

IMPLICACIONES DE SEGURIDAD INFORMÁTICA

Julio TÉLLEZ VALDÉS

SUMARIO: I. *Introducción.* II. *Principales actividades y problemáticas en un centro informático.* 1. *Análisis y diseño de sistemas.* 2. *Programación.* 3. *Funcionamiento de sistemas.* 4. *Codificación de datos.* 5. *Captura de datos.* 6. *Operación de sistemas.* 7. *Control de documentos fuente.* 8. *Control de documentación de sistemas.* 9. *Control de inventarios de suministros informáticos.* 10. *Control de resultados.* 11. *Mantenimiento de equipo.* III. *Consideraciones finales.* IV. *Bibliografía.*

I. INTRODUCCIÓN

El servicio informático, por sus funciones y acciones sobre el conjunto de la información de toda empresa computarizada, ejerce un poder centralizador que sería vano tratar de minimizar. Hay que proteger a todo el personal y a todos los locales de la empresa; sin embargo, los cursos informáticos reclaman una atención prioritaria y muy particular.

Es indudable lo difícil y oneroso que representa el prevenir y controlar todos los riesgos. Sin embargo, y habida cuenta de las enormes pérdidas susceptibles de presentarse ante dichas problemáticas, es entonces imperioso menester estudiar, proponer y, en su caso, introducir, instalar, o modificar, todo un sistema de medidas preventivas y/o correctivas que reduzcan al mínimo toda eventual dificultad.

Estas medidas se derivan de una serie de elementos tanto de orden técnico, ético y jurídico, por lo que dicha situación reviste caracteres eminentemente transdisciplinarios, según veremos a continuación.

II. PRINCIPALES ACTIVIDADES Y PROBLEMÁTICAS EN UN CENTRO INFORMÁTICO

Hemos considerado pertinente enumerar las principales actividades así como los problemas que pueden llegar a surgir dentro de un centro informático, los cuales pueden representar enormes pérdidas económicas a los usuarios.

1. *Análisis y diseño de sistemas*

Esta es una etapa muy importante, pues depende de ella el buen funcionamiento (la mayoría de las veces) de la empresa. Si no se toman las medidas necesarias, será muy difícil que la empresa cumpla con sus objetivos. En seguida mostramos los problemas que suelen presentarse con mayor frecuencia.

A. Complejidad

Algunos analistas, si no es que la mayoría, procuran hacer de sus sistemas una obra de arte, moldeándolos de una manera tan sofisticada que es muy difícil que otras personas entiendan cuáles son los fines para los que fue creado el sistema. Por lo tanto, las consecuencias son obvias, dichos analistas se vuelven indispensables y llega a tal grado la dependencia que se tiene de ellos, que cuando no están presentes la empresa no funciona satisfactoriamente. Si la empresa no funciona como se debe, se provocan pérdidas económicas y pérdidas de tiempo.

B. Insuficiente participación de los usuarios

Es bien sabido que la gente, en muchas ocasiones, es renuente al cambio. Nos referimos con esto a la automatización de las actividades. Debido a esa renuencia dificultan la tarea del analista, piensan que si colaboran con éste, sus labores serán sustituidas por la ayuda de una computadora. Es muy cierto que la computadora es una herramienta muy valiosa, pero el hombre es también parte importante dentro de la empresa.

Algunos usuarios se niegan a participar con el analista del sistema porque desean esconder, muchas veces, actividades delictivas, y que de llevarse por medio de un sistema automatizado, ya no estarían bajo su custodia. Un ejemplo de esto es el control de almacenes ya que si hay fuga de artículos nadie se percataría de ellos, máxime si aquel que está llevando dicho control es muy posiblemente quien esté vendiendo dichos artículos, cometiendo así un doble ilícito contra los intereses de la empresa.

Ahora bien, cuando el usuario da información equivocada o escasa acerca de lo que el sistema debe hacer, lógicamente el concepto del sistema resulta erróneo y a su vez acarreará pérdida de tiempo y hasta pérdidas económicas.

C. Alteración del sistema con fines delictivos

Este problema se presenta con frecuencia sobre todo en instituciones bancarias u otras en las que se manejan grandes cantidades de dinero. En el caso de estas instituciones podrían crearse rutinas dentro del sistema, las cuales generen una cuenta ficticia en la que se pueden ir depositando todos los centavos que sobren de las cuentas existentes que se encuentran en movimiento, de tal modo que nunca aparecerá el desfalte y será muy difícil que detecten el delito (acción conocida como la "técnica del salami").

La nómina de personal es un sistema muy tentador y puede ser violado por sus hacedores, pues son los que conocen el funcionamiento de dicho sistema. Aquí el analista puede filtrar nombres de personas que no existen o que existieron en el archivo maestro y de esta manera cobrar un sueldo que no le corresponda, cometiendo así un robo a la empresa.

D. Revelación de información confidencial

En toda empresa existe información, la cual debe ser confidencial por así convenirle a la empresa. El manejo de dicha información debe llevarla a cabo personal de confianza para evitar que ésta sea divulgada, afectando así los intereses de la empresa. Sin embargo, no siempre es como se planea, ya que existe gente que debido a otros intereses personales rompe la confianza que se le ha brindado ocasionando con esto conflictos entre el personal de la empresa; muchas veces, el grado de divulgación de la información confidencial (por ejemplo, el sueldo de jefes y compañeros) provoca que el personal renuncie a su empleo, generando así pérdidas cuantiosas a la empresa.

Otro ejemplo de este problema de divulgación podría ser el siguiente: suponiendo que una empresa está preparando su presupuesto de ventas para el próximo año y sucede que el analista responsable se ve tentado a vender dicha información a la competencia y si lo hace lo único que se deja entrever en este caso es casi la ruina total de la empresa afectada debido a la ambición y abuso de confianza por parte de este analista.

Imaginemos entonces lo que pasaría si los secretos de Estado fueran violados en la transmisión de datos transfronteriza; esto sería ya de carácter político a nivel internacional.

Cada uno de los casos anteriores (según su trascendencia) serían considerados dentro de las leyes existentes.

E. Deficiencia en la elaboración del lenguaje de control para el procesamiento de la información

Para que los procesos de ejecución de los sistemas trabajen con eficiencia es necesario que los procedimientos estén bien elaborados, tomando en consideración todas las posibilidades de error que puedan existir durante el proceso, ya que de no ser así trae como consecuencias pérdida de tiempo y por lo tanto pérdidas económicas.

Este tipo de pérdidas las podemos apreciar cuando la ejecución de un proceso enlaza varios de éstos y si por ejemplo el proceso tiene un tiempo promedio de ejecución de tres horas aproximadamente, y la ejecución se detiene en cualquier etapa de ésta debido a algún error dentro de los procedimientos, habrá que dar marcha atrás para ver en qué fase de la ejecución estaba, viendo además la posibilidad de continuar a partir de donde ocurrió el problema o definitivamente reiniciar el proceso para mayor confiabilidad de la información.

2. Programación

Nos referimos aquí a la elaboración de programas para que sean ejecutados por computadora.

A. Factible alteración de programas

Es factible que los programas sean alterados con fines fraudulentos por parte de su creador; a veces esto es muy difícil de descubrir, pues algunos programadores elaboran rutinas complicadas que se pueden confundir con los objetivos reales del programa.

B. Creación artificiosa de programas

La constante creación artificiosa de programas que no cumplen con el objetivo deseado es también otro problema que se presenta con frecuencia.

Muchos programadores, ya sea por falta de experiencia, de conocimientos o por sabotaje, son los que hacen este tipo de programas que

aparentemente son de alta calidad; sin embargo, están muy lejos de cumplir el objetivo deseado.

C. Selección de personal no idóneo

Es un problema que aqueja a varias empresas, pues, la mayoría de las veces, prefieren conseguir personal "barato" y no personal altamente calificado.

Algunas empresas optan por contratar personal sin experiencia o reubican al personal ya existente con escasos conocimientos sobre informática y lo capacitan de tal manera que cumplan con los requisitos mínimos de dicha empresa. Ahora bien, cuando se hace una selección de personal errónea y no se le capacita, lo único que se origina es pérdida de tiempo y se ve afectado el bien económico.

D. Complejidad en la creación de programas aunque cumplan el objetivo deseado

En muchas ocasiones los programadores se hacen dueños absolutos de su creación (programa o sistema) y tienden a hacerse indispensables. ¿Por qué? Es la única forma de adquirir poder dentro de la empresa, ya que si el programa falla, el indicado para hacerlo funcionar muchas veces será su creador.

Esto se hace con frecuencia debido a la inseguridad que el programador siente con respecto a su trabajo, el temor de que en un momento dado lo despidan; o quizá lo haga con la mira de obtener un mejor sueldo en el momento que lo desee, bajo amenaza de desertar si es que no le pagan lo que él pide. Como se puede ver, estos tipos de problemas causan contratiempos a la empresa.

3. *Funcionamiento de sistemas*

Al terminar un sistema, así como su documentación, se procede a incorporarlo, es decir, empieza a funcionar y a producir resultados.

Muchas veces se tiene la seguridad de que los sistemas funcionarán porque han sido probados previamente; pero las pruebas realizadas se llevan a cabo con datos ficticios la mayoría de las veces. Cuando el sistema se encuentra trabajando con datos reales, es el momento en el cual se presentan las fallas que no fueron previstas en la etapa de

análisis del sistema, como por ejemplo: la compatibilidad de equipos de cómputo, en el caso de que éstos sean descentralizados. Al darle la importancia debida a este tipo de problema se provocarán grandes pérdidas de tiempo y dinero.

4. *Codificación de datos*

La actividad de codificación es la transcripción de los datos a formatos especiales para su posterior procesamiento. En esta actividad se pueden presentar situaciones tales como: escritura ilegible, la cual se detecta al momento de efectuar la captura de datos, ya que esta actividad es posterior a la codificación (documento fuente). Esta situación puede ser ocasionada por la falta de interés de las personas asignadas a desarrollar dicha actividad, así como la interpretación errónea de los datos, queriendo decir con esto que si los datos que son codificados no son entendibles, o como ya mencionamos anteriormente son ilegibles, provocarían con esto una posible alteración en la información, pérdida de tiempo y, como consecuencia, pérdidas económicas, sin descartar la posibilidad de que estas situaciones sean provocadas por así convenirle a la persona que lleva a cabo dicha actividad para beneficio propio.

5. *Captura de datos*

Para alimentar o procesar los sistemas que se llevan por computadora, es necesario tener la información en tarjetas, cintas magnéticas o *diskette*; la actividad que se lleva a cabo para obtener los datos en estos medios se le conoce con el nombre de captura de datos. Para realizar este tipo de actividad se requiere de personal bien capacitado y con un grado de responsabilidad alto, ya que si no es así, existirá alteración en la información ocasionada por error de digitación o por alteración mal intencionada de la misma. Para detectar este problema existe un proceso llamado verificación de datos, el cual debe realizarse por una persona distinta a la que realizó para la captura (la verificación es de acuerdo a la manera en que cada empresa verifique sus datos).

Por otro lado, el personal encargado de transcribir los datos a los documentos fuente (ver actividad 4) debe hacerlo con escritura legible, ya que de no ser así, puede ocasionar diversas confusiones al momento de la captura originando con esto que la captura sea muy lenta y corriendo el riesgo de que los datos pasen erróneos; en caso de no en-

contrar en ese momento a la persona que pudiera aclarar este tipo de anomalías, la información quedará alterada, y aunque el responsable esté presente, esto no deja de ser un atraso en la actividad, ya que ésta se detiene durante el tiempo en que se hacen las aclaraciones.

También el diseño de los documentos fuente (labor del analista) es otro factor importante para el buen funcionamiento de esta actividad, ya que de ésta depende la interpretación de los datos, influyendo así en la rapidez de la captura.

Es responsabilidad del área de captura la realización de respaldos de todos los datos que se cataloguen, ya que pueden existir problemas posteriores en el procesamiento de la información por los cuales se tenga que recurrir a dichos datos, y en caso de no existir estos respaldos habría la necesidad de volver a realizar el trabajo.

Los problemas expuestos anteriormente traen como consecuencia pérdida de tiempo, pérdidas económicas y en ocasiones alteración en la información.

6. *Operación de sistemas*

Existe la posibilidad de que la persona encargada de operar los sistemas cometa errores por falta de atención o en forma intencional al desarrollar sus actividades; estos errores pueden ser los siguientes:

- a) Montaje erróneo de las cintas que contienen la información a usar en el proceso.
- b) Alteración de la secuencia lógica del proceso.
- c) Caso omiso de mensajes o mala interpretación de los mismos.

Normalmente, cuando se tiene que ejecutar un proceso, se cuenta con información almacenada en medios magnéticos; en este caso pudiera estar en una o más cintas magnéticas, y cuando el operador del sistema se equivoca en la secuencia en que debe de montar las cintas para la ejecución del proceso, ocasiona que la información generada sea errónea.

Suponiendo que nos encontramos en una compañía donde se da crédito al público por la compra de un bien y el control de su estado de cuenta es emitido por medio de un sistema automatizado de crédito, se puede dar el caso de que al ejecutar el proceso para la emisión de datos de cuenta, el operador del sistema cometa el error de montar una cinta que no corresponda, las cifras que se reflejarán en el reporte del mismo serían erróneas, pudiendo ocasionar problemas de carácter legal para la compañía, ya que si a una persona se le envía su estado de

cuenta equivocado podría interponer una demanda en contra de la empresa; pero si el estado de cuenta de la persona es a su favor, existe una pérdida económica para la empresa.

Cuando se altera la secuencia lógica de la ejecución del sistema puede generar información "inconsistente", esto es, si se tiene una secuencia de cinco pasos para la ejecución del proceso y son dependientes uno del otro, es decir, que no se puede ejecutar el paso tres sin antes haber ejecutado los pasos uno y dos, se origina el problema mencionado.

Cuando se hace caso omiso de los mensajes o se hace una mala interpretación de los mismos, se pueden suscitar pérdidas económicas.

7. Control de documentos fuente

A través del documento fuente se obtienen los datos necesarios para el procesamiento de éstos.

La falta de responsabilidad de la persona encargada de efectuar el traslado de los documentos fuente, desde el usuario hacia el lugar de registro (mesa de control) donde deban capturarse, o bien si no existe un adecuado control del registro de dichos documentos, ocasionaría la pérdida o extravío de uno o más documentos, provocando con esto pérdidas de tiempo y pérdidas económicas tanto para el usuario como para la empresa, y en un momento dado a terceras personas.

Por ejemplo, si consideramos que el documento extraviado es de algún movimiento para dar de alta o dar aumento de sueldo de algún empleado de esa institución, a través del sistema de nómina y pago, el afectado en este caso sería el empleado.

Otro ejemplo podría ser el extravío de algún documento referente a alguna de las pólizas para llevar a cabo la contabilidad de la empresa; en este caso sí sería un problema muy serio para la institución.

Asimismo, si no se detecta el extravío de alguno de los documentos, la información puede ser "inconsistente". Esta falta de responsabilidad por parte del trabajador, no deja de ser un problema laboral.

8. Control de documentación de sistemas

En una estructura tan compleja como lo es un centro informático, el control de documentación es de suma importancia.

Para tener bien controlados los sistemas realizados debe existir la documentación necesaria referente a los sistemas.

Si lo anterior se lleva a cabo, evitará varios contratiempos. Algunos problemas que se presentan son:

A. Extravío de documentación

La documentación de los sistemas fluye constantemente dentro del centro informático. Cuando un sistema está en desarrollo, las carpetas de análisis (requerimientos para un programa) son enviadas al departamento de programación para que el programa sea elaborado; cuando el programa ya está listo para ejecutarse, entonces es trasladado al departamento de análisis para detallar la versión, y si en dicho departamento detectan fallas en el programa, se envían las correcciones pertinentes al departamento de programación y el ciclo mencionado vuelve a repetirse.

Debido al ir y venir de la documentación es necesario tener un control estricto de la misma, pues si llega a extraviarse acarreará grandes pérdidas de tiempo y, a la vez, pérdidas económicas.

Al momento de liberar el sistema, toda la documentación de los mismos es entregada al departamento de computación para que sean operados y se entreguen los resultados al usuario correspondiente. Si la documentación está incompleta, el sistema no se puede dar por liberado; por lo tanto, retrasará la producción (reporte del sistema) que la empresa necesita.

Otra causa del extravío de documentación puede ser (y en muchos casos lo es) que los analistas inconformes se apoderan de ella y al renunciar a sus labores se lleven dicha documentación para perjudicar a la empresa. Como se puede ver, la falta de ética profesional de estos individuos puede ser considerada, de acuerdo al agravio, en el Código Civil, en el reglamento interior de trabajo, en la Ley Federal del Trabajo y hasta en el Código Penal conforme a la magnitud del daño cometido con tal acción.

Otra razón por la cual se extravía la documentación es porque los analistas responsables del sistema deciden vender la documentación a otras empresas, obteniendo así un beneficio propio. Esto también le generará problemas a la empresa.

Pero también son responsables de estas acciones nocivas los encargados de llevar este control; por lo tanto, hay que tratar el problema basándose en las leyes y reglamentos mencionados.

B. Falta de control de documentación

Si la empresa no cuenta con un control de documentación, difícilmente llevará a buen término la elaboración de los sistemas. Se puede presentar el caso de que el sistema que se está realizando o se ha terminado ya, sea en extremo confidencial y si algún documento es extraviado, no se percaten de ello en el momento oportuno. La información confidencial de ese sistema puede llegar a divulgarse y hasta afectar la economía de la empresa. De esto no es responsable nadie más que los encargados del sistema.

C. Inexistencia de documentación

En muchas empresas donde la organización no es muy estricta en todos los departamentos y principalmente en el departamento de computación (centro informático), los sistemas se realizan sin la documentación necesaria, de tal manera que cuando los responsables no asisten a sus labores nadie puede operar dichos sistemas, pues no existen los instructivos de operación del mismo.

El planteamiento anterior es más grave cuando los responsables del sistema renuncian a la empresa; por ende, cuando se contrata nuevo personal, los sistemas tienen que empezar de nuevo acarreando con esto grandes pérdidas de tiempo y dinero a la empresa.

La falta de documentación se presenta también como el arma más apropiada que los responsables del sistema utilizan para tener a la empresa en sus manos y conseguir de ella lo que deseen, como por ejemplo, sueldos muy elevados bajo la amenaza de irse de la empresa si no se les paga lo que piden.

D. Documentación incompleta

La documentación más importante que los sistemas deben contemplar son: manual del sistema, manual del usuario y manual de operación del sistema y las carpetas de programas.

El manual del sistema debe contener los objetivos del sistema, descripción de archivos de entrada, entrada/salida y salida, así como la descripción genérica de los programas diseñados en el mismo; se debe indicar también el tipo de programas de utilería que serán usados por el sistema y los productos que se obtienen con cada programa.

El manual del usuario contendrá entre otras cosas los objetivos del sistema y los productos que se obtienen, así como los trámites (dentro del centro informático) que debe realizar para la obtención de dichos productos y la periodicidad considerada para la entrega de los mismos.

El manual de operación del sistema indicará los objetivos del sistema, el tipo de programas que utilizará (incluyendo los de utilería), el tipo de dispositivos, así como las unidades (de disco o cinta) y el requerimiento de memoria a utilizar; se mencionará también el tipo de parámetros (si es que el sistema los contempla) que utilizará el sistema, los mensajes que se enviarán por pantalla, su interpretación y la acción a realizar conforme a la misma y el tipo de archivos, así como su ubicación (tipo de dispositivos) dentro del centro informático. La periodicidad con que le serán entregados los productos al usuario deberá ser mencionada.

Si alguno de estos manuales faltara o tuviera información raquítica, provocaría confusión al área afectada, ya sea al usuario, en la operación o al mismo departamento de análisis. Lo anterior se traduciría en pérdida de tiempo y esto en pérdidas económicas.

E. Documentación desactualizada

En ocasiones los sistemas presentan cambios de acuerdo a las necesidades de los usuarios y es muy común dejar desactualizados los manuales, lo cual se presta a confusiones posteriores. Notamos, pues, que estos detalles al parecer sin importancia hacen perder a la empresa tiempo y dinero.

9. *Control de inventarios de suministros informáticos*

Cuando no se lleva un control de existencias de los suministros informáticos se pueden generar serios contratiempos. Si el control existe, pero no se lleva a cabo con oportunidad, convierte dicho control en "inconsistente".

Si se presentan los casos anteriores, la empresa se verá afectada con posibilidades de ocurrir lo siguiente: suponiendo que se está elaborando un trabajo muy importante como la nómina de los trabajadores por ejemplo, y debido a que no tenemos control sobre la existencia de papel especial para este fin, el trabajo no queda terminado a tiempo, provocando retraso en la información y, por otra parte, la inconformidad del personal, pues no recibirá su retribución oportunamente.

Lo mismo sucede con la falta de cinta entintada para impresión (u otro suministro según la impresora utilizada).

Como se puede notar, lo que parece simple puede tener consecuencias serias. Se debe considerar la preponderancia de estos problemas tomando en cuenta el tipo de empresa y el servicio que presta.

En todo caso, el no ejercer sumo cuidado en el control de inventarios de suministros informáticos puede producir pérdidas económicas y pérdidas de tiempo.

10. *Control de resultados*

Tanto el usuario como el responsable del sistema deben checar los resultados que reporten los sistemas viendo si son congruentes con lo que esperaban, ya que de no hacerlo su información podría llegar a ser "inconsistente".

Por ejemplo, se entrega el reporte del estado de pérdidas y ganancias arrojando una pérdida errónea, el responsable y el usuario directo no se toman la molestia de revisarlo previamente y lo entregan a la dirección; posteriormente, los directivos verifican los resultados y ven que no concuerdan con lo que se había obtenido en periodos anteriores y empiezan a indagar en todas las fuentes de información disponibles para detectar en dónde fue ocasionada la falla. Después de varios días de atraso se percatan de que el error fue originado por uno de los programas del sistema y como consecuencia el resultado obtenido no es real.

Si el responsable del sistema y el usuario directo hubiesen checado los resultados con anterioridad, habrían evitado tanto pérdidas de tiempo como económicas por esa falla en el sistema.

Se debe llevar también un control de las personas que reciben los resultados, porque de no hacerlo, si existe un extravío de información, no habrá manera de probar si realmente se entregaron o no, y además, si es información confidencial, ésta puede caer en manos de personas no autorizadas, las cuales divulgarían la información o la utilizarían para fines ventajosos, provocando serios problemas a la empresa.

En resumen, los problemas que se presentan son por:

a) *Inexistencia*. Deben existir controles de los resultados para evitar tanto pérdidas de tiempo como pérdidas económicas.

b) *Inconsistencia*. Se debe llevar a cabo una calendarización de los resultados.

c) *Falta de validación.* Los resultados se deben checar siempre, y por medio de sus cifras de control se pueden dar cuenta si están bien o no.

11. *Mantenimiento de equipo*

Los problemas que se presentan son:

- a) Incumplimiento del contrato de mantenimiento.
- b) Falta de vigilancia del estado físico de las cintas y discos magnéticos.

La computadora, el equipo periférico, así como los dispositivos de cintas y discos magnéticos deben ser revisados periódicamente y no sólo cuando presentan fallas, pues en este último caso se originará el hecho de mantenimiento inoportuno; cuando éste ocurre, la información es alterada.

Desde otro punto de vista, el personal de mantenimiento es responsable de cumplir la calendarización establecida por la empresa que utiliza el servicio.

III. CONSIDERACIONES FINALES

Como nos hemos podido percatar a lo largo de este trabajo, la mayoría de las actividades que se realizan ya sea dentro y/o fuera del centro informático van ligadas unas con otras, de aquí que se requiera de personal responsable y capacitado para realizar las mismas.

Sin embargo, ello no basta para prevenir y en su caso corregir aquellos problemas que se presentan a nivel de la seguridad informática, por lo que es conveniente la depuración de los dispositivos técnicos, así como la existencia de un verdadero código ético (aparejado a un reglamento interno de trabajo) junto con la aplicación de aquellos ordenamientos legales que sean conducentes (reiteramos la necesidad de una ley general de informática), como es el caso del Código Civil, el Código Penal, la Ley Federal del Trabajo y, en general, todos los preceptos jurídicos que tengan relación con el tema (incluyendo las leyes internacionales si fuera el caso).

IV. BIBLIOGRAFÍA

- BENSOUSSAN, Alain y Maurice Salvator, *Risques Informatiques: parades techniques et juridiques*, París, Editions des Parques, 1983.
- BERTRAND, André, *Contrats Informatiques*, París, Editions des Parques, 1983.

- PARKER, Donn, *Computer Crimes y Fighting Computer Crimes*, Nueva York, Edit. Scribners, 1978.
- SANDERS, Donald, *Informática: presente y futuro*, México, Mc. Graw-Hill, 1986.
- SECRETARÍA DE PROGRAMACIÓN Y PRESUPUESTO, *Informática y derecho*, México, INEGI, 1983.
- TÉLLEZ VALDÉS, Julio, *La protección jurídica de los programas de computación*, México, 1985.
- , *Derecho informático*, México, Instituto de Investigaciones Jurídicas, UNAM, 1987.
- , "Contratos informáticos", *Anuario Jurídico*, XIV, UNAM, 1988, pp. 257-274.
- VIVANT, Michel y otros, *Droit de l'Informatique*, París, Editions Lamy, 1986.