguridad, control o buen uso de la información y de la informática? Retomó propuestas para el mejoramiento de la seguridad informática.

Los aspectos más relevantes, recogidos en cada una de estas preguntas, se refieren a continuación.

7.1.- ¿QUE ES LA SEGURIDAD INFORMATICA?

En general, La visión de la seguridad informática se encontró sumamente limitada. Muchos entrevistados denotaron una percepción simplista o fácil del problema. Contemplan su solución con la mera utilización de claves o llaves de acceso a los equipos o programas y con la generación de respaldos de los propios datos y programas. La dimensión de la seguridad, para los entrevistados, varió desde la afirmación del gerente de sistemas de una importante entidad paraestatal, que dijo "aquí la seguridad no se contempla para nada", hasta las percepciones más complejas de los especialistas de auditoria o seguridad informática del sector bancario. Estos reconocieron que el problema tiene mucchas facetas, que se presenta en distintos tipos y niveles de información, así como en ámbitos lógico, físico y

---

2.- El anexo num. 3 de este trabajo presenta este cuestionario.

de personal. Para ellos, la seguridad significa el correcto uso, integridad y confidencialidad de la información. Algunos afirmaron que la solución óptima se logra con base en aplicación de estudios de análisis de los riesgos, que presentan los elementos informáticos y con una cuidadosa administración de los servicios computacionales. El sector financiero constituyó el más avanzado en la materia, de los que se visitaron. La razón es evidente: para ellos la información es dinero. Reconocen que éste es factor de alto riesgo.

No obstante, la cobertura de la seguridad informática es, todavia, insuficiente. El grueso del personal bancario desconoce el problema. Unos cuantos especialistas tienen la misión de extender la sensibilidad hacia esta materia y velar por su ejercicio. Uno de ellos afirmó: "la seguridad es dificil, todavia hay pocas bases teóricas. No se ha desarrollado con amplitud el tema. Las obras o artículos al respecto son muchas, pero están muy dispersas y dan recomendaciones que son inaplicables, debido a que están descontextualizadas y son genéricas... Hay pocas obras sobre seguridad en específico y los tratados sobre informática tocan marginalmente la seguridad".(3)

En general, para la Administración Pública, la seguridad es contemplada como un refinamiento o una necesidad posterior al desarrollo de sistemas de información. En muchos casos, se está tan atrasado en este último, que la

3.- Entrevista sostenida en febrero de 1989.

consideración de la seguridad o privacía se desatiende por completo. Cuando se ponen en ejercicio normas o mecanismos técnicos de protección o control, es porque, casi siempre, ya ocurrió algun incidente con repercusiones negativas considerables, ya sea por error, desfalco o catástrofe natural. Los sismos de 1985 contribuyeron a que se tomaran en cuenta aspectos de seguridad, al menos a nivel físico.

En todos los casos, el desarrollo informàtico de los organismos públicos consistió en adquirir equipos y programas, sin fundamentarse en un proceso de planeaciòn adecuada, que contemplara aspectos de costo-beneficio, asi como de viabilidad de uso y de control de los activos computacionales. El paso del tiempo reflejò han existido recursos informáticos obsoletos, sobrados en su capacidad o subutilizados por la institución usuaria.

Se dotó de atribuciones, en materia de regulación informática, al Instituto Nacional de Geografía, Estadistica e Informática, organo desconcentrado de la Secretaria de Programación y Presupuesto. A la fecha, su campo de acción en la computación ha sido limitado. Se concentra en dictaminar y autorizar adquisiciones de bienes informàticos, en busca de que haya congruencia entre las necesidades del usuario, los equipos o programas o servicios a contratar y los costos de compra. Esta labor se desarrolla para las dependencias y entidades de la Administración Pública Federal. La seguridad la desatiende por completo y ello refleja el nivel del desarrollo informático nacional. Por

ahora, el interés se concentra en extender las aplicaciones de proceso automatizado de datos, más que en asegurar que las existentes funcionen adecuada y controladamente.

7.2.- ¿QUE INFORMACIONES SE PROCESAN ELECTRONICAMENTE EN LOS ORGANISMOS PUBLICOS?

Las informaciones incorporadas a medios de cómputo, son de todo genero y abarcan todos niveles y tipos de funciones del Gobierno Federal. En el ámbito de esta pregunta, se buscó obtener una tipología de los datos que operan los organismos públicos federales.

La información es clasificable en tres grandes tipos.
a) Sustantiva, correspondiente al cumplimiento de los objetivos o fines organizacionales. Por ejemplo: comunicaciones, salud, transporte, vivienda, desarrollo rural, justicia, seguridad ciudadana, entre otras.
B) Adjetiva o regulatoria, referente al establecimiento de "un marco de referencia que fije fronteras, tiempos y responsabilidades... y que planee, presupueste, organice y evalue la actividad de un sistema en su conjunto".(4)
c) De apoyo, correspondiente al manejo de los recursos humanos, financieros y materiales o servicios.

A su vez, en la Administración Pública se maneja un esquema para los niveles de información. Esta abarca tres

---

4.- Tomado de Castelazo, Jose R.: Técnicas y especialidades en la administración del personal público.-- s.p.i. mimeo, 1985. (Documento de apoyo para el curso de administración del personal público en El Colegio de México.) P. 3.

segmentos: estratégico, tàctico y operativo. El primero se refiere a la interrelaciòn del organismo con su medio ambiente. Se preocupa por descubrir en qué forma la institución puede convivir de una manera eficaz y rentable con su medio externo --incluyendo competencia, fuentes de financiamiento, sistemas políticos, económicos y sociales. En este nivel se determinan los objetivos institucionales, su filosofía de trabajo, las políticas o lineamientos que le permiten seguir un rumbo hacia el cumplimiento de sus fines. Una gran parte de la información, que le es genuinamente útil, es la referida al medio externo a la institución y la obtiene de medios también externos. La informaciòn estratégica fundamenta toma de decisiones destinada al logro de eficacia y eficiencia del organismo frente a su entorno. Y en ello se basa el funcionamiemto de la institución en su conjunto.(5)

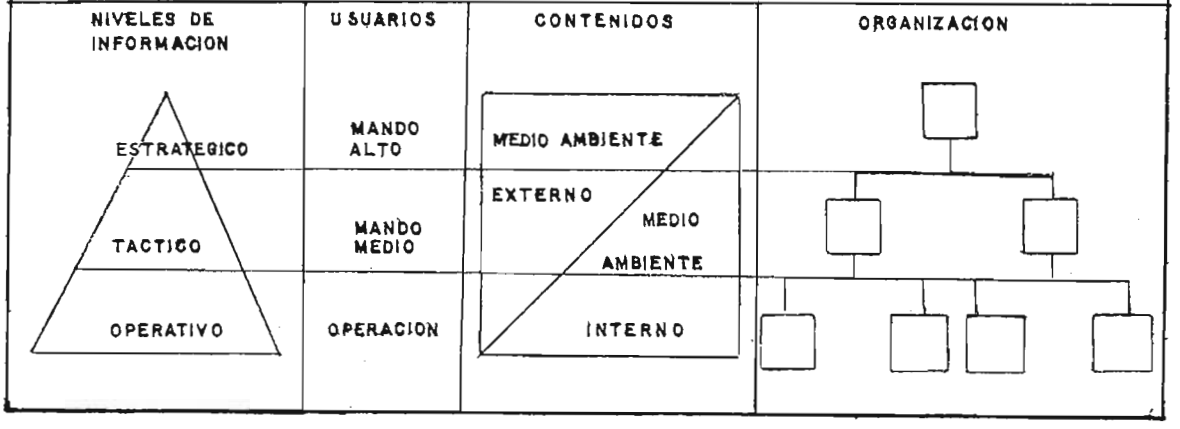
El nivel de información táctica se refiere a tareas de organización, supervisión del ejercicio de la toma de decisiones y determinaciòn de métodos y procedimientos. El operativo, por su parte, incluye la masa de datos o documentación que se capta y almacena para las tareas cotidianas de los organismos. Del procesamiento de ésta se genera la información táctica y de ésta se obtienen

---

5.- V. Simon, Herbert A: "El comportamiento administrativo: un estudio de los procesos decisorios en la organizaciòn administrativa".-- Madrid: Aguilar, 1962. P.12.

elementos para la estratégica. Un director de informática presentó el siguiente esquema a manera de ilustración.(6)

FIGURA 2
CLASIFICACION DE LA INFORMACION EN LOS ORGANISMOS PUBLICOS



De acuerdo al esquema, la información estratégica se destina a apoyar toma de decisiones para un mejor desempeño institucional, primordialmente frente a su medio externo, es decir, la sociedad. La información táctica lidia menos con el medio ambiente y apoya la instrumentación de decisiones estratégicas, por medio de la definición de métodos y procedimientos y medios de control o supervisión. Le concierne el desarrollo y supervisión de mecanismos administrativos u operativos que satisfagan con eficiencia y eficacia las necesidades de la sociedad, que se respeten sus derechos y cumpla sus obligaciones. En el segmento operativo, la toma de decisiones cumple las disposiciones emanadas de los otros niveles y le corresponden tareas rutinarias.

6.- Este esquema se recogió durante entrevista sostenida por el autor, en octubre de 1988, en la dirección de informática de una dependencia.

Durante la investigaciòn desarrollada para este trabajo, se descubriò que la seguridad informática es aplicable en los tres niveles referidos y en los tres tipos de información mencionados (sustantiva, adjetiva y de apoyo). Los datos en todos ellos son necesarios e importantes para el funcionamiento de los organismos, y en todos los niveles se halla informaciòn calificable como confidencial.(7) Datos sobre aspectos financieros, contables, nòminas y prestaciones, registros de salud, derechos de autor, patentes, certificaciones académicas, licencias sanitarias, licencias de construcciòn, aspectos de justicia, entre muchos otros, son disponibles a nivel operativo, tàctico y estratégico y revisten caracteristicas sensitivas y vulnerables. Los esquemas tipològicos sobre información confidencial son sòlo desarrollables en el seno de cada organismo pùblico y, con base en ello, se establecen prioridades para ejercicio de la seguridad informàtica.

7.3.- ¿QUE IMPORTANCIA SE OTORGA A LA SEGURIDAD INFORMATICA EN LOS ORGANISMOS PUBLICOS?

La percepciòn sobre la dimensiòn de la seguridad computacional, en los organismos, parece crecer a medida que se presentan tres factores.

7.- Por informaciòn confidencial se califica aquella que es vital para la operaciòn, toma de decisiones o evaluaciòn de las instituciones, asi como la referente al respeto de los derechos o ejercicio de las obligaciones de la ciudadania; y que debido a ello merece un tratamiento y control, màs o menos ciudadoso.

A) Cuando el personal directivo del organismo o responsable de los sistemas de información se sensibiliza de la vulnerabilidad informatica de uno o varios elementos computacionales en uso.

B) Cuando ocurren daños o pérdidas con impacto negativo para la propia institución.

C) Cuando existe rumor o conocimiento de pérdidas sufridas por terceros, que pueden tener lugar en el organismo o unidad administrativa propia, e infunden temor. Este último es, tal vez, el que más ha incidido en la búsqueda de seguridad.

Los errores humanos son fuente importante de problemas en sistemas de información. Se escuchó sobre casos frecuentes de pérdidas a causa de instrucciones equivocadas por parte de los operadores. Ello se acompaña de falta de rutinas de respaldo de datos. La reconstrucción de archivos llega, en estas situaciones, a ser proceso arduo y lento, segun el caso. La causa más inmediata es falta de capacitación y de cultura informática, tanto del personal directivo, como del operativo. Los usuarios suelen ser instruídos sólo en aspectos específicos del manejo de los sistemas.(8) En el conocimiento limitado de los operarios de sistemas, se presenta un fenómeno interesante. Es el que un entrevistado denominó "seguridad por desconocimiento". Se

---

8.- Los errores mencionados se presentan con mayor recurrencia en unidades administrativas que operan equipos personales (PC) o que cuentan con terminales remotas de sistemas de cómputo centralizados.

manifiesta en que el personal no viola ciertos archivos o programas porque ignora la existencia de ellos o no sabe cómo los podría accesar. Él mismo afirmó, respecto al área bajo su dirección que "...aquí la seguridad que hay depende mucho de la ignorancia del operador."(9

La seguridad es aspecto que se atiende cuando ya existe la necesidad inminente de hacerlo. (10) Todo organismo ejerce algun mecanismo o medio de protección -- aunque no se reconozca-- con base en alguno de los tres factores anteriores. La datos, que por su carácter, son reconocidos como confidenciales, son, por lo general, sujetos de control debido a los conflictos que puede generar fugas de ellos. No obstante, existen agregados de información sin proteccion o control adecuados, ante el argumento de que "no son tan confidenciales"(11). Criterios de esta naturaleza dieron lugar a que los sismos de 1985, en la Ciudad de México, ocasionaran pérdidas irremediables de información estadística, administrativa u operativa en varias dependencias y entidades, que representaban miles de horas-hombre de análisis, captura y proceso y que

---

9.- De entrevista sostenida por el autor en una subdirección de información de una dependencia. Octubre de 1988.
10.- Russell Ackoff habla de la propensión a enfrentarse a los cambios tecnológicos en los sistemas (organizaciones) y menciona que la problemática se enfrentan por lo general, no con base en análisis y estudios planeatorios, sino que se responde cuando ya existe una situación de desesperación. V. Ackoff, Russell: Rediseñando el futuro.-- México: Editorial Limusa, 1980. P. 6.
11.- Este fue argumento de un servidor público, director general de informática de una dependencia, entrevistado en febrero de 1989.

sustentaban decisiones públicas. Con el impacto de los sismos se dió atención, sin precedente, a la seguridad fisica de los equipos e instalaciones. Se comenzó a atender con mayor cuidado aspectos de ubicación de centros de cómputo, creación de sitios de respaldo, edificación de instalaciones con base en normas internacionales, entre otras. (12)

La conclusión importante, en el terreno que aborda la pregunta que nos ocupa, es que a mayor sensibilidad o temor por la vulnerabilidad de los sistemas de información, se atiende la problematica de la seguridad. Esta se ejerce, por lo general, de manera correctiva, a veces detectiva y casi nunca preventiva. En otras palabras, se atiende al tener que enfrentarse un desastre o riesgo de ocurrencia inminente. Los recursos con que se cuenta, como ya se refirió, se destinan más a adquirir nuevos recursos informáticos y ampliar su cobertura, que a asegurar el correcto y seguro desempeño de los sistemas ya existentes.

12.- A manera de ilustración, cuatro sociedades nacionales de crédito perdieron sus centros de cómputo durante los mencionados sismos. Por fortuna, para ellas, no se perdieron sus archivos de datos, pero los daños pudieron haber sido irreparables. La Asociación Mexicana de Bancos ha promovido, desde entonces, la organización de foros sobre el tema de la seguridad, a los que asisten especialistas de todas las instituciones bancarias. Las reuniones son de carácter restringido. Asisten solo funcionarios bancarios y en ellas se ha fomentado el desarrollo de los sistemas de seguridad informática para este sector. Ello explica su mayor adelanto en esta materia, respecto al resto de la Administración Pública.

7.4.-¿QUE PROBLEMATICA SE HA PRESENTADO EN MATERIA DE SEGURIDAD EN LOS ORGANISMOS PUBLICOS ?

De manera general, la problemàtica de la seguridad informática se fundamenta en que no se reconoce el problema como tal. Factores derivados de éste son múltiples. Primero, el desarrollo de sistemas computacionales òptimos y eficientes tiene mucho camino por recorrer. Un gerente de informática aseveró "los analistas de sistemas y programadores ni les interesa ni tienen la mentalidad ni la exigencia ni el tiempo de atender la seguridad".(13) Adicionalmente, la seguridad implica costos asociados importantes. En materia de equipos de proceso y dispositivos de almacenamiento, el respaldo implica, al menos, doble costo y los administradores lo reconocen.

Segundo, todavia muchos organismos, a falta de recursos, comparten equipos y dispositivos informàticos con otros. Dependencias que cuentan con grandes centros de cómputo apoyan el proceso de datos de instituciones menores. Bajo esta circunstancia, el ejercicio de la seguridad se torna muy precario.(14)

Tercero, està difundida la idea que la seguridad obstaculiza rapidez en accesos, procesos y reportes de datos. El problema colateral es que, con frecuencia, desde

---

13.- Afirmaciòn de un directivo informático de un organismo del sector financiero. Sostenida en noviembre de 1988.
14.- El compartir recursos informáticos entre instituciones corresponde a una etapa inicial de informatizaciòn. Con el paso del tiempo tiende a desaparacer. Cada organizaciòn adquire sus propios equipos.

el punto de vista del usuario o del directivo, "todo urge". Este genero de situaciones denota la poca valoración que existe hacia la seguridad y falta de previsión para que el manejo de datos se realice en plazos racionalmente establecidos y no con premura.

Cuarto, poco ayuda el terreno legal. En materia de seguridad informática está practicamente desierto. Cada organismo crea sus propias reglas y las establece de forma casuística y dispersa. El siguiente capitulo aborda con más detalle esta cuestión.

Estos factores denotan vicios habituales y ancestrales de la Administración Pública: imprevisión, indiferencia, ignorancia, morosidad, entre muchos. Aspectos màs especificos de la problemática en los distintos niveles de la seguridad, según el marco analítico presentado, (15) se presentan a continuación, a saber, en 7.4.1) nivel de seguridad operacional o administración informática y 7.4.2) la seguridad en otros niveles informáticos.

7.4.1.- A NIVEL DE SEGURIDAD OPERACIONAL O ADMINISTRACION INFORMATICA.

Para este apartado se utilizaron cuatro categorias. 7.4.1.1) Planeación de la seguridad. 7.4.1.2) Organización y métodos de protección y control. 7.4.1.3) El personal computacional. 7.4.1.4) Evaluación Informática.

15.- V. Supra, capitulo num.6

7.4.1.1.- PLANEACION DE LA SEGURIDAD.

Este subnivel atañe a la previsión o definición de qué hacer, con qué recursos, quienes están implicados y en qué momento, en el tema de la seguridad computacional. La única manifestación de planeación de la seguridad informática encontrada en el Gobierno Federal fue la existencia de planes de recuperación ante casos de desastre, con los que cuentan las instituciones financieras, principalmente. Estos planes se destinan a programar el restablecimiento de las operaciones del organismo cuando ocurren siniestros, de diversas magnitudes, que causan daños en equipos o en sistemas de información. Se establecen objetivos, metas, responsabilidades y medios de recuperación de las funciones normales. Los siniestros pueden ser de origen intencional, natural o errores de operación. Constituyen un avance importante en materia de control y protección computacional.(16)

7.4.1.2.- ORGANIZACION Y METODOS DE PROTECCION Y CONTROL.

En este subnivel se comprenden las formas con las que se jerarquiza y distribuyen las funciones informáticas entre unidades administrativas y entre el personal. La problemática es diversa en este terreno y se tratan tres rubros. 7.4.1.2.1) Formas de organización de sistemas. 7.4.1.2.2) Métodos y procedimientos para la seguridad. Y por

16.- El anexo num. 1 de este trabajo plantea las caracteristicas de los planes de recuperación ante casos de desastres informáticos.

último, 7.4.1.2.3) selección e implantación de medidas especificas de protección y control.

7.4.1.2.1.- FORMAS DE ORGANIZACION DE SISTEMAS.

Al cuestionar sobre la vulnerabilidad informática que presenta una institución en su conjunto, varios entrevistados afirmaron que, el nivel de riesgo, depende de la forma de organización de sus servicios de cómputo. Para ello, se pueden diferenciar tres esquemas centralizado, descentralizado y distribuído o redes. Los sistemas que tienen un procesador central y las terminales y dispositivos de salida de información se hallan en el mismo sitio del equipo de proceso, los llamaremos centralizados. Los descentralizados serán aquellos que tienen un equipo de proceso central, pero que cuentan con terminales en otras unidades administrativas de la organización, sea o no en el mismo edificio. Los sistemas distribuidos o redes se reconocerán como aquellos que consisten en la interconexión de varios equipos de proceso, almacenamiento, y salida de datos. Se afirmó que los sistemas centralizados y los descentralizados presentan mayor vulnerabilidad que los sistemas distribuídos. Para ello, se aseveró que los organismos se ven más afectados en los casos que un procesador central y un sólo almacen de datos sirve a todo un sistema de información --centralizado y descentralizado. En éstos casos son frecuentes los problemas de "caída del sistema" o fallas en las comunicaciones, que afectan a todas las terminales y se paraliza el sistema en su conjunto.

Asimismo, si falla o se daña o se pierde el procesador central, se afecta irremediablemente a todos los usuarios. Este tipo de sistemas es común en las dependencias y entidades más pequeñas. Los organismos públicos mayores cuentan con sistemas distribuidos, es decir, con múltiples recursos computacionales de proceso, transmisión y almacenamiento. Los daños que sufre una unidad administrativa, afectan poco o nada a otros.

Adicionalmente, es necesario anotar aspectos característicos de la problemática de los tres esquemas. En el centralizado, se presentan varios hechos problemáticos. Primero, en el centro de cómputo se crea una élite de operarios y programadores que conocen todos o muchos sistemas. Tienen acceso y disponen de facilidades para operar o manipular, practicamante, cualquier programa o archivo de datos. Por el hecho de ser conocedores de la informática, se les deja vía libre para manejar los sistemas. No hay quien los administre porque el personal directivo o de alto mando es ignorante del fenómeno informático. Segundo, por lo regular, el manejo de los sistemas es bajo procesos *batch*. En éstos, el usuario de la información se mantiene ajeno a los dispositivos o equipos de cómputo. Entrega un cúmulo de datos para ser procesados en un centro de cómputo y recibe posteriormente reportes o listados con información ya depurada o analizada.

Bajo estos hechos, en lo físico, la vulnerabilidad es alta cuando se pierde o falla del centro de cómputo. En lo

lógico, el control sobre el flujo de información es escaso en sus diversas fases: generación, captura, proceso, listados y tránsito de la información entre el equipo de informática y la unidad administrativa o persona usuaria de los datos.

El esquema de organización descentralizado presenta problemas similares. (17) No obstante, cabe mencionar un aspecto distintivo. Cuando el equipo de cómputo cuenta con terminales remotas se efectúan procesos conocidos como de "tiempo real". El usuario ingresa los datos desde la terminal a su disposición y en todo momento puede efectuar accesos, reportes o consultas. Es frecuente que éstos sistemas cuenten con medios de seguridad, a nivel de sistema operativo, para que cada usuario accese archivos y ejerza funciones autorizadas.

La tercera forma de organización es la de redes. Se instalan por ventajas en la distribución de los servicios de informática, reducción de costos --cuesta menos contar con varias unidades de proceso y almacenamiento interconectadas, que con un solo gran centro de cómputo --, disponibilidad de datos y programas (18). La problemática, en materia de seguridad, para éste tipo de sistemas, es ámplia. Entre los factores más destacados están los siguientes.

17.- V. Nota 6.
18.- V. Lara Marquina, León y Adalberto Vela Sánchez: "Seguridad en procesos distribuidos".-- (Tesis que presenta para recibir el grado de licenciatura en informática) México, D.F.: U.P.I.I.C.S.A., 1984. P. 10

a) Las irregularidades o fallas o ineficiencia de algùn equipo o usuario, degradan el desempeño de otros.

b) Una vez implantado el sistema distribuìdo, técnicamente, es muy dificil modificarlo y los costos de rediseño o conversión son altos.

c) La instrumentaciòn de planes de recuperación ante desastres son complejos. Se involucran muchas personas, muchas responsabilidades, muchos equipos y agregados de datos dispersos entre los diferentes equipos del sistema.(19)

Enn general, de la investigación desarrollada, se notó la ausencia de métodos y procedimientos claramente definidos. Se carece de métodologia de análisis de riesgos, que constituya base para evalùar necesidades y niveles de control, protección y respaldo.

7.4.1.2.2.- METODOS Y PROCEDIMIENTOS PARA LA SEGURIDAD.

En éste ámbito, se encontró que ningún organismo visitado tiene establecidos y controlados, debidamente, métodos y procedimientos de seguridad informática, de manera integral. Los métodos de protecciòn de equipos, programas y datos han sido definidos, por lo general, sin considerar su viabilidad para cumplir los fines propuestos y estar sujetos a un adecuado seguimiento.

El establecimiento de medios para proveer seguridad implica, al menos, considerar catalogaciòn o clasificación

---

19. Para abundar en aspectos de vulnerabilidad o riesgo en sistemas distribuidos, ver. Lara Marquina, ibid., p. 11.

de información; documentación de los sistemas de información; y determinación, aplicación y seguimiento de mecanismos de control en todas las etapas del flujo de la información (20). Se acostumbra poner en función medidas que dan protección a una o algunas de éstas etapas, pero no a todas. Ello no resuelve el potencial de fugas incontroladas de información. Esta seguridad "limitada" se ilustra con varios fenómenos comunes en la Administración Pública.

a) Cuando existen medidas de seguridad, se ejercen en él ámbito del centro de cómputo. Después de su proceso, la información se remite al usuario que, sin noción alguna de la seguridad, la deja fuera de control.(21)

b) Se han creado instalaciones o centros de cómputo de respaldo, pero no se hacen simulacros y no se tiene previsto a quién y cómo acudir en caso de contingencias. Con el paso del tiempo, se descubre que los sistemas operativos de los equipos principal y de respaldo resultan incompatibles.

20.- El flujo de información va desde el origen de ésta hasta su destino final. En general, los pasos de este flujo son: 1) generación de datos (origen de la información), 2) captura --al sistema de cómputo--, 3) procesamiento, 4) almacenamiento, 5) consulta, 6) reportes o listados y 7) destino final --poner la información procesada a disposición del usuario para la toma de decisiones.

21.- Entre los ejemplos más comunes se cita la emisión de reportes con información confidencial. Al ser recibidos por el usuario, sin previsión alguna, éste los fotocopia, desatiende o circula. Un servidor público, conocedor de la seguridad informática, en el INEGI, insistió en la fotocopia como medio de alto potencial de fugas de información, que descalabra cualquier sistema de seguridad, por más sofisticado que sea. Tomado de entrevista en febrero de 1989.

c) Se aplican medidas de seguridad de diferentes tipos, sin embargo no ha existido obligatoriedad en documentarlas. Asi, cuando se remueve el personal que los puso en servicio, los nuevos servidores públicos desconocen su existencia, funcionamiento y posibilidad de ser controladas.

d) En muchas instituciones se practican limitaciones para el acceso de personal a los centros de còmputo. Sin embargo, el personal de limpieza o mantenimiento suele estar ajeno de toda supervisión y puede ingresar libremente en areas restringidas.

e) Las claves de acceso a equipos y archivos permiten controlar los agregados de información con que se trabaja y las funciones que un determinado usuario puede efectuar con los datos. No obstante, la eficacia de un sistema de control por claves de acceso implica modificar éstos con frecuencias predeterminadas. Los directivos computacionales no promueven estas modificaciones y, con el tiempo, unos usuarios conocen las claves de otros.

En general, se tiene una visiòn insuficiente de la problemática de la seguridad, en una perspectiva integral. En el flujo de la informaciòn se presentan múltiples pasos o etapas y se desatienden puntos débiles.

7.4.1.2.3.- SELECCION E IMPLANTACION DE MEDIDAS ESPECIFICAS DE PROTECCION Y CONTROL.

Por lo común, la instrumentación de medidas es pragmática y no es objeto de un proceso administrativo. Muchas veses, su definición se basa en la intuición. Una

vez puestas en servicio no son sujetas de control y evaluación. Entre las implicaciones de ello destacan las siguientes. Primero, la administración o dirección no desea o no le interesa o se le olvida efectuar verificaciòn de su funcionamiento. Segundo, el personal està poco sensibilizado de la importancia de la informaciòn y se resiste a que se le obligue a respetar medios de control. Tercero, cuando el personal se percata que no hay vigilancia en el ejercicio de la seguridad, se acostumbra a no respetar medidas y, cuando se implantan nuevos ordenamientos o técnicas, los aceptará con dificultad. Acerca de esta situaciòn abundó un investigador en informàtica. Aseveró que "la costumbre mina poco a poco toda seguridad". Dos ejemplos que refiriò son. 1) Cuando se instalan puertas de acceso a centros de còmputo con chapas que operan con base en claves complicadas, el personal opta por dejarlas abiertas. Les causa molestia dar la clave adecuada cada vez que entran y salen de la instalación. 2) El personal de vigilancia o seguridad deja de efectuar revisiones al personal que va conociendo, al paso del tiempo. (22) En general, la indiferencia directiva da lugar a que el personal no esté adecuadamente encauzado y busque modos de omitir medidas de control.

22.- David Hsiao ofrece también un ejemplo de este tipo de situaciónes. Hsiao, David; Douglas Kerr y Stuart Madnick: "Computer security".-- San Francisco: Academic Press, 1979. P. 52.

7.4.1.3.- EL PERSONAL COMPUTACIONAL.

éste es el eslabón más débil en la cadena de la seguridad. Un investigador universitario, en materia de informática, afirmó "...el mexicano es su propio enemigo..". Más adelante dijo: "un operador mal entrenado es peor que la dinamita". Estas palabras no exageran uno de los aspectos más esenciales de la seguridad informática: la calidad del personal. En realidad, toda medida de protección y control se destina a seres humanos. Cuando éstos tienen condiciones de trabajo adecuadas y están debidamente sensibilizados y capacitados acerca de la informática y su protección, la seguridad se optimiza. Al contrario se minimiza. En la Administración Pública Federal de México, al menos, la realidad es de éste último tipo. En materia de personal, la problemática existe en muchos sentidos. El directivo no administra la seguridad porque la desconoce. El administrador o receptor de la información no sabe cómo pedirla y cómo manejar información sensitiva o confidencial. El operador de los sistemas tiene libertad de hacer lo que desee, aunque no deba, bajo la premisa de que "el sí sabe de computación". (23) Del mismo modo, está poco consciente de la responsabilidad que implica manejar o procesar o disponer información. Hace su trabajo con descuido. Las autoridades, con facultad de regular en materia de computación, suelen

---

23.- Aseveración de un entrevistado, investigador universitario, en marzo de 1989.

trabajar sobre equipos o programas, y, pocas veces, sobre aspectos del personal.(24)

La introducciòn de la informática en las agencias públicas ha provocado una problemática, en el terreno de recursos humanos, mal comprendida e insuficientemente abordada. La aplicación de computadores conlleva cambios en métodos, procedimientos, rutinas o tareas especificas, para diferentes personas. El personal, acostumbrado a laborar bajo esquemas tradicionales, repentinamente es obligado a cambiar su modo de trabajar, por la introducciòn de nuevas tecnologias. Se resiste al cambio y obstaculiza. No comprende el fenómeno computacional y no concibe los alcances ni la responsabilidad que se deriva del manejo electrónico de datos. Los procesos que antes hacía manualmente, ahora los efectúa con máquinas. En muchos casos, el servidor pùblico siente que pierde espacio o poder. La informática altera o anula intereses creados, quita libertades. Ante todo ello, sobrevienen tensiones derivadas de los cambios. Hacia las nuevas formas de trabajo se suele promover capacitación, pero desde el punto de vista de las computadoras y se olvida el elemento humano.

24.- Ya se abordó en el primer capítulo del trabajo, las funciones que ha desempeñado el INEGI. éstas se centran en dictaminar adquisiciones y las revisiones que lleva a cabo en las dependencias y entidades pùblicas se dirigen a verificar que los equipos estén en su lugar y que el conteo de ellos corresponda a las adquisiciones efectuadas. El qué se hace con esos equipos, quién los utiliza y para qué, no se atiende.

Se trata de momentos de crisis en todo proceso de informatización, ya sea de una sociedad o de una organización. Es una adaptación cuya solución, a veces, tiene un carácter forzoso. Ello provoca resentimientos que, en algún momento, se volcarán contra las instituciónes.(25)

Otro aspecto importante es que los equipos de informática son operados sin que se alteren condiciones generales de trabajo o aspectos de seguridad e higiene. Esto es un tema sumamente relevante y no atendido. Algunos ejemplos, en particular, son los siguientes. El trabajo continuo con pantallas de visualización o con impresoras provoca *stress* o tensión, por cansancio de vista y vibraciones de los equipos impresores, respectivamente. Los centros de cómputo instalados con requerimientos técnicos de humedad, temperatura y ventilación dan lugar a enfermedades respiratorias, en personal no habituado a ellos.

En México, la documentación sobre condiciones generales de trabajo no contempla, en lo absoluto, estos efectos. En el futuro cercano se tendrá que investigar en ésta materia y atender, al menos, las recomendaciones de la Oficina

---

25.- Son las situaciones que en el vocabulario de los administradores de recursos humanos se denominan "cuentas por cobrar". El servidor público, afectado por alguna medida arbitraria o mal canalizada o mal enfocada, buscará el momento de ejercer acciones de venganza, en detrimento de sus superiores o de la propia organización. El terreno computacional presenta un campo fértil para éste tipo de acciones. Con instrucciones o técnicas simples se pueden bloquear o borrar o alterar sistemas de información vitales para una institución.

Internacional del Trabajo, aplicables al personal informático.(26)

7.4.1.4.- LA EVALUACION INFORMATICA.

El instrumento más conocido para la evaluación computacional es la auditoria informática. Su campo de acción es amplio. En general, se destina a revisar el desarrollo, mantenimiento y operación de los sistemas de cómputo, incluyendo equipos, dispositivos, instalaciones, programas y datos. (27) Una de sus areas de anàlisis es la seguridad informàtica. Se verifica la buena conservación de equipos, datos y programas, apego a la normatividad aplicable, respeto de las medidas de protección y aseguramiento de la integridad y confidencialidad de la información. Con la excepción de algunas sociedades nacionales de crédito y grandes entidades paraestatales, la auditoria informática no existe en la Administración Pública Federal de México y, en lo general, las acciones que se ejercen en materia de evaluación hacia la computación son escasas.(28)

26.- En la sección sobre administración de personal informático, del capítulo num. 9 , se hará referencia con más detenimiento hacia éstas recomendaciones.

27.- Definición adaptada del documento, A.M.A.I.:"Normas generales para la auditoria por medio de sistemas de informática", en "Boletín Informático" (México), Num. 1, p. 4.

28.- Los procesos de evaluación, que existen en la Administración Pública de México, atañen a la propia información que se procesa. Consisten en arqueos, conciliaciones y validación de información procesada. En materia de equipos, se suele revisar que estén presentes donde deben estarlo.

La falta de evaluación conlleva el desconocimiento del parque de datos almacenados, de los modos como se acccesan archivos, de su grado de confidencialidad, su disponibilidad, su respaldo, entre muchos. Los programas, por su parte, se hallan expuestos a ser alterados o borrados sin control alguno.

El desarrollo de nuevas aplicaciones se efectúa sin la intervención de auditores y no se garantiza que los programas estén diseñados e implementados de acuerdo a las necesidades de la institución. Los equipos de cómputo están expuestos a daños por agentes fisicos o humanos. Los fraudes, con intermedio de la informàtica, tienen alto potencial de ocurrir, al no verificarse que existan mecanismos de previsión, detección y corrección.

Sin la presencia de programas de evaluación informática, los organismos públicos están altamente vulnerables, en lo que a seguridad se refiere.

7.4.2.- LA SEGURIDAD EN OTROS NIVELES INFORMATICOS.

Para este rubro se tratan dos apartados. 4.2.1) La seguridad física y 4.2.1) La seguridad en *hardware*, en *software* y en datos.

7.4.2.1.- LA SEGURIDAD FISICA.

Un directivo informático afirmó "la vulnerabilidad fisica nos afecta a todas las instituciones". No se equivoca. Con base en apreciaciones propias, al efectuar visitas, es factible afirmar que ni las sociedades nacionales de crédito tienen adecuadamente atendida la

seguridad en sus instalaciones. En la seguridad fisica se diferencian dos aspéctos. 7.4.2.1.1) Acceso fisico a instalaciones y equipos. 7.4.2.1.2) Protecciòn contra desastres intencionales o naturales.

7.4.2.1.1.- ACCESO FISICO A INSTALACIONES Y EQUIPOS.

El acceso fisico es atendido en tòda institución, de una forma u otra. Los grandes procesadores se ubican en sitios que cuentan con algún medio de control de acceso. -- por ejemplo, presencia de policias, existencia de chapas con combinaciones numéricas o lectores de tarjetas magnetizadas, entre otros. Sin embargo, la sola existencia de la medida de seguridad no resuelve el problema de manera satisfactoria. Durante las visitas a centros de còmputo, se pudieron constatar varios hechos.

a) En varias instalaciones con equipos grandes de proceso las puertas, aunque tienen cerraduras sofisticadas, estaban abiertas.

b) En muy pocos casos, los edificios se destinaban exclusivamente a instalaciones de còmputo. Por lo general hay diversas unidades administrativas en los edificios y algunas de ellas se destinan a atención al público. Una vez que se traspasa el retén de seguridad del acceso principal de los inmuebles, ya no hay control de vigilancia en los sitios que albergan equipos o dispositivos informàticos.

c) Se hallaron centros de còmputo tras ventanales --algunos con vista a la via publica. Asimismo, a pesar de que se cuente con puertas sofisticadas, las instalaciones se rodean

de cancelerias de madera o aluminio, que enmarcan grandes cristales. Se protege las puertas, pero no las ventanas ni los muros.

7.4.2.1.2.- PROTECCION CONTRA DESASTRES INTENCIONALES O NATURALES.

En este ámbito la problemática es más critica. A pesar de la experiencia de los sismos de 1985, en la Ciudad de México, no se han destinado recursos para atender suficientemente el problema. Ante ese siniestro, ninguna institución estaba preparada para enfrentar un cataclismo de tal magnitud. El impacto fue tal que hasta algunos centros de respaldo de datos se dañaron o desaparecieron.

Los riesgos éste género de desastres se han enfrentado con la generación de respaldos de programas y datos, y que son almacenados en sitios alejados o en bòvedas tipo bancario. Las sociedades nacionales de crédito, por su parte, han desarrollado planes de recuperación ante desastres.

A pesar de las acciones correctivas emprendidas se detectaron varias sitaciones problemáticas, entre las que destacan las siguientes.

a) Hay instituciones que no cuentan con cintotécas de respaldo de datos.

b) De los organismos que generan respaldos, se conocieron casos en los que no se tiene un programa claramente establecido para efectuarlos. Las labores de actualización de las copias se hacen ocasionalmente. En un caso se afirmò

que el respaldo se hace cada seis meses, lo que implica que un desastre puede tener efectos hasta de seis meses de trabajo.

c) Los organismos afectados por los sismos mencionados, que han construido centros de respaldo, han elegido sitios al azar y no donde conviene tecnicamente hacerlo.

d) En muchos casos se han dispuesto en sitios cerrados para el almacén de datos de las instituciones, pero son lugares inseguros, ante desastres de fuego, descargas electricas, radiaciones, inundación, sismo o terrorismo.(29) Algunas dependencias y entidades mayores han considerado la construcción y utilización de bóvedas. Sin embargo, éstas son dejadas abiertas en el transcurso de los dias laborables. Si ocurre un siniestro en horas hábiles, se corre el riesgo de no poder cerrar éstas a tiempo y el efecto es como si no existiesen.

e) Las instalaciones no siempre estan construidas o terminadas con materiales no peligrosos o no flamables. Algunos cuentan con detectores de humo, de calor y de bióxido de carbono, así como con extinguidores de fuego y alarmas de operación manual. Sin embargo, suelen carecer de servicios de revisión y mantenimiento preventivo, de estos dispositivos.

29.- Las instituciones menores suelen utilizar habitaciones con puertas de madera y chapas convencionales. Hay casos en los que el mencionado almacén se sitúa en cubículos de cancelería y cristal.

No obstante las situaciones anteriores, los administradores informáticos se jactan de las caracteristicas novedosas de sus recursos tecnológicos de control de acceso y prevenciòn de desastres. En realidad, como se ha afirmado a lo largo de este capitulo, carecen de una visiòn suficiente de la seguridad.

7.4.2.2.- SEGURIDAD EN *HARDWARE*, *SOFTWARE* Y DATOS.

En los niveles se *hardware* y de *software*, se pueden apuntar los siguientes hechos problemáticos, hasta ahora no referidos.

1) Como se anotó arriba, en los sistemas de redes, el diseño y funcionamiento de medidas de control es complejo.(30) Los problemas de seguridad más frecuentes son los que siguen.

a) En cada equipo de proceso y almacenamiento conectado a las redes se generan archivos y programas, pero se carece de un inventario general de éstos.

b) Hay poco control sobre las operaciones de cada usuario, sobre todo cuando las redes se utilizan en unidades administrativas cuya funciòn sustantiva no es la informática. Los directivos de éstas areas desconocen la seguridad informática y no ejercen debido control sobre los operadores. Asimismo, se han ingresado programas "virus", que afectan a múltiples usuarios.

c) La seguridad depende, en mucho, de las limitaciones de los operadores. Si tienen suficientes herramientas técnicas

30.- V. Supra. Secciòn 7.4.1.2.1.

pueden llegar a accesar cualquier programa o archivo de información de cualquier equipo del sistema.

A nivel de los datos, se encontraron casos de segmentación de los mismos y de aplicación de la criptografía. Estos son utilizados, principalmente, por las sociedades nacionales de crédito, para almacen y transmisión de información. Sin embargo, no fue posible obtener información sobre la problemática que ello conlleva.

7.5.- ¿COMO SE HA AFRONTADO LA SEGURIDAD INFORMATICA EN LA ADMINISTRACION PUBLICA FEDERAL?

La seguridad informática, como integridad, no está cubierta en ningún organismo público, pero sí existen, de algún modo, medios de control en todos los casos. Los más comunes son controles de acceso a inmuebles, controles a nivel de sistema operativo, respaldos de datos y programas, prevenciones ante siniestros, entre otros ya mencionados.

El sector bancario, ha atendido más que otros la seguridad. Debido a que el potencial de fraude es alto, deben guardar el "secreto bancario" y evitar que las instituciones con las que compiten se enteren de algo inconveniente. Han previsto y aplicado medidas, algunas muy sofisticadas tecnicamente. Sus esfuerzos se han concentrado a nivel de seguridad en *hardware*, en *software*, en datos y en transmisión de información. Los controles a nivel de sistema operativo han permitido efectuar bitácoras de las operaciones que efectúa cada usuario. Por medio de la clave

asignada a cada persona, se controlan funciones de capturar, leer, listar, alterar o borrar datos.

En las mayores instituciones bancarias funcionan unidades administrativas tipo *staff* para apoyar a toda la organización en un mejor desempeño de la seguridad computacional. Con base en la gestión de éstas unidades se ha logrado incorporar medios de seguridad a los sistemas de cómputo, desde su fase de diseño, con resultados satisfactorios.

Lo que no se ha desarrollado es una adecuada administración de la seguridad o seguridad operacional.

7.6.- ¿QUE SE PROPONE PARA MEJORAR LA SEGURIDAD?

En éste tópico, se escucharon opiniones para optimizar el ejercicio de la seguridad informática. La mayoría de las propuestas recogidas continuaron abordando el problema de la seguridad de manera fragmentada o dispersa. Un investigador universitario se refirió a la capacitación como "...la única arma contra la indiferencia y la ignorancia" y que es elemento esencial para el logro de cualquier seguridad.(31)

Hubo dos entrevistados que aportaron ideas sumamente valiosas y con base en ellas se desarrollan las propuestas de administración de seguridad informática en este trabajo. Se dejó ver la seguridad operacional o administrativa como elemento necesario para integrar y coordinar el

---

31.- Tomada de entrevista a un investigador en informática, en enero de 1989.

funcionamiento de controles y protecciones en los otros niveles de seguridad. Se mencionaron, basicamente, cuatro areas de propuesta: planeaciòn, organización y ejecución, personal y evaluación. Como ya se mencionó, el problema fundamental de los organismos que cuentan con medios de seguridad es que carecen de congruencia, integración y seguimiento.

7.6.1.- PLANEACION.

La planeación es la primera fase de todo proceso administrativo. En materia de seguridad, en ella se determina qué es valioso y qué hay que proteger; de qué manera; con qué recursos y en qué tiempo. Es precisamente del nivel directivo organizacional de donde provienen las medidas a ser aplicadas y no de los niveles técnicos.

Para planear con certidumbre es necesario, primero, tener cierto control sobre la operación. Esto implica conocer equipos, dispositivos y otros bienes tangibles; todas las informaciones con que cuenta una determinada organización y las personas y unidades administrativas implicadas. Se trata de conocer el acervo informàtico en toda su extensiòn y la intervención humana en los sistemas. De este conocimiento se deriva una visiòn completa de la problemática de la seguridad, en todos los niveles. Algunos directivos computacionales de las sociedades nacionales de crédito insistieron que para una óptima protección y control se requiere ser exhaustivo. No basta con asegurar algunos elementos informáticos, es necesario contemplar el todo.

Otra sugerencia fue la de partir de metodologías de análisis de riesgos para derivar de ellas programas de acción. ésto implica asociar valor de equipos, información y seguridad del personal, con escalas cualitativas o cuantitativas de vulnerabilidad y con costos de seguridad.(32) Entre los elementos sugeridos para un análisis de riesgo están los siguientes.

a) Definir claramente los fines del organismo y la imagen que debe tener ante la sociedad y la Administración Pública.

b) Identificar y determinar medios para minimizar los riesgos mayores.

c) Decidir si el riesgo,

c.1) se debe minimizar (con medidas de seguridad),

c.2) se debe trasladar (con pólizas de seguro), o

c.3) se debe absorber (asumirlo plenamente en el organismo).

La opción a tomar se hará con base en el tamaño del riesgo, su vitalidad y los recursos para afrontarlo.

d) Elaborar cuestionarios para medir la seguridad existente y ponderarla con los niveles de protección deseados o necesarios para la organización.

Para la definición de políticas y normas, los aspectos a observar son los siguientes.

32.-En un solo caso se propuso una metodología concreta para análisis de riesgos y es la que se refiere en el apartado de planeación de la seguridad en el capítulo #9 y en el anexo num.4.

1) Los logros en materia de seguridad se obtienen gradualmente. Primero se cubren los riesgos mayores y después los menores.

2) Para cada dependencia o entidad, la búsqueda de seguridad debe ser de acuerdo a necesidades de integridad y confidencialidad de la información.

3) El personal técnico o administrativo deberá proponer a la junta de gobierno, o a la alta dirección, los objetivos de seguridad. Esta decidirá sobre su viabilidad y definirá las politicas y normas a seguir, así como los recursos destinados para ello.

4) El ejercicio de la seguridad debe ser compulsivo.

5) Debe existir alguien que recuerde y diga lo que se debe hacer, de manera permanente en los organismos.

6) La seguridad deberá ser parte de la función informática.

7) Las normas, en el terreno de la seguridad fisica, al menos, deberán ser acordes con las caracteristicas de la localidad -- temperatura, humedad, sismologia, propensión a actos terroristas, entre otros.

8) El que evalúa deberá ser distinto al que ejecuta.

9) Se recomienda la formación de un comité de seguimiento y evaluación del funcionamiento de la seguridad, que opere en todos los niveles informáticos. Se integraría de manera multi-disciplinaria, con la participación de directivos, analistas de sistemas, programadores, administradores y juristas.

7.6.2.- ORGANIZACION.

Para el diseño y buen ejercicio de las normas, métodos, procedimientos y medidas, se sugiere atender las siguientes características.

1) Si no se pueden implantar son inviables.

2) Si se establecen normas, hay la necesidad de controlarlas y regularlas. Si esto no es factible, es mejor no establecerlas. Asimismo, deberán existir responsables de su ejercicio y vigilancia.

3) Serán acordes con los requerimientos reales del organismo. No exagerar en precisión o rigidez si el organismo no lo amerita.

4) Si son genéricas, no sirven.

5) Deberán estar debidamente apoyadas por escrito, es decir, documentadas y respaldadas en manuales de procedimientos, ya sean de uso general o restringido.

6) Para las medidas de seguridad, se deberá buscar una combinación idónea de eficacia y sencillez.

7) Intervendrán los administradores para opinar sobre la viabilidad de las medidas y su impacto en el personal. Es importante que las normas tengan un carácter humano. éstas son obedecidas por personas, no por máquinas y se debe responder al cuestionamiento de qué hacer para que sean obedecidas.

Se recomienda que existan como categorías funcionales, para apoyo a la administración de la seguridad las siguientes: auditoria informática y seguridad informática.

La primera se constituye como instrumento técnico de validación y reconocimiento del apego a normas en las tareas computacionales. La segunda atañe a aspectos de protección computacional a manera de garantizar la confidencialidad e integridad de los datos. Son funciones complementarias.

La responsabilidad directa del ejercicio de la seguridad compete, en primera instancia, al propio operario o usuario de los equipos o datos. En segunda instancia, a su jefe inmediato y así sucesivamente, de tal modo que la seguridad sea asumida plenamente en cada área o unidad administrativa informatizada. No es factible que el comité de seguridad o el auditor o el experto en seguridad se responsabilicen de ello. Los aspectos de protección y control deberán ser parte de la función cotidiana del personal y, por ello, cada unidad administrativa asumirá y responderá por la observancia de la seguridad informática.

7.6.3.- PERSONAL.

El personal constituye uno de los aspectos más importantes en el problema de la seguridad y, en general, de la administración informática. A pesar de ello, fueron pocos los entrevistados que comentaron al respecto y menos los conceptos valiosos que aportaron como propuesta.

Se afirmó que en la medida que se logre que los recursos humanos apeguen su gestión a las normas, se optimizará la seguridad. Ello significa que se debe capacitar al personal para que desarrolle con seriedad y profesionalismo las tareas encomendadas. Un alto directivo

informático afirmó que "la seguridad es una cultura...debe estar en todas las personas que trabajan para un organismo" y "... la respuesta debe ser mayoritaria", si no es así, es inutil todo esfuerzo o costo de los medios de protección y control.(33) La presencia de esta cultura se considera fundamental para cualquier propósito de seguridad. Ella facilita el éxito de todo objetivo o proyecto.

Para el personal operativo, esta cultura se adquiere por medio de la práctica y con apoyo de cursos de capacitación. Para el alto mando, dado que no es factible que participe en cursos, se le sensibiliza por medio de informes o estudios, que le hagan concebir integramente la problemática.

Complementario a la capacitación está la propia política de personal de los organismos, que debe buscar la satisfacción y el bienestar del elemento humano. Para ello, se recomienda atender las recomendaciones de la Oficina Internacional del Trabajo. Un entrevstado advirtió sobre la importancia de reconocer el trabajo intelectual que efectúan los programadores y los diseñadores de los sistemas de información. Son precisamente éstos los que tienen mayores facilidades o potencial de daños informáticos. Propuso reconocer el trabajo de éstos mediante estimulos vía regalias o compensaciones, acordes con los beneficios que aportan al buen funcionamiento de los organismos. Asimismo,

33.- De entrevista sostenida por el autor con un especialista en informática, que labora para un despacho privado. Enero de 1989.

se mencionó la factibilidad de que las dependencias y entidades públicas inscriban sus programas de cómputo en el Registro Nacional de Derechos de Autor, de la Secretaría de Gobernación, otorgando coautoría a los programadores o analistas. De ese modo, se reconoce la labor del programador y las instituciones se protegen legalmente ante daños en sus sistemas.(34)

7.6.4.- EVALUACION.

La evaluación de la seguridad informática es la fase en la que se emite opinión acerca del buen uso y funcionamiento de la computación. La auditoría informática cumple esta finalidad. Debe proponer elementos de detección, prevención y corrección de disfuncionalidades. Sus tareas parten de las normas, políticas, métodos y procedimientos establecidos y se evalúa el grado de apego a éstas y la eficacia y eficiencia de los controles establecidos.

Es necesario, como se mencionó antes, que existan previsiones claramente establecidas que se constituyan como marco de referencia para evaluar. Asimismo, se debe buscar poner en funcionamiento los recursos para auditoría informática que proporcionan los sistemas operativos de las computadoras. Son recursos técnicos y ayudas que facilitan el control y la protección computacional.

34.- De entrevista sostenida con un funcionario del INEGI. Enero de 1989.

CAPITULO 8.- MARCO LEGAL APLICABLE A LA INFORMATICA Y SU SEGURIDAD.

La informática ha penetrado en la sociedad, con rápido desarrollo, difusión y con efectos que impactan actitudes y valores tradicionales. Como se ha anotado, se está en el umbral de una sociedad informatizada, a nivel global y nacional. Hoy, la computación es elemento importante en la sociedad, al permitir mayor y mejor acceso y tratamiento de información.

La computación abre perspectivas de desarrollo. No obstante, se trata de tecnologías generadas en otras sociedades y, por ello, su asimilación y desarrollo deben establecerse en un marco jurídico adecuado a la realidad mexicana y de definición de políticas para su óptima utilización.

El primer nivel de seguridad, del modelo presentado, es, precisamente, el referente al marco legal. En muchos países, los gobiernos han implantado el funciónamiento normas jurídicas y políticas para regular el fenómeno informático, de acuerdo, en cada caso, a su situación particular de desarrollo y perspectivas futuras. Se busca establecer leyes y disposiciones que otorguen "seguridad jurídica" a la utilización de herramientas informáticas. (1) Es el Estado quien debe promover esta seguridad y, para

---

1.- Término de Vera Vallejo, Luis: "Algunos aspectos legales de la seguridad en informàtica".-- s.p.i., mimeo. (1988) (Ponencia presentada en diversos seminarios organizados por la Asociación Mexicana de Bancos). P. 2

ello, generar normatividad aplicable, con la garantía de su poder coactivo.

El fenómeno computacional ha sido regulado mediante la creación de un Derecho Informático. Más que una nueva disciplina, se proyecta como un "cuerpo jurídico que integra normas ya existentes con otras nuevas, resultado de la tecnología, en ámbitos público, privado y social."(2)

Para el sector público este marco normativo es base de implantación de toda política u ordenamiento atañente a la informática. El Gobierno Federal es el mayor usuario de bienes y servicios computacionales y, además, el mayor creador de programas o sistemas de aplicación. Es por ello que requiere hacer uso racional de estos recursos y acorde con los objetivos de la función pública y modernización administrativa.

Los temas que cubre el derecho informático, y que se han tratado más a nivel internacional, están los siguientes.

1.- La informática frente a los derechos individuales (la problemática de la privacía). (3)

2.- Los contratos informáticos, que revisten un carácter especial por la complejidad técnica de los medios computacionales.(4)

2.- Tomado de México, Instituto Nacional de Geografía, Estadística e Informática: Derecho Informático.-- Talleres Gráficos de la Nación, 1983. P.10.

3.- Ver. capítulo num. 4.

4.- En general, en el terreno de la informática, el comprador tiende a estar en desventaja frente al vendedor, que muchas veces determina las necesidades del usuario y le

3.- Protección jurídica de los programas. Referente a protección de los soportes lógicos (*software* o programas), por medio de patentes, derechos de autor, u otros.(5)

4.- El flujo de datos transfronterizos, materia de preocupación al crecer volúmenes y variedad de datos transmitidos a través de las fronteras. Ello conlleva problemática de "armonización internacional", en aspectos de "protección de confidencialidad, propiedad intelectual, soberanía y seguridad nacional", entre otros.(6) La transmisión de datos reviste un carácter económico al ser sujeto de prácticas comerciales.(7)

5.- Los delitos informáticos y valor probatorio de los elementos computacionales. Estos delitos tienen lugar cuando los recursos tecnológicos no son utilizados para el bien del hombre y la sana convivencia social. Se hacen daños en el contexto económico-financiero, en los valores o derechos individuales o en la soberanía de las naciones. El terreno informático ha sido nuevo campo potencial de actos ilícitos. Ello ha impulsado esfuerzos por tipificar actos ilegales y,

---

vende lo que él decide. En la Administración Pública, el INEGI, organismo regulador computacional, interviene con dictámenes para condiciones de compra, importación, topes de precio, viabilidad técnica, etc. V. México, INEGI, op.cit. P. 23.

5.- El valor relativo de los programas tiende a crecer frente al de los equipos, en términos de precios. El mismo Gobierno Federal requiere instrumentos de protección jurídica a sus programas, siendo un gran creador de éstos en el país.

6.- INEGI, op. cit. P. 10.

7.- Para mayor profundidad en este tema, INEGI, op. cit. P. 29. Tellez Valdés, Julio: "Derecho informático".-- México, D.F.: Universidad Nacional Autónoma de Méxio,1987. Pp. 79 a 86.

con base en ello, emitir normas preventivas, correctivas o detectivas, así como establecer responsabilidades y penalizaciones.

El valor probatorio de los elementos computacionales se manifiesta como esencial en el derecho informático. En muchos lugares, los soportes magnéticos, en especial, carecen de validez para sustentar investigaciones delictivas.(8)

Estos temas, sin ser exhaustivos en la problemática jurídica de la computación, son los más abordados en el plano internacional. Algunos paises, sobre todo los del mundo capitalista desarrollado, han generado marcos legales dirigidos a todos, o la mayoría de los temas señalados. (9)

8.- Al no constituir los soportes magnéticos instrumentos de evidencia, la información se desprotege. Se debe comprender que la computación es un giro para las reglas tradicionales del derecho probatorio. En un futuro cercano, se tendrá que tratar este aspecto, al asimilarse los medios computacionales como recursos de almacenamiento de información y de simplificación de procesos repetitivos.

9.- Destacan entre ellos los Estados Unidos de America, Gran Bretaña, Alemania Federal, Suecia y Suiza. V. INEGI, op. cit. Pp. 3 a 30. y Tellez, Valdés, op. cit., anexos. Este último adiciona a su obra copias de los textos más representativos en materia de regulación informática de los paises mencionados y algunos otros.

8.1.- MARCO JURIDICO PARA LA INFORMATICA Y SU SEGURIDAD EN MEXICO.

En nuestro país, por ahora, no existe un marco jurídico integral a la informática. Solamente se presentan algunos ordenamientos dispersos y 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 ésta sección se hace referencia a las disposiciones vigentes, que afectan el fenómeno informático, así como el planteamiento de las necesidades de legislación en un futuro previsible. Con ello se pretende contemplar el panorama de un derecho informático mexicano.

En México no existe ley alguna que se dirija a la informática, y menos a su seguridad. La misma Constitución General de la República no alude tema ni aspecto alguno de computación. 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 tecnologías para proceso de datos.

En ningún caso, los ordenamientos jurídicos estudiados, refieren aspectos de seguridad informática en forma explícita. En ésta sección se presentan los elementos

legales que existen, en México, aplicables a la informàtica y su seguridad.

A nivel constitucional hay dos aspectos que conviene destacar: el derecho a la información y la libertad de expresión. Ellos tienen como límites el respeto a la vida privada y a la dignidad personal y "que no se ataquen derechos de terceros ni provoque la comisión de delitos o perturbe el orden pùblico".(10) En materia de seguridad se apuntan éstos como soporte al derecho a la privacìa o al manejo confidencial de la información.

El artículo 134 prevee la utilización racional de los recursos del Gobierno Federal. De ello se fundamenta la labor del INEGI en regulación y dictaminación de adquisiciones de bienes informàticos.

A nivel de ley, en la "Ley Orgánica de la Administración Pública Federal",(11) se enumeran los atributos de la Secretarìa de Programación y Presupuesto (S.P.P.), como normadora de adquisiciones y coordinadora de los servicios de cómputo en las dependencias y entidades. Se le constituye como cabeza reguladora en materia informática.

En acuerdo publicado el 16 de enero de 1978, (12) se precisan las atribuciones de la S.P.P., en materia

---

10.- Tomado de INEGI, op. cit. P. 9.
11.- Ley Orgánica de La Administración Pública Federal, artículo 34, fr. XVII.
12.- Publicado en el Diario Oficial el 16 de enero de 1978. En este acuerdo se detallan los objetivos y las actividades que desarrollará la S.P.P. en materia informática.

informática. Se le confiere promover eficiencia, regular adquisiciones, uso racional y desarrollo computacional en la Administración Pública Federal, así como el mejoramiento de la infraestructura administrativa de la informàtica.

En el Reglamento interior de la S.P.P., se establecen las atribuciones del Instituto Nacional de Geografía, Estadística e Informática (INEGI), como órgano desconcentrado de la S.P.P. En el art. 26, Fracciòn III, en relación con la informática, se mencionan sus atribuciones. Entre ellas destaca la formulación de políticas y normas técnicas, así como regular adquisiciones y promover el desarrollo tecnológico nacional en informática.

En el art. 28, del mismo, se habla de la Direcciòn General de Política Informática, del INEGI, como unidad administrativa que coordina la política informática nacional e integral de la A.P.F.(13)

En materia de derecho a la información y privacia, el único ordenamiento jurídico que lo trata es la "Ley de

---

En materia de contratos informáticos y adquisiciones, además de los ordenamientos referentes a S.P.P. e INEGI, se puede citar el Reglamento de la Ley de Presupuesto, Contabilidad y Gasto Público Federal, que habla de la atribución de S.P.P. de dictaminar contratos relacionados con bienes y servicios informáticos. Este reglamento fue publicado en D.O. el 18 de noviembre de 1981. También en aspectos de adquisiciones se destacan los siguientes. "Ley de Adquisiciones, Arrendamiento y Prestaciòn de Servicios relacionados con Bienes Muebles", en art. 39, distingue modos de adjudicación de contratos (asignación directa, licitación pública o invitación). El Presupuesto de Egresos de la Federaciòn, del 31 de diciembre de 1989, establece los montos para adjudicaciòn de contratos (según los tres mencionados).

13.- El Reglamento Interior de la S.P.P., se publicó en D.O. 29 de julio de 1985.

Información Estadística y Geográfica"(14). En su art. 5o. se establece la garantía a los informantes censales de la confidencialidad en el manejo de los datos recabados. El art. 37 asienta el derecho a la rectificación. Dice que "El informante puede exigir rectificación de los datos que le conciernen al demostrar que no son correctos o completos o son obsoletos". Asimismo menciona que el informante puede exigir constancia de correcciones efectuadas y denunciar infracciones al principio de confidencialidad. Por su parte, el art. 38 establece que los datos censales serán manejados con "confidencialidad y reserva" y menciona el modo de divulgación de los mismos. Asimismo, afirma que datos censales no serán prueba ante ninguna autoridad administrativa ni fiscal; ni en juicios ni fuera de ellos.

Estas referencias constituyen el mayor avance nacional en materia de protección de la privacía del individuo.(15)

14.- La Ley de Información Estadística y Geográfica se publicó en el D.O. el 30 de diciembre de 1980.

15.- Esta ley tiene otras referencias para aspectos de informática y de derecho a la información. Su art. 2o., fr.V, dice que la ley tiene como objetivo el desarrollo y la utilización de la informática en los "servicios nacionales de información estadística". El art. 3o., fr. VII, da una definición del término informática. El art. 30 refiere a la S.P.P. como normadora nacional en informática. En su fr. VIII enuncia la tarea de S.P.P. de investigación y capacitación en materia de estadística, geografía e informática.
Los arts. 33 y 34 refieren el INEGI, como órgano desconcentrado de S.P.P., encargado de ejercer las atribuciones en materia de informática, antes citadas. El art. 39 se indica que el informante deberá conocer sus derechos al informar y los enumera: 1) saber si los datos son obligatorios o no, 2) saber las consecuencias de dar datos falsos, 3) conocer su derecho de rectificación, 4) conocer su derecho de confidencialidad y 5) saber la forma en que se divulgará la información.

Sin embargo, la información que protege esta ley se refiere, exclusivamente, a la información estadística o censal.

En el ámbito de protección al trabajo intelectual informático, está vigente el Acuerdo 114, de la Secretaría de Educación Pública, en la que se dispone que los programas de cómputo podrán inscribirse en el Registro Público del Derecho de Autor y detalla requisitos y procedimiento para ello (16). Este ordenamiento es adicion a la Ley Federal de Protección a los Derechos de Autor. Constituye, tal vez, el mayor avance de nuestro País en materia de legislación sobre la seguridad informática.(17) Ello permita dar seguridad jurídica a los programas desarrollados en las dependencias y entidades de la A.P.F.

El último aspecto en que se puede citar, respecto a la informática y su seguridad, son las disposiciones en materia de telecomunicación de información. Destaca el "Acuerdo para el establecimiento y operación de los sistemas de transmisión de señales de datos y su procesamiento"(18)

El art. 49 establece infracciones y sanciones y los motivos que las originan.

16.- Acuerdo publicado en D.O. el 8 de octubre de 1984. La Ley Federal de Protección a los Derechos de autor, en su art. 1o., menciona la protección al autor como materia de orden público e interés general. En su art. 7o. se enumeran las obras técnicas sujetas de registro y en este artículo se insertan las disposiciones del acuerdo 114, para el registro de programas de cómputo.

17.- En el mismo ámbito de protección al trabajo intelectual, se inserta la Ley de Invenciones y Marcas, del 10 de febrero de 1976. En ella se señala que no son invención ni la presentación de información ni los programas de cómputo. Esta Ley no ha sido modificada y denota la poca valoración que existe en México hacia el trabajo computacional.

18.- D.O. 12 de febrero de 1981.

Establece la competencia y coordinación entre la Secretaria de Comunicaciones y Transportes (S.C.T.) y la S.P.P. para el procesamiento remoto de datos de las dependencias y entidades de la A.P.F. Asimismo, faculta a la S.C.T. para normar sobre la garantia de la confiablilidad y confidencialidad del servicio. (19)

19.- V. art. 2o., fr. II y ss.

8.2.- HACIA UN DERECHO INFORMATICO MEXICANO.

Las referencias anteriores, a los ordenamientos jurídicos mexicanos, no constituyen una presentación exhaustiva del marco legal aplicable a la informàtica y su seguridad. Más bién, se efectuó una aproximación a estos tópicos, en busca de los aspectos más relevantes, que tienen relación con el tema que ocupa este trabajo. Existen, adicionalmente, muchos ordenamientos que abordan temas familiares a la seguridad computacional. Basta citar la cuestión del secreto bancario, relacionado con la privacià del individuo y la seguridad informática institucional.(20)

En realidad, la seguridad informática está olvidada en las leyes mexicanas. Un hecho fundamental es la falta de una norma jurídica que de congruencia y consistencia a una política informática nacional, aplicable, en principio, a la A.P.F. Las actividades pùblicas tienden a incrementar el uso, y dependencia, de los computadores. Con ello crece la propensión a situaciones disfuncionales y, además, el desarrollo informático tiene lugar de modo anárquico. Hasta el momento, no parece existir suficiente interés de legislar la informática, de manera amplia. Será, tal vez, hasta el momento en que tengan lugar desastres, cuando se genere preocupación por el buen uso y control de las tecnologías de proceso de datos, así como otorgarle seguridad jurídica.

20.- V. Ley de Instituciones de Crédito y Organismos Auxiliares. Título, 5o. art. 93. V. También, Reglamento del Servicio Público de Banca y Crédito.

La seguridad informàtica, en el nivel legal, debe abordarse de manera prospectiva, es decir, antes de que ocurran siniestros destructivos. El volumen de las pérdidas es potencialmente alto, que es conveniente manejar la vulnerabilidad computacional antes de que se sufran consecuencias.

El derecho informático tiene función de canalizar el desarrollo y la aplicación del cómputo, de modo que se aproveche su potencial para los objetivos nacionales. Asimismo, se busca minimizar los efectos negativos que se pudieran conllevar. Para México es necesario promover la creación de una legislación informática integral, apoyada en la misma Constitución General de la República. En particular, para el artículo 28 se sugiere ampliar el dominio del Estado al àmbito de la regulación de la informática nacional. De ello se derivaria una ley de carácter general, aplicable a las nuevas tecnologias de proceso de datos. Para la A.P.F. se sugieren normatividad para el funcionamiento de los servicios de cómputo, en aspectos de adquisiciones; instalaciones; administración y prestación de servicios computacionales e informacionales; capacitación; desarrollo o modificación de programas de aplicacion; operación de sistemas y generación de planes, programas, métodos y procedimientos de seguridad, entre otros aspectos. Es necesario, en este sentido, que el Estado

disponga del instrumento jurídico necesario para racionalizar el uso que él mismo hace de la informatica.(21)

En los temas abordados queda mucho por investigar y legislar. Expertos en informàtica tendrán que coordinar esfuerzos con juristas para establecer necesidades y marcos normativos acordes con la realidad nacional.

El derecho a la privacía, para las personas --físicas o morales--, tendrá que desarrollarse en sus diversas modalidades --como son derecho de acceso y control de éste, derecho de rectificación, etc.--. Será un derecho extensivo a todos los tipos de informaciones, nominativas, que captan, almacenan y procesan las instituciones públicas y, también, las privadas.(22) Se regularía sobre la posesión, uso o intercambio de datos en dependencias, bancos, instituciones aseguradoras, policiales, de servicios médicos, y otras. La sociedad reclamará sobre derechos de privacía en un futuro cercano.

En el renglón de contratos informáticos, la A.P.F. está suficientemente protegida. Ello es logro de la gestiòn del INEGI. Sin embargo la preocupaciòn computacional de este organismo no ha ido màs allá de este aspecto.

La protecciòn jurídica a programas se tendrá que asentar a nivel de ley. De la computaciòn se derivan

---

21.- V. INEGI, op. cit. P. 45.
22.- Esto tendrá que ser en el mismo sentido que las prescripciones de la Ley de Informaciòn Estadística y Geográfica, que como se mencionó, ya prevee manejo confidencial para datos censales. V. nota 15, de este capítulo.

conceptos novedosos acerca del derecho autoral y se tendrà que considerar las nuevas tecnologias como terreno de trabajo intelectual, totalmente reconocido y legitimado. La protección de derechos de autor será elemento de seguridad jurídica contra la circulación y reproducción ilegal de programas.

El flujo de datos transfronterizos debe ser objeto de normatividad amplia. El intercambio de informaciònes entre México y el exterior ocuparà mayor peso, progresivamente, en la balanza comercial. En el àmbito cultural este flujo de datos será relevante para el mantenimiento de valores nacionales y difusiòn de conocimientos. En lo politico, se tendrà que buscar preservar la seguridad y soberanía nacionales; controlar penetraciòn ideológica y espionaje.

El delito computacional deberà tipificarse, por ser conducta que afecta el orden pùblico e interés de las instituciones, la sociedad y los individuos.(23) A nivel de código penal, en su parte genérica, deberà considerar este tipo de hechos, como lo hace con los actos ilícitos tradicionales --robo, espionaje, sabotaje, etc. En su parte especifica tendrà que abordar aspectos más particulares de los delitos computacionales, segùn algún esquema de clasificaciòn para tipificar.(24)

23.- Esta y las siguientes sugerencias fueron expuestas verbalmente por Luis Vera Vallejo. Entrevista sostenida en febrero 1989.

24.- Como apoyo a la tipificación, se puede partir de algún esquema de clasificaciòn de delitos, como los que se refirieron en el capitulo num. 5.

En general, como afirma Vera Vallejo, urge contar con instrumentos legislativos que otorguen seguridad jurídica a la informática, en todas sus facetas --física, lógica, operacional--. Es necesario que se permita el florecimiento o extensión de nuevas tecnologías que apoyen el desarrollo de nuestro país, en conjunto con sus instituciones. Solo con un esquema normativo adecuado, se puede avanzar en la definición de políticas computacionales y en la procuración de protección y control. Será, a partir de un derecho informático adecuado, cuando pueda desarrollarse, de modo óptimo, el siguiente nivel de seguridad informática: la seguridad operacional o administración de la seguridad.

CAPITULO 9.- LA ADMINISTRACION DE LA SEGURIDAD INFORMATICA.

El segundo nivel de seguridad informática, en el marco analitico adoptado para esta tesis, corresponde a la seguridad operacional o administración de la seguridad informática. Este capitulo desarrolla un esquema administrativo, para atender la problemática compleja que se deriva de la aplicación de sistemas de procesamiento electrónico de datos.

Se ha mencionado la seguridad informática como un problema de muchas facetas. Asimismo, la literatura sobre este tema, a nivel internacional, se ha ocupado de aspectos especificos en lo juridico, operacional, técnico o fisico. Pero la coordinación y supervisión de éstos, de un modo integral es casi inexistente. Ello es relevante porque, a pesar de que en las instituciones se atiendan algunos aspectos de resguardo de equipos o datos, la problemàtica compleja de seguridad persistira por su propia naturaleza: la vulnerabilidad.(1)

En el nivel operacional, se ha trabajado prolificamente en terrenos como la administración de servicios de cómputo y de servicios informacionales. Sin embargo, la seguridad ha sido marginalmente abordada y, casi siempre, en lo fisico.

Una propuesta fundamental de este trabajo es de ejercer una adecuada administración de la seguridad, como forma posible de enfrentar y solucionar el problema. Se destaca la

---

1.- V. Hsiao, David; Douglas Kerr y Stuart Madnick: "Computer security".-- San Francisco: Academic Press, 1979. P. 43.

bondad del proceso administrativo como medio que permite asegurar el cumplimiento de los objetivos que se proponen, a través de la definición de un curso concreto a seguir y que incluya mecanismos regulatorios y de control. Se establecen principios, orientaciones y, con base en ellas, se precisa la secuencia de eventos para llegar a los fines propuestos.

El primer supuesto normativo de este trabajo sostiene que en la modernización de la Administración Pública, es necesario conllevar la incorporación de recursos tecnológicos con un rediseño de la organización, de modo que ambos tengan un desarrollo armónico. Se trata de dar congruencia al fenómeno informático con una modernización administrativa en las instituciones públicas, como requisito esencial para una sana operación computacional, funcional a los objetivos organizacionales y nacionales.

El supuesto normativo de este estudio, en consecuencia, sostiene que la seguridad informática debe se administrada, es decir, ser objeto de una toma de decisiones racional, ordenada y sistematicamente fundamentada. (2)

En el capitulo 6, se presentó un marco analítico para la seguridad informática integral, compuesto por seis niveles de análisis. Cada uno de ellos actúa concéntricamente sobre los niveles inscritos. De la sana operación y congruencia de todos, se deriva una adecuada seguridad. Bajo estas consideraciones, la administración de

---

2.- la hipótesis de trabajo y el supuesto normativo, se hallan descritos en la inroducción.

la seguridad informática hallará fundamento y norma en el entorno nacional o local, del que emana el marco legal aplicable. Esta administración se materializa en la toma de decisiones, que asegure el adecuado control de los riesgos o problemas informáticos.

Se presentan cuatro secciones, equivalentes a cuatro fases de proceso administrativo: 9.1) planeación de la seguridad informática, 9.2) organización y ejecución de la seguridad informática, 9.3) el personal informático y 9.4) evaluación de la seguridad informática. La planeación corresponde al análisis de necesidades, análisis de riesgos, definición de objetivos de seguridad, determinación de políticas e integración de planes y programas de ejecución. La organización es fase de definición de categorías funcionales, rediseño de estructuras organizacionales, documentación de la seguridad y desarrollo de métodos, procedimientos y medidas específicas. En la fase de personal se presentan elementos para la administración de recursos humanos. Se tratan políticas generales de personal, selección e inducción, capacitación y desarrollo, responsabilidades directivas e impacto de la informática en las condiciones 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.

Es necesario destacar que la dinámica de las organizaciones informatizadas presenta cambios con respecto a las formas manuales o tradicionales de trabajar. Como agente de eficiencia, productividad, liberación de cargas de trabajo manual y rutinario, se tienen alcances innegables. El acceso a tecnología de proceso de datos se ha extendido en pocos años, a nivel global, y adquiere, paulatinamente, un carácter masivo. Tiene impacto, al menos, en una integración económica mundial, dice Greenspan, con lo que se promoverán cambios importantes en las concepciones sociales y políticas tradicionales.(3)

En materia de seguridad informática, una de las mayores dificultades que afectan su administración es la presencia de concepciones erróneas hacia el mundo de la computación. En todos los casos, el punto de partida es la falta de reconocimiento de que la naturaleza de la seguridad de los datos ha cambiado. En el extremo, la protección de información es una necesidad inadecuadamente percibida y se le desatiende por completo. No obstante, algunos de sus aspectos son modalidades de los sistemas de información que existían antes del advenimiento de las computadoras. Otros son novedades desprendidas de los cambios tecnológicos y sociales.

3.- Tomado de entrevista a Alan Greenspan, ex director de la Federal Reserve Board, de Estados Unidos de Norteamérica. En Excelsior (México), sección financiera, 26 de octubre de 1988.

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.

Adicionalmente, como se anotó en la introducción del trabajo, la esencia del ejercicio de seguridad está en la autorización. En la medida que los volúmenes de información y complejidad de las instituciones crece, la determinación de autorizaciones adquiere mayor complejidad. En sistemas manuales de proceso de datos se presenta discrecionalidad en el acceso físico al manejo de ciertas informaciones y ésta se apoya en la confianza hacia los empleados --sin necesidad de ser explícita la determinación de normas. En un sistema de automatización masiva de información, las normas de discrecionalidad requieren mayor precisión y, por ello, la intervención decidida del personal de mando.

El riesgo de pérdidas o problemas administrativos, con la aplicación de la informática, es alto. La visión inicial que debe prevalecer es la de asumir el control de ese riesgo a manera de anticipar eventos destructivos. Ello se opone a la mentalidad de introducir medidas correctivas una vez que ocurrió el daño. La potencialidad de impacto negativo de un

fraude informático, o de un siniestro natural, puede ser de tal magnitud que ponga en peligro la operación o viabilidad de una institución y su entorno. Y al igual que en cualquier contexto, se supone que en el largo plazo es menos costoso enfrentar problemas, si se anticipa su posible advenimiento. Es por eso que el ejercicio de la seguridad se propone enfocar, siempre, de manera preventiva.

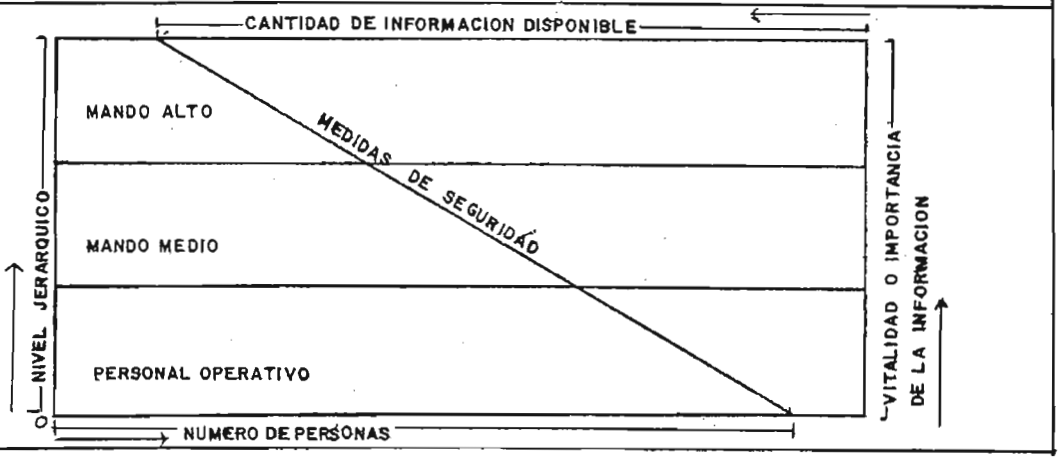
Las instituciones, ya afectadas por ilícitos computacionales, han sido herméticas para informar a terceros sobre lo acontecido, o siquiera para denunciar los hechos ante autoridades judiciales. La justificación de esto es desde el punto de vista de imagen institucional y de sus funcionarios. Sin embargo, por otro lado, se presenta la necesidad del conocimiento de experiencias negativas, que enriquezca la determinación de políticas o medidas o mecanismos técnicos de control y seguridad. Se trata de un conocimiento particularmente valioso, toda vez que el fenómeno computacional es relativamente nuevo. La comunicación de este tipo debe tener lugar a niveles restringidos, interinstitucionales, o por medio de contacto con tribunales.

Por su propia naturaleza, todo aspecto de seguridad es confidencial. Poner en evidencia la mayor o menor vulnerabilidad de una organización, de manera incontrolada, equivale a abrir puertas para actos ilícitos. En la medida que un defraudador conozca los eslabones débiles de un sistema de seguridad, podrá efectuar daños. Así, los

recursos de protección de datos, en conjunto con la clasificación de información, según su grado de vitalidad o confidencialidad, deben ser conocidos en detalle por el menor número de personas posible y de alto nivel jerárquico, preferencialmente. La siguiente figura es ilustrativa al respecto del control de la información.

FIGURA No. 3

EL CONTROL DE LOS SISTEMAS DE INFORMACION.



Fuente: Figura del autor, desarrollada con base en argumentos obtenidos durante las entrevistas sostenidas con personal directivo informàtico de diversas dependencias.

El esquema se refiere a la superposición de dos relaciones: 1) número de personas y nivel jerárquico y 2) cantidad de información y vitalidad de la misma. La primera relación es inversamente proporcional: a medida que asciende el nivel jerárquico, disminuye el número de personas implicadas. La segunda es directamente proporcional. A medida que crece la disponibilidad de información, crece la presencia de datos vitales o confidenciales. La

superposición de ambas muestra el principio del control computacional, a saber, reducir la disponibilidad de información en cantidad y vitalidad conforme se desciende en el nivel jerárquico y más personas se involucran en el sistema de información. Las medidas de control constituyen medio de contención, o filtros, en el flujo de datos hacia los distintos niveles organizacionales. El control computacional se convierte en elemento esencial para la procuración de seguridad. El logro de ese control se propone con base en la aplicación de esquemas de administración.

En adelante, este capítulo desarrolla las cuatro fases propuestas para el proceso administrativo de la seguridad informática.

9.1) PLANEACION DE LA SEGURIDAD INFORMATICA.

La planeación consiste en fijar el curso de acción a seguir, estableciendo los principios que habrán de orientarlo, el orden a seguir en las operaciones para realizarlo y la asignación de recursos, que implica.(4)

Para la precisión de elementos de planeación de la seguridad se tratarán tres fases: 9.1.1) Estrategias preliminares, 9.1.2) Definición de objetivos de la seguridad informática y 9.1.3) Investigación y definición de políticas y programas de trabajo.

4.- Tomado de "Introducción al proceso administrativo", s.p.i., mimeo (documento de apoyo para el curso de "Técnicas de investigación administrativa" en la licenciatura en administración pública, de El Colegio de México.

9.1.1.- ESTRATEGIAS PRELIMINARES.

El tema que se aborda en este trabajo, como se indicó, es un fenómeno de surgimiento reciente y evolución continua, que en pocos años se ha constituido tema importante para las instituciónes informatizadas. Las estrategias de planeación de la seguridad informàtica consisten en orientaciones o referencias fundamentales en la determinaciòn y consecución de objetivos de seguridad.

Estas estrategias son las siguientes.(5)

Primero. Todo sistema de informaciòn está diseñado y opera con base en los fines por los que fue creado. Esta es la prioridad mayor a atender en la administración informática. La aplicación de tecnología avanzada para el proceso de datos se destina a mejorar valores de eficiencia, productividad y dinamismo en las organizaciones. La seguridad tiene como misión que se resguarde el cumplimiento de los objetivos primordiales de los sistemas, así como la confidencialidad y sano manejo de los datos. De esta manera, la seguridad es objetivo subordinado a los objetivos sustantivos informàticos y es elemento que se debe integrar armonicamente con los sistemas y no a la inversa.

Segundo. El grado de cobertura de los programas de seguridad debe presentarse como resultado de un análisis amplio de requerimientos institucionales, en todos los niveles de protección ya mencionados (fisico, *hardware*,

5.- Basadas en conceptos de Krull, Alan: "Ten loging strategies for data security".-- en Computer Security Journal, (U.S.A.) Vol 4. No.1, 1986.

software y datos). Ello contrapone decisiones de resolver la seguridad con medidas aisladas --vía el uso de claves de acceso y respaldos de datos. Medidas dispersas ofrecen soluciones parciales y limitadas. No compensan problemas derivados del desempeño del personal ni del diseño de los sistemas ni de la mala administración ni de otros. Por eso se requiere abordar integralmente este àmbito.

Tercero. En el terreno de las políticas institucionales, se debe hacer una redefiniciòn en aquellas que atañan a unidades administrativas con servicios informáticos, en función de dinamizar y eficientar su desempeño. Las políticas son normas aplicables para efectuar las tareas organizacionales de cierto modo. En areas que manejan procesamiento electrónico de datos, por lo general, las necesidades crecen màs ràpido que el diseño de las políticas existentes.

Cuarto. La integraciòn de planes o programas informáticos se enfrenta a constantes cambios en el medio ambiente. Asi, se hace importante definir qué medio de protecciòn puede funcionar y cuál no. Ello solo se logra cuando ha sido completamente probada una medida. Es de suma utilidad la puesta en operación de prototipos de planes, medidas o lineamientos con miras a conocer sus efectos en el sistema de información o en el medio ambiente, para después ser adoptados en forma definitiva y evitar su obsolescencia en el corto plazo.

9.1.2.- DEFINICION DE OBJETIVOS DE LA SEGURIDAD INFORMATICA.

Hay objetivos genéricos a alcanzar en todo esfuerzo por la seguridad informática. Se trata de los siguientes.

a) Salvaguarda de la integridad, calidad y buen uso de los elementos informáticos --instalaciones, equipos, programas, datos y otros dispositivos.

b) Aseguramiento de la continuidad en la operación de las instituciones y sus unidades administrativas.

c) Intimidación contra la comisión de delitos informáticos.

d) Conocimiento y sensibilidad, en el personal de todos niveles, de requerimientos de seguridad en las diversas fases del flujo de informaciòn y en el diseño y administración de los sistemas.

e) Registro e investigación de pérdidas relacionadas con la informática y retroalimentación para los medios de seguridad.

f) Establecimiento de métodos y procedimientos de recuperación para casos de desastre.

Estos son objetivos generales. Cada organismo tendrá la tarea de seleccionar entre éstos o definir otros, con base en sus requerimientos.

9.1.3.- INVESTIGACION PRELIMINAR Y DEFINICION DE POLITICAS Y PROGRAMAS DE TRABAJO.

Para la conformación de políticas y programas de seguridad informàtica se implican las siguientes tareas.

A) Sensibilizaciòn del personal de alto mando, acerca de la vulnerabilidad informática.

B) Análisis y clasificación de la información institucional y su utilización.

C) Comunicación interinstitucional, y con instancias judiciales para el conocimiento de casos reales de pérdidas informáticas y el modo como ocurrieron.

D) Análisis de riesgo informático.

E) Identificación de los elementos informáticos a proteger, --equipos, informaciones, dispositivos, instalaciones, personas, etc.

F) Desarrollo de propuestas para programas de seguridad informática, diseño de prototipos y fijación de recursos y plazos para operación.

Cada una de estas tareas se abordará en detalle a continuación.

A) Sensibilización del personal de alto mando, acerca de la vulnerabilidad informàtica.

El apercibimiento por parte del personal directivo de las organizaciones sobre la vulnerabilidad informàtica constituye piedra angular de toda acción de seguridad. Es tarea de los administradores pùblicos o directivos informáticos conocer el panorama de la seguridad computacional con objeto de dimensionar el problema y transmitirlo a la alta dirección, por medio de estudios o informes. Para el contenido de éstos se sugieren los siguientes tópicos.

I) Esquematizar las características y funcionamiento de los sistemas de información de cada institución pública.

II) Presentar un panorama de los beneficios que aportan las nuevas tecnologías para el proceso de datos, en la instituición en cuestión.

III) Referir aspectos del impacto computacional en la propia institución, en la política, la economía y la sociedad.

IV) Esbozar la vulnerabilidad informática del organismo, en consideración de riesgos reales y de eventos catastróficos mayores o menores ya ocurridos.

De estudios de esta naturaleza se buscará desprender interés del alto mando organizacional para apoyar, con recursos y plazos, la investigación y abordaje de la problemática de la seguridad.

B) Análisis y clasificación de información y su utilización.

Una vez que la alta dirección de un organismo está consciente de los impactos del fenómeno informático en diversos terrenos, es factible desarrollar labores en materia de seguridad computacional, de modo sistemático. El primer paso de ejecución es la adecuada clasificación de los datos y análisis de su utilización. Ello implica un levantamiento global de toda la información procesada electronicamente en el organismo con miras a que los programas de seguridad brinden protección integral. La forma de clasificación puede ser en tres niveles, según Hsiao.(6)

I) Clasificación por documentos específicos. Para ello, cada documento se identifica de manera individual y exclusiva y

---

6.- Hsiao, David, op. cit. P.50.

toda autorizaciòn relacionada con su uso se hace sobre esa base.

II) Clasificación por función de la información. A través del rol que desempeñe en la dependencia o entidad o unidad administrativa, se definen tipos de datos (p.e., administrativa, de personal, de producciòn, que, a su vez se subdividen en subtipos a discreciòn)

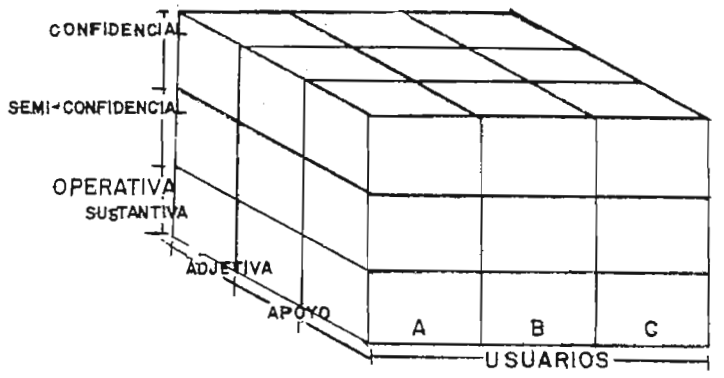
III) Clasificaciòn por unidad administrativa. Se identifica la informaciòn segùn el organigrama de la institución.

Estos tipos no son excluyentes. Se combinan de acuerdo las necesidades de cada institución. El menor o mayor grado de detalle en el desglose de la clasificaciòn es denominado por Hsiao como "granularidad". Es el grado de detalle al que se llega en una clasificación. Como ejemplo, la granularidad aumenta al clasificar informaciòn en archivos - documentos - conceptos - datos específicos. Un archivo o documento pueden tener variedad de informaciòn que requieran clasificación con mayor detalle. Más aún, en ciertos tipos de archivos computacionales se almacenan datos de alta confidencialidad en conjunto con otros que no lo son. En general, a mayor granularidad, o detalle, segùn las informaciones de cada organismo, se puede identificar con precisión los datos vitales o vulnerables.

Una vez definidos los tipos y subtipos de informaciòn, en un grado tal que sea factible diferenciar datos confidenciales de los que no lo son, se ubican categorías de usuarios autorizados para utilizar cada nivel de informaciòn

y para ejecutar cada tipo bàsico de operacion: captura, lectura, modificación, borrado, copiado y listado. El resultado se esquematiza en una figura tridimensional, en la que cada usuario puede accesar ciertos tipos de información y ejecutar ciertas funciones con ella.

FIGURA No. 4
CLASIFICACION DE INFORMACION, USUARIOS Y OPERACIONES. (7)



El último paso de clasificación de información es la determinación de niveles de seguridad requerido por cada tipo de información identificada, de tal modo que se evalúe las consecuencias de la pérdida o mal uso de cada tipo de datos.

Una vez definido el mapa tipológico de los datos organizacionales, se confronta con un esquema de flujo de información. Este consiste en la ubicación de cada una de las fases de transformación que experimentan los datos. Para cada tipo de información institucional se deben precisar las fases de generación --origen de los datos--, captura --

7.- La figura es diseño propio, adaptado de explicaciones recibidas en varias entrevistas sostenidas con personal directivo informática, de varias dependencias públicas, durante el primer trimestre de 1989.

ingreso a los sistemas informàticos--, proceso --depuración o alteración--, transmisión o circulación --envio de datos a diversas unidades administrativas o equipos--almacenamiento --registro en soportes magnéticos-- y salida --reportes o listados.(8) De este anàlisis, se desprenden las necesidades de controles a ejercer en todos los flujos de datos de la institución. Los controles equivalen a medios de seguridad y su ejercicio se verificarà a través de decisiones de autorizaciòn.(9) Estas constituyen llave que permite habilitar o inhabilitar medios para que las personas, internas o externas a la organización, operen sistemas de informàtica, bajo ciertos lineamientos.

C) Comunicaciòn interinstitucional y con instancias judiciales para el conocimiento de casos reales de pérdidas informáticas y el modo como ocurrieron.

El trabajo en equipo entre personal directivo y operativo puede ser benéfico para estudiar los malos usos a los que se presta la informaciòn computarizada. El fenómeno informático ha tenido difusión tan explosiva en la sociedad, que la variedad de técnicas o artimañas para comisiòn de actos ilícitos es amplia.

Se propone comunicaciòn entre instituciones públicas con efecto de intercambiar experiencias de casos reales o potenciales, que enriquezcan la visión de la problemática a ser atacada y con ello tratar de no omitir atenciòn a

8.- V. Anexo num. 4. Fases de transformaciòn de los datos.
9.- En la siguiente secciòn, referente a organización se dedicarà un apartado a las cuestiones de autorización.

riesgos no contemplados por unas organizaciones, pero sí por otras. Asimismo, aunque son pocos los eventos informáticos ilegales que se han ventilado en instancias judiciales, se recomienda comunicación con tribunales que pueden proveer elemento de juicio sobre casos presentados y sus implicaciones legales.

Esta comunicaciòn facilita encauzar la problemática de la seguridad computacional de manera preventiva, ademas de que otorga bases para tipificar eventos ilegales y preparar o evitar su eventual advenimiento.

Se trata, en suma, de conocer de la manera más amplia posible, la gama de riesgos que presenta la revolución informática y con base en ello se instrumenten adecuados programas de seguridad para cada institución.

D) Análisis de riesgo informático.

En esta fase se contempla un anàlisis más riguroso de la problemàtica de seguridad de los organismos. De la visión de problema obtenida en las fases anteriores, se pasa al ejercicio de estudios técnicos, que califiquen cualitativa o cuantitativamente los riesgos y costos. Se propone la utilización de esquemas de análisis de riesgos, con los que se evalùen informaciones sensitivas y puntos vulnerables en el flujo de la iunformaciòn. A éstos se les asignan valores nùmericos o cualitativos, que midan la propensión o probabilidad de ser violados, en un determinado perìodo de tiempo --por ejemplo, un año. Adicionalmente, se les refiere un costo o valor de pérdida total, directo --es decir de

reposición de la información o del activo informático-- e indirecto --según su impacto en la propia institución y su entorno. La relación entre probabilidad de ocurrencia y valor de pérdida, da lugar a un índice o factor de riesgo.

Debido a que en la Administración Pública se procesan informaciones que no son fácilmente cuantificables, la medición de su pérdida se debe efectuar con base en evaluación cualitativa, en la que se consideren escalas de daño en términos de confidencialidad, continuidad de las operaciones institucionales, imágen pública, impacto político, entre otros. Se trata de calificar qué informaciones y qué puntos de su flujo representan niveles de riesgo considerable y, por ello, deben se objeto de protección. Como apoyo a este fin, se presenta una metodología de análisis de riesgo en el anexo 4 de este trabajo.

El análisis de riesgos permitirá listar, en escala de prioridades, los riesgos a cubrir. Para cada uno de ellos, se deberá decidir si,

a) se absorbe --la institución asume el costo del riesgo, cuando son de corto alcance--,

b) se trasladan --se busca la posibilidad de asegurarlos mediante la contratación de pólizas de seguro,(10)

10.- Por el momento, en México solo se puede contratar póliza de seguro que ampare daños o pérdida en los activos computacionales tangibles: equipos de proceso, terminales impresoras e instalaciones. Las informaciones, programas y todo elemento soportado en medios magnéticos carecen de protección en este rubro. De ese modo, los daños indirectos

c) se reducen --mediante la aplicaciòn de mecanismos de seguridad.

Es importante anotar que los riesgos no se pueden eliminar o anular. En la medida que se tengan activos físicos o lógicos que puedan afectarse con siniestros de cualquier tipo, persistirá un cierto nivel de amenaza.

La seguridad implica costos. La minimizaciòn de riesgos es inversamente proporcional a estos costos. Por ello debe buscarse un punto de equilibrio: si el costo de aplicación de un medio de seguridad es menor al factor de riesgo del elemento informàtico a proteger, se justifica su uso.

Es recomendable elaborar análisis de costo-beneficio, que presenten tablas comparativas de los diversos mecanismos normativos, administrativos, operativos, físicos o lógicos. De estas tablas se determinaràn los medios más idóneos para cumplir las necesidades institucionales. Con esta base, se establece una ruta crítica en la que se determinan plazos --corto, mediano o largo-- para cubrir los aspectos seleccionados de seguridad, con base en la disponibilidad de recursos materiales, financieros y humanos.

Un criterio primordial a seguir en la selección de mecanismos de protecciòn específicos, es que su cobertura abarque el mayor número de aspectos posible de los riesgos

---

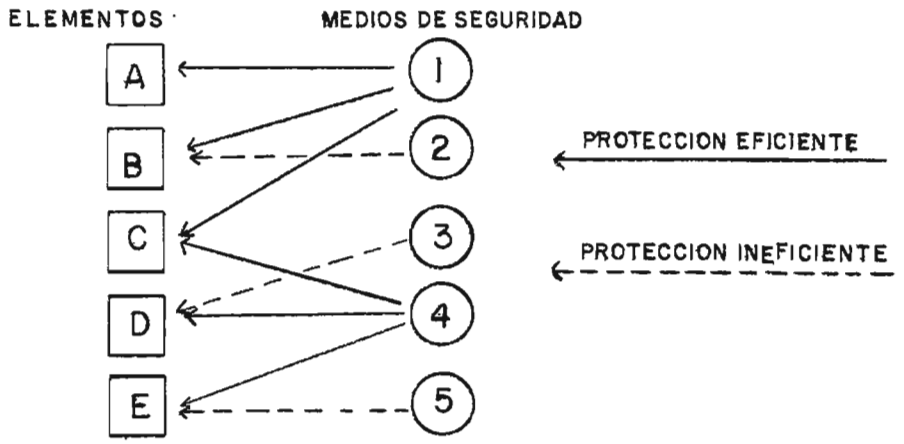
derivados de sistemas de información de instituciones financieras, no estàn cubiertos.

importantes que corre el organismo, es decir, se debe buscar eficiencia.

La finalidad de identificar los elementos informáticos a proteger, es la integración de las medidas de seguridad en esquemas eficaces --en los que cumplan de la mejor manera los requerimientos organizacionales de seguridad-- y congruentes con el presupuesto disponible.

Esquematicamente se ilustra de la siguiente manera.

FIGURA No.5
IDENTIFICACION DE LOS ELEMENTOS INFORMATICOS A PROTEGER, CONFRONTADOS CON LOS MEDIOS POSIBLES DE SEGURIDAD.



E) Desarrollo de propuestas para programas de seguridad informática, diseño de prototipos y fijación de recursos y plazos para operación.

Como consecuencia de las fases anteriores, se desarrollan propuestas de implantación. Se presentan a la alta dirección institucional con objeto de: 1) formular políticas y normas, 2) fijar métodos y procedimientos para el desempeño del personal, y 3) Asignar recursos. Las

políticas constituirán el patrón de conducta esperado en el desempeño del personal a todo nivel de la institución. Las normas son las reglas a seguir para ejecutar adecuada, correcta y previsiblemente las tareas. Estas, al igual que las políticas, deberán quedar asentadas por escrito, en reglamentos interiores, manuales, oficios o circulares.

La fijación de métodos y procedientos consiste en estandarizar las formas y secuencia de pasos para efectuar trabajos. En la fase, del proceso administrativo, de planeación, se establecerán los lineamientos de estandarización, o criterios. En la fase de organización, se definirán en detalle los propios métodos y procedimientos, categorías funcionales, reestructuración jerárquica, descripción de puestos, esquemas de autorización, entre otros. La estandarización en los métodos de trabajo permitirá una correcta dirección, seguimiento y control de las operaciones que se lleven a cabo.

La asignación de recursos, por último, es tanto financiera, como material y de personal. Con éstos, se da lugar a la concreción del ejercicio de la seguridad. los montos, tipos y calidad de los recursos serán correspondidos con el espacio que la dimensión de la seguridad informática haya alcanzado en los altos niveles de mando de la institución.

9.2.- ORGANIZACION Y EJECUCION DE LA SEGURIDAD INFORMATICA.

9.2.1.- CATEGORIAS FUNCIONALES DE APOYO AL EJERCICIO DE LA ADMINISTRACION DE LA SEGURIDAD.

Debido al carácter innovatorio del tema que ocupa este trabajo, es necesario mencionar tres categorías funcionales sugeridas para la conducción de la administración de la seguridad informática. Estas son 9.2.1.1) administración de la seguridad, 9.2.2.2) auditoría informática y 9.2.1.3) comité de seguridad informática. Estas categorías se materializan en personas o en unidades administrativas, dentro de la jerarquía institucional. Si se trata de grandes dependencias públicas, se propone crear unidades administrativas. En otros casos, las funciones pueden recaer en personas. La característica primordial de las tres categorías funcionales es que deben depender y reportar a los mandos más altos de la organización.

9.2.1.1.- ADMINISTRACION DE LA SEGURIDAD INFORMATICA.

Esta función es desempeñada por medio de la gestión de un administrador de la seguridad, que puede tener a su cargo un area administrativa con los mismos fines. Sus funciones serán las siguientes.

a) Coordinar la capacitación al personal sobre apreciación de la seguridad y la informática.

b) Administrar la planeación de recuperación ante desastres computacionales.

c) Plantear la problemática de la seguridad informática ante la alta dirección institucional.

d) Proponer los objetivos de seguridad, en la salvaguarda de la integridad, confidencialidad, continuidad y sana operación de los sistemas de información.

e) Conducir estudios de análisis de riesgos computacionales.

f) Determinar los elementos informacionales a proteger.

g) Proponer estrategias, programas, métodos, procedimientos y mecanismos técnicos y operativos para el cumplimiento de los objetivos de seguridad.

h) Practicar control y auxiliar la evaluación de los recursos o medios de seguridad en ejercicio.

i) Investigar hacia la optimización de la seguridad.

j) Asesorar los usuarios en aspectos de control y protección.

l) Ejercer control y vigilancia sobre el *software* de seguridad.

m) Revisar permanentemente la documentación de sistemas y de recursos de seguridad.

n) Ser perceptivo hacia las posibilidades de ocurrencia de actos ilícitos o pérdidas en el ámbito de la utilización de las nuevas tecnologías para el proceso de datos.

En conjunto con la propia administración de centros de cómputo o de servicios informacionales, la administración de la seguridad deberá participar en la toma de las siguientes decisiones.

a) Definir periodicidad para la operación de rutinas de respaldo.

b) Definir resguardo de copias en sitios separados de los centros de cómputo y en lugares remotos.

c) Definir centro de cómputo de respaldo y su correcto funcionamiento. Si éste pertenece a otra institución, será necesario prevenir la comisión de accesos fraudulentos a la información propia. Se deberán revisar las características técnicas del equipo de respaldo: sistema operativo, capacidad de memoria, disponibilidad en caso de emergencia, entre otros.

9.2.1.2) AUDITORIA INFORMATICA.

Esta función también se atribuye a una persona o a una unidad administrativa, según sea el tamaño de la institución. Entre sus funciones, en el terreno de la seguridad, se destacan las siguientes.

a) Evaluación de la consecución de objetivos de integridad, confidencialidad y continuidad de operación, por parte de los sistemas de proceso de datos que se aplican en las instituciones.

b) Evaluación de la eficiencia y eficacia de los recursos de seguridad en ejercicio.

c) Evaluación de los modos como se operan los sistemas y se siguen las prescripciones, administrativas o técnicas, de protección y control.

d) Evaluación de formas de acceso a archivos de datos y sus modificaciones.

e) Participación en desarrollo de sistemas, con objeto que estos incluyan recursos de seguridad y puedan ser auditados.

En coordinaciòn con la categoría funcional de administración de la seguridad, se desarrollarán las siguientes funciones.

f) Participación en desarrollo de sistemas, en todas sus fases, para que incluyan provisiones de seguridad y posibilidad de auditar su operación y los datos implicados.(1)

g) La función auditora retroalimentará aspectos de seguridad, en sus planes, programas, métodos y procedimientos para optimizar la protección, control y buen uso informàtico.(2)

9.2.1.3.- COMITE DE SEGURIDAD INFORMATICA --o equipo interdisciplinario de estudio de la problemàtica de la seguridad.

Para la integración de este comité, se sugiere la participación de los siguientes.

a) Dirección de la institución: alto funcionario con autoridad para tomar decisiones y capacidad para resolver conflictos.

b) Administrador de la seguridad informática.

c) Auditor interno, que opine sobre los aspectos contables y financieros del organismo y emita criterios para el tratamiento de la información.

1.- Este tipo de pruebas se destina a asegurar la correcta lógica y operación de los sistemas. Las técnicas más comunes para ello son: muestreos, distribución de frecuencias, listados de verificación. Todos ellos, con base en la utilización de datos ficticios.

2.- La sección 9.4 profundiza sobre la auditoría informática, como medio de evaluación de la seguridad.

d) El mejor analista-programador de sistemas de cómputo de la institución.

e) Asesor jurídico, que opine sobre el marco normativo aplicable al fenómeno informático y sugiera ordenamientos nuevos.

f) Administrador de recursos humanos. Su participación es vital para coadyuvar en la determinación de normas y políticas de selección, inducción, capacitación, adiestramiento en servicio, motivación y generación de ambiente adecuado de trabajo para el personal cuya labor gira en torno a la informática.

Las funciones a desempeñar por el comité son las siguientes.

a) Apreciar la vulnerabilidad informática y los análisis de riesgo que le son relativos.

b) Analizar el nivel de vitalidad o confidencialidad de las informaciones institucionales.

c) Planear la administración de la respuesta ante desastres computacionales.

d) Desarrollar políticas y normas de análisis, diseño, programación, liberación, operación y evaluación de sistemas.

9.2.2) ORIENTACIONES PARA LA IMPLANTACION DE MEDIDAS DE SEGURIDAD.

En el ejercicio de recursos de seguridad, una vez seleccionados éstos, segùn las necesidades de protección de la organización, se proponen algunas estrategias para su óptimo desempeño.

Primero. Con base en el supuesto de que el sistema de cómputo está orientado hacia el usuario, los mecanismos de seguridad, en todos los casos implican un esfuerzo adicional o inconveniencia para los usuarios. Hsiao afirma "si tales mecanismos no son fàciles de operar, es muy factible que no sean utilizados efectivamente" (3). La razòn màs inmediata de ello es que la seguridad no es el trabajo principal de los usuarios de la informática. Por ejemplo, si toma demasiado tiempo o esfuerzo traspasar --o respetar o hacer valer-- los controles de seguridad, es esperable que en el largo plazo el servidor pùblico busque la forma de evadirlos, para dedicarse màs fàcilmente sus labores cotidianas. Al ejercer seguridad, ésta debe ser lo màs compatible con esfuerzos de simplificaciòn operativa o administrativa, para asegurar su eficiencia.

Segundo. Los sistemas de seguridad deben ser confiables y ostentar garantía en la efectividad de su funcionamiento. De hecho, està en juego la propia seguridad de la institución y ésta debe estar protegida contra descomposturas o mal funcionamiento.

3.- Hsiao, op. cit. P.52.

Tercero. Se deberán establecer diversos sectores de protección y servicios de cómputo, de acuerdo a las funciones y vitalidad de la información. Ello equivale a aislar problemas y dar lugar a ubicar equipos de cómputo en lugares más seguros, si los datos son más críticos. Adicionalmente, proporciona ventajas para que el acceso a las áreas más críticas sea por un camino preestablecido y se diseñe adecuadamente el control y evacuación de instalaciones en caso de siniestro.

Cuarto. Los medios de seguridad deberán estar debidamente estandarizados. Scoma entiende la estandarización no sólo en mecanismos de seguridad, sino para toda una institución y sus elementos informáticos. Afirma que "se debe poner el mismo nivel de protección a información sensitiva que esté almacenada en discos, cintas o papel".(4) Es inefectivo proteger datos durante su proceso electrónico y dejarlos desatendidos en listados o reportes, en oficinas abiertas o basureros. Asegura que un esquema de seguridad informática eficaz comprendería estandarización de medios y normas de protección para todas las áreas y normas en la institución. La cobertura de estos medios se dirigirá a todas las etapas del flujo de la información, en que se establezca una buena combinación de controles generales, específicos, manuales, mecánicos, electrónicos o magnéticos.

4.- Scoma, Louis: "Protecting privacy of information".-- en Journal of information systems management (E.U.A.). Vol.3, No.3, Verano 1984, P. 80.

Quinto. Se pueden reconocer los siguientes atributos para los mecanismos de la seguridad informática, los cuales constituyen referencia a seguir.

I.- Integración armónica de las medidas de seguridad, de tal modo que haya consistencia, congruencia y, a la vez, independencia entre ellas.(5

II.- Documentaciòn suficiente de cada medida, procedimiento, método o politica.

III.- Provisiòn de medidas para monitoreo, es decir, recursos para vigilar su buen funcionamiento y posibilitar auditoría --ninguna medida es efectiva si no se le puede vigilar y detectar en caso de violaciòn.

IV.- Continuidad, de modo que permita su uso por largo tiempo.

V.- Manejar múltiples formas de seguridad, en lo posible, a la vez: Disuasiòn, detección, recuperación, entre otros.

VI.- Dependencia, lo menos posible, de intervención humana y de factores como el suministro de energia eléctrica.

VII.- Estandarización, y posibilidad de aplicación universal, de los mecanismos de protecciòn y control, en una organización. Ello facilita su funcionamiento, seguimiento y control.

VIII.- Confiabilidad de diseñadores, proveedores y usuarios, respecto de la medida.

5.- Cf. Sección 9.2.5.1, inciso B.2.

IX.- Posibilidad de ser anulada o modificada, controladamente, para casos de urgencia o emergencia.(6)

9.2.3.- DISTRIBUCION DE FUNCIONES Y RESPONSABILIDADES.

Básicamente, los mismos aspectos administrativos que existen en un sistema de informaciòn manual o mecánico, se presentan en un medio informatizado: asignaciòn de responsabilidades, identificaciòn y separación de funciones.

La incorporaciòn de la tecnologia informática en las dependencias y entidades de la A.P.F., como parte de un fenómeno global, ha traido cambios en los esquemas con que se distribuyen funciones y responsabilidades, entre unidades administrativas y entre los funcionarios mismos. La informática, con los efectos que "per se" trae el manejo más ràpido, más oportuno y más grande de datos, es un fenòmeno que gradualmente alterarà aspectos formales e informales del desempeño de las unidades administrativas públicas. En general, el cómputo, al inducir mayor productividad, el elemento humano deberà adecuarse irreversiblemente a un estándar de desempeño más moderno y más eficiente.

La asignaciòn de responsabilidades es uno de los componentes fundamentales en la administraciòn de la seguridad. De ella se establece que cada elemento humano en la organización asuma su rol plenamente y sea capaz de responder por el buen o mal desempeño de sus labores. Asi se

---

6.- Estos nueve atributos se tomaron de Parker, Donn: "20 factores a considerar en la selecciòn de medidas para proteger la informaciòn", en Data Processing Digest (U.S.A.). Vol 15, no.6, junio 1987. P. 5.

permite establecer responsabilidad ante cada problema específico, por un lado, y estructurar los niveles en la organización al conocer el personal a quien deberá dirigirse para reportar y consultar sobre aspectos relevantes a la institución.

En vista de la importancia vital de la seguridad informática para la operación, confidencialidad, vulnerabilidad y viabilidad organizacional, ésta debe siempre depender de la alta dirección de la dependencia o entidad, (7), donde recae la màs alta responsabilidad.

Los grandes agregados de responsabilidades directivas serán los siguientes.

a) Determinaciòn de politicas. A los niveles directivos compete establecer y velar por el buen funcionamiento de una politica informática institucional, que incluya todos los aspectos mencionados de la administraciòn de la seguridad.(8)

7.- Lo dicen los siguientes. Hsiao, op. cit. P. 75; González Castellanos, Herbin Amory:"Fraudes en sistemas de procesamiento electrónico de datos" (Tesis para obtener el titulo de contador público y auditor).-- Guatemala: Universidad de San Carlos (Facultad de Ciencias Econòmicas), 1978. P. 57; Peters, A.J.: "Elementos para el desarrollo y revisión de normas a seguir en torno a equipos de computación personal".- en Data Processing Digest (U.S.A.), Vol.15, No.6, junio 1987, P. 8. y Burton Squires: "Una visión resumida de la seguridad de los datos para el administrador de procesamiento de datos".-- en Data Processing Digest (U.S.A.), Vol.3, No.10, octubre 1975, P.13.

8.- Tomado de Mérida Muñoz, Jorge: "Auditoría informática: metodologia, normas, estándares y técnicas"; en Actas: I Congreso iberoamericano de informática y auditoria.(San Juan, Puerto Rico, 2 a 6 de noviembre de 1987), pp.144-145.

b) Operacional, es decir, traducciòn de las politicas en práctica. Ello implica un conocimiento detallado de los sistemas de informaciòn institucionales y la disponibilidad de tecnologias de protección, técnicas o administrativas.

c) Económico, como toma de decisiones que implican erogaciòn y el desarrollo de análisis de riesgos.

En un esquema òptimo de organización informática se debe asignar la responsabilidad de la seguridad a cada usuario, oficina o unidad administrativa. Se trata de que el operario asuma la responsabilidad por los activos informacionales a su cargo --instalaciones, equipos, programas, informaciòn, manuales, etc. El jefe de oficina se responsabiliza por la seguridad de su àrea, de su personal y asi debe ocurrir, sucesivamente, en otros mayores niveles de mando, màs bajos o más altos.

Para los funcionarios pùblicos, las atribuciones y funciones deberàn ser claras, en materia de servicios de informática. El servidor debe saber a quien reportar o a quien recurrir para consultar. En una etapa de informatización joven, una sola unidad administrativa suele prestar servicios de còmputo a una institución completa. Ella, al nivel jeràrquico que esté, se constituye en polo de poder importante. Este esquema cambiarà al tener cada área organizacional sus propios equipos, programadores y operarios. Y en ellos la autoridad formal deberá ser también autoridad en computaciòn.

9.2.4.- ADMINISTRACION DE LA AUTORIZACION.

Como se refirió en la introducción de este trabajo, el proceso de "autorización" es vital en materia de seguridad. Es llave que controla el acceso a espacios físicos o lógicos de una organización. Se constituye esencia de control, al decidir quién sí y quién no deberá accesar recursos computacionales. David Hsiao explica dos aspectos problemáticos para precisar una autorización: a) el control de la autorización y b) rigidez de la autorización. El control de la autorización es propiamente un sistema de información específico, en el que su utilización tiene implicaciones importantes. Es un sistema de control para otros sistemas. Su estructura se ubica en tres categorías.
1a. Centralizado. En éste un individuo o unidad administrativa efectúa todas las autorizaciones.
2o. Jerárquico o Descentralizado. La autoridad central delega atribuciones a unidades subordinadas.
3o. Individual. Cuando no existe jerarquía de autorización y los individuos pueden crear y controlar información. Ellos serán propietarios de sus datos y decidirán su transferencia a otros usuarios.

Estas categorías pueden ejercerse como tales o desarrollarse en combinaciones, para satisfacer las necesidades de la organización. La determinación de la

solución adecuada implica un análisis de ventajas y desventajas en cada caso.(9)

En el tópico de rigidez de autorización se presenta una problemàtica crucial: la seguridad debe detener u obstaculizar intentos de afectar la privacía de la información o la continuidad en la operación de un organismo, pero, a su vez, no debe ser obstaculo para reaccionar oportunamente ante situaciones prioritarias. Ello sugiere la necesidad de ejecutar la estrategia, antes mencionada, de posibilidad de anulación o modificación.(10)

9.- Hsiao menciona las siguientes ventajas y desventajas para cada categoría. El esquema centralizado es viable para organizaciones pequeñas o altamente estructuradas -- militares-- donde el control es simple o inamovible. En casos de instituciones descentralizadas es inoperante, dado que las funciones e información cambian rápidamente. El esquema descentralizado presupone la delegaciòn como norma. Sus problemas radican en que los niveles màs altos de la jerarquia pueden revocar u omitir las decisiones de autorización efectuadas por mandos medios. Ello tiene justificación al defender la postura de que "el jefe es el jefe", pero elimina la posibilidad de existencia de información privada, que en muchos casos es necesaria para el desempeño del servidor. Una posibilidad de soluciòn es permitir creación de archivos de datos cuyo propietario sea el empleado y que se traduzca en informaciòn que sólo él controle. En la categoría individual, la problemática se presenta en ocasiones en que es necesario traspasar mecanismos de seguridad. Si el mecanismo es fácil de violar, se pone en peligro la privacía. Si es difícil, la institución puede sufrir consecuencias negativas ante circunstancias de emergencia --muerte, enfermedad o renuncia. Por todo esto, la definición de esquemas de autorización requiere estudiarse en cada caso bajo la consideración de factores conflictivos y soluciones.
De Hsiao, op. cit. P. 74 Y 75.

10.- V. Supra. Sección 9.2.2, segundo párrafo y atributos de los medios de seguridad, en el quinto tòpico. Un ejemplo, de este tipo de situaciones, es el caso de un hospital donde cada médico tiene acceso exclusivo a los historiales de sus pacientes. Si uno de éstos llega de emergencia al hospital y no se encuentra el médico autorizado y se requiere revisar su historial clínico, se debe preveer la posibilidad de que

Una posible solución es definir niveles de acceso a sistemas. Por ejemplo, 1.- acceso normal o cotidiano, 2.- acceso necesario --en el que quede debidamentese registrado quién acceso, por qué, cuándo y cómo-- y 3.- acceso de emergencia, en que el responsable en turno pueda tomar decisiones ante casos prioritarios.(11)

Estos niveles serán adjudicados a personas de distinto nivel de responsabilidad y con diferentes funciones. En particular cada organismo informatizado, o en proceso de serlo, necesita analizar su propia problemática para integrar soluciones acordes a sus requerimentos.

Las tareas de autorización tienen lugar en cuatro tipos básicos de operación de sistemas: 1) lectura o consulta, 2) alteración o modificación o borrado, 3) creación de archivos o documentos y 4) duplicación o copia de información o programas. La emisión de autorizaciones considerará los siguientes aspectos.

Primero. Si el usuario --empleado o servidor-- trabaja en desarrollo de sistemas o programas, se establecen jerarquías y funciones que cada usuario podrá ejecutar. Asi, cada programador puede leer, alterar, crear o borrar ciertos programas que le son permitidos de acuerdo con su nivel jerárquico, capacitación y funciones.

Segundo. En el proceso de los datos se delimitan tareas con el mismo criterio anterior. Cada operario o usuario, ya

---

otros usuarios --médicos-- accesen esa información. El ejemplo es de Hsiao, op. cit. Pp. 52 Y 53.
11.- Hsiao, op. cit. Pp.71 a 75.

sea area administrativa o persona especifica, estará autorizado para ejecutar una o màs de las cuatro operaciones señaladas con determinado(s) tipo(s) de informaciòn o datos, acordes con sus funciones sustantivas.

Tercero. Una norma fundamental a seguir en el ámbito de autorizaciòn de operaciones es de evitar que el mismo personal que crea o modifica programas sea el mismo que los opere cotidianamente. La no observancia de ello es fuente de manejos ilegales ccon la informaciòn.

Aspectos màs sofisticados de la seguridad son los controles o autorizaciones de dònde y cuándo se pueden efectuar operaciones diversas. Por lo general se aplican en sistemas de cómputo distribuídos. Es decir, en los que existen terminales y equipos situados en diversas localizaciones geográficas e interconectados entre si. El control de "dònde" equivale a definir y limitar las terminales en las que se autoriza efectuar ciertas operaciones con ciertos datos o informaciones. El control de "cùando" consiste en definir horarios o prioridades para ejecutar tareas con los sistemas. Es comùn, ahora, que los sistemas operativos de los equipos modernos de còmputo contengan mecanismos técnicos o lògicos o "utilerias" para efectuar los controles del qué, quién, para qué, dònde y cuándo se utilizan las computadoras y sus archivos.(12)

12.- En la resoluciòn de quién desea o está autorizado a utilizar informaciones, estàn implicados dos procesos a considerar: identificaciòn y verificación. La primera consiste en proveer al equipo o programa de còmputo de informaciòn que distinga a un usuario en particular. Este

9.2.5.- DEFINICION DE METODOS Y PROCEDIMIENTOS PARA LA SEGURIDAD.

La informática se constituye como poderoso recurso en la operación de las instituciones modernas. Por ello, la necesidad de mayor definición y mayor claridad en las políticas, normas, métodos y procedimientos, así como mejor consciencia, mejor desempeño y mayor responsabilidad por parte del personal se harán fundamentales. Con tecnología manual hay mucho espacio para que aspectos como indefinición u omisión de ordenamientos o irresponsabilidad o incapacidad del personal, no provoquen efectos mayores sobre las organizaciones. Sin embargo, con tecnología informática,

---

puede ser ubicado como individuo, como rol o como función. Como individuo, la persona es identificada como tal --p.e. Horacio Albarrán. Como rol, la identificación se corresponde con un cargo administrativo específico y como función, de acuerdo con determinados tipos de operaciones que empleados o servidores de la misma categoría pueden realizar. --p.e. analistas, capturistas. Estas tres formas van de más a menos en cuanto a precisión. La elección a aplicar depende de la complejidad del organismo. Si el número de personas usuarias es bajo, se puede optar por la tercera opción. Por el contrario, con muchos operarios se debe optar por la primera. Los tres tipos no son excluyentes y su combinación es materia de elección en cada organismo.

Por otra parte, la verificación consiste en validar si la persona que accesa el sistema de cómputo es la indicada. Esto se hace por diversos medios: a través de algo que el usuario sabe (clave), lleva consigo (llave o tarjeta magnética) o posee (huellas digitales, firma, geometría de la mano, entre otros).

Una situación usual a evitar es que personal subordinado accese sistemas de información y ejecute operaciones a nombre de altos funcionarios, usando claves de éstos. Esto tiene lugar, dado el desconocimiento informático de los directivos organizacionales o pereza de operar ellos mismos los equipos computacionales. Son por lo general los analistas o secretarias o asistentes quienes accesan archivos y obtienen reportes para determinados funcionarios. Estos aspectos de verificación y identificación se tomaron de Hsiao, David, op. cit. Pp. 49 Y 50.

estas irregularidades pueden tener impactos considerables. Y si se trata de la Administración Pública, la politica y la economia pueden resentir daños criticos.

El objetivo de la definiciòn de métodos y procedimientos es coadyuvar a establecer un esquema de seguridad integral para una dependencia, entidad o unidad administrativa. Esto se logra al formar un sistema de protecciòn y control en el que los procedimientos o medios estén debidamente definidos, estandarizados, obedezcan políticas institucionales de informática, atiendan metodologias de trabajo y documentación completa, aceptada y plasmada en manuales institucionales. --manuales de organizaciòn, de procedimientos, de descripciòn de puestos, entre otros.

9.2.5.1.- LINEAMIENTOS PARA DEFINICION DE METODOS Y PROCEDIMIENTOS PARA LA SEGURIDAD INFORMATICA.

A) En desarrollo de sistemas.

El análisis y desarrollo de sistemas de información debe obedecer a un plan informàtico de la dependencia o entidad, que debe estar en evaluaciòn y actualización permanente. En ese desarrollo deben participar operadores, programadores, asi como auditores y especialistas de seguridad.(13) Con el trabajo en equipo de ellos, se definen instancias de autorización, evaluación y control. Se busca que los sistemas de informaciòn incluyan, desde su diseño, recursos de protección de la confidencialidad e integridad de los datos, según las necesidades del organismo.

13.- De Mérida, op. cit. P. 139.

B) En la operación de los sistemas.

Se define metodología y procedimientos de actuación para la operación de equipos y programas, flujos de información, administración de centros de cómputo y servicios informacionales. En ellos se contemplan acciones que aseguren la recepción adecuada de datos, control durante el proceso, control sobre el personal operativo de captura o emisión de reportes y sobre las operaciones de transmisión o remisión de información a sus usuarios finales.

En este ámbito es necesario atender dos consideraciones.

B.1) El personal operativo deberá ser ignorante, en lo posible, de los alcances y límites del control y la seguridad que se tiene en el organismo.

B.2) Deberá existir independencia entre controles y usuarios, de modo que se eviten colusiones y que un perpetrador no sea detectado.

Durante las etapas de procesamiento de datos, se debe asegurar que la totalidad de ellos guarde valores de privacia e integridad durante las transformaciones, cálculos, respaldos, actualizaciones o validaciones que sufra.

El personal que tenga acceso a la información final, deberá seguir políticas y procedimientos para asegurar que se vele por la calidad, oportunidad y confiabilidad de los datos.

C) En la planeación para enfrentar desastres.

Será trabajo del comité de seguridad la elaboración de planes o métodos de recuperación ante desastres informáticos. Estos consisten en previsiones para responder con oportunidad ante daños mayores o menores, de origen intencional, natural o de errores, que afectan la sana operación de las instituciones. El anexo 1 de este trabajo incluye una descripción completa de un método de recuperación ante desastres informáticos.

9.2.6.- DOCUMENTACION DE LA SEGURIDAD INFORMATICA.

La documentación es sustento fundamental de toda organización y su funcionamiento. Los documentos son la materialización de la institucionalidad de toda dependencia o entidad pública.(14) En aspectos de seguridad constituyen también sustento de toda acción de protección ejercicio de control.

Los documentos importantes para la administración de la seguridad informática son los siguientes.

a) Manual de organización, de cada dependencia o entidad, en el que se plasmen los fundamentos legales para el ejercicio de la seguridad y salvaguarda de la privacia de la información y las atribuciones de las unidades administrativas de cómputo, seguridad y auditoria.

b) Manual de descripción de puestos, que incluya las posiciones de seguridad y auditoría informática, con sus

---

14.- V. Supra. capitulo 3, sección 3.4.

funciones, responsabilidades y lineas de reporte y comunicación en la institución.

c) Manual de procedimientos del organismo, que contemple procedimientos a seguir para la seguridad computacional.

d) Método o plan de recuperación ante casos de desastre informático.

e) Método o plan de respuesta ante el crimen computacional, con el que se buscara minimizar los daños informáticos criminales en las instituciones y aprender al máximo de éstos. El anexo 2 de el trabajo describe el contenido de éste.

f) Manual de inducción al puesto, en el que se contemplen elementos de cultura informática y respeto por la seguridad computacional, a toda persona que ocupe posiciones relacionadas con las aplicaciones informáticas.

g) Documentación de las medidas de seguridad en ejercicio, ya sean de tipo técnico, administrativo, jurídico, etc. Normalmente se plasman en manuales de usuario y manuales técnicos.

9.2.7.- ESTRUCTURA ORGANIZACIONAL- JERARQUIA.

La incorporación de equipos o dispositivos de cómputo genera necesidad de crear unidades administrativas para su operación o modificacion en las unidades ya existentes, que utilizan servicios informáticos. Con base en el tamaño de la institución y de la cobertura de los servicios informáticos, se establece una unidad, independiente de otras de tipo operativo, sustantivo o de apoyo. Su creación se asienta en

el manual de organización de la dependencia o entidad y se le define su posición jerárquica, así como los mecanismos regulares de comunicación y reporte a instancias superiores.

Las categorías funcionales de administración de la seguridad y de auditoría, se establecen en niveles tales que reporten directamente a los altos mandos organizacionales. Tendrán que ser funciones independientes, inclusive, de la administración del centro de cómputo institucional.

Para las unidades de informática, las de auditoría y las de seguridad, se deberá contar con definición de políticas, métodos y procedimientos, descripción de puestos, segregación de funciones y normas de control. (15)

15.- De Mérida, op. cit. Pp. 142 a 145.

9.3.- EL PERSONAL INFORMATICO.

Los aspectos de personal constituyen el principal asunto de la seguridad computacional. Son personas las que diseñan, operan y controlan sistemas de información y hacia ellos se dirige toda previsión de errores, pérdidas o problemas. Los especialistas consultados, durante la fase de investigación para este trabajo, coincidieron que los recursos humanos propios de las instituciones constituyen el reto principal en toda acción dirigida al control o protección informática. Los factores que apoyan esta postura son varios. Primero, el personal que labora en una determinada dependencia o entidad tiene facilidades para el acceso y utilización de los bienes y recursos computacionales e información. Segundo, los individuos que tienen contacto rutinario con los sistemas de proceso de datos, conocen mejor su operación, alcances y limitaciones. Tercero, pueden conocer ampliamente el valor de la información, equipos o dispositivos, así como su vulnerabilidad al ser objeto de manipulaciones diversas.

Bajo estas consideraciones, se hace crítica la instrumentación y ejercicio de políticas adecuadas hacia el desempeño del personal. Hsiao reconoce que la educación de los usuarios de servicios de cómputo es requisito fundamental para el ejercicio de nuevos y efectivos procedimientos de seguridad.(1) De ello se desprende que el éxito de todo plan o medio de protección está condicionado a un buen desempeño del personal. Kearby, por su parte, afirma

1.- Tomado de Hsiao, op.cit. P. 56.

que las pérdidas, efectivas o potenciales, en sistemas de cómputo, pueden ser reducidas, de manera importante, con la aplicación de un buen plan de seguridad hacia el personal.(2)

Este capítulo aborda diversos aspectos relevantes para una administración de personal, orientada hacia la seguridad informática. Se tratarán seis temas. 9.3.1) Lineamientos de políticas de personal. 9.3.2) Selección e inducción de personal. 9.3.3) Capacitación y desarrollo del personal. 9.3.4) Responsabilidades de la alta dirección, en materia de personal. 9.3.5) Implantación de nuevas medidas de seguridad en materia de recursos humanos. 9.3.6) Impacto de la informática en las condiciones de trabajo.

9.3.1) LINEAMIENTOS DE POLITICAS DE PERSONAL.

Las organizaciones administrativas son sistemas de comportamiento cooperativo. Se espera que los miembros de éstas se orienten y comporten de acuerdo con ciertos fines que se adoptan como objetivos de la institución.(3) El papel de las políticas de personal es de coordinar el comportamiento de las personas hacia objetivos o fines comunes en el organismo.(4)

2.- Kearby, D'Ann: "Personnel policies, procedures & practices: the key to computer security", en Computer Security Journal (U.S.A.), Vol.4, No. 1.,1986. P.65.
3.- Simon, Herbert: "El comportamiento..." , op. cit. P.66.
4.- Simon sostiene que "el objetivo de la organización es, indirectamente, un objetivo personal de todos los participantes"..."Es el medio por el que sus actividades organizativas se ligan para satisfacer sus móviles personales." V. Simon, op, cit. P.17. Ante ello, las políticas de personal tenderán a incrementar el bienestar de sus servidores, para que de ello se derive un óptimo

En el ejercicio de la seguridad informática se proponen diez lineamientos a seguir en la administración del personal, con miras a hacer eficaz y efectivo el control y resguardo de activos informáticos. Son los siguientes.

A) Las normas de seguridad deben estar claramente definidas por el alto mando de la institución. Se requiere, para ellas, completa documentación y determinación de responsabilidades y penalidades ante la falta de observancia en su ejercicio. Ello es requisito para hacer valer una disposición.

B) El empleado o servidor debe conocer la importancia y procedimiento de las normas de seguridad, así como recibir entrenamiento acerca de su funcionamiento.

C) El concepto de seguridad debe introyectarse en el servidor público desde el dia que ingresa a la organización y permanecer para siempre, aún después de separarse de sus funciones públicas.(5)

D) Se buscará que el empleado se sienta satisfecho. Así es leal y respetuoso de las normas y procedimientos establecidos. El descontento hace dar da poca importancia, y es amenaza, a la seguridad.(6)

---

ambiente de trabajo, en apoyo al ejercicio de la seguridad informática.

5.- El concepto de seguridad no debe desaparecer o menospreciarse en el momento que un servidor público se separa de sus funciones. Al conocer la dinámica y operación de los sistemas informáticos y estar fuera de la organización, puede, aún, ser potencial de amenaza a la seguridad computacional.

6.- Afirmación de Kearby, ibid.

E) La responsabilidad del ejercicio de la seguridad, para cada departamento o unidad administrativa, corresponde al dirigente de ella, que debe estar consciente de las necesidades y tareas de protección y control en el area a la que sirven. El administrador informático, el auditor o el especialista en seguridad constituyen elementos de apoyo a la seguridad. Diseñan, desarrollan, prueban y ponen en función medidas o mecanismos de resguardo. La responsabilidad de operación corresponde al propio usuario.(7)

F) El número personas que tenga acceso a la información o a dispositivos computacionales debe ser el mínimo necesario, en cualquier fase de su flujo --captura, proceso, consultas, reportes o copiados.(8) Se debe descartar personal innecesario en la operación informática. Asimismo, cada individuo tendrá acceso a datos y operaciones que sean absolutamente necesarias para el desempeño de su trabajo.

G) A cada persona que labora con equipos o datos se le atribuye responsabilidad directa sobre el buen y correcto funcionamiento y protección de éstos.(9)

H) Es necesario que haya independencia entre usuarios y controles. Ello permite evitar violación de medidas de

---

7.- V. Sección 9.2.3. Distribución de funciones y responsabilidades.
8.- Idea de Kearby, ibid. P. 66.
9.- Peters, op. cit. P. 8.

seguridad y colusión entre servidores de una o varias unidades administrativas.(10)

I) La rotación de personal debe observar procesos adecuadamente controlados, con objeto de garantizar la continuidad en los proyectos o programas en ejecución y que las operaciones se mantengan en un ambiente de estricta seguridad.

9.3.2) SELECCION E INDUCCION DE PERSONAL.

Al constituirse las areas de informática en las organizaciones, se convierten en sistemas nerviosos y elementos de productividad. Las exigencias hacia la calidad del personal toman, entonces, un matiz crítico. Por ello, los métodos y procedimientos de selección de recursos humanos e inducción al puesto presentan requerimientos más cuidadosos que las formas de operación o administración tradicional.

Con base en la descripción de puestos, efectuada en la etapa de organización --del proceso administrativo--, se determina el perfil de cualidades o caracteristicas de candidatos para las diversas funciones y a ello se apega la selección de personal. En adición, se sugiere considerar los siguientes aspectos.

Primero, toma un grado relevante el hecho que la persona se sienta plenamente satisfecha con el puesto que ocupa. Como se comentó anteriormente, de ahí subyace la lealtad a la

---

10.- Parker, Donn, op. cit. P.4. V. Supra. Sección 5.3, referente al delito informático.

organización. En areas informatizadas esta lealtad debe ser óptima.

Segundo, como consecuencia del anterior, se debe evitar que el nivel de preparación técnica del empleado o candidato supere significativamente los requerimientos del puesto que ocupa. Cuando el mercado laboral es limitado, los individuos pueden conformarse con posiciones inferiores a su capacidad, con el fin de obtener estabilidad en el empleo. En informática, es riesgoso para una institución que un servidor sepa más de equipos, programación o comunicaciones de lo que es necesario para su puesto. Bajo esta premisa, el empleado se convierte en violador potencial de la seguridad.

La siguente fase es la inducción a la institución y al puesto. Consiste en familiarizar a la persona con su entorno organizacional, con el trabajo y las relaciones que tendrá que desarrollar, asi como con sus derechos y obligaciones. Es recomendable que exista, para ello, un manual de inducción al puesto, en la dependencia o entidad, que unifique criterios, metodos y procedimientos al respecto.

En etapas sucesivas, se adiestra al personal en forma teórica y práctica, hacia sus labores y, a partir de ello, se fundamenta un proceso de adecuación de aptitudes y actitudes que incorporen al servidor objetiva y subjetivamente a la organización.

Herbert Simon sostiene que esta adecuación se da cuando las decisiones de la alta jerarquía organizacional surten efecto en el personal. Para ello es necesario que tales decisiones se comuniquen adecuadamente a traves de dos medios. 1) Formación en el empleado de hábitos y espíritu que lo conduzcan a tomar decisiones ventajosas para la institución y 2) imposición al trabajador operativo de las decisiones tomadas en los mandos medios y altos, lo que equivale al ejercicio de autoridad y al de medios de comunicación administrativa. Esta imposición deberá tener lugar de tal modo que se minimice la posibilidad de resistencia ante el cambio por parte de los servidores afectados. (11)

Desde el punto de vista, tanto de eficacia y eficiencia, como de seguridad, las fases de inducción y adiestramiento son vitales y condicionantes de la calidad del trabajo que el individuo desarrolle. Elementos como la asimilación de una mística o ética de trabajo, conocimiento de estándares de cumplimiento de las tareas, la familiarización con la normatividad aplicable y criterios para su ejercicio, son factores relevantes en la incorporación de las personas a un nuevo ambiente laboral. Para el caso de aprendizaje de reglas y controles, no se pretende que el empleado los asimile en forma intensiva y

---

11.- Ver. Simon, op. cit. Pp. 12 y 13. Para una discusión sobre diversos conceptos acerca de la aceptación de una decisión por parte de un subordinado, ver el apartado denominado "El comportamiento administrativo". Ibid. P.13.

extensiva, en lapsos cortos de tiempo. Más bien se trata de que se familiarice, primero, con los principios fundamentales de trabajo y, con el tiempo, conozca las reglas en mayor detalle. Más que aprender completamente las normas, en materia de seguridad o protección o control, es más relevante la presencia de un espíritu de trabajo donde se conjunte satisfacción personal con elementos de respeto a la organización, prudencia y responsabilidad --hacia la organización y sus elementos de trabajo. De la mística del servidor se desprende la seguridad institucional y el correcto desempeño para llegar a los fines que se proponen las dependencias y entidades públicas.

9.3.3) CAPACITACION Y DESARROLLO DE PERSONAL.

En materia de seguridad informática la sensibilización hacia la vulnerabilidad o amenazas, que pueden afectar un ambiente determinado, cobra reviste un alto valor. En países desarrollados esta sensibilidad ha crecido en la medida que las pérdidas por actos indebidos o errores, en torno a la informática, crecen y son comunicados . En México es prácticamente inexistente. Salvo personal directivo o especialistas en instituciones bancarias, académicas y judiciales, las personas rara vez comprenden las cuestiones de protección y privacía como asuntos de interés. Inclusive, es frecuente que el personal directivo, con pocos conocimientos prácticos de la computación, pero que tiene a su cargo importantes activos informacionales, vea con ingenuidad los aspectos de seguridad.

Hsiao presenta conclusiones de estudios sobre sensibilidad hacia la seguridad informática. Afirma que el grado de seguridad demandado por un usuario es proporcional a su conciencia de las posibles amenazas. Afirma que se percibe a los "violadores" como espejos de si mismos. Es decir, que en la medida que el usuario conoce medios o "trucos" para traspasar un sistema de seguridad, asume que los "enemigos" son equivalentemente capaces.(12) Si, por el contrario, no conocen medios de violar la seguridad, asumen que los sistemas informáticos son impenetrables.(13) Esta visión es relevante porque de ella parte la problemática que se aborda en este trabajo. Al existir correspondencia directa entre el conocimiento informático, amenazas y seguridad, se refleja que toda iniciativa de proveer seguridad computacional será resultado del conocimiento -- sensibilidad-- de la vulnerabilidad informática que exista en los niveles de toma de decisiones de las instituciones -- alta dirección.

Asimismo, el personal operativo o usuarios se preocupan por proteger la información y los dispositivos técnicos en la medida que tienen una cultura informática. Esta consiste en una visión global del mundo informacional de la que se desprenden aptitudes y actitudes encauzadas a adecuarse a nuevas formas prácticas, métodos, mentalidad y mística de

12.- Las comillas son del autor y traducidas al español.
13.- Cita que estas conclusiones son congruentes con la teoría psicológica de la atribución. Los individuos evalúan las motivaciones y comportamiento de otros atribuyéndoles sus conocimientos, valores y sentimientos. Ver. Hsiao, ibid.

trabajo.(14) Se trata de comprender y asumir la dinámica de la "revolución informática" que se vive en la actualidad y su impacto en la vida de la sociedad. Es una etapa evolutiva del pensamiento humano, donde la información se reconoce como activo. Las mentalidades adecuadas a una sociedad de información manual se tornan inconsistentes en un mundo informatizado.(15)

En general, la capacitación, o entrenamiento, "prepara al miembro de una organización para que tome, por si mismo y satisfactoriamente, decisiones sin necesidad de una supervisión e imposición de decisiones continua". Es por ello una alternativa al ejercicio de la autoridad, como medio de control sobre la operación o decisiones del personal subordinado. La capacitación provee al servidor del conocimiento de soluciones o criterios aceptados, que deberá considerar al desarrollar sus labores.(16)

14.- Esta definición de cultura informática es propia.
15.- Existen factores externos a las organizaciones que crean mayor conocimiento en los individuos acerca de las potencialidades derivadas de la aplicación de la computación y avances en comunicaciones. Entre estos factores destacan 1) los medios masivos de comunicación que incrementan utilización y difusión de las nuevas tecnologías y 2) el contacto directo de mayor número de personas con medios informáticos, para su vida cotidiana. Estos constituyen medio de apercibimiento en las personas de un nuevo modo de funcionar de la sociedad. No obstante, para fines de las instituciones, se necesita más que eso para la difusión de una auténtica cultura informática. V. Hsiao, David, op. cit. P.56.
16.- Simon, op. cit. P.17. Es conveniente consultar algunos aspectos problemáticos que presenta el entrenamiento o capacitación y que cuyo abordaje rebasa los objetivos de este trabajo. V. Ibid. Pp. 161 a 163.

Para un ambiente de seguridad informàtica, se hace necesario que el servidor pùblico conozca esta seguridad y la respete. Ante ello, cobran importancia especial los programas de capacitación en materia de resguardo de los bienes informacionales y los equipos y dispositivos de cómputo, así como de cuestiones de privacía y control. Es necesario, además, proveer al personal de una adecuada educaciòn en el momento que se ponen en ejercicio programas de seguridad o medios o mecanismos especificos de control.

Para las acciones de capacitaciòn, se recomienda tener en cuenta las siguientes alternativas de acciòn.

A) Desarrollar mesas redondas o cursos o conferencias motivacionales que promuevan la satisfacción o bienestar del servidor y den salida o canalicen su posible descontento o tensiones que pudieran existir. Ello debe acentuarse entre el personal que desempeña funciones criticas en la operación de la dependencia o entidad, que redunde en mayor compromiso y lealtad hacia la institución, que lleve a un mejor ejercicio de la seguridad.

B) Orientar al usuario sobre los requerimientos de cuidado en equipos y dispositivos informàticos, asi como de las responsabilidades que debe asumir para el buen uso de los datos que se procesan.

C) Al personal de mando alto y medio, hay que hacerlo sensible de los riesgos que presenta un ambiente computarizado y los cuidados que deben observarse en las areas bajo su dirección. Adicionalmente, deben comprenderse

a si mismos como los responsables de sus unidades administrativas, en materia de seguridad.

D) Al entrar en funciones nuevas normas, métodos o procedimientos de seguridad, es necesario que el personal,

D.1) conozca los riesgos que originaron la medida o mecanismo,

D.2) aprenda las caracteristicas de su funcionamiento,

D.3) reciba entrenamiento adecuado,

D.4) conozca los castigos derivados del incumplimiento u omisiones y

D.5) sepa que existe documentación escrita sobre las medidas de resguardo para ser consultadas. Se sugiere lea manuales y asiente, con rubrica, que se comprendió lo leído.

9.3.4) RESPONSABILIDAD DE LA ALTA DIRECCION EN MATERIA DE PERSONAL.

Son los altos mandos los que definen normas a seguir y las responsabilidades de cada area en materia de seguridad informática. En los aspectos de personal se recomienda la observancia de los siguientes lineamientos.

A) Ejercer supervisión permanente para que no haya empleados que tengan acceso a informaciòn innecesaria o superflua para su trabajo.

B) Al tener lugar una renuncia, conviene entrevistar al interesado y sus compañeros de trabajo, para detectar problemas en la unidad administrativa en que se desempeñó. Es importante que exista comunicaciòn fluida entre la alta

dirección y los mandos medios que tengan bajo su jurisdicción personas con problemas.

C) Al ascender o promocionar servidores hacia puestos en los que se tenga acceso o se procese información vital o confidencial, es necesario que se estudie minuciosamente los antecedentes del candidato.

D) De la debida estandarización de métodos, procedimientos y normas, se desprenderá su ejercicio bajo principios de justicia y equidad. Asimismo, con base en su aplicación universal, se facilita la evaluación de su operatividad.

E) Promover evaluación periódica de los empleados con base en estándares establecidos, así como aconsejar, entrenar o reasignar al personal de acuerdo con las evaluaciones.

9.3.5) IMPLANTACION DE MEDIDAS DE SEGURIDAD EN MATERIA DE RECURSOS HUMANOS.

Para la puesta en función de una determinada medida de seguridad, se recomienda atender las siguientes premisas.

Primera. Karabin, recomienda una estrategia valiosa de implantación de mecanismos de seguridad. Plantea orientar a los propietarios o usuarios de datos a que ellos determinen la importancia de su información, con base en políticas predefinidas y con miras a asegurar la sana operación de la organización. De ahí sugiere que el mismo personal participe en la implantación de programas o sistemas de seguridad, de tal modo que los sienta como suyos. Así, el servidor asume

su parte en el proyecto y en el largo plazo se pueden derivar resultados satisfactorios. (17)

Para valorar la importancia de la protección y control, es necesario que las personas conózcan los recursos informáticos bajo su responabilidad. Con base en ello, se puede apreciar la verdadera dimensión, razón de ser de la seguridad y las necesidades a cubrir. Se pretende, con ello, que el servidor público conozca que hay ciertas restricciones y normas. No se espera que las respete como tales, sino que comprenda los requerimientos de seguridad, los haga suyos y los apoye. Es tarea del alto mando organizacional promover ambientes de trabajo propicios para hacer valer estas premisas.

Segunda. En principio, el éxito de una política o medida de seguridad informática, depende de la sensibilidad, responsabilidad y cultura computacional que esté presente en el personal. Sin embargo, por otro lado, revisten importancia la consideración del impacto que un determinado medio de protección puede tener entre el personal, y el resultado al que se llegará. Cierto tipo de medidas inciden en la reducción de errores, ofrecen mejor confiabilidad, aunque haya menor productividad. En ese sentido puede resultar contraproducente ejercer medidas estrictas en extremo, que aunque pueden reportar mayor eficacia provocan

---

17.- Adaptado de Karabin, Steven: "Clasificación de datos: una breve guía".-- en Data Processing Digest" (U.S.A.), Vol. 15, No.2, febrero de 1987. P. 7.

ambientes tensos de trabajo. (18) Donn Parker menciona que, además de satisfacer requerimientos de costo y efectividad, para los medios de seguridad se deben estudiar modificaciones en la operación y en el medio ambiente de trabajo, en cada caso.(19)

9.3.6) IMPACTO DE LA INFORMATICA EN LAS CONDICIONES DE TRABAJO.

Como efecto natural de la introducción de nuevas tecnologías en los ambientes humanos, la informática altera dramaticamente la dinàmica de las organizaciones, en sus funciones, estructuras y valores.(20) El personal resiente cambios en sus rutinas y modos de trabajo y responsabilidades. Ello afecta, de algùn modo, su bienestar y satisfacción personal, el buen desempeño de sus funciones, asi como la lealtad a la institución.

La Organización Internacional del Trabajo ha reconocido, en diversas publicaciones, que la incorporaciòn de nuevas tecnologías para proceso de información puede tener efectos adversos sobre el personal, en caso de no rediseñarse las condiciones de trabajo de las instituciones. Señala los efectos negativos sobre el personal, causados por las tecnologías informáticas y propone medios de solución.

En general, la falta de acoplamiento o adaptación de los ambientes y condiciones de trabajo, hacia las

---

18.- Parker, Donn, ibid. V. Supra. Sección 9.2.2. Orientaciones para la implantaciòn de medidas de seguridad.
19.- Parker, ibid.
20.- V. Supra., introducción, p. i y ss.

necesidades los operadores computacionales, se traduce en *stress* o tensión física y nerviosa que, con el tiempo, se revierten en contra de las instituciones. El trabajador insatisfecho, desmotivado, reprimido o resentido; dificilmente puede ser productivo. Manifiesta su descontento a través de reacciones irracionales, resistencia o rebeldia. Los efectos sobre si mismo y sobre la organización se presentan en el cuadro 11.

CUADRO NUM. 11

EFECTOS DEL *STRESS* OCUPACIONAL

EFECTOS EN EL SERVIDOR	EFECTOS EN LA ORGANIZACION
Apatia en el trabajo.	Ausentismo
Irritabilidad	Alta rotación de personal
Depresión	Dificultad en relaciones de trabajo
Propensión al trabaquismo, y drogadicción o alcoholismo	Pobre control de calidad poca productividad
Afecciones fisicas.	
Cansancio.	

Fuente: Basado en, International Labour Office Geneve: "Automation: work organisation and occupational stress".-- Geneva: I.L.O., 1982. P. 166.

El trabajo informático es generador del *stress* ocupacional en varias vertientes, entre otras.

Primero. El trabajo con monitores, o pantallas, de cómputo provoca cansancio o tensión nerviosa en los operadores. En general, al trabajar en tiempos prolongados frente a una terminal o equipo de microcomputación, el empleado resiente problemas de vista, dolores de cuello y espalda y fatiga. En el aspecto visual, el ojo sufre cansancio al tener que moverse continuamente entre pantalla-teclado-documento escrito. Cada movimiento ocular implica adaptación a diferentes niveles de iluminación, reflejos, brillantez y distancias. Adicionalmente, las pantallas o los documentos pueden no tener suficiente nivel de contraste y la vista tiene que ejercer esfuerzos adicionales para comprender escritos.(21)

El operador informàtico, adicionalmente, suele padecer dolores de cuello y de espalda, por estar sentado frente a un determinado equipo durante tiempos prolongados.

Segundo. Con la computación, el trabajo se vuelve más repetitivo y rutinario. La informática provoca un trabajo "acompasado al de la maquina", que genera aburrimiento, monotonia y, por lo tanto, insatisfacción del trabajador.(22) En muchos casos, las labores computacionales

21.- International Labour Office: "New technologies: their impact on employment and working environment.-- Geneva: I.L.O., 1982. Pp. 34 a 39.
22.- Oficina Internacional del Trabajo: "Las repercusiones socioeconómicas de las nuevas tecnologías".-- Ginebra: O.I.T., 1985. (Comisión Consultiva sobre Tecnología. Primera Reunión. Ginebra 15-19 de abril 1985.) P. 39. V. también International Labour Office:" New Technologies...", op. cit. P. 128.

dan lugar a aislamiento o reducción de contactos personales, al venir largos periodos de trabajo, exclusivamente, con equipos informáticos. Aunado a ello, el servidor tiene menos libertad de decidir dónde y cuándo actuar. El trabajo se torna más intenso y menos interesante.(23)

Tercero. Conforme los empleados tienen mayor edad, se dificulta su adaptación a nuevos ambientes tecnológicos. Por ello, se requiere dar atención al desarrollo de programas de adiestramiento y motivación. (24)

Cuarto. Debido a que los sistemas informáticos tienen diversos controles de operación, se reducen las funciones de supervisión. De ese modo, desaparecen, cada vez más, las posiciones intermedias y se hace más amplia la división entre el trabajo directivo y las operaciones ordinarias subordinadas. Ello merma las perspectivas de ascenso del personal. De hecho, en unidades administrativas altamente informatizadas, son muy pocos los sevidores con funciones supervisoras.(25)

Quinto. El trabajo con equipos impresión de reportes genera niveles considerables de *stress* o tensión, debido al

---

23.- Ibid.
24.- International Labour Office Geneve: "Automation: work organisation and occupational stress".-- Geneva: I.L.O., 1982. P. 17.
25.- Oficina Internacional del Trabajo: "Las repercusiones...", op. cit. P. 40. Cabe resaltar en este aspecto la afirmación de Herbert Simon en el sentido de que las operaciones o decisiones programadas tienden a desplazar las no programadas. Así, la discrecionalidad en la toma de decisiones se restringe cada vez más para los mandos altos de las instituciones. V. Simon, Herbert: "La nueva ciencia...", op. cit., p.45.

ruido y vibraciones que emiten éstos y que, a la larga, afectan el oido.(26)

Sexto. Cuando se tienen excesivas medidas de control, y se trata, adicionalmente, de sistemas de información criticos, el servidor se tensa. Hay, por ejemplo, programas que registran cada error cometido al digitar, con fines de eleboración de estadísticas de productividad, pero el efecto puede ser adverso.(27)

En diversos foros, convocados por la Organización Internacional del Trabajo, se han propuesto medios de solución de estos y otros aspectos problemáticos de la informática en el medio ambiente humano. Entre las medidas mas destacadas, están las siguientes.(28)

Primero. Se requiere que la luminosidad y contraste, en las pantallas y documentos escritos se uniformice a modo de evitar esfuerzos innecesarios en los operadores. Asimismo, la luminosidad de las habitaciones que alojan equipos informáticos deberá ser regulable.

Segundo. Se recomienda que los servidores que operan equipos informáticos se sometan a exámenes médicos, psicológicos y de vista, de manera periódica, a modo de garantizar su buena salud.

26.- Esto pasa con las impresoras de carro movil, pero no con las que funcionan a base de rayo laser, que son de la tecnología más moderna.
27.- Oficina Internacional del Trabajo: "Las repercusiones...", op. cit. P. 40.
28.- Basadas en International Labour Office: "New technologies...", op. cit. Pp. 124 y 125.. Del mismo autor", "Automation...", op. cit. P. 60.

Tercero. Se deberá profundizar sobre estudios ergonométricos para las instalaciones informáticas y su operación. Así, se buscaría evitar generación de dolores o cansancio en los operadores.

Cuarto. Ante los efectos de *stress* informático, la Organización Internacional del Trabajo recomienda reconsiderar las jornadas laborales para los servidores que operan equipos de computación. Sugiere que el trabajador no esté más de cuatro horas frente a un monitor, en un sólo dia. Y, adicionalmente, después de cada hora y media de trabajo tome quince minutos para descanso o distensión.

El terreno de la seguridad, higiene y condiciones laborales de los trabajadores de la informática se encuentra poco desarrollado. En el terreno computacional, se tendràn que plantear modalidades en las formas de desempeño de los servidores públicos, en busca de que se sienta siempre estimulado y tenga un entorno adecuado para un trabajo sano. En el corto plazo, será necesario investigar más profundamente estos aspectos, constitutentes esenciales de la seguridad informática.

9.4.- EVALUACION DE LA SEGURIDAD INFORMATICA.

La evaluación de sistemas de información se ha polularizado, a nivel internacional, como fase importante de la administración computacional, en general. El instrumento básico para ello se conoce como "auditoria informática" o "auditoria computacional". Es una nueva disciplina, en el ámbito del procesamiento electrónico de datos. Hasta ahora, han sido auditores en informática los que se han ocupado de la evaluación de los aspectos de seguridad, como una de las múltiples áreas que atienden. Del trabajo de muchos de ellos se obtuvieron elementos que han sustentado parte importante de este estudio. Esta sección, abordará aspectos de bases, metodologia, técnicas de auditoria y participación de la función auditora en el desarrollo de *software*.(1)

1.- La auditoria informática nace en la década de los 50. El Departamento de Marina de los Estados Unidos de América publica un libro sobre este tema. Ello es mencionado por Lambarri, Alejandro: "La auditoria informática: bases, normas y *software*".-- mimeo, s.p.i., feb. 1989. P.2. En 1969 nace la "Electronic Data Processing Auditors Association" (EDPAA), agrupación de especialistas en evaluación de sistemas de cómputo. Nace ante la necesidad de contar con profesionales para señalar los riesgos y posibles efectos en las instituciones, así como formas de solución. Se definen las bases y responsabilidades para los auditores en informática, Dirige sus esfuerzos a promover la investigación, educación y certificación de la auditoria de sistemas de información. En 1985 se aprobó el establecimiento de normas para la práctica profesional en este campo. En 1976 se crea en México la "Asociación Mexicana de Auditores en Informática, A.C." (AMAI), capítulo de la de la EDPAA, para abordar en nuestro país problemas similares a los tratados en los Estados Unidos. Las normas propuestas por la EDPAA y la AMAI rigen el trabajo de los auditores en términos de garantizar la calidad de sus servicios. Estos se basan en un código de ética profesional el cual estipula que los miembros de dichas asociaciones y los poseedores de certificados CISA --certificación de cualidades profesionales de auditor en sistemas de

La misión genérica de la auditoría informática es emitir opinión profesional, a semejanza de la auditoría tradicional, sobre el desempeño de los sistemas de información, en fases de diseño, desarrollo y operación. Asimismo, evalúa el correcto tratamiento del acervo de datos institucionales. Con base en los estándares, políticas, normas y métodos institucionales, se evalúa la medida en que los recursos computacionales responden a ellos y el apego a los fines propios de la organización. La auditoría informática permite ponderar y mejorar la calidad, cantidad, seguridad y rentabilidad de los servicios de informática, de modo que se garantice 1) un control preventivo en la confiabilidad, integridad y confidencialidad de la información y los sistemas tecnológicos que la soportan y 2) control detectivo de disfunciones e la operación y control correctivo, así como sugerencia de medios para mejorar la gestión informática. La auditoría informática evidencia, finalmente, la calidad de la información que sustenta las decisiones y operaciones institucionales.(2) Es así un

---

información, a los asociados que pasan el exámen para ello-- estarán sujetos a la normatividad adoptada por la misma asociación. La no observancia de las normas da lugar a la revocación de la membresía y, en su caso, de la certificación. Forman parte de la A.M.A.I., fundamentalmente, los servidores públicos que desempeñan funciones de auditoría o seguridad en sistemas de información en las sociedades nacionales de crédito y especialistas que laboran en despachos privados. Para ellos existe una "Carta de los deberes y derechos del asociado de A.M.A.I." Ver, Boletín Informátivo-A.M.A.I. (México),Feb.89. Pp.16 y 17.

2.- Martínez Margarida, Rafael: La automatización de la auditoría: la auditoría del futuro; en Actas (Primer

valioso auxiliar de la gestión de la dirección de tareas informáticas y de la alta gerencia institucional.(3)

Para la evaluación de la seguridad, se propone la aplicación de la propia auditoría informatica, adaptada a la evaluación de la protección, control, buen uso, confidencialidad e integridad de la información y de los propios sistemas. El desarrollo de esta función se propone efectuar de manera independiente a las tareas de planeación, organización y ejecución y de administración de personal, abordadas en secciones anteriores. Se desempeñará en los siguientes conceptos a evaluar.

i) El apego o cumplimiento de políticas, normas, métodos y ordenamientos legales vigentes. Es decir, de las

---

congreso iberoamericano de informàtica y auditoría).-- Puerto Rico, Nov. 1987. P. 82.

3.- La auditoría informática es citada en esta sección del trabajo como el instrumento màs popular de evaluación de sistemas de información. La seguridad es solo uno de sus campos de trabajo. Le compete además, por citar algunos aspectos, el análisis de oportunidad en adquisiciones de equipos y dispositivos, anàlisis de viabilidad y eficiencia de sistemas de información en proceso de diseño, evaluación de la consistencia de la información procesada electrónicamente y otros. Para profundizar acerca de la cobertura de la "auditoría informática" ver "Normas generales para la auditoría por medio de sistemas de informática", en Boletín informativo-A.M.A.I.(México), febrero 1989. Pp.4-10. Mérida Muñoz, Jorge: "Auditoría informática: conceptos, evolución y perspectivas"; en Actas (Primer congreso Iberoamericano de informàtica y auditoría).-- Puerto Rico, Nov. 1987, pp.69 a 80. En ésta misma publicación ver colaboraciones de los siguientes. Martinez Margarida, op. cit. Pp. 80 y ss., Mérida Muñoz, Jorge: "Auditoría informática: metodología, normas, estándares y técnicas". D'Amore, Marta: "La auditoría informática y su metodología de realización". Pp.205 y ss. Ramírez Márquez, Miguel y Armando Espinosa Palomino:" La función de la auditoría informática en Petroleos Mexicanos", pp. 435 y ss.

disposiciones emanadas de la propia administración de la seguridad o administración de servicios de cómputo.

2) Que se controle la consistencia e integridad de los sistemas o aplicaciones desarrolladas internamente. Se evalúa la calidad y suficiencia de los controles y se vigila su aplicación práctica.

3) Que se asegure la eficaz y adecuada operación de los sistemas.(4)

5) Que tenga verificativo el adecuado proceso de protección, contra destrucción o daño, de archivos y datos, equipos y dispositivos. Asimismo, se verifica el control de datos en cuanto a integridad, confidencialidad y exactitud.

La evaluación informática se tratará bajo los siguientes frentes. 1) El auditor informático. 2) Bases para la auditoría informática. 3) Metodología para la función auditora. 4) Algunas técnicas para la auditoría informática. 5) Participación de la función auditora en la creación o modificación de sistemas de información computarizada.

9.4.1) EL AUDITOR INFORMATICO.

Wheatley define: "Un auditor en informática es un profesional especializado en el análisis, diseño, implantación y evaluación de controles en los sistemas de información" (5). Se trata de un especialista altamente

---

4.- Mérida Muñoz, op. cit. P. 75. y Pérez Gómez, José Manuel: "La Auditoría de los sistemas de información"; en Actas (Primer congreso Iberoamericano de informática y auditoría).-- Puerto Rico, Nov. 1987. P. 94.

5.- Wheatley,Jorge: "Formación y desarrollo del auditor en informática"; en Actas: I Congreso iberoamericano de

capacitado para comprender las características de los controles informáticos, implantados en un organismo, y opinar sobre su viabilidad y desempeño. Con objeto de ser capaz de evaluar un sistema integral de seguridad informática, deberá conocer los distintos niveles de ésta y familiarizarse con la administración de la seguridad, en las areas de planeación, organizacion y ejecución y personal, expuestas en las secciones anteriores.

9.4.2) BASES Y CONDICIONES PARA LA FUNCION DE AUDITORIA INFORMATICA (6).

Como bases para realización de auditoria informática se pueden citar las siguientes, según el cuadro 12.

---

informática y auditoria,(San Juan, Puerto Rico, 2 a 6 de noviembre de 1987). P. 150.

6.- Las bases para la auditoria informática se tomaron de Lambarri, Alejandro, op. cit. Pp. 6 a 10.

CUADRO 12 BASES PARA LA AUDITORIA INFORMATICA
1) La auditoría informática es una evaluación independiente de cualquier actividad sujeta a control.
2) Se evalúa algo definido con parámetros establecidos, que pudieran ser plasmados en el desarrollo y documentación de sistemas, en la emisión de normas o políticas o reglas de uso y control de las computadoras, terminales o dispositivos.
3) Se necesita la aprobación y apoyo de la más alta dirección y desarrollar un plan de trabajo, así como la colaboración estrecha con la función de administración de la seguridad.
4) Acordar responsabilidades y estructura de organización, incluyendo lineas de reporte.
5) Desarrollar descripción de puestos para las posiciones de auditores en informática. El auditor revisará descripción de puestos en las areas informatizadas. Deberá, por lo tanto, también responder a un puesto claramente definido en sus atribuciones y responsabilidades.
6) Definir prioridades, metas y objetivos de la unidad administrativa dedicada a la auditoría informática. Se deben cubrir los aspectos de evaluación màs críticos, al principio, y, con el tiempo, extender su cobertura a todas las areas deseadas.
7) Desarrollar requerimientos de entrenamiento y educación continua en ambas areas: auditoría e informática. Es necesidad absoluta para mantener las habilidades de auditoria y permanecer actualizado en la tecnología de procesameinto de datos.
8) Buscar un real compromiso de la dirección de la institución con la función. Se requiere apoyo abierto hacia la auditoria. Solo una dirección comprometida con la seguridad y consciente de los riesgos asociados, otorgará los recursos necesarios para alcanzar el nivel profesional de la función de la auditoría informática. Además, ese apoyo es componente de la autoridad final del auditor.

Fuente: Lambarri, Alejandro: "La auditoría informática: bases, normas y *software*".-- mimeo, s.p.i., feb. 1989. Pp.6 a 10.

Las normas, en el terreno de la auditoria informática, han sido emitidas por asociaciones profesionales, en nuestro País y a nivel internacional. Tienen como objetivo informar a los auditores sobre el nivel mínimo de ejecución aceptable, requerido para cumplir las responsabilidades, de los propios códigos de ética de las mencionadas asociaciones y de informar a la administración de los organismos o a las partes interesadas, hacia los trabajos de auditoria de sistemas.(7)

Para que un grupo de auditoría funcione efectivamente en una organización, necesita contar con la confianza y respeto de los usuarios y de la dirección de informática. Estos deben proporcionar los recursos necesarios para cumplir con sus deberes.(8)

El costo de mantenimiento de un buen programa de auditoria es creciente. Ello se debe a la complejidad de los mismos sistemas de información y, con ello, la necesidad de óptima capacitación de los auditores. El asumir estos costos implica el compromiso creciente de la administración institucional para establecer y mantener sistemas de cómputo y medios de control, de alta calidad. En este sentido, el costo de no implantación de buenos sistemas de control, puede resultar muy alto, hoy en dia. (9)

7.- Para normas generales y código de ética del auditor en informática ver secciones al respecto en Boletin informativo-A.M.A.I. (México), Febrero 1989. Pp.9 y 10.
8.- Ibid. P. 12.
9.- Ward, Gerald,M.: "Cómo manejar los riesgos en la computación: el eslabón vital", en Contaduria Pública (México). Enero 1989. P. 44.

Entre las condiciones para un correcto desempeño de la función auditora, se destaca la integración de un equipo de auditoria interna, efectivo, como eslabón para asegurar que las politicas, normas, sistemas, etc. funcionen como deben. Los objetivos del auditor, del administrador o experto en seguridad, del alto funcionario y del operador del centro de cómputo, no son o no deben ser conflictivos. El trabajo conjunto de ellos se requiere para cumplir con los objetivos que tienen los sistemas de información para los organismos.(10)

Para la evaluación de los sistemas de información se propone promover la actuación del comité de seguridad, para efectuar investigación de areas vulnerables y optimizar soluciones a la problemática compleja de la seguridad en el procesamiento electrónico de datos.

9.4.3) METODOLOGIA PARA LA FUNCION AUDITORA.

Como metodologia para la realización de la auditoria informática, se proponen las siguientes etapas (11).

i) Entrevista preliminar del auditor con personal directivo. Se detectan necesidades planteadas por el alto mando y se le sensibiliza acerca de la necesidad de efectuar

---

10.-Ibid. P.45. V. Supra. Este equipo de auditoria interna es similar al comité de seguridad informática, propuesto en la sección 9.2.1.3.

11.- Adaptado de Perez Gòmez, op. cit. Pp. 91 a 118. Mérida Muñoz, op. cit. Pp.138 a 146. Para una metodologia especifica de auditoria informática, ver. Martin Berrueco, Jose Maria: "Una metodologia de realización de una auditoria informática"; en Actas: I Congreso iberoamericano de informática y auditoria,(San Juan, Puerto Rico, 2 a 6 de noviembre de 1987.) Pp. 345 a 356.

evaluaciones a los recursos informáticos y las vulnerabilidades que presentan los sistemas.

ii) Planeación de la auditoría. Se trata de definir qué objetivos se perseguirán, la cobertura de la evaluación, los métodos y procedimientos de realización, la oportunidad para realizarla y con que recursos humanos se contará. Ello se hace a partir de un acopio preliminar de información: acerca de los servicios de cómputo: su organización, funciones, usuarios, y problemática.

iii) Determinación de las areas de análisis. Se deberá seleccionar qué aspectos serán auditados, entre los que deberan considerarse aspectos planeatorios, de personal, normativos, administrativos, métodos, procedimientos, estructuras y relaciones de organización, aspectos de instalación física, instalaciones de respaldo, contratos con terceros, estándares técnicos para operación de *hardware* o *software*, protección de datos --vía segmentación de archivos o criptografía, entre muchos. En la determinación de las areas a auditar, primero se cubren las más críticas para el organismo y después los que son menos vitales. (12)

12.- En el proceso de revisión, se atiende los siguientes.
a) Procedimientos de preinstalación. Orientación correcta y bien organizada de actividades previas a la instalación de computadores y los sistemas de información que se involucrarán. Se debe revisar que los equipos se adquieran cuando se prevea que su presencia producirá mayores beneficios que otras alternaltvas de procesamiento.
b) Procedimientos de organización. Funciones internas y externas del departamento o unidad a cargo del procesamiento electrónico de datos, con normas y elementos que rijan la conducta de dicha unidad. El objetivo de esto es evitar la concentración de funciones, responsabilidades y poder en las

iv) Evaluación de los procedimientos de control interno. Se refiere a conocer estàndares definidos, grado de implementación de los mismos, su operatividad y, con ello, su resguardo y confiabilidad, en cada una de las areas a auditar predefinidas.

v) Operación de programas de auditoría.

Es la programación de los procedimientos de auditoria a llevar a cabo. Se describe el sistema, o subsistemas, o componentes que se está examinando, se comenta la evaluación de los controles existentes y se enuncian los procedimientos de auditoria que deben desarrollarse, con sus

---

areas informàticas y que existan niveles gerenciales que ejerzan supervisión efectiva.V. Supra. Sección 9.3.
c) Procedimientos de operación. Atañe a estándares de operación o manejo de computadores y elementos adicionales que permiten que éstos procesen datos y generen información. Se trata de prevenir erores y detectar intentos de malos manejos.
d) Procedimientos de procesamiento. Son los elementos que permiten producir información exacta, completa, válida y oportuna. Incluye procedimientos para cautelar el comportamiento de componentes físicos del equipo. Se busca, además, que existan controles en los programas, que aseguren la totalidad, exactitud, autenticidad y autorización de los datos procesados.
e) Procedimientos de documentación. Su objetivo es la estandarización en cuanto a documentación para los sistemas, programas, manualea de operación, procedimientos de mantenimiento y explotación de aplicaciones, políticas informáticas, planes de trabajo, etc. Ello se dirige a permitir comprensión clara, precisa y completa de las actividades informàticas.
f) Procedimientos para servicios externos computacionales. Se refieren a los requerimientos técnicos, econòmicos y legales que deben considerarse una vez definida la necesidad de servicios externos.
g) Normas de seguridad. Se destinan a la protección de los datos, programas, equipos y personas, así como las facilidades inherentes al manejo de los sistemas, confrontados con los peligros derivados por causas intencionales o no intencionales, políticas, sociales, técnicas o humanas. De Mérida, op. cit. P. 141.

objetivos, extensión y operaciones. Es ésta la fase de ejecución de pruebas a nivel físico, lógico, de organización y de personal.

vi) Etapa final. Incluye análisis de resultados, opinión sobre el funcionamiento, eficacia y eficiencia de los sistemas de información, validación de la consistencia de los datos y planteamiento de soluciones para mejorar aspectos erróneos, problemáticos, ineficaces o ineficientes de los sistemas.

Se confecciona y entrega un informa o dictámen a las autoridades que corresponde, con atribuciones para estudiar dicho documento y considerar la aplicación de medidas acordes con los hechos informados.(13)

9.4.4) ALGUNAS TECNICAS Y *SOFTWARE* PARA AUDITORIA INFORMATICA.

Las técnicas aplicables a la auditoria informática son de dos tipos fundamentales: 1) pruebas de cumplimiento -- verificación de la correcta ejecución y registro de las operaciones, con base en conductas predeterminadas y de funcionamiento habitual y 2) pruebas de carácter sustantivo --revisión analitica de los datos, validando sus atributos.(14)

Los auditores en informática buscan utilizar los mismos equipos de cómputo de la institución para efectuar auditoria y sus procesos implícitos o muestreos. Ello trae ventajas

13.- Estos pasos se tomaron de Mérida Muñoz, op. cit. Pp. 139-143.
14.- De Mérida Muñoz, op. cit. P. 143.

en el tiempo de los auditores. Se elimina trabajo manual rutinario y el tiempo del especialista se dedica a análisis que requiere la aplicación de un criterio profesional.

La auditoria debe utilizar programas computacionales como herramienta. Implica analizar cómo se llega a los resultados, qué procesos se efectúan, cómo, cuándo, dónde y porqué.

La manipulación de los datos es relativamante sencilla. Lo sutil de un fraude por computadora es que, para la comisión de éste, se puede hacer conciliar los datos implicados para que los auditores no detecten el ilícito. (15)

El uso del computador para la auditoría es en dos frentes. a) Analizar el flujo normal de datos y b) apoyar la función auditora con procesos automatizados, para conciliaciones, arqueos y muestras.

Respecto al *software* para apoyo de la función que nos ocupa, cabe señalar que existen programas de auditoría, valiosos para extraer información, resumir y ordenar ciertos tipos de datos --ello con la finalidad de efectuar arqueos y conciliaciones y hacer funcionar técnicas de prueba y corroboración-- y aislar transacciones o información para ser verificada.

15.- Whiteside, citado por Lambarri, Alejandro: "Utilizando el computador para realizar la auditoria"; en Actas: I Congreso iberoamericano de informàtica y auditoria,(San Juan, Puerto Rico, 2 a 6 de noviembre de 1987). P. 271.

Las herramientas de *software* que apoyan las funciones de auditoría son de los siguientes tipos. (16)

-- Paquetes de auditoria, en los que se pueden obtener confirmaciones, análisis, cálculos, comparaciones y excepciones, para realizar trabajos normales dentro del campo de la auditoria.

-- Programas de aplicación específica. Son desarrollados por el personal del departamento de auditoria con fines similares al anterior.

-- Utilerías de sistema operativo. Como generadores de reportes que pueden cubrir parcialmente las funciones del auditor.

-- *Software* de apoyo a la función. En este rubro existen graficadores, hojas electrónicas de cálculo, procesadores de palabras, generadores de diagramas de flujo y documentación, paquetes para analizar la exposición a riesgos a partir de cuestionarios aplicables en diferentes partes del area de informática y paquetes para comparar diferentes versiones de programas, con afán de detectar diferencias entre ellos.

9.4.5) PARTICIPACION DE LA FUNCION AUDITORA EN LA CREACION O MODIFICACION DE SISTEMAS DE INFORMACION COMPUTARIZADA.

En la creación de nuevos programas o sistemas, la función auditora es importante. Resaltan las siguientes consideraciones. 1) Deben existir técnicas de prueba, verificación y conciliación, así como de protección,

---

16.- Tomado de Lambarri: "La auditoria informática...", Pp. 9 y 10.

consideradas desde el diseño de sistemas de proceso de datos. 2) En el desarrollo de los programas deben incluirse rutinas de evaluación, en módulos de auditoria. 3) Se deben controlar los procedimientos para autorizar y efectuar cambios en los programas de cómputo que sirven a la institución. Los procedimientos para el control de cambios en los programas son de particular importancia cuando los procesos y controles los efectúa el mismo programa y son transparentes para el usuario.

Los sistemas computarizados modernos, que manejan grandes volùmenes de transacciones, para los cuales los rastros de auditoria son limitados o de poca duración, requieren del desarrollo de nuevas técnicas tales como los "módulos de auditoria integrados en la programación"(17). La intervención del especialista en auditoria es indispensable para ello.

17.- De Martinez, Margarida, op.cit. P. 87.

CONCLUSIONES

A lo largo del tiempo se han sucedido apariciones de nuevas tecnologías que ejercieron fuerte impacto y condicionamiento sobre la vida del hombre. En su momento, la escritura, la rueda, la imprenta, la máquina de vapor y la electricidad revolucionaron la dinámica de las sociedades y determinaron el curso de la historia.

En nuestro siglo, en la década de los 50 apareció una nueva era en la evolución del hombre: la era de la información. En ella, paulatinamente, el valor económico se ha trasladado de activos o bienes físicos hacia espacios conceptuales, es decir información.(1) También, en la misma década se acentuó el desarrollo y la extensión de nuevas tecnologías para el procesamiento de datos, conocidas, asimismo, como informática o computación. A través de medios magnéticos y electrónicos se facilitó enormemente el proceso, almacenaje y transmisión de datos. Ello, a velocidades cada vez mayores. Sobrevino una "revolución informática" y, paralelamente, una "informatización de la sociedad", (2) que se extendió primero en los países más desarrollados y después en los restantes.

El desarrollo tecnológico informático ha apuntado hacia el logro de procesos más eficientes, a mayores velocidades y con mejor capacidad de almacenamiento y transmisión de

---

1.- En el capítulo 3 se presentó, desde diversas ópticas, cómo la información se ha constituído crecientemente en el recurso estratégico de la época actual.
2.- Término de, Simon, Nora y Alain Minc: "La informatización de la sociedad".-- México: Fondo de cultura Económica, 1981.

datos. Ello ha buscado apoyar la productividad, competencia y precisión en la toma de decisiones, de modo que coadyuve al cumplimiento de los objetivos de los organismos públicos. No obstante, las enormes posibilidades que permite la computación apuntan también hacia su vulnerabilidad. Con base en su potencial, la informática introduce mayor complejidad que las tecnología manuales, para funciones de protección, control y auditoría. De ello deriva la aparición de mayores riesgos de errores, omisiones, fraudes, accesos no autorizados, pérdidas o daños.

La problemática derivada de la aplicación de nuevas tecnologías para el proceso de datos se definió como campo de atención de la seguridad informática. Se trata de un aspecto crítico en el funcionamiento y viabilidad de los organismos. Hasta ahora, los estudios disponibles acerca de la informática, parecen haber tratado y comprendido la seguridad computacional como aspecto poco relevante, costoso y que genera beneficios poco claros. Los propios directivos informáticos de diversas instituciones o unidades administrativas, no reconocen el problema como tal. Este estudio difiere de la mayoría de los trabajos documentales, en materia de seguridad y auditoría informática, que exponen series de recomendaciones, muchas veces ajenas a los contextos nacionales y organizacionales de los propios autores. Asimismo, esta tesis desaprueba puntos de vista pragmáticos que se ocupan de la seguridad de manera ocasional y sólo cuando se tiene que hacer frente a daños.

El trabajo tuvo partida en la consideración de que el desarrollo o incorporación de medios que aseguren el correcto y sano funcionamiento de los sistemas de computación, no ha sido en la misma magnitud que el desarrollo de las propias tecnologías informáticas. La computación ha ingresado en las agencias públicas, sin corresponderse con suficientes adecuaciones administrativas, organizativas, ambientales y culturales para ello.(3) Es un fenómemo a nivel global y que el trabajo resalta para el caso de México, en general, y de su Administración Pública, en particular. Se mostró que la informática altera maneras de pensar y de trabajar tradicionales, que ejerce impacto en el "sistema nervioso" de las organizaciones y, con ello, en el de la sociedad entera.

El objetivo del trabajo fue mostrar que la seguridad informática constituye un problema y terreno de consideración importante en la Administración Pública y, asimismo, que el uso de técnicas administrativas es esencial en la solución del problema. Este objetivo, se considera cumplido.

En el desarrollo del estudio, no se discutió o pretendió demostrar la validez o relevancia de la seguridad informática. El logro de ésta se tomó como fin deseable y suficiente. Tampoco se buscó demostrar empiricamente que la

---

3.- La administración de los recursos informáticos tendrá que avanzar en el rediseño organizacional, de ambientes y prácticas de trabajo y adecuarlos a las características de a administración moderna, automatizada.

seguridad debe administrarse. Ello también se consideró, desde el inicio, como verdad evidente. No obstante, hubo varios capítulos y secciones que evidenciaron la importancia, magnitud y complejidad de la problemática de la seguridad y por lo cual se afirma la necesidad de administrarla. Entre ellos destacan los capítulos 2, sección 2.3; capítulo 5 y capítulo 7.

Se plantearon dos supuestos o hipótesis normativas en la introducción. Del primero se desprendió que la fuente primaria de la inseguridad informática está en la falta de adaptación o falta de rediseño de los ambientes sociales u organizacionales donde se incorporan las nuevas tecnologías. Se sostuvo que es necesario buscar un cabal desarrollo armónico entre la informática y el contexto donde se inserta, de modo tal que se eviten o que se controlen los desequilibrios que conlleva cambiar modos de trabajar, de pensar, de comunicar o de mandar, entre muchos. Los capítulos 2, sección 2.3; el 3, sección 3.1; el 4; el 5; el 7 y el 8, sección 8.1; mostraron el impacto y desequilibrios que provoca o permite la adopción de las tecnologías computacionales. El capítulo 8, sección 8.2, y el 9, apuntaron hacia el rediseño del ambiente organizacional y administrativo de modo que se facilite el control, buen uso de la informática y la armonía entre las tecnologías y la dinámica de las instituciones.

El segundo supuesto normativo sostuvo que la seguridad informática debe ser administrada. Ello equivale a que debe

ser abordada con visión amplia y enfoques sistemáticos. Con ello, se requiere la instrumentación de procesos ordenados, congruentes y eficientes de toma de decisiones, que aseguren el cumplimiento de los objetivos de protección y control que requieren los organismos públicos.

Se destacó el papel del administrador público, como profesional en la toma de decisiones. La sección 2.2 presentó su perfil y estructuró diversos elementos que intervienen en el proceso decisorio racional. Ello pretendió fundamentar la participación del administrador en el ejercicio y logro de los fines de la seguridad informática. Su papel en este ámbito se hace sumamente importante. Tiene elementos valiosos para instrumentar un proceso ordenado de planeación, con definición de prioridades, objetivos, costos, beneficios, impactos organizacionales, medios de control, evaluación y retroalimentación. Asimismo, se reconoce en él la capacidad de tomar decisiones en modo tal que se coordinen esfuerzos y supervise la sana operación computacional. En materia de recursos humanos, puede aportar elementos para la formación de personal sensibilizado, responsable y motivado, capaz de integrarse en esfuerzos colectivos. En suma, el administrador público se propone como profesional adecuado para conducir la administración de la seguridad, es decir, la solución de un problema que día a día se hace más crítico en la operación de las instituciones gubernamentales.

La Administración Pública mexicana ha sido cada vez más dependiente de la aplicación de los recursos informáticos. Es requerimiento primordial que tome previsiones que le aseguren continuidad en sus operaciones, correcto funcionamiento y el mantenimiento de la integridad y confidencialidad de la información, que es sustento de la propia función pública. Con base en ello y en la exposición de este trabajo, se subraya el valor de las siguientes recomendaciones.

Primero, el proceso administrativo de la seguridad informática deberá enfocar el problema de manera preventiva, primordialmente. Ello se contrapone a enfoques detectivos o correctivos -- que se ocupan de la seguridad una vez que ya ocurrieron problemas. La toma de decisiones de protección y control de sistemas de información, como consecuencia de haber experimentado siniestros, puede resultar sumamente costoso en términos de afectación de la continuidad de operación, de la recuperación ante el daño, de rediseño del sistema o de impactos sociales, económicos o políticos. El problema tiende a ser más crítico en la medida que se involucran masas importantes de información que significan dinero o poder y que ponen en peligro los sistemas nerviosos, que cimentan el funcionamiento del país. (4) Las organizaciones deben anticiparse a las consecuencias de la vulnerabilidad computacional. Solamente con iniciativa y

4.- Afirmación de Sendrow, Martin: "Impact of rapid changing computer technology on computer crime: advance computer security concepts".-- S.P.I., mimeo, 1980. P.16.

vigilancia permanente, es posible progresar en la prevención o disminución de niveles de riesgo informático.

Segundo, como se afirmó en la sección 9.2.1, es necesario que en cada organismo existan las categorías funcionales de administración de la seguridad y de auditoría informática. La primera conducirá el ejercicio de la seguridad y la segunda ejercerá evaluación y retroalimentación. (5) Ambas deberán reportar directamente a los altos mandos directivos. Dada su importancia crítica en la operación y viabilidad de la institución, coadyuvarán a lograr control sobre la operación, y con base en ello, se aplicarán medios de protección y regulación.

Tercero, la responsabilidad directa del ejercicio de la seguridad informática recae en cada servidor público que trabaje en torno a la computación. Al poner en disposición de un usuario, equipos o accesorios o información, se le debe conferir, correlativamente, la responsabilidad de su protección y hacer la seguridad parte de su trabajo diario. Así, el personal deberá estar capacitado para desempeñar sus funciones con adecuadas previsiones hacia la salvaguarda y buen uso de los activos físicos de cómputo y la confidencialidad e integridad de la información. El administrador de la seguridad velará que se cumplan las normas y se respeten los controles establecidos en todas las

---

5.- Por retroalimentación se entiende alimentar un sistema, unidad administrativa, plan o programa, con base en información generada por su propio desempeño o *output*, con objeto de mejorar su rendimiento o funcionamiento.

unidades administrativas del organismo. Además de capacitar, evaluará al personal y dará seguimiento al proceso administrativo de la seguridad. De ese modo, sus tareas no son de ejecución, sino de administración, es decir, coordinación y toma de decisiones.

Cuarto, toma un valor sustancial el hecho de que el administrador de la seguridad informática, así como los auditores, se comprometan firmemente, con la institución a la que sirven, a apoyar permanentemente el ejercicio de la regulación y control sobre los sistemas de información. La sensibilidad directiva que exista en cada organización, hacia la seguridad informática, será siempre la pauta del grado de atención que se dé a ésta. La labor que desarrolle el administrador de la seguridad o el asesor en este terreno, es de suma importancia. Es necesario que insista y defienda, ante niveles directivos, la noción de que las computadoras constituyen herramienta con la cual se pueden cometer acciones ilícitas. Muchas veces se tendrán que enfrentar visiones fáciles o simplistas de la protección y control informático. de hecho, para muchos directivos, la seguridad se resuelve técnicamente con la generación y uso de claves de acceso y el respaldo de archivos. No obstante, ello no compensa problemas de mala administración, de personal, de instalación errónea ni de otros aspectos.(6) Se deberá tomar conciencia que los riesgos crecen a medida

6.- Idea tomada de Krull, Alan: "Ten loging strategies for data security".-- en Computer Security Journal, (U.S.A.) Vol. 4. No.1, 1986. P.24.

que se incrementa la dependencia hacia las computadoras y que la resolución óptima de la seguridad se halla en cubrir todo el conjunto de elementos que componen los sistemas de información o constituyen recursos informáticos --a saber, equipos, dispositivos magnéticos, datos, instalaciones, personal, métodos y procedimientos, normas, políticas y planes de desarrollo informático, entre otros.(7) Ello significa contemplar todos los niveles de seguridad indicados en el marco analítico que sustenta este trabajo, expuesto en el capítulo 6, bajo la premisa de hacerlos complementarios todos ellos. Se llegará al establecimiento de una adecuada combinación de controles generales y específicos, ya sean manuales o automáticos, en los diversos niveles de seguridad. Se busca la salvaguarda del flujo completo de la información y activos computacionales. Un esquema así constituye garantía para evitar infracciones o errores computacionales.

El nivel de sencillez o sofisticación a que se llegue, en el ejercicio de la seguridad informática, es decisión de cada organismo. Con base en la medida de requerimientos específicos de protección y control, se derivará el modo de abordar el problema. En cualquier caso, ya se trate de una gran institución o una pequeña agencia pública, la seguridad

---

7.- La creación de cursos, o generación de informes, basados en casos reales de desastres o daños o desfalcos, puede ser una forma útil a los directivos organizacionales de conocer y enfrentar mejor la problemática computacional.

deberá administrarse y abordarse en todos sus niveles, es decir, de manera integral.

Quinto, los medios de control y sus métodos y procedimientos derivados, es necesario que estén estandarizados y obedezcan a políticas y normatividad institucional claramente establecidas y asentadas en manuales de organización, de procedimientos, de descripción de puestos, así como en documentación específica para la función de la seguridad (8) y 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.(9)

Para todo recurso o medio de seguridad se deberá probar su eficaz y correcto funcionamiento y documentarlo. Se capacitara al personal sobre la operación de los medios de protección, hasta su plena comprensión. Una vez asegurados estos requisitos, se les pondrá en servicio. Sólo así puede

---

8.- 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.
9.- Se recomienda, más que crear nuevas políticas, obtener mayor provecho de las ya existentes y conocidas por el personal, pero adaptadas al fenómeno informático.

tener efecto el funcionamiento, seguimiento y evaluación de la operación de los mecanismos de seguridad.

Séxto, el delito o daño informàtico aparece y se desarrolla ante la falta de definición y tratamiento jurídico, que impide o retrasa la elaboración de legislación especifica al respecto. Ello crea un ambiente propicio para la comisión de este tipo de actos. Tendrá que ser preocupación institucional el análisis y solución de los hechos ilegales, con base en el conocimiento de quién los comete, cuándo, cómo y dónde. De la misma manera, se deberán buscar mecanismos para reaccionar con prontitud ante ellos. El tener que enfrentar errores o pérdidas suele ser costoso, no obstante, las experiencias negativas deben ser capitalizadas (10) y buscar el mayor provecho y aprendizaje de ellas. Los anexos 1 y 2 de este trabajo apoyan estos aspectos.

Séptimo, el personal constituye el eslabón más débil en la cadena de la seguridad informàtica. Son seres humanos los que diseñan, operan, controlan o mantienen sistemas de información. Si ellos se desempeñan optimamente, al asumir la responsabilidad que les confiere el uso de información o activos computacionales, actuan con discreción, prevención de problemas y ostentan valores de productividad y eficiencia, la seguridad en todos ls otros ámbitos o niveles se facilita enormemente y se hace menos crítica. Es por

---

10.- Afirmación de Lic. Ramón Ocampo, del INEGI, al hablar de los delitos informàticos, durante entrevista sostenida en la Cd. de México, en febrero de 1989.

ello, que se exige conducir una adecuada política de administración de recursos humanos, en la que se consideren aspectos de capacitación, desarrollo, motivación, productividad, entre otros, en el marco de la administración de la seguridad informática.

Octavo, es necesario profundizar conocimientos sobre tecnologías de la información en aspectos de seguridad y auditoría. Ello es más crítico mientras más grandes y complejos son, para una organización, los servicios de cómputo.

En las instituciones de educación superior se propone desarrollar programas de formación de especialistas en la materia de seguridad y auditoría informática, ya sea dentro de los planes de estudio existentes o con la creación de programas de postgrado. La reacción ante ello ha sido lenta, hasta ahora. No obstante, la necesidad de recursos humanos en estas áreas aumenta rapidamente. La mayoría de los expertos que existen en México se han formado en el extranjero o a través de la experiencia de trabajo. Hoy por hoy, al menos, hay algunas instituciones de educación que ofrecen programas de formación en auditoría informática. La seguridad, por su parte, sigue desatendida. De un análisis efectuado en el desarrollo de este trabajo, se descubrió que solo un programa de estudios, en una universidad privada, incluía, específicamente, una asignatura sobre la seguridad

computacional.(11) A nivel licenciatura, en general, los aspectos de control interno, seguridad, control de calidad de sistemas o métodos para operación de sistemas de información, son escasos. Esto es incongruente con la realidad de un país en proceso de informatización. Se explotan a gran escala los recursos informáticos, pero la formación de especialistas en su control es mínimo.(12)

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 (13) 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

11.- En la Universidad del Valle de México, en el programa de licenciatura en informática administrativa.
12.- Los auditores en informática, entrevistrados, han afrontado la seguridad a través del ejercicio de la función auditora, como método de supervisión y vigilancia de todo el ámbito computacional. A través de ella de evalúan y detectan deficiencias o irregularidades, se emiten opiniones sobre la funcionalidad de los sistemas de información y se proponen medidas correctivas.En este trabajo, se ha propuesto un abordamiento más amplio sobre la problemática computacional en materia de seguridad: administrarla. A juicio propio, el ejercer la función auditora, como control y evaluación de los sistemas, es insuficiente ante la dimensión que cobra, cada dia, la seguridad. Se ha insistido en ejercer una administración integral sobre ésta, en la que se ejecute un proceso ordenado de toma de decisiones en etapas diferenciadas de planeación, organización-ejecución, personal y evaluación. Las disfunciones del fenómeno informático deben ser abordadas desde sus orígenes, no auditadas una vez que ya existen y provocan consecuencias.
13.- Excepto en sistemas de información de alta confidencialidad o críticos para la seguridad económica o política o social de la Nación.

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.

México está en una fase de familiarización con el fenómeno informático. El desarrollo de sistemas reviste atrasos en el diseño de programas eficientes para efectuar los procesos de datos que requiere la sociedad moderna. La problemática, en aspectos de seguridad, se agudiza en la medida que ni los auditores informáticos ni expertos en seguridad ni administradores, intervienen en ese diseño ni en la operación de los que constituyen sistemas nerviosos de instituciones nacionales fundamentales. 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 tecnologia, 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."(14)

Se sugiere que futuros estudios, en materia de seguridad informátita o areas afines, se orienten hacia alguna de las tres siguientes areas, en las que se

14.- Nora, Simon y Alain Minc, op. cit. P. 25.

desarrollen estudios especializados sobre los aspectos más importantes de una administración de la seguridad.

1) El personal que labora en ambientes informatizados. Como aspecto crítico de la seguridad, es un terreno poco explorado y de él dependen, con mucho, el nivel de vulnerabilidad informática de un organismo y su capacidad de responder ante la problemática que ello plantea.

De la misma forma, se deben profundizar conocimientos acerca del rediseño de las condiciones de trabajo o seguridad e higiene del personal informático. Es un campo de consideración, de aparición reciente y que puede ser determinante en un ambiente de seguridad informática.

2.- Reorganización organizacional. Al alterarse líneas, formas o prácticas de comunicación en los organismos, se afecta su funcionamiento. En la medida que la revolución informática provocó alteraciones en los sistemas de comunicación administrativa, afectó líneas y residencia de poder, de responsabilidad y de capacidad de toma de decisiones. Por ello, se considera necesario reelaborar la estructura jerárquica u organizacional de las instituciones que dependen, en mayor o menor grado, de la operación de sistemas de información.

3.- Análisis global o integral de la vulnerabilidad informática. En este trabajo se ofreció una clasificación o tipología, propia, de los daños o pérdidas informáticas. No se encontró ninguna publicación que presentara cabalmente los riesgos, de todo tipo, que amenazan los sistemas de

información. Por ello, se considera importante que trabajos futuros se orienten hacia el conocimiento amplio o completo del problema de la seguridad computacional y que, con base en ello, se le aborde y resuelva de modo óptimo.

El Estado mexicano deberá atender de manera rigurosa los problemas que conlleva la informática. Debe partir de una politica pragmática y ecléctica, tomando en cuenta la realidad que se vive en la informatización de la sociedad. Se exige conocer las fuerzas y debilidades, directas o derivadas de las nuevas tecnologias. El efecto deberá ser impulsar el desarrollo tecnológico para evitar que nuestro país se quede atrás en el desarrollo global a la vista.

Las tecnologias de información juegan cada vez un papel más importante en el proceso de modernización publiadministrativo. Las computadoras deben ofrecer alta rentabilidad en lo politico, administrativo, económico y siocial. Esto equivale a ser plenamente funcional a los objetivos del Estado Mexicano. La importancia de contar con una visión estratégica, que aborde la problemática de la seguridad informática para la Administración Pública Federal, en un futuro cercano, será crítica.

BIBLIOGRAFIA CITADA

Ackoff, Russell: "Rediseñando el futuro".-- México, D.F.: Editorial Limusa, 1984.

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

Aguilar Villanueva, Luis F.: "Política y racionalidad administrativa".-- México, D.F.: Instituto Nacional de Administración Pública, 1982. 151 pp. (Estudios, Serie V, Teoría de la Administración Pública, No.3)

Ahumada Rivera, Sergio: "Primera conferencia mundial de la Oficina Intergubernamental para la Informática (I.B.I.) sobre políticas en flujo de datos transfronterizos", en Comunidad Informática (México), No. 27, pp.19-20

Alvarado, Miguel Angel: "Seguridad en la banca electrónica".-- Banco Nacional de México, mimeo s.p.i., s.f. (Ponencia presentada ante la Asociación Mexicana de bancos)

Alvarez, Fernando: "Protección a los recursos de cómputo y la integridad de los datos para asegurar continuidad en la operación y seguridad en la información", (Ponencia en Seminario sobre seguridad y protección bancaria, México, D.F., Feb.26 y 27 de 1988.) pp. 35-66.

Ampudia Mello, Jose Enrique: "Institucionalidad y gobierno: un ensayo sobre la dimensión archivística de la Administración Pública".-- México, D.F.: INAP-Archivo General de la Nación, 1988. 117 pp.

Anning, P.: "Protegiendo una red", en Data Processing Digest (U.S.A.) Vol 15, No.6, junio 1987.

Asociación Mexicana de Auditores en Informática: "Normas generales para la auditoría por medio de sistemas de informática", en Boletín Informático (México), Febrero 1989. Pp. 4-10.

Asociación Mexicana de Bancos: Relatoría mesa No.7: la seguridad informática técnica y física; en Seminario sobre seguridad y protección bancaria, México, D.F., Feb.26 y 27 de 1988. Pp. 121 a 126.

Ayala, Sara Isabel: "Riesgos y controles en aplicaciones desarrolladas en cédulas electrónicas", en Boletín Informático (México), Febrero 1989. Pp. 20 y 21.

Bertalanffy, Ludwig von: "Teoría general de los sistemas".-- México, D.F.: Fondo de Cultúra Económica, 1982.

Bria, Ricardo: "Delitos en un ambiente informatizado"; en Actas: I Congreso iberoamericano de informática y auditoria, (San Juan, Puerto Rico). 2 a 6 de noviembre de 1987, pp.119-126.

Buerger, David J.: "Detecting and combating computer viral infections" en "Infoworld" (U.S.A.), March 21, 1988. P. 14.

Burton Squires: "Una visión resumida de la seguridad de los datos para el administrador de procesamiento de datos".-- en Data Processing Digest (U.S.A.), Vol.3, No.10, octubre 1975, Pp. 13 y 14.

Caso Lombardo, Andrés: "Administración pública y desarrollo", en Revista de administración pública (México), febrero 1983, pp.283-290. (Antología 1 - 54)

Castelazo, Jose R.: "Tecnicas y especialidades de administyración del personal público".-- mimeo, 1985.

D'Amore, Marta: La auditoria informática y su metodologia de realización"; en Actas I Congreso iberoamericano de informática y auditoria, (San Juan, Puerto Rico, 2 a 6 de noviembre de 1987) pp.205-216.

De la Torre Rodriguez, Armando G. y Maria Teresa Muñoz Hernández: "Guía de controles para el buen funcionamiento del departamento de procesamiento electrónico de datos".-- (Tesis que presenta para recibir el grado de licenciatura en informática) México, D.F.: U.P.I.I.C.S.A., 1984.

Del Pozo y Contreras, Luz María: "Prospectiva del derecho informático".-- en Comunidad Informática (México), No.27, pp. 29-35.

Deutsch, Karl: "Los nervios del gobierno: modelos de comunicación y control políticos".-- Buenos Aires: Paidos, 1980.

Dile, Christine: "Los controles en los nuevos sistemas de aplicación: ¿de quién es la responsabilidad de implantarlos?".-- en Data Processing Digest (U.S.A.) Vol.15, No.6, junio 1987.

Elmer De Witt, Philip: "Invasion od the data snatchers: a "virus" epidemic strikes in the computer world".-- en Time (U.S.A.). Vol.132, No.13, Septiembre 26, 1988, pp.30-35.

Forrester, John: "Bounded racionality and the politics of muddling through", en Public Administration Review (E.U.A.), vol. 44, num. 1. Pp. 23 a 31.

García Cárdenas, Luis: "Las innovaciones administrativas en el sector público mexicano y su importancia en el campo", en Revista de Administración Pública (México), feb. 1983, pp. 155-162. (Antología 1-54)

Garzón C., Gregorio: "La protección jurídica de los datos personales: consideraciones metodológicas".-- en Comunidad Informática, No.15 ene-mar 1983, pp.12-16.

Gatica, Alejandro: "Seguridad en redes locales: conceptos y estándares de redes locales", en Boletín Informático (México), Febrero 1989. Pp. 18 y 19.

Gigch, John P. van: "Teoría general de sistemas".-- México, D.F.: Editorial Trillas, 1987. 607 pp.

Gil Villegas, Francisco: "la crisis de legitimidad en la última etapa del sexenio de López Portillo", en Foro Internacional (México) No.98, octubre-diciembre de 1984.

Gilson, Milo: "Fraude en una computadora ¿Quién lo impide?:, en Data Management (U.S.A.), 1975.

Goldslager,L.: "Computer science: a modern introduction".-- New Jersey: Prentice Hall International,Inc.,1982.

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. 150 pp.

Graham M.,Robert: Principles of systems programming.-- New York: John Wiley & Sons Inc.,1975.

Hices, G.F. et.al.: System development methodology.-- New York: North Holland Publishing Company, 1974.

Hirscham, R.A.: "Computers & Privacy", en Computer Bulletin" (U.S.A.), march 1983.

Holsti, Ole R.: "Modelos de relaciones internacionales y política exterior", en Foro Internacional. (México), vol. xxix, num. 4 (abril-junio de 1989). Pp. 525 a 560.

Hsiao, David; Douglas Kerr y Stuart Madnick:"Computer security".-- San Francisco: Academic Press, 1979. 299 pp.

International Labour Office Geneve: "Automation: work organisation and occupational stress".-- Geneva: I.L.O., 1982. P. 187 pp.

International Labour Office: "New technologies: their impact on employment and working environment.-- Geneva: I.L.O., 1982. 174 pp.

Jimenez Cruz, Daniel (et al): "Administración de servicios a usuarios de sistemas".-- (Tesis que presenta para recibir el grado de licenciatura en informática) México, D.F.: U.P.I.I.C.S.A., 1985

Johnston, Stuart: "Computer virus spreads to commercial software", en "Infoworld" (U.S.A.), March 21, 1988.

Johnston, R.E.: "El camino que lleva al desastre", en Data Processing Digest" (U.S.A.), Vol. 15, No.6, junio 1987.

Johnston, R.E.: "The risks of change", en Infosystems (U.S.A.), Vol.33, Dic. 1986.

Karabin, Steven: "Clasificación de datos: una breve guia".-- en Data Processing Digest" (U.S.A.), Vol. 15, No.2, febrero de 1987. P. 7.

Kearby, D'Ann: "Personnel policies, procedures & practices: the key to computer security", en Computer Security Journal (U.S.A.), Vol.4, No. 1.,1986.

Krauss, Leonard: y Aileen Mc Gaham: "Computer fraud and countermeasures".-- New Jersey: Prentice Hall, 1979.

Krull, Alan: "Ten loging strategies for data security".-- en Computer Security Journal, (U.S.A.) Vol 4. No.1, 1986.

Lambarri Valencia, Alejandro: "Utilización del computador para realizar auditoria"; en Actas: I Congreso iberoamericano de informática y auditoria, Pp.267-292 (San Juan, Puerto Rico, 2 a 6 de noviembre de 1987.)

Lambarri Valencia, Alejandro: "La auditoria informática: bases, normas, y software".-- s.p.i., febrero 1989. (Ponencia presentada en seminario "Politicas y normas de seguridad y auditoria informática", México, D.F., 7 a 9 de febrero de 1989.

Lara Marquina, León y Adalberto Vela Sánchez: "Seguridad en procesos distribuidos".-- (Tesis que presenta para recibir el grado de licenciatura en informática) México, D.F.: U.P.I.I.C.S.A., 1984.

Lozano Arévalo, Luis Alberto: "Sistemas de información computarizados: sus riesgos y evaluación".-- (Seminario de investigación para obtener el título de licenciado en Administración) México, Universidad Panamericana, 1984. 130 pp.

Lucas, Henry: "El análisis, diseño e implementación de sistemas de información".-- México, D.F.: Mc Graw Hill Book Company, 1976.

Martín Berrueco, Jose María: "Una metodología de realización de una auditoría informática"; en Actas: I Congreso iberoamericano de informática y auditoria,(San Juan, Puerto Rico, 2 a 6 de noviembre de 1987.) Pp.345-356.

Martínez Margarida, Rafael: "La automatización de la auditoría: la auditoría del futuro"; en Actas: I Congreso iberoamericano de informática y auditoria,(San Juan, Puerto Rico, 2 a 6 de noviembre de 1987), pp.81 a 90
Mc Lellan, Vin:"Computer systems under siege", en EDP Auditor Journal-(E.U.A.), Vol.3, 1988. Pp. 33-38.

McLuhan, Marshall: "Understanding media: the extensions of man".-- New York: Signet Books, 1964. 318 pp.

Mc Menamy, Edward: "On the trail of a hidden threat", en Infosystems (E.U.A.), Vol.33, Dic. 1986.

Mérida Muñoz, Jorge: "Auditoría informática: metodología, normas, estándares y técnicas"; en Actas: I Congreso iberoamericano de informática y auditoria,(San Juan, Puerto Rico, 2 a 6 de noviembre de 1987),pp.137-148.

Mérida Muñoz, Jorge: "La auditoría informática: conceptos, evolución y perspectivas"; en Actas: I Congreso iberoamericano de informática y auditoria,(San Juan, Puerto Rico, 2 a 6 de noviembre de 1987),pp.69 a 80.

Merino, Marco Antonio: "El virus informático".-- s.p.i., mimeo, s.f.

México. Instituto Nacional de Geografía, Estadística e Informática: Guía para la elaboración del programa institucional de desarrollo informático.-- México, D.F.: Talleres Gráficos de la Nación, 1987.

México. (José López Portillo), Presidencia de la República, Coordinación General de Estudios Administrativos: Análisis, diseño y control de formas: guía para su elaboración.-- México, D.F.: Talleres Gráficos de la Nación, 1978.

México. pres.(José López Portillo), Presidencia de la República, Coordinación General de Estudios Administrativos: Guía para la elaboración de manuales de procedimientos.-- México, D.F.: Talleres Gráficos de la Nación, 1978.

México. (José López Portillo), Presidencia de la República, Coordinación General de Estudios Administrativos: Glosario de términos administrativos.-- México, D.F.: Talleres Gráficos de la Nación, 1978.

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.

México. Secretaría de Programación y Presupuesto, Instituto nacional de Geografía, Estadística e Informática: Normatividad en informática.-- México, D.F.: Talleres Gráficos de la Nación, 1983.

México. Secretaría de Programación y Presupuesto, Unidad de Modernización de la Administración Pública: Políticas y normas iniciales de organización.-- México, D.F.: Talleres Gráficos de la Nación, 1983.

Morales, Jorge: "Los fabricantes opinan sobre la piratería".-- en Computerworld (México), abril 13, 1987. Año 7, No.138.

Naisbitt, John: "Macrotendencias".-- México, D.F.: Edivisión, 1985. 269 pp.

Nasuti, Frank: "Investigando delitos relacionados a la computación".-- en Data Processing Digest (U.S.A.) Vol.15, No.6, junio 1987.Pp. 5 y 6.

Neugent, Bill: "A University course in computer security".-- U.S.A.: System developement Corporation, mimeo, s.f. 16 pp.

Noguera Lara, Juan Antonio: "Auditoría del plan de desastre y recuperación"; en Actas; I Congreso iberoamericano de informática y auditoria,(San Juan, Puerto Rico, 2 a 6 de noviembre de 1987) Pp.393-414.

Nora, Simon y Alain Minc: "La informatización de la sociedad".-- México, D.F,: Fondo de Cultura Económica, 1981. 244 pp.

Nussbaum, Bruce: "El mundo tras la era del petroleo: los nuevos ejes de poder y riqueza".-- México, D.F.: Editorial Planeta, 1985. 274 pp.

Oficina Internacional del Trabajo: "Las repercusiones socioeconómicas de las nuevas tecnologías".-- Ginebra: O.I.T., 1985. (Comisión Consultiva sobre Tecnología. Primera Reunión. Ginebra 15-19 de abril 1985.)

Oficina Internacional del Trabajo: "Trabajo con pantallas de visualización".-- Ginebra: O.I.T., 1988. (Recopilación de fichas informativas).

Offe, Claus: "Ingobernabilidad: el renacimiento de las teorías conservadoras", en Revista Mexicana de Sociología (México), Num. 81, 1981.

Parker, Donn: "20 factores a considerar en la selección de medidas para proteger la información", en Data Processing Digest (U.S.A.). Vol 15, No.6, junio 1987. Pp. 3 y 4.

Perez Gomez, Jose Manuel: "La auditoria de los sistemas de información"; en Actas: I Congreso iberoamericano de informática y auditoria, (San Juan, Puerto Rico, 2 a 6 de noviembre de 1987), pp.91-118.

Peters, A.J.: "Elementos para el desarrollo y revisión de normas a seguir en torno a equipos de computación personal".- en Data Processing Digest (U.S.A.), Vol.15, No.6, junio 1987, pp.8 y 9.

Quibriera Matienzo, Enrique: "La informática nacional: primeras aproximaiones".-- México, D.F.: Universidad Autónoma Metropolitana-Xochimilco, (D.U. de C.S. y H.-T.I.C.O.M.), 1984.

Rada, J.: "The impact of micro-electronics: a tentative appraisal of information technology".-- Geneva: I.L.O., 1981 109 pp.

Ramirez Márquez, Miguel y Armando Espinosa Palomino: "La función de auditoría informática en Petroleos Mexicanos"; en Actas: I Congreso iberoamericano de informàtica y auditoria.(San Juan, Puerto Rico, 2 a 6 de noviembre de 1987), pp.435-446

Rein, Turn: "Problemas de seguridad en los sistemas de comunicación para procesamiento electrónico de datos", en Computer Communication Review (E.U.A.), Jan. 1975. Pp. 35-44.

Rivera Soler Ricardo: "Apuntes de Informática".-- s.p.i. mimeo, s.f.

Rodriguez Araujo, Octavio: "El perfil profesional del administrador pùblico", en Revista de Administración Pública (México), feb. 1983. Pp. 501-505. (Antología 1-54)

Scoma, Louis: "Protecting privacy of information".-- en Journal of information systems management (E.U.A.). Vol.3, No.3, Verano 1984, pp.79-81.

Scoma, Louis: "Security policy in the P.C. environment", en Journal of information systems management" (E.U.A.). Vol.4, No.2, Primavera 1985, pp.85-86.

Scott, William G.:"Organization theory", en Journal of the Academy of Management. (E.U.A.), vol. 4, num. 1 (abril 1961), Pp. 7 a 26.

Sendrow, Martin: "Impact of rapid changing computer technology on computer crime: advance computer security concepts".-- S.P.I., mimeo, 1980.

Shannon, C.E. y W. Weaver: "The mathematical theory of communication".-- Urbana: University of Illinois Press, 1949.

Simon, Herbert A.:"La nueva ciencia de la decisión gerencial".-- México: Librería "El Ateneo" Editorial, 1982. 163 pp.

Simon, Herbert A."The administrative behavior: a study on decision making process in administrative organization".-- New York: The Free Press, 1957. 253 pp. (2nd. Edition)

Simon, Herbert A:"El comportamiento administrativo: un estudio de los procesos decisorios en la organización administrativa".-- Madrid: Aguilar, 1962. 240 pp. (Traducción al español de la anterior).

Sotomayor, Jesùs y A. Sánchez: "Planeación de la recuperaciòn informática en casos de desastres".-- Ponencia en XIII Reuniòn de sistematización de bancos centrales americanos e ibéricos. (realizada en Santo Domingo, Repúblíca Dominicana del 25 de noviembre al 1o. de diciembre de 1984).sp.i. 75 pp.

Stanley, Philip: "Investigación e investigadores en el crimen omputacional", en Data Processing Digest (E.U.A.), Vol.15, No.6, junio 1987. Pp.2 y 3.

Tellez Valdés, Julio: "Derecho informático".-- México, D.F.: Universidad Nacional Autònoma de Méxio,1987. 248 pp.

U.S.A., Department of the Air Force: "Guía para la auditoría de sistemas automatizados de procesamiento de datos".-- México, D.F.: Herrero Hermanos y Sucs., S.A., 1968.

Van Eck, Win: "Las radiaciones electromagnéticas han de ser revisadas nuevamente", en Data Processing Digest (E.U.A.),Vol.15, No.2 Febrero 1987.Pp.85 a 92.

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).

Ward, Gerald,M.: "Cómo manejar los riesgos en la computación: el eslabón vital", en Contaduria Pública (México). Enero 1989. Pp. 44 a 48.

Wasserman, Joseph: "Auditoría y control en el procesamiento electrónico de datos", en Data Processing Digest (E.U.A.), vol.3, No.7.Julio 1975.

Westin, Alan: "Privacy, technology and regulation", en Donnelly, D.P. (Ed.): The computer culture.-- London & Toronto: Associated University Press, Inc. 1985. Pp. 136-152.

Wiener, Norbert: "Cybernetics".-- Cambridge, Mass.: M.I.T. Press, 1961.

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

Wilson, David R.: "Tendencias en cuanto a la seguridad de la información".-- en Data Processing Digest (E.U.A.) Vol 15, No.6, junio 1987. Pp. 9 y 10.

Wheatley,Jorge: "Formación y desarrollo del auditor en informática"; en Actas: I Congreso iberoamericano de informática y auditoria,(San Juan, Puerto Rico, 2 a 6 de noviembre de 1987), Pp.149-158.

Wolfe, Alan: "Los límites de la legitimidad".-- México, D.F.: Siglo XXI, 1980.

DOCUMENTOS LEGALES CITADOS

Acuerdo (Para la Secretaría de Programación y Presupuesto). Publicado en D.O. el 16 de enero de 1978.

Acuerdo 114 (Para la Secretaría de Educación Pública). Publicado en D.O. el 8 de octubre de 1984.

Acuerdo para el establecimiento y operación de los sistemas de transmisión de señales de datos y su procesamiento (para la Secretaría de Comunicaciones y Transportes). Publicado en D.O. el 12 de febrero de 1981.

Constitución Política de los Estados Unidos Mexicanos.

Ley de Información Estadística y Geográfica. Publicada en D.O. el 30 de diciembre de 1980.

Ley de Invenciones y Marcas. Publicado en D.O. el 10 de febrero de 1976.

Ley Orgánica de La Administración Pública Federal.

Reglamento de la Ley de Presupuesto, Contabilidad y Gasto Público Federal. Publicado en D.O. el 18 de noviembre de 1981.

Reglamento Interior de la Secretaría de Programación y Presupuesto. Publicado en D.O. 29 de julio de 1985.

GLOSARIO.

Administración. "Arte de conseguir que se hagan las cosas". "Se establecen principios para asegurar la acción comprobada entre grupos de hombres" De un proceso de elección se lleva a la acción. Esto es, en esencia, toma de decisiones.(1)
Amenaza. Siniestro o daño que puede materializarse o tener lugar.
Analista de sistemas --computacionales. Persona hábil en la definición y el desarrollo de técnicas encaminadas a resolver un problema, por medio de la aplicación de las nuevas tecnologías para el procesamiento electrónico de datos.
Archivo. Un caudal organizado de información, dirigido a una finalidad determinada.
Batch o proceso *batch*, o proceso en lote. Ejecución de procesos a la información en tiempo diferido de la captura.
Capturista. Persona que hace ingresar o alimenta datos a los sistemas de cómputo.
Bitácora. Registro de maniobras efectuadas en *hardware*, *software* o datos, de modo tal que se identifican usuarios, operaciones efectuadas y tiempos.
Clave de acceso. Conjunto de caracteres, numéricos o alfanuméricos, de tipo confidencial, que permiten al usuario la utilización de equipos, programas, archivos de datos o segmentos de éstos, con fines predeterminados.
Computarizado. Alude procesos o unidades administrativas que apoyan su operación con equipos de informática y programas de proceso de datos.
CPU (*central processing unit*). Unidad central de procesamiento. Es el procesador central de un sistema de computación. Comprende circuitos aritméticos y lógicos, los circuitos de comando y, en muchos casos, una memoria de rápido acceso. En torno a esta unidad se organizan los intercambios con otras memorias y con unidades de entrada y salida (periféricos). Es sinónimo del cuerpo principal de una computadora.(2)
Confidencial. Al referirse a la información, se alude aquella sujeta a circulación controlada o restringida. El carácter confidencial se adquiere con base en la protección de los derechos humanos, de las organizaciones, de los secretos bancarios, de estado, de seguridad nacional o soberanía y de la sana convivencia de la ciudadanía consigo misma y frente al aparato gubernamental.
Cultura informática. Consiste en una visión global del mundo informático, de la cual se desprenden aptitudes y actitudes encauzadas a adecuarse a nuevas formas prácticas, métodos, mentalidad y mística de trabajo. Se trata de

---

1.- Simon, Herbert A.: "El comportamiento administrativo: un estudio de los procesos decisorios en la organización administrativa".-- Madrid: Aguilar, 1962. P.13.
2.- De Nora y Minc: "La informatización de la sociedad".-- México: Fondo de Cultura Económica, 1981. P. 236.

comprender y asumir la dinámica de la "revolución informática" que se vive en la actualidad y su impacto en la vida de la sociedad.

Datos. Término genérico que se usa para denotar los hechos, números, letras y símbolos que se refieren o describen un objeto, idea o condición. Connota un elemento básico de información que puede ser procesado o producido por una computadora. En este trabajo se usa como sinónimo de información.

Delito. Infracción de una ley o cualquier ordenamiento jurídico o norma consuetudinaria, que impacta negativamente la sana operación de un país o de sus instituciones o los derechos de las personas y la sana convivencia social.

Dependencia. Se refiere a secretarías de estado, departamentos administrativos o procuradurías de justicia, a nivel federal.

Eficiencia. Utilización de los medios menos costosos o breves, para alcanzar las metas que se proponen.

En linea. Similar a tiempo real. Se refiere a aplicar transacciones al momento de ser capturadas.

Entidad. Hace referencia a organismos descentralizados, desconcentrados, empresas estatales u organismos de participación estatal.

Equipos informáticos. Sinónimo de computadoras o equipos de procesamiento electrónico de datos.

Flujo de la información. Secuencia de eventos o transformaciones que sufre la información. Incluye fases como origen, captura --al sistema de cómputo--, transmisión, proceso --cálculos o depuración--, actualización, almacenamiento --grabado en medios magnéticos--, consultas, borrados y salida --en reportes o listados.

Hardware. Partes mecánicas, electromecánicas o electrónicas de los computadores. Está constituido por la estructura física de captura, proceso, almacén, transmisión y listado de de datos.

Informática. Tratamiento automatizado de información. Se usa como sinónimo de computación, de procesamiento electrónico de datos y de nuevas tecnologías para el proceso de información.

Informatizado. Sinónimo de computarizado. Alude también las sociedades o instituciones que valen en amplia medida de procesos rápidos y manejo masivo de información, para su desenvolvimiento cotidiano, en lo económico, político y social.

Lenguaje ensamblador. Es un lenguaje computacional que facilita la programación en lenguaje máquina.

Lenguaje máquina. Es el lenguaje en sistema binario, octal o hexadecimal que es entendido directamente por las el CPU.

Lenguaje de alto nivel. Lenguaje que no puede ser entendido directamente por las computadoras, pero que es facilmente comprensible por las personas. Para ser ejecutado, debe traducirse a un lenguaje maquina.

Manual. Medio escrito que comunica las prácticas de la organización, destinado a tener vigencia relativamente

permanente en su aplicación. Apoyan a que la rotación de personal no afecte la operación de un organismo. Entre los manuales más usuales en la administración pública mexicana destacan, 1) manuales de organización, 2) manuales de descripción de puestos, 3) manuales de inducción al puesto, manuales para el desarrollo de funciones específicas de las unidades administrativas, entre otros. En el terreno de la informática destacan los manuales técnicos y del usuario, para equipos, periféricos, programas, archivos de datos y comunicaciones, en sistemas computarizados.

Método. Conjunto armonizado de procedimientos que permite la realización de tareas hacia metas u objetivos específicos, en tiempos y con uso de recursos predeterminados.

Microprocesador. Procesador miniaturizadodonde, en principio, sus elementos están conjuntados en un solo circuito. Hace operaciones lógicas o aritméticas.

Norma. Término genérico que refiere cualquier tipo de ordenamiento aplicable a una materia o tema o aspecto de la operación de personas morales, o vida de personas físicas.

Normatividad. Conjunto de ordenamientos, de origen constitucional, de leyes --generales o específicas--, de reglamentos, oficios, acuerdos, decretos, políticas , entre otros, aplicable a un tema o materia específica.

Paquete. Sinónimo de programa fuente. Consiste en programas con base en los cuales se desarrollan aplicaciones para las instituciones.

Password. Es una clave o código, que ingresa un usuario informático

Périféricos. Todo accesorio que se conecta al "CPU" o cerebro de una computadora.

Política. En un sentido microadministrativo, es lineamiento a seguir en el comportamiento del personal o desarrollo de sus tareas cotidianas. Es orientación a seguir sobre la cual no se ejerce vigilancia continua, pero sí evaluaciones periódicas. Las políticas ponen límite a la discrecionalidad del personal subordinado.

Política informática. Es política derivada de procesos de planeación en la que se establecen aspectos de desarrollo de equipos de cómputo y programación, difusión ordenada de la informática y sus aplicaciones, contratación gubernamental de bienes y servicios computacionales, formulación de normas y estándares de operación, control, seguridad y auditoría.

Privacía. Derecho del individuo consistente en el respeto a los espacios físicos y conceptuales de su propiedad y a su derecho de no ser molestado en sus asuntos personales.

Procedimiento. Tarea, o conjunto de tareas, a efectuar para el alcance de una meta específica o desempeño de una función cotidiana.

Programa. Conjunto de instrucciones utilizados por un computador para procesar datos. Se forman con base en lenguajes de programación (p.ej. BASIC, Fortran, Cobol, Pascal, C, entre otros) o en paquetes de "software" (p.ej.Dbase III, Lotus 123, Framework, etc.)

Programa de aplicación. Nombre genérico aplicable a programas de alto nivel, o *software*.
Programa fuente. Es un programa desarrollado en un lenguaje de alto nivel. Se trata de programa escrito en un lenguaje concebido para facilitar la expresión de cierta clase de procedimientos planteados por el usuario computacional.
Programa objeto. Es un programa de aplicación, elaborado con algún lenguaje de programación o de alto nivel, pero ya traducido a lenguaje de màquina.
Racionalidad. Es criterio de elección entre alternativas preferidas de actividad, de acuerdo con un sistema de valores cuyas consecuencias consecuencias de comportamiento pueden ser valoradas. Una decisión es "objetivamente racional" si es en realidad el comportamiento correcto para maximizar unos valores dados en una situación dada. En el contexto de una organizaciòn, un acto es racional si se orienta hacia las finalidades de la propia organizaciòn.(3)
Retroalimentaciòn. Alimentar un sistema, unidad administrativa, plan o programa, con base en información generada por su propio desempeño o *output*, con objeto de mejorar su rendimiento o funcionamiento.
Riesgo. Propensiòn a que tenga lugar un daño, medido con base en elementos objetivos (datos estadísticos y presencia de medidas de control o seguridad) y subjetivos.
Seguridad informática. Provisión de un conjunto integrado de normas jurídicas, políticas, métodos, procedimientos, mecanismos y medios, en general, que garanticen la sana operación de los sistemas de información en todos sus niveles, y el mantenimiento de la integridad y confidencialidad de los datos.
Seguridad Computacional. Sinònimo de seguridad informática.
Siniestro. Evento que ocasiona daños en los activos de alguna persona física o moral. Pueden ser de origen intencional o natural.
Sistema. Conjunto de elementos que interactúan congruente y armonicamente.
Sistema de información o sistema de computación. Conjunto armonizado de programas y bases de datos, destinado a recibir, procesar y emitir reportes de información depurada, hacia fines especificos en una organización o en una unidad administrativa, que permite una operaciòn y toma de decisiones altamente eficiente. Cuando se menciona el tema de la seguridad en los sistemas de información o informática, se incluye, además, los equipos, dispositivos físicos, así como las instalaciones que albergan éstos.
Sistema de comunicación administrativa. Es el conjunto de canales o estructura de intercambio de información en una institución, que permite su operación cotidiana y sustenta la toma de decisiones en los diferentes niveles de mando -- jerarquía y responsabilidad. El sistema de información administrativa atañe las comunicaciones formales de la institución y se da de manera horizontal o vertical. La

---

3.- De Simon, op. cit. Pp. 73 y 74.

comunicación horizontal se plasma en memorandums, por lo general. La vertical es descendente y ascendente. La primera fluye mediante órdenes, informes, avisos o capacitación. En ella se comunican normas, políticas, criterios de actuación y evaluaciones, entre otros. La ascendente fluye mediante quejas, sugerencias, reportes, informes a mandos supervisorios o altos o consultas.(4)

Software. Estructura lógica, que permite al computador la ejecución de trabajos. Se integra por paquetes y programas de todo tipo.

Staff. Unidad administrativa o grupo de personas, en una organización, que apoya la gestión o toma de decisiones en mandos altos o medios, sin tener una posición de subordinada en la jerarquía institucional.

Stress. Sinónimo de la tensión nerviosa que acumulan las personas, por lo general, al desarrollar trabajos rutinarios, repetitivos, o ejecutados bajo presiones de tiempo o de alto esfuerzo intelectual.

Tiempo real o procesos en tiempo real. Ejecución de procesos a los datos, en forma simultánea que se capturan o ingresan a los sistemas de cómputo.

Terminal. Sitio de entrada o de salida, o de ambas cosas, vinculado con un computador. En la terminal se efectuan emisiones o recepciones, o ambos, de datos. (5)

Unidad administrativa. Oficina o grupo de oficinas que integran una casilla en el organigrama de una institución.

Utilerías. Programas pequeños que facilitan el trabajo del usuario o programador, al trabajar con sistemas operativos o con otros programas. P.e. relojes en las computadoras, instrucciones para efectuar búsquedas de datos, copias, reemplazos, etc.

4.- Esta explicación de los sistemas de comunicación administrativa se formó con base en diversos elementos aportados a lo largo del trabajo de Simon, Herbert A.,op. cit.

5.- De Nora y Minc, op. cit., p. 233.

ANEXO 1.- PLANEACION DE LA RECUPERACION INFORMATICA EN CASOS DE DESASTRE.

El desastre informàtico puede ser definido como el momento en el que la operaciòn de un organismo o la integridad o la confidencialidad de la informaciòn, se ven impactados negativamente o disminuidos. Sotomayor distingue tres categorías básicas de desastres.(1)

1) Desastre menor. Es el que no tiene repercusiones fundamentales en la operación diaria de las instituciones. Normalmente, es recuperable con algunas horas de trabajo.

2) Desastre grave. Es aquel que afecta significativamente la operación del organismo, pero resulta recuperable con algunos dias de trabajo, si se han tomado medidas preventivas.

3) Desastre critico o fatal. Tiene lugar cuando su recuperación no es posible o es muy costosa, en tiempo y recursos financieros. Afecta gravemente el funcionamiento y la viabilidad de la institución.

Los desastres son inevitables cuando existe vulnerabilidad. Pueden ocurrir en algùn lugar y en algún momento. El deber del administrador de seguridad informática, asi como de los auditores, es de evitar que cuando éstos tienen lugar, no se inscriban en la tercera categoria.

1.- Sotomayor, Jesus: Planeaciòn de la recuperación informática en casos de desastres.-- Mimeo. P. 13. Este anexo, en lo fundamental, extracta el trabajo citado.

Existen otros esquemas de clasificación de desastres, útiles de citar. Por la naturaleza del daño, los desastres pueden tener lugar en los siguientes.(2)

1) Instalaciones (a causa de sismos, inundaciones, descargas eléctricas, entre otros).

2) En el *hardware* (descompostura o daño de equipos o dispositivos de proceso o almacenamiento de datos).

3) En los medios de comunicación, (equipos o lineas de teleproceso).

4) En el *software* (pérdida o daño de programas o paquetes).

5) En los datos o información (pérdida de archivos de datos o porciones de éstos).

Por otro lado, los desastres también pueden categorizarse en intencionales o no intencionales.(3)

Con base en el análisis de riesgo informático que cada institución efectúe, se determinan los tipos de daños que pueden tener lugar, sus impactos, costos de reposición y costos de reducción de nivel de riesgo. En el capitulo No. 9, en la sección que aborda la planeación de la seguridad, se indicó que los riesgos se a)absorben, b)reducen o c) se trasladan. Para cada riesgo identificado se define una combinación de éstas, para afrontarlo.

2.- Esta clasificación es acorde con los niveles de seguridad informática, descritos en el marco analítico que se expuso en el Cap. 6.
3.- Ver supra. Tipología de daños informáticos. Sección 5.4.

La planeación de la recuperación de desastres es aplicable a los desastres de la categoría 3, para convertirlos en categoría 2 o 1.

La integración de un marco de planeación para recuperación ante desastres informáticos implica cinco fases, según Sotomayor.

I) Manejo del riesgo.

II) Prevención mïnima.

III) Determinación básica.

IV) Reducción máxima.

V) Planeación para la recuperación.

I) MANEJO DEL RIESGO.

La recuperación de desastres informáticos es efectiva para riesgos de categoría 2 y 3. Los de categoría 1 son asumidos por la propia organización, dado su corto alcance. El elemento básico para cubrir riesgos mayores es la transferencia de los mismos, es decir, que sean asumidos por una empresa aseguradora, a través de la contratación de pólizas que cubran instalaciones, equipos, dispositivos y, si lo acepta el asegurador, los propios programas y archivos de datos.

II) PREVENCION MINIMA.

Esta fase comprende los medios y mecanismos para evitar, según los riesgos organizacionales, que ocurran daños o pérdidas. Ello reduce las posibilidades de que tengan lugar los siniestros y, a su vez, se minimizan los costos de pólizas de seguro. Los ámbitos de prevención

corresponden a los niveles de seguridad, pero se pueden aglutinar en dos areas: instalaciones y equipos y programas y archivos.

II.1) Prevención mínima en instalaciones y equipos.

Respecto a ésta area se recomienda la observancia de los siguientes lineamientos.

Primero. Planeación adecuada para las instalaciones físicas. El lugar deberá ser suficientemente alto, para evitar inundamientos y alejado del bullicio popular, para evitar acciones terroristas o vandalismo. Asimismo, deberá tener pocas o ninguna ventana hacia el exterior, lo que equivale a no exhibir los equipos.(4)

Segundo. Deben existir medios eficientes de enfrentar incendios, a través de la instalación de detectores de humo, de temperatura, alarmas, salidas de emergencia y equipos de extinción.(5)

Tercero. Habrá controles de acceso físico, según las necesidades de cada organización.

Cuarto. Se debe contar con equipos de suministro de aire acondicionado y energía de respaldo.

4.- Esta recomendación se opone a la práctica común, en México, de situar centros de proceso de datos ante ventanales que dan a la vía pública o sitios de alta circulación de personas en los edificios. Esto se acostumbra hacer de manera que el centro de cómputo se exhiba como aparador. V. Supra. Sección 7.4.2.1.1.

5.- Para la extinción de fuego se deberá usar, preferencialmente, el gas conocido como "halón", que absorbe el oxígeno del aire y sofoca el fuego. En su defecto se aplicará gas CO2. Bajo ninguna circunstancia se debe aplicar agua, para no generar corto-circuito y evitar polvos químicos, que son difíciles de remover de los componentes electrónicos y los pueden dañar.

Quinto. Los respaldos de *software* y de archivos de datos se situarán en lugares remotos y seguros.(6)

Sexto. Las labores de limpieza tienen que ser sujetas de seguimiento cuidadoso. Se recomienda que se programen periódicamente rutinas de destrucción de discos o documentos inservibles para que no estén al alcance de personas ajenas a la operación de los sistemas. El personal que efectúa aseo a un centro de cómputo deberá ser capacitado, a modo de evitar que su impericia genere desastres.

Séptimo. Para la prevención de desastres en operación de equipos, la herramienta más eficaz es la contratación de pólizas de de mantenimiento detectivo y preventivo, que reduzcan la posibilidad de fallas eléctricas o electrónicas. Es éste, en realidad, el medio más óptimo para asegurar el correcto funcionamiento electrónico de los equipos.(7)

II.2) Prevención de desastres en programas y archivos.

Cuando los equipos operan en condiciones normales y adecuadas, es dificil que se dañen programas. Por lo general, los daños en *software* se atribuyen a errores u operaciones fraudulentas. Por ejemplo, montaje equivocado de discos o cintas; pérdida, robo o copia de los mismos;

6.- Para la constitución de un centro de respaldo, Sotomayor recomienda que se cuente con los siguientes elementos.
1) Dispositivos magnéticos que contengan sistemas operativos, programas de todos tipos, archivos de datos y archivos de utilerias.
2) Material de trabajo, tal como papelería membretada, formas, componentes de *software* básico (equipos y partes).
3) Documentación, como manuales de recuperación ante desastres, manuales de usuario o de operación de equipos y programas y copia de pólizas de seguro.

7.- Defiende esta posición, Sotomayor, op. cit. P.28.

alteraciones intencionales a programas; borrados accidentales y errores el la lógica de los programas.

Para la comprensiòn de los daños en los datos se distinguen dos tipos de operaciòn de sistemas: procesos "batch" (o en paquete) y procesos en linea (o de tiempo real). Si se trata de los primeros, la recuperaciòn es sencilla con un adecuado manejo de respaldo de los datos.(8) Si existe algún daño en el *hardware* que afecte archivos de datos, o programas, inclusive, la existencia de respaldos resuelve el problema. Para operaciones en linea, en las que operan coordinadamente fases de captura, transmisiòn, proceso y almacenaje, la recuperaciòn se logra con la existencia de respaldos de los archivos base y bitàcoras de las operaciones efectuadas o movimientos. Esta consiste en registro en el que se asientan todos los cambios u operaciones que tienen lugar en determinados archivos de datos, en cierto tiempo. La bitácora registra quién, cómo, cuándo, dónde y qué hizo con la información, en cada movimiento o acceso.

III) DETECCION BASICA.

Para determinar la existencia de un desastre, deben existir medios adecuados para ello, en los niveles de institución, equipos, programas y datos. En las instalaciones se cuenta con detectores de humo y fuego,

---

8.- Se recomienda, al menos, contar con tres copias de las informaciones organizacionales.

alarmas, circuitos cerrados de televisiòn, vigilancia las 24 horas, entre otros.

A nivel de *software*, las herramientas de detección son los respaldos a los mismos, que deben ser cotejados periódicamente con los programas en operación. De ese modo se verifica su integridad. Adicionalmente, la detecciòn se auxilia de las bitácoras de operaciones o movimientos

En el nivel de los datos, el medio de detecciòn es la auditoria. Existen programas para ello y el diseño de los propios sistemas de informaccción de las organizaciones deben incluir medios prácticos para efectuar revisiones tales como arqueos, conciliaciones, cotejar sumas. La auditoría de los datos opera en forma no sincronizada con la operaciòn normal de los sistemas.

IV) REDUCCION MAXIMA.

Una vez detectada la ocurrencia de un desastre, se debe evitar que éste se agrave, es decir, se trata de detener o minimizar sus consecuencias.

En el caso de instalaciones, en lo posible, se controlan siniestros como fuego, a través de los medios antes mencionados. En el caso de daños a *software* o datos, se envían mensajes a los usuarios para cerrar archivos y detener operaciones, que puedan dar lugar a mayores destrucciones.

V) PLANEACION DE LA RECUPERACION.

Es necesario plantear diferentes tipos o metodologías de recuperación, según la naturaleza del desastre que se

trate. Esto es con el fin de que la recuperación sea eficiente y ordenada.

El plan inicia con la formación de un comité de desarrollo --éste puede ser el comité de seguridad informática, porpuesto en la sección 9.2--, que identifique y defina los siguientes aspectos, según Sotomayor.

1) Definición de necesidades mínimas de supervivencia operativa en, por lo menos, tres categorías. a) Prioridad alta: sujetos a fechas de entrega límite y que de su ejercicio depende la viabilidad y funcionamiento esencial del organismo. b) Prioridad media: operaciones importantes o críticas para un organismo, pero que pueden retrasarse. c) Prioridad baja: no críticos y cuyas fechas de entrega pueden posponerse durante un tiempo previsible.

2) Preparación de recuperación de desastres, según sean de impacto en instalaciones, equipos, personas, programas, datos u otros implementos informáticos. Se plantean medios de recuperación, según tipo de desastre.

3) Establecimiento de relaciones con instituciones de respaldo. Ello se efectúa vía acuerdo mutuo o vía contractual. Si los sistemas operativos de ambas partes son distintos, deberán existir medios de conversión de uno al otro.

4) Instrumentación de planes. Se definen rutas críticas o métodos a seguir para efectuar recuperación y respaldos.

5) Simulación y retroalimentación de información. Es necesario efectuar simulacros periódicos con objeto de

validar las previsiones de recuperación y retroalimentar los planes para ello.

6) Definición de respaldos y frecuencia de los mismos. En el centro de cómputo de respaldo se actualizarán archivos de datos con una óptima periodicidad, de modo que la recuperación sea eficiente y oportuna.

7) Elaboración de manuales de emergencia y recuperación, en los que se contemplen desastres según su naturaleza y gravedad.

8) Establecimiento de personal de guardia mínimo para la recuperación.

Los manuales de recuperación son herramienta indispensable para el restablecimiento de operación informática, minimizar daños y optimizar la respuesta frente a siniestros. El contenido sugerido para un manual de recuperación se presenta en el cuadro siguiente.

CUADRO 13.
CONTENIDO DEL MANUAL DE RECUPERACION
1) Procedimientos iniciales de avisos y acciones.
2) Lista de personas que pueden iniciar la ejecución del plan de recuperación.
3) Requisitos de personal para recuperación.
4) Direcciones y números telefónicos de: -- vendedores; -- centro de cómputo alterno; -- clientes; -- médicos, policía, bomberos; -- servicios, -- personal.
5) Procedimiento en caso de amenazas.
6) Mecanismos de notificación y control de actividades.
7) Operación en el centro de apoyo.
8) Plan de evacuación.
9) Recuperación y conmutación telefónica.
11) Reporte y evaluación de riesgos existentes en el centro.
12) Copias de contratos y seguros.
13) Guías de comunicación con terroristas.
14) Mecanismos de respaldo existentes.

Fuente: Sotomayor, Jesús, op. cit. P. 38 (9)

9.- Como complemento a este cuadro, Sotomayor enumera las condiciones que dan lugar a efectuar cambios o actualizaciones en manuales de recuperación. V. Ibid. P. 39. Entre ellas están las que siguen. 1) Cambios de personal. 2) Cambio de equipo o instalación. 3) Cambio de teléfonos. 4) Cambio de sistemas. 5) Cambio de las condiciones sociopolíticas de la ciudad o país. 6) Cambios en contratos de mantenimiento. 7) Cambio de pólizas de seguros. 8) Ruptura de la privacia en el plan de desastre o

Las labores de recuperación se pueden contemplar en dos frentes temporales. a) En el corto plazo, tendrán verificativo las siguientes tareas.

-- Operación temporal sin recuperación total.

-- Operación desde un centro alterno.

-- Notarización del desastre.

-- Comunicación con usuarios y proveedores.

-- Enrutado de lineas telefónicas.

b) En el largo plazo, se efectuarán las siguientes tareas.

-- Recuperación total.

-- Reconstrucción o reubicación.

-- Cobro de primas de seguro.

-- Reprogramación. (10)

El cuadro siguiente resume las fases de recuperación hasta el momento expuestas.

---

recuperación. 9) Cambio de instalaciones de respaldo y alternas.

10.- Tomadas de Sotomayor, ibid. P. 44.

CUADRO 14.
MANEJO DE DESASTRES: FASES DE RECUPERACION.

1) Compromiso institucional.

2) Prevención mínima.

3) Detección máxima.

4) Reducción máxima.

5) Planeación para la recuperación.

6) Recuperación temporal.

7) Recuperación total.

8) Retorno al inciso 2.

Fuente: Basado en Figura XXI de Sotomayor, op. cit. P. 63.

El comité de desastres informàticos será quien defina y regule los daños informáticos y recuperación de sistemas. No obstante, la responsabilidad de la ejecución de labores de prevención, así como de restablecimiento de operaciones, será el propio personal directivo de cada uno de los centros de cómputo o unidades informáticas del organismo. Contarán con los recursos necesarios, y personal, para cumplir esta tarea.(11)

En la puesta en marcha del plan de recuperación es necesario verificar los siguientes lineamientos, según Sotomayor.(12)

11.- Para la recuperación específica de diversos tipos de desastre ver. Sotomayor, Jesus, ibid. Pp. 41 a 49.
12.- Ibid. Pp. 43 y 44.

1) Verificar la imposibilidad de recuperación básica en las instalaciones. Solo en caso contrario se procede al uso de una instalación alterna.

2) Revisar los requerimientos de compatibilidad de equipo en la instalación alterna. Si los sistemas operativos son diferentes, deberá existir paquetería --de programas-- para conversión del uno al otro o que los programas serán grabados, ya convertidos, en cintas o discos de apoyo, a fin de minimizar el tiempo de operación de la instalación alterna.

3) Revisar procedimientos de seguridad, privacia y planes de desastre en la instalación alterna, a fin de evitar doble desastre, que sería crítico o irrecuperable. La seguridad, privacia y buen uso de la información en la instalacción de apoyo, deberán observarse con mayor rigor que en la instalación o condiciones normales, si se está en contacto con personal o usuarios ajenos. Se recomienda cambiar los "passwords" o claves de acceso al tener lugar la mudanza a la instalación alterna o regresar a la propia.

4) En caso de amenaza terrorista y evacuación, el directivo contestará las llamadas y grabará las comunicaciones. Tendrá preparadas preguntas que ayuden a la identificación del responsable. La evacuación deberá ser ordenada y evitando al máximo que se genere pánico colectivo.

Las tareas de recuperación se deberán llevar a cabo en dos frentes, paralelos. En uno, se lleva a cabo la operación

del organismo y en otra, se restablece la operaciòn total del centro o sistema de còmputo.(13)

ANEXO 1.1.-BITACORAS DE OPERACION

Las bitàcoras constituyen herramienta esencial para la recuperaciòn ante desastres. Son bases de datos que registran informaciòn acerca de movimientos en archivos de datos o programas, permiten su reconstrucciòn en caso de pérdida y facilitan la identificaciòn de causas o medios por los que ocurrieron desastres.

Su utilidad se presenta en las labores siguientes.

1) Auditoria informática. Constituye una guia de todas las actividades de lectura, escritura o borrado de archivos o programas.

2) Recuperaciòn. Es forma segura de restablecer la integridad de archivos.

3) Análisis de fallas. Conocer las causas por las que falla un programa.

4) Correción. Permite efectuar correcciones en archivos mal capturados, de manera intencional o accidental.

5) Monitoreo. Permite el monitoreo o seguimiento de usuarios y terminales en sistemas de còmputo que efectúan procesos o transacciones en linea o en tiempo real.

13.- Como ilustraciòn de caso real de recuperación informática V. Noguera Lara: Juan Antonio: Auditoria del plan de desastre y recuperaciòn (caso real, que tuvo lugar en la Ciudad de Mexico, en septiembre de 1985.), en Actas: Primer congreso iberoamericano de informàtica y auditoria: San Juan, Puerto Rico, noviembre 1987. Pp.405 y ss. Este mismo trabajo aporta elementos para auditar planes de recuperaciòn de desastres informáticos.

Sotomayor propone tres tipos de bitácoras.

1) Bitácora de uso/modificación de archivos. Registra quién, cómo, cuándo y qué se hizo con un archivo de datos o programa.(14)

2) Bitácora de errores de sistema o de programas. Se elabora manualmente por los usuarios.(15)

3) Bitácoras de usuarios/terminales. Es un registro de funciones de cada archivo, así como las atribuciones de cada usuario. Esta bitácora es consultada por el sistema para permitir acceso a archivos, decodificar datos, en su caso, y autorizar ejecución de programas.

14.- Este tipo de bitácora registra los siguientes datos. 1) Nombre del usuario. 2) Archivo accesado. 3) Tipo de acceso (leer, modificar, borrar). 4) Hora de acceso. 5) Terminal o medio usado. 6) Registro accesado. 7) Programa o rutina usada. 8) Imagen o datos anteriores o viejos. 9) Imagen posterior o nueva. 10) Mensaje de terminación de transacción. 11) Prioridad usada o violada. Tomado de Sotomayor, ibid. P. 54.

15.- El contenido de éste incluye los siguientes puntos. 1) Tipo de programa (rutina de sistema operativo, programa fuente, programa de aplicación, etc.) 2) Nombre del programa o rutina donde se presentó el error. 3) Nombre del sistema o aplicación. 4) Nombre del usuario. 5) Hora de ocurrencia. 6) Archivos de datos utilizados. 7) Linea del programa. 8) Tipo de error. 9) Descripción del error. 10) Mensaje emitido. 11) Acción tomada. 12) Acción sugerida. Sotomayor, Ibid. P. 56.

ANEXO 2.- ASPECTOS METODOLOGICOS DE RESPUESTA FRENTE AL CRIMEN COMPUTACIONAL E INVESTIGACION DE DELITOS.

El universo de los delitos computacionales puede ubicarse en tres categorías, según Philip Stanley.

1) Los relativos a grandes sistemas de cómputo con usuarios internos y externos.

2) Los relativos a sistemas de mediana capacidad, con un número determinado de terminales y dedicados, por lo general, a aplicaciones prácticas en una organización.

3) Los relativos a sistemas pequeños, de una a cuatro terminales y con pequeño número de usuarios.

Los primeros son los de mayor complejidad en su investigación y requieren trabajo extenso. El delincuente puede ser uno o muchos usuarios y estar en cualquier parte, dentro, o, tal vez, fuera de la institución afectada. La historia común de este tipo de delitos, en los últimos años, es que son descubiertos mucho tiempo después de cometidos.(1)

Los segundos son más fáciles de investigar. El culpable está dentro de la organización, pero su identificación no es sencilla.

Para el tercer tipo de delitos, es sencillo detectar al culpable, pero es complicado conocer la magnitud del daño. En equipos o sistemas pequeños, el usuario, por lo general,

---

1.- Uno de los fraudes más grandes, detectado en los Estados Unidos de Norteamérica, se conoció hasta que el criminal lo confesó al F.B.I., después de cometer ilícitos de otra naturaleza, muchos meses después.

puede efectuar manipulaciones en *hardware*, en los sistemas operativos, en lenguajes o paquetes de programación, en programas de aplicación y en los mismos archivos y registros de datos. La facilidad de que el usuario u operario efectúe manipulaciones en estos ámbitos es poco probable en sistemas medianos o grandes.

Sea cual sea el tipo de delito, la investigación es de alta utilidad para la institución, en el conocimiento de su vulnerabilidad informática y en la mejoría de la cobertura de la seguridad.(2) Ello requiere la instrumentación de un plan, a nivel directivo, para reaccionar rápida, oportuna y apropiadamente ante cualquier ilícito. Adicionalmente, es necesario integrar un equipo de trabajo eficiente, con especialistas en *hardware* y *software*, contadores, auditores informáticos, abogados y administradores.(3)

El especialista en *hardware* orienta e investiga formas de rastreo de operaciones o archivos que, quizá, el delincuente da por borrados. El especialista en *software* determina el modo en que los programas fueron operados y opina sobre formas factibles de detectar y demostrar irregularidad en los procesos. El contador interviene en la definición de la naturaleza del daño y su cuantía. El abogado orienta sobre disposiciones legales, vigentes, para

---

2.- Ver Nasuti, Frank: "Investigando delitos relacionados a la computación".-- en Data Processing Digest (U.S.A.) Vol.15, No.6, junio 1987. P. 5.
3.- Este equipo para investigación de delitos equivale al comité de seguridad informática, referido en la sección 9.3.1.

encauzar judicialmente el problema y satisfacer los requerimientos de la ley para aceptar pruebas, así como los derechos y obligaciones del delincuente o sospechosos. Por su parte, el auditor informático es el responsable de que los controles establecidos sean continuamente revisados y operados y ayuda a coordinar la investigación del crimen informático --en su calidad de evaluador. Los documentos y rutinas de auditoria pueden aportar elementos de juicio en la caracterización del delito y dimensionamiento de su alcance. El administrador tiene el papel de coordinar esfuerzos del equipo que interviene en la investigación, tomar decisiones de acción o respuesta, gestionar cobros a compañias aseguradoras --en caso de existir pólizas de seguro aplicables a la informática y contratadas por la institución-- y ser intermediario entre la alta dirección de la institución y el equipo mencionado.(4)

Por su naturaleza, los planes de investigación de delitos computacionales son de circulación restringida y deben ser mantenidos en secreto. Se recomienda que sea conocido por el alto mando de la organización, la administración informática, los responsables de auditoria y seguridad informática de la institución, compañias de seguros con las que se contraten pólizas, despachos de abogados que presten servicios a la organización y asesores en seguridad computacional.

4.- Tomado parcialmente y adaptado de Nasuti, op. cit. P. 6.

El trabajo en equipo se recomienda debido a la complejidad que representa el fenómeno informático. Stanley afirma que en el mundo no hay experto que conozca todos los posibles aspectos de delincuencia y su enfrentamiento. Refiere que en los Estados Unidos ha existido buena experiencia del trabajo en equipo, con especialistas de diversas disciplinas.

Los ilícitos informacionales se tratan de un fenómeno criminológico reciente. El proceso de aprendizaje de esta problemática ha surgido de estudios de casos reales. Con base en ello, mientras más eventos sean conocidos en lo posible, ya sean reales o simulados, por los equipos de trabajo, se pueden enfrentar crímenes de diversas modalidades.

El mismo autor habla de cuatro tipos de situaciones de crimen computacional posibles.

1) Cuando el delito ha sido detectado y el culpable identificado.

2) Cuando el delito ha sido descubierto, pero no el perpetrador.

3) Cuando no se ha detectado delito, pero se sospecha de algún individuo.

4) Cuando no se ha detectado delito ni tampoco culpable, pero hay un nivel considerable de vulnerabilidad informática en la institución. (5)

5.- De Stanley, Philip: "Investigación e investigadores en el crimen computacional", en Data Processing Digest (E.U.A.), Vol.15, No.6, junio 1987. P.2.

Si se conoce la naturaleza del delito es màs fácil encontrar al culpable, dado que es posible la elaboraciòn del perfil del mismo y de su forma de actuar.

Con base en un método propuesto por Nasuti, se proponen los siguientes pasos para la investigaciòn de delitos informáticos. El objetivo general es asentar con claridad todas las caracteristicas y dinámica del acto cometido en el fraude. Se busca a) castigar delincuentes, b) reparar daños, c) conocer más la vulnerabilidad de la organización, d) difundir entre los empleados la importancia de la seguridad en el manejo de sistemas de cómputo, así como el interés en ella de la alta direcciòn. De esa manera se busca constituir elementos de intimidaciòn hacia los empledos, en la comisión de actos ilegales.

Los pasos en el método de Nasuti son los siguientes.(6
1) Determinar cuàl fue el delito y sus caracteristicas, con la inclusiòn de sus alcances o monto desfalcado.
2) Determinar si ya fue cometido o està en proceso, es decir conocer la oportunidad cde la detecciòn. Si está en proceso de cometerse o continùa la vulnerabilidad es necesario bloquear los canales que llevan al delito.
3) Determinar si participó una o más personas, es decir, si fue un fraude solitario o por colusiòn de diversos empleados, que pueden pertenecer a diversas areas de la organización.

6.- Nasuti. Ibid.

4) Conocer si la responsabilidad del acto ilícito es de servidores de la propia organización.

5) Localizar testigos.

6) Localizar sospechosos.

7) Entrevistar a testigos y sospechosos.

8) Detectar fuentes de prueba.

9) Obtener información de las fuentes de prueba posibles y analizarla hasta contar con elementos para emitir conclusiones. Ello implica la revisión de toda la documentación relacionada con el delito: documentos originales, documentación de sistemas, reportes o listados computacionales, registros históricos, documentación contable, entre otros. El investigador o equipo de investigación deberá conocer en detalle cómo funciona el sistema de cómputo implicado en el delito. Todo esto determina las causas y el modo de realización del delito.

10) Informar a la alta dirección de los resultados y tomar medidas de corrección de puntos vulnerables en los sistemas de informática: en lo operativo, en lo físico, en lo lógico y en el propio personal.

La presencia de una metodología en la investigación de desastres intencionales informáticos es ayuda importante para reacción oportuna ante cualquier contingencia de esta naturaleza. Facilita el aseguramiento de activos informáticos e informacionales, minimiza costos de contratación de pólizas de seguro, da lugar a registrar aecuadamente las experiencias negativas experimentadas por

una institución, reduce la vulnerabilidad computacional y permite enfrentar eficientemente y reducir impactos de los delitos informáticos.

ANEXO 3.- METODOLOLOGIA DE ANALISIS DE RIESGOS INFORMATICOS.

Con base en los aspectos expuestos hasta ahora, se desprende la seguridad informàtica como aspecto que responde, fundamentalmente, a toma de decisiones de la alta dirección de las organizaciones. Estas decisiones, por su naturaleza, deberàn estar sustentadas en análisis de costo-beneficio. Se hace necesario resolver ¿ cuàl es el costo de falta de seguridad computacional, parcial o integral? ¿ Qué beneficios aporta la instrumentación de planes o medios o mecanismos de protecciòn y control? La respuesta implica, al menos, cuatro consideraciones. 1) La determinaciòn del valor de la informaciòn y los activos informáticos. 2) Identificaciòn de amenazas a que está expuesta la información y los medios que la soportan y procesan. 3) Valoraciòn del grado de riesgo que representan esas amenazas. 4) Estudio de costo de los mecanismos o medios de seguridad, cotejado con los beneficios derivados o su efectividad.

La justificación primordial de la valoración y protección en informática, se asienta en el valor que tienen los datos para el mantenimiento de la privacía personal o institucional y para la continua y sana operaciòn de los usuarios o instituciones. La asignaciòn de valor a la información se constituye como paso crucial en cualquier decisiòn que se tome en la materia de seguridad. El proceso para ello es análogo a la toma de decisiones en otros

ámbitos de la administración: con base en la eficacia y comparación de costo-beneficio se llega a una decisión.

Han existido incontables esfuerzos para formalizar el proceso de valoración de los datos. Se han utilizado esquemas de análisis basados en la Teoria de la Información --de Shannon y Weaver--, teorias para toma de decisiones, entre otras. No obstante, hasta hoy continùa siendo terreno de amplia subjetividad.

Como declara Hsiao, el proceso de evaluación de la información no solo requiere asignarle un valor --en una escala que la jerarquice entre los polos de vital o extrema confidencialidad y no vital o poco trascendente--, sino que implica la consideraciòn del hecho de que la misma información puede tener diferentes valores, según puntos de vista de diversos individuos.(1) El mismo autor menciona tres grupos de personas que dan diferente valor a la información, como ejenmplo. 1) El tenedor, es decir, la organizaciòn que tiene y usa los datos. 2) La fuente, o sea, la persona o institución que suministró la información o que es propietaria de ésta. 3) El intruso, como aquel individuo u organización que puede desear la información, pero que no tiene acceso, normalmente, a ella. A manera de ilustración, la informaciòn sobre los programas de tráfico de carga para una compañía ferrocarrilera son vitales para el tenedor, pero puede no ser objeto de interés del cliente que contrata

---

1.- V. Hsiao, David; Douglas Kerr y Stuart Madnick:"Computer security".-- San Francisco: Academic Press, 1979. P.59.

fletes o los intrusos. De la misma manera, la información que en un momento es muy importante para alguien, puede no serlo en otro momento. Por ejemplo, los datos sobre variables macroeconómicas que se anuncian en informes de gobierno, son altamente confidenciales antes de su publicación. Después no requieren protección o control alguno.

En términos generales, la evaluación de los datos está inmersa en factores dinàmicos, que requieren ser considerados al buscar mantener en vigencia todos, o ciertos, de sus atributos . La evaluación de los activos físicos de soporte, proceso y transmisión de datos y programas es màs sencilla: se puede traducir con facilidad relativa a expresiones monetarias.

Paralelo al establecimiento del valor de la información, aparece el factor de medición de amenazas o vulnerabilidades. La evaluación de éstos se fundamenta en la determinación del impacto económico, político o social de un cierto daño en la información o en activos computacionales. En otras palabras, se trata de la valoración de pérdida o costo al tenedor o fuente de los datos o,poseedor de activos físicos, de la ocurrencia de una amenaza. (2)

Practicamente cada autor que aborda cuestiones de amenazas informáticas plantea criterios particulares en la clasificación de las amenazas. Ya sean intencionales o no y

---

2.- Ver ibid. P. 60.

respondan a naturalezas diversas. (3) Los daños operativos resultan en, 1) interrupción de la operación --que puede ser igual o más dañina que la misma pérdida de información--, 2) espionajo o robo de datos --que implique lectura o copiado, para beneficio de terceros--, 3) alteraciones --o sea, cambios ilegales en la información-- o 4) destrucción ilegal y permanente de la información.

En consecuencia, la medición de amenazas incluye variables como su tipología, daño operativo derivado, además de los factores ya mencionados para la valoración de la información.

La identificación de riesgo es la determinación de grado de probabilidad de que ocurra un siniestro a cierta información, que a su vez tiene mayor o menor valor. Al instrumentar un plan racional de seguridad, se hace necesario el estudio de riesgos. Por ejemplo, en términos de seguridad física, le pérdida total de un centro de cómputo por robo, sería inmensa, en términos de valor de equipos, materiales e información grabada. No obstante, no se tiene conocimiento de un robo total de centro de cómputo y se trata de un evento poco probable. Por lo tanto al grado de amenaza se le otorga muy poca probabilidad de ocurrencia.

El objetivo de la determinación de riesgos es llegar a expresiones cuantitativas, de preferencia. Para ello existen metodologías, que se aplican, sobre todo, en instituciones de seguros, fianzas y financieras. Será valioso que cada

3.- V. Supra. Sección 5.4. .

organismo público cuente con asesoría actuarial, profesional, en este ámbito y que, con base en ella, se definan esquemas prácticos de análisis de riesgos.

El método usual consiste en establecer el valor de la pérdida informática en caso de un siniestro determinado. El valor de un riesgo equivale al valor de pérdida multiplicado por un índice o probabilidad estimada de ocurrencia. Algebraicamente, VxC, donde V es valor de pérdida y C es índice de frecuencia. Hacia el cálculo del valor de pérdida destacan algunas consideraciones. Primero, es difícil determinar el daño monetario de una amenaza, salvo el caso de activos tangibles. Segundo, los individuos suelen ser reacios a asignar valores cuantificables a amenazas con impacto social o político, por ejemplo, el caso de manipulación de informaciónes médicas o electorales. Tercero, como se mencionó antes, puede existir distinto valor para la información, según el grupo interesado. No obstante éstas consideraciones, es necesario salvar las dificultades que presentan y ubicar los daños en valores medibles, exactos, o dentro de un rango.

A continuación se establece el índice de consecuencia. Consiste, más específicamente, en la relación entre el siniestro y la frecuencia con que se presenta. Esta se calcula con base en su facilidad de ocurrencia, interés de intrusos, viabilidad técnica, etc. Este proceso también reviste dificultades. Si se trata de siniestros naturales -- inundaciones o terremotos, por ejemplo--, se puede hacer uso

de información estadística. En otros casos se tendrá que asignar valores subjetivos, a menos que se cuente con otras bases.

El aspecto de costo-efectividad de los mecanismos de seguridad o controles, es el siguiente terreno a considerar. La eliminación total de riesgo es, en términos prácticos, imposible, no obstante sus alcances y efectos son limitables. Los controles tienden a 1) decrecer el impacto de una amenaza o 2) disminuir la probabilidad de ocurrencia o frecuencia. Para ello se utilizan controles preventivos, controles detectivos, controles correctivos, así como controles maestros --con los que se ejerce la supervisión por parte de personal especializado en seguridad o auditoría informática.

Si la operación informática ya existe en la organización, se pueden identificar controles ya instalados, que de alguna manera existen. Es necesario detectarlos y considerarlos en el análisis que se efectúe para la seguridad de un sistema completo. Para conocer la trascendencia de los controles, se debe tener en cuenta, por lo menos, dos consideraciones mayores: su efectividad y su costo. La optimización de la seguridad se logra, entre otros, con la búsqueda de máxima efectividad, a menor costo, o sea, eficiencia.

En particular, una medida o recurso de seguridad es economicamente razonable cuando el monto decrecido del impacto económico excede el costo de instalación de una

cierta medida de seguridad. (4) Es decir, la aplicación de un medio de protección ejerce control sobre un riesgo determinado, al prevenir, corregir o detectar un daño y al minimizar su impacto en lo económico, social o político. Si el monto del impacto es superior al costo de la medida de seguridad, se justifica su implantación. Ese costo representa importes de adquisición, instalación, conservación, operación y evaluación. Si la base de cálculo del riesgo es anual, se debe traducir a montos anualizados los costos del medio de protección.

A esto llegan los estudios de riesgo informático. Las metodologías específicas para ello deberán ser seleccionadas y precisadas por el personal directivo informático de las instituciones, con asesoría de especialistas.

En particular, para este trabajo, se cita una metodología de análisis de riesgos para instituciones financieras, elaborada por "Banking Administration Institute", de los Estados Unidos de América. Presenta el llamado "modelo de transacciones", que da seguimiento al flujo de la información, desde su origen, hasta su destino final. Pasa por las que denomina como seis zonas de transformación. En cada una de ellas, los datos experimentan procesos. Es precisamente en los momentos de proceso donde reconoce que se presenta la vulnerabilidad.

Las zonas de transformación que presenta son las siguientes.

4.- Tomado de Hsiao, op. cit. P.65.

1) Origen (fase en la que se generan o crean los datos).

2) Entrada (ingreso al sistema automatizado).

3) Transmisión (flujo a través de canales de comunicación hacia puntos de proceso o almacenamiento).

4) Proceso (Depuración o transformación de datos, de tal manera que se genera información con atributos superiores a los de los propios datos sin procesar).

5) Almacenamiento y recuperación (grabado de datos o información en medios magnéticos y acceso a ellos para consultas o otros procesos).

6) Salida o Acción (emisión de reportes o listados e impacto de la información en la toma de decisiones).

Una consideración adicional, en materia de amenazas informáticas, es el costo de intrusión. Un intruso que toma decisiones económicamente racionales no gastará más recursos en iniciar una amenaza si el costo de ésta es mayor a los beneficios esperados de ganancia. (5) Este costo incluye experiencia, tecnología, oportunidad y costos de penalización en lo económico, personal y social --en caso de ser descubierto--, además de costos monetarios que implique la intrusión. De ese modo, es objetivo adicional de las medidas de seguridad, incrementar los costos de intrusión, que, correlativamente, reduce niveles de riesgo. Esto justifica la validez de considerar controles detectivos, que pueden ser igual o más eficaces que otros tipos de control.

5.- Hsiao es el que esboza esta consideración. No obstante la menciona superficialmente y no la considera para la elaboración de estudios de análisis de riesgos.

ANEXO 4.- CUESTIONARIO BASICO PARA EL DESARROLLO DE LA INVESTIGACION EXPLORATORIA.

ASPECTOS GENERALES.

1.- ¿ Qué se entiende por seguridad informática ?

2.- ¿ Existen normas internas para regulaciòn y control en la computación ? ¿Se asegura el buen uso, confidencialidad e integridad de la informaciòn ?

3.- ¿ Existe algùn comité o persona que vigile y haga cumplir las normas de seguridad ?

NIVEL FISICO.

4.- ¿ Cómo se planeó el sitio para ubicar el centro de cómputo ? ¿ Se consideró resguardarlo contra desastres naturales o acciones terroristas ?

5.- ¿ Cómo se planeó la localización de equipos de microcomputación ?

6.- ¿ Cómo se controla el acceso físico a sus instalaciones de informática, las visitas y la permanencia de personas ?

7.- ¿ Cómo se controla el resguardo de dispositivos magnéticos de almacenamiento de datos y su circulaciòn ?

NIVEL DE *HARDWARE*.

8.- ¿ Qué tipo de controles existen, a nivel del *hardware*, hacia el acceso a éste, a los programas y a los datos ?

9.- ¿ Con qué recursos de *hardware* se cuenta para efectos de auditoria informática ? ¿ Se utilizan éstos ?

NIVEL DE *SOFTWARE*

10.- ¿ En ésta institución se usan programas originales o genuinos ?

11.- ¿ Cómo se controla el uso de programas que procesan información institucional ?

12.- ¿ Qué formas de control se aplican para evitar que se carguen programas no autorizados en los equipos de este organismo ?

13.- ¿ Cómo es la metodología de este organismo para el diseño, desarrollo e implantación de programas ? ¿Se contempla algún aspecto de seguridad en ello ?

NIVEL DE DATOS

14.- ¿ Que recursos se tienen para la protección de los datos ?

15.- ¿ Cómo son sus procedimientos de etiquetado o identificación de archivos, cintas y discos ?

16.- ¿ Qué tipo de datos se procesan electronicamente en esta institución ? ¿ Cómo se clasifican ?

NIVEL DE TRANSMISION DE INFORMACION

17.- ¿ En la transmisión de información, o teleproceso de datos, se utiliza algún medio de seguridad ?

18.- ¿ De qué manera se controlan las operaciones de usuarios en terminales remotas ?

SEGURIDAD OPERACIONAL

19.- ¿ Existen rutinas de respaldo de información y programas ?

20.- ¿ Se tienen respaldos de documentación de sistemas ? ¿De sistemas operativos ? ¿ De programas fuente ? ¿ De archivos maestros ? ¿ De los manuales de equipos ?

21.- ¿ Cómo se controlan accesos, modificaciones, borrados y listados ?

22.- ¿ Se efectúa algún proceso de evaluación informática o de auditoria ?

23.- ¿ Qué previsiones se tienen para afrontar casos de desastres o pérdidas ?

24.- ¿ Se tiene actualizado su manual de descripción de puestos y de oranización, con base en las funciones informáticas ? ¿ Se contempla algún aspecto de seguridad en éstos manuales ?

25.- ¿ Hay procedimientos determinados para controlar la circulación de la información ?

26.- ¿ Cómo se controla el acceso a la documentación de sistemas y de seguridad ?

27.- ¿ Existe personal responsable de la informática, en cada unidad administrativa, donde se hace uso de ella ?

28.- ¿ Se tiene convenio con alguna otra institución para apoyo en caso de contingencias ? ¿ Para los sistemas operativos de ambos se ha verificado su compatibilidad ?

A NIVEL DE PERSONAL

29.- ¿ Existe algún medio de capacitación para el desarrollo de una cultura informàtica en el personal ?

30.- ¿ Se ha capacitado al personal acerca de los medios de seguridad en ejercico ?

PROPUESTAS PARA EL MEJORAMIENTO DE LA SEGURIDAD INFORMATICA.

31.- ¿ Con apóyo de qué medidas se puede mejorar la gestión de la seguridad computacional en la A.P.F. ?

32.- ¿ Cuales serían las características de una adecuada seguridad informática ?

EXPERIENCIA

33.- ¿ Qué tipo de eventos disfuncionales han tenido lugar en esta institución, con intermedio de la informática ?

34.- ¿ Qué problemàtica conoce, que haya tenido lugar, en materia de seguridad informàtica, en la A.P.F. ?