Capítulo III

RIESGOS INFORMÁTICOS

A. Generalidades

La acepción "riesgo informático" es un concepto nuevo en la terminología jurídica sin existir por tanto una definición específica.

El riesgo se refiere a la incertidumbre o probabilidad de que ocurra o se realice una eventualidad, la cual puede estar prevista; en este sentido podemos decir que el riesgo es la contingencia de un daño.

En función de lo anterior, podemos aseverar que los riesgos informáticos se refieren a la incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos como por ejemplo los equipos informáticos, periféricos, instalaciones, proyectos, programas de cómputo, archivos, información, datos confidenciales, responsabilidad civil que éstos ocasionan frente a terceros por la prestación de un servicio informático, etcétera.

En nuestro medio, los riesgos informáticos no constituyen una figura jurídica especial, aunque se pueden aplicar en su tratamiento ordenamientos tales como la Ley del Contrato de Seguro y la Ley General de Instituciones de Seguro; sin embargo, lo que motiva y justifica el señalar los riesgos informáticos como un fenómeno jurídico especial es la complejidad de los problemas que presentan en la práctica.

Por otra parte, es conveniente enunciar que la forma de apreciar un riesgo de esta índole es muy diferente al tratamiento que se les da a los riesgos comúnmente conocidos en el mercado de seguros.

De esta forma, el concepto de riesgo informático es una noción *in extenso* que se desarrolla al parejo de la tecnología, siendo objeto de estudio del llamado derecho informático bajo el rubro de los contratos informáticos.

B. Prevención de riesgos

La prevención contra los riesgos diversos tiene como finalidad la protección de las personas, equipos y trabajos vinculados con la actividad informática.

Dentro de la protección se distinguen tres niveles básicos como lo son:

- La protección amplia, la cual debe ser eficaz y concierne a los locales de procesamiento y sus anexos. En algunos casos también los locales de disposición de las informaciones de entrada y los de almacenamiento y archivo disfrutan de esta protección.
- La protección media, cuyos efectos deben ser compensadores y complementarios. Se instala en los locales de control y de disposición de resultados.
- La protección restringida, en función del grado seleccionado de vulnerabilidad. Es conveniente para los locales de gestión y también para los de análisis y programación.

Dichas protecciones, independientemente del nivel de que se traten, reclaman decisiones directivas en lo que concierne a:

- Implantación de locales y equipos.
- Selección de medios de protección, alarmas, evacuación y servicio.
- Circulación de las personas y los medios de control.
- Circulación de informaciones y control de esta circulación.
- Previsión de medios de reinicio de operaciones después de un siniestro.

La selección de los medios de protección distingue a las personas, equipos y trabajos, puesto que impone los de alarma, evacuación y servicios además de la circulación de personas, información y medios de control correspondientes.

De esta manera podemos decir que la seguridad es un todo que no se puede fraccionar y que está sometida a un reglamento general que describe entre otras cosas:

- La lista de los objetos en cuestión, su valor, su vulnerabilidad y las consecuencias de su deterioro.
- La lista de los medios de prevención, alarma, servicio y recuperación.

- Los criterios de repartición de los equipos y trabajos entre los diferentes niveles de protección.
- Las consignas generales de puesta en operación de las protecciones y acciones.
- Las pérdidas posibles de explotación y los costos correspondientes.
- Los controles de aplicación de los reglamentos.

C. Clasificación

Con base en lo anteriormente señalado podemos distinguir cuatro diferentes categorías de riesgos agrupados de la siguiente manera:

1) Respecto a los equipos
2) Respecto a los programas
3) Respecto a las personas, y
4) Respecto a los trabajos.

Hablemos de cada uno de estos grupos:

1. *Riesgos provenientes del equipo*

Dentro de este tipo de riesgos podemos mencionar los siguientes::

- Pérdida o cambio de mensajes durante el proceso de transmisión.
- Desastres e interrupciones (sean temporales o prolongadas) en la capacidad de funcionamiento del equipo o sus líneas. Éstos pueden ser causados por fuego, inundaciones, terremotos, disturbios, terrorismo, pérdida de energía eléctrica, fallas en el sistema de aire acondicionado, etcétera (sean fenómenos de la naturaleza o del hombre).
- Falta de facilidad de respaldo al equipo, líneas de comunicación y personal en el seno de la empresa.
- Fallas del equipo, las cuales pueden provocar la aparición de datos erróneos, omisiones, pérdida de información y problemas similares.

Cabe mencionar que la protección respecto a estos riesgos, se ha centrado tradicionalmente en la lucha contra dos elementos altamente nocivos para los equipos como lo son el agua y el fuego, cuyo especial control debe ser completo y muy diversificado, estribando fundamental-

mente en la instalación de sistemas de detección apropiados, medios de extinción automáticos, así como los accesorios de lucha contra los riesgos.

Así, tenemos que los sistemas de detección apropiados son los relativos al incendio, distinguiéndose los de tipo gas-humo, instalados en la sala de máquinas bajo el piso falso, en el cielo falso, al igual que en los conductos de aire acondicionado. En este sentido los sistemas de alarma son visuales y/o audibles.

Por cuanto concierne a los medios de extinción automática, se puede utilizar el CO_2, el agua o la espuma de gran expansión complementados por los medios portátiles de primera intervención cuyos materiales son de la misma naturaleza. Ahondemos brevemente sobre cada uno de estos elementos:

1. El CO_2 puede proteger al conjunto de las instalaciones de las salas de proceso y sus anexos. En razón de su toxicidad su empleo debe estar estrictamente limitado a los locales que alberguen equipos costosos que sean vulnerables al agua y a la espuma.

La emisión del CO_2 puede ser automática y estar controlada por un detector de humo o aun por un accionamiento manual. El CO_2 no daña los circuitos electrónicos, sin embargo es necesario secar por ventilación a los aparatos que fueron alcanzados por él.

2. Agua rociada por duchas *(sprinklers)*. Este procedimiento, muy utilizado en Estados Unidos, ofrece grandes ventajas como lo son el disparo automático por medio de una alarma; actúa rápidamente desde el inicio del fuego localizándolo con rapidez y con una superficie de cobertura de 10 m^2.

Dicho método es eficaz; sin embargo, requiere, entre otras cosas, de un corte instantáneo de alimentación eléctrica, una impermeabilidad perfecta de los circuitos eléctricos, así como de los pisos y cielos falsos, al igual que un sistema de drenaje para el agua.

3. La espuma de gran expansión es un procedimiento que permite obtener un metro cúbico de espuma con un litro de agua. Ciertos equipos proporcionan hasta 1000 m^3 por minuto. Dicha espuma tiene un buen poder de extinción y no penetra más que en pequeñas cantidades en el interior de las máquinas. Este procedimiento presenta el inconveniente de que la espuma es difícil de eliminar después del siniestro. Cabe agregar igualmente que el uso de extintores de agua pulverizada no son recomendables en la sala de máquinas.

En resumen, los dispositivos de lucha contra los riesgos provenientes de los equipos engloban:

- La instalación, en lugares señalados y accesibles, de interruptores eléctricos, extintores de CO_2 de 2 y 6 Kg., ventosas para levantar las duelas del piso falso, un control manual para disparar la extinción por CO_2 bajo el piso falso, una válvula de control de los *sprinklers* a fin de detener la emisión de agua al extinguirse el siniestro, aparatos autónomos de respiración (eventualmente), cestos de metal con cubierta y linternas de emergencia, así como un evacuador de humo controlado manualmente.
- La verificación periódica de la red eléctrica normal, red eléctrica de emergencia y de los extintores.
- El mantenimiento y limpieza cotidiana de los locales accesibles, y periódica en los no accesibles.

Es conveniente que las superficies cimentadas bajo el piso falso o en la sala de acondicionamiento de aire se recubran con una pintura antipolvo especial.

- La prohibición de fumar en los locales de procesamiento y en general en los locales climatizados, no utilización de productos corrosivos o solventes, así como de otros medios de calefacción que no sea de vapor o de agua; no poner papeles o cartones a lo largo de los conductos eléctricos, de calefacción, así como de los sistemas de iluminación.
- La obligación de retirar regularmente de los locales los papeles inútiles y cajas de cartón vacías; acomodar las cajas de cartón llenas, así como vaciar los cestos de basura por lo menos una vez por día.

Y por último, el respeto de las consignas de prevención y lucha contra los riesgos, de evacuación del personal, así como las alusivas a la protección y evacuación de los archivos.

2. *Riesgos provenientes de los programas*

Dentro de este tipo de riesgos podemos mencionar los siguientes:

- Fraude o desfalco mediante la afectación de los activos de la empresa (incluyendo información), por persona no autorizada y en su propio provecho, pudiendo ser un empleado en la compañía o persona ajena a la misma.

- Robo de programas, que bien podrá darse mediante el apoderamiento físico o a través del copiado ilícito de los mismos.
- Falta de posibilidad de recuperación y reinicio del proceso o comunicación de datos.
- Modificaciones no autorizadas, ya sean de carácter temporal o permanente o aun las realizadas por personal normalmente autorizado ya sea por dolo o por imprudencia.
- Alteración de secuencias. Al no contar con medios para rastrear la información en la función de proceso de datos, ésta se puede alterar o perder indebidamente, lo cual provoca, entre otras cosas, la complejidad y pérdida de tiempo al tratar de rehacer los movimientos en proceso.
- Deficiente validación de datos-programa. Esto es, que en la edición de datos, comprobación de cálculos, acciones específicas que el sistema pueda generar y cualquier otra función relacionada con la entrada o salida controlada por programa, puede no estar debidamente planteada, lo cual puede traer consigo el continuar con un proceso con base en datos erróneos.
- Falta de comprobación intermedia. Es decir, que la falta de un control debido a los diferentes pasos del proceso puede provocar el no estar en condiciones de saber si se están procesando bien o no los datos o si no se ha perdido la integridad de la información durante el ciclo de proceso.

3. *Riesgos respecto de los trabajos*

Dentro de este tipo de riesgos tenemos a los siguientes:

- Riesgos en los proyectos informáticos. Un examen estadístico al respecto pone en relieve la frecuencia de perjuicios o problemas para las empresas o clientes dada la inejecución o deficiencias en cuanto a la realización de este tipo de proyectos.
- Riesgos contra los datos. Estos son los provocados por la destrucción voluntaria o involuntaria de los soportes que contienen la información como lo son las cintas, discos, etcétera, lo cual genera la desaparición o distorsión de datos; a este respecto también tenemos la divulgación intencional o imprudencial de datos confidenciales, así como otro tipo de manifestaciones caracterizadas por su alto grado de repercusión económica.

- Robo de información, ya sea con el retiro malintencionado de datos relacionados con una persona o asunto de la empresa; estas acciones están relacionadas con el control del flujo, proceso y archivo de la información.
- Provocación accidental o intencionada de errores y omisiones durante el proceso informático, pudiendo traducirse en información incompleta o inexacta, mal funcionamiento del equipo o cualquier otra irregularidad que pueda afectar los archivos de la empresa.
- Falta de control de documentos negociables. Esto es, que el manejo indiscriminado de documentos negociables (cheques en el banco, pagarés, letras de cambio, etcétera) puede provocar su extravío o mal uso.
- Acceso indebido a los sistemas. El acceso no autorizado a los sistemas en desarrollo y en operación expone a la empresa a otra serie de riesgos tales como el fraude, robo, sabotaje, chantaje, etcétera.
- Acceso indebido a las instalaciones. Similar a lo anterior, el acceso no controlado al equipo o a las terminales representa una posibilidad muy amplia de alteración o conocimiento de información confidencial.

Cabe mencionar que la protección contra riesgos debidos a agentes físicos obligan durante la construcción de los locales de procesamiento a evitar exposiciones a las radiaciones magnéticas o electromagnéticas. Esta protección se relaciona también con las concernientes a los riesgos debidos a los agentes químicos a efecto de que se apliquen íntegramente las consignas de protección del personal y las máquinas.

Los trabajos también están expuestos a riesgos derivados de los errores en la concepción de las aplicaciones, la redacción de programas, captación de información, preparación de procesamientos, explotación de programas, funcionamiento de la biblioteca de los soportes magnéticos; edición, formato y difusión de soportes, así como la actualización y mantenimiento de la información.

Estos errores, cuyo costo de reparación puede llegar a afectar fuertemente el presupuesto del servicio informático, pueden evitarse si el proceso de gestión informática se controla firmemente durante la ejecución de los procesamientos; de esta forma, la instalación, mantenimiento y control de este proceso requiere de una total formalización.

De la distensión en la realización del proceso de gestión informática puede surgir un cierto número de riesgos debidos a posiciones de deshonestidad, venganza o idealismo. Estas actitudes son difíciles de detectar por lo que es necesario tomar las precauciones debidas desde la concepción del plan de funcionamiento del servicio informático.

La gama de ilícitos es muy extensa, englobando riesgos de todo tipo y aun sin relación aparente. Enlistarlos en forma íntegra resulta difícil; sin embargo, podemos mencionar los siguientes:

- Huelga con ocupación de los locales con los consecuentes riesgos de destrucción o alteración de las informaciones fundamentales.
- Destrucción de los soportes de información por agentes físico-químicos no detectables de inmediato como lo son limaduras de hierro, cenizas de cigarro, imanes permanentes, etcétera.
- Alteración o sustracción de informaciones.
- Espionaje industrial.
- Robo de fondos, de tiempo-máquina y de programas.
- Falta de respeto voluntario de las consignas de protección.

Los disturbios son un hecho social y la prevención contra ese riesgo radica en el reforzamiento de los medios materiales de cierre de locales, el uso de buenas cerraduras, barras de hierro en las ventanas, así como cristales triplex para las aberturas que den al exterior.

La huelga es también un riesgo social; el peligro no está en el personal informático que está plenamente consciente de sus responsabilidades sino en los elementos externos incontrolables e incontrolados, de tal suerte que la seguridad de la información debe preverse en el proceso de gestión informática.

La destrucción por agentes físico-químicos puede evitarse con la prohibición de circulación por parte de personas extrañas en los locales cuyas prioridades de protección hayan sido definidas previamente.

Los robos, alteraciones y espionaje industrial plantean el problema deontológico de las profesiones informáticas. A este respecto, algunos acuerdos interprofesionales tácitos u oficiales pueden constituir un freno eficaz.

El incumplimiento de las consignas de seguridad es también un hecho ético. Seguramente que un conjunto de sanciones y una información preventiva de motivación limitarían este riesgo.

Por último, los disturbios, huelgas y/o la destrucción de los soportes de información son irregularidades que ameritan una protección física,

mientras que las otras acciones (que se pueden calificar de morales) pueden limitarse o incluso hacerse desaparecer si se estudian a fondo los procesos de gestión informática.

4. *Riesgos respecto de las personas*

Están ligados a la protección contra los otros riesgos e incluyen simultáneamente una acción de sensibilización, formación y control.

a) La acción de sensibilización es informativa y presenta al personal los diferentes peligros a los cuales hay que enfrentarse y los medios que están a su disposición para combatirlos; por ello, todo el personal, cualquiera que sea su posición jerárquica, debe conocer perfectamente el reglamento de las consignas de seguridad.

Cada quien debe ser advertido de sus responsabilidades en materia de seguridad respecto a sus colegas, equipos y trabajos.

El personal de explotación (y en menor grado el de estudios y programación) deben tener conocimiento de los comandos manuales de alarma, condiciones de seguridad de los equipos, trabajos y programas, así como de las consignas a respetar en caso de siniestro), como lo son:

- Operación de los medios de alarma.
- Instalación de los primeros dispositivos de servicio y combate.
- Modalidades de evacuación de los locales para las personas.
- Consignas de guardia durante las horas de cierre de los locales: rondas, consignas de protección de primera urgencia (80% de los siniestros se declaran durante las horas de cierre).

b) La acción de formación implica para todo el personal la obligación de conocer el reglamento de seguridad y sujetarse a él, la selección de equipos de primera intervención, cuyos miembros tengan por misión combatir los siniestros, así como la formación de este personal en el uso de los medios de prevención y de servicio o de lucha.

Esta formación debe ser tanto teórica como práctica e incluir la disposición de las consignas de seguridad, eventualmente la constitución de un grupo de bomberos voluntarios que reciban una formación avanzada, así como la ejecución de ejercicios de alerta, operación de los medios de servicio y combate, al igual que la de ejercicios de evacuación mediante fuegos simulados.

Una mención muy especial concierne a los accidentes de las personas y/o la electrocución, para los cuales se colocan letreros, además de otros implementos.

c) La acción de control comprueba la permanencia de la sensibilización y formación asegurando un firme conocimiento de las consignas y efectuando su actualización inmediata en el caso de modificaciones debidas a mutaciones y/o transformaciones.

D. Metodología de análisis y evaluación

Una de las técnicas nuevas para definir estos riesgos y proponer medidas de prevención consiste en revisar los recursos y activos de la empresa manejados por sistemas de información con el propósito de determinar su susceptibilidad de riesgos. Como resultado de ellos, un análisis proporcionará una relación de activos, clasificados en orden a la probabilidad de que ocurra una pérdida o daño; derivado de su lectura una orientación de esfuerzos de prevención con base en el costo de los bienes o activos y a su vulnerabilidad.

Por lo que respecta a una metodología, ésta se puede desarrollar con base en los siguientes pasos:

1) Revisar las medidas de seguridad existentes, lo cual implica que también sean identificados los activos que son protegidos.

2) Determinar el valor de los activos por proteger. Esto se hará en función del costo de pérdida y reposición de los activos si éstos fueran destruidos, robados o deteriorados hasta el punto de dejarlos sin uso.

A este respecto, cabe mencionar que como regla práctica no se consideran en la evaluación destrucciones parciales.

Por otra parte, se pueden preparar cuestionarios que sirvan de base para una evaluación. En este caso la determinación final se tomará en razón de la recopilación de las respuestas a dichos cuestionarios.

3) Identificar los riesgos a que están expuestos.

4) Estimar la probabilidad de que ocurran. Este aspecto es el más subjetivo, pues depende de muchos factores para determinarla.

5) Cuantificar las pérdidas ocasionadas. Se recomienda formular una matriz de activos valuados contra riesgos probables.

6) Determinar los requerimientos de seguridad y recomendar las medidas de prevención consecuentes. Esta es la parte más importante para la empresa ya que de ella depende la reducción de riesgos.

De acuerdo con lo anterior, se estará en condiciones de elaborar un

plan valorizado de seguridad en donde se asigne a cada activo, según sus riesgos, las medidas de prevención y control adecuadas.

Ahora bien, por cuanto concierne a los métodos para evaluar los riesgos informáticos, es menester mencionar la importancia de estadísticas al respecto, las cuales son escasas en países en desarrollo como el nuestro en donde el proceso de informatización es gradual.

Lo anterior es importante puesto que al no conocerse los riesgos informáticos con exactitud, es difícil que una compañía aseguradora los acepte y pueda valorar su magnitud para fijar primas, límites y deducibles. El método que se sigue para llegar a una evaluación lo más certera posible es tomar en cuenta los casos en que haya sucedido determinado siniestro y el número de casos posibles de que esto llegue a suceder; se evalúa entonces el límite de frecuencia relativa por medio de estadísticas hacia la probabilización de algunos acontecimientos. Si se encuentran las causas es más factible determinar qué tan probable es que sucedan los siniestros y a su vez impedirlos o disminuir sus efectos.

E. Medidas preventivas

1. *En cuanto al centro de cómputo*

El asegurador tiene la obligación por sus mismos intereses de evaluar y hacer inspecciones en cuanto al riesgo informático para así decidir si lo cubre o no lo cubre; si la decisión es afirmativa, la compañía aseguradora puede exigir se cumpla estrictamente con determinadas medidas de seguridad y previsión.

Consideramos que en cuanto al equipo, algunas de estas medidas podrían ser que los locales informáticos se construyan a prueba de fuego (especialmente con muros contra fuego) equipados con extintores automáticos y con techos de material resistente tanto al calor como a grandes pesos; se deben reducir al mínimo el número de ventanas y protegerlas con muros contra fuego; por otro lado, se debe equipar con pararrayos el edificio o local donde se encuentre el centro de cómputo.

Otro requisito importante que pide el asegurador es que se construyan los techos en forma acanalada para atravesar los cables de la corriente; asimismo, se deben evitar los materiales plásticos dentro del local y emplear detectores de fuego en los locales, así como suficientes salidas de emergencia y personal ampliamente capacitado para afrontar apropiadamente este tipo de situaciones.

Para reducir los riesgos de mal funcionamiento del equipo informático se debe mantener uniforme la temperatura del local y con un constante sistema de ventilación y aire acondicionado que pase por los cables de las máquinas al igual que conductos de aspiración adecuados. La empresa debe controlar la fuente eléctrica de la planta a fin de proteger el ambiente electromagnético e interrumpir la alimentación eléctrica cuando sea necesario.

Debe haber una estrecha vigilancia en los locales informáticos previendo rondas de vigilantes, así como una adecuada instalación de alarmas y medios de supervisión.

Por otro lado, se deben proteger los locales informáticos contra fugas de agua importantes para disminuir los riesgos de inundación; por ello es conveniente pasar por debajo del suelo los conductos y tuberías que llevan el agua y tomar toda clase de medidas de seguridad contra este riesgo que puede llegar a inutilizar el centro de cómputo.

Se debe contar asimismo con extintores de alto poder y detectores de agua, ya sean lineales (bandas lineales que se deslizan a los lugares de más probable aparición de agua) como podrían ser las tuberías y los de niveles que vigilan si hay agua en un punto bajo llamados hidrómetros.

Los locales informáticos deben ser áreas restringidas con operativos de seguridad y custodios que limiten el acceso al local a fin de evitar cualquier tipo de daño o siniestro por parte de un tercero. Cuando la empresa informática es muy grande se pide que haya vigilancia automática por medio de video o televigilancia para detectar intrusiones, sabotaje o cambios de frecuencia, para lo cual se usan señales de luz infrarroja; debe haber también cerraduras con bandas de ondas.

Los aseguradores deben llevar a cabo exámenes previos del equipo y todos sus componentes certificando su buen funcionamiento y calidad.

Ahora bien, cabe destacar que lo anteriormente expuesto es deseable, pero, desgraciadamente, debido a la alta competencia existente, las compañías de seguros "toman" los riesgos sin llevar a cabo un detallado análisis, y sin exigir adecuadamente las medidas de seguridad necesarias, lo que trae como consecuencia una alta tasa de siniestros en el área informática.

2. *En cuanto a los archivos y datos informáticos*

Una vez que los programas han pasado las pruebas de validez se archivan en la computadora durante el proceso de extraer los datos para

crear el programa o cuando éste se evalúa y luego se archiva pueden ser objeto de daños de diversa índole como por ejemplo el que se modifiquen o alteren los programas, lo cual trae consigo graves problemas y perjuicios, de aquí que la compañía aseguradora deba exigir la adopción de estrictas medidas de seguridad respecto a este tipo de riesgos.

Consideramos que las medidas de seguridad más importantes aquí son el tener un control periódico del número de impulsiones de cada programa, llevando a cabo una comparación constante de códigos; asimismo, cuando hay sistemas de programas repartidos, prever el número de ellos a partir del sitio central para evitar la subderivación de programas, evitando que un mismo programador haga la entrada y salida de otro programa. Por otra parte, no se debe permitir que las terminales periféricas estén reconfiguradas como consola central debiendo trabajar dos operadores juntos cuando hay cambio de valor de parámetros en la memoria.

El desvío de datos confidenciales tiene implicaciones muy severas en el ámbito del seguro, por lo que la compañía aseguradora debe exigir que haya un estricto control de instrucciones que permitan analizar los archivos de los clientes, es decir, que tenga lugar dentro de eficaces medidas de seguridad bajo el control del sistema de operación. Se deben criptar o cifrar asimismo los elementos claves de cada programa para que no tengan acceso al mismo más que los técnicos capacitados y encargados de ello.

Se pide también que se ponga cuidado en borrar del sistema todas las "memorias" luego que se transmitió el programa al usuario. Se debe prever la protección de los parámetros conservados en la memoria luego de fallas en el sistema a fin de que no se vaya a hacer mal uso de esos datos; esta misma previsión debe tomarse en cuenta cuando se pasa un programa a otro sistema y que dan parámetros en la memoria del sistema anterior.[25]

Se debe instalar un dispositivo de alarma muy especial para cuando haya tentativas de conexión al sistema por parte de terceros. También se debe tener mucho cuidado en los sistemas de tiempo compartido de máquinas en cuanto al archivo de información por medio de claves y códigos para que no se presente el pirataje de datos. Por otro lado, se debe vigilar que un programa no invada el desarrollo de otro.

[25] A este respecto M. Greene dice que "el procedimiento que se llevará a cabo es archivar estos parámetros en bandas o discos y borrar automáticamente los residuos de información que haya en la memoria". *Riesgo y seguros*, edición controlada por la Revista Mexicana de Seguros.

En cuanto a los archivos informáticos, es importante proteger el acceso a los listados que versen sobre la configuración y procedimiento de los mismos, vigilar que los sistemas de control de acceso a los archivos sean eficaces a fin de reducir los riesgos de intrusión, sabotaje, utilización indebida de los datos y programas contenidos en disketes o bandas, así como el robo físico o de la información que contienen. Debe haber consignas de seguridad muy estrechas para las salas de archivo y registros. Por otra parte, cuando haya daños provocados por agua en los archivos, paralelo al aviso a la compañía de seguros del siniestro se debe realizar una copia de los documentos registrados en los archivos a fin de prever una oxidación de los medios magnéticos mojados.

En los Estados Unidos las compañías de seguros exigen al asegurado un estricto control del centro de cómputo en cuanto a errores, degradación de la información, pérdida de confidencialidad y fraude. Para prevenir los errores se pide un control de captura por duplicidad tomando en cuenta su fecha de captura. Existe un manual de procedimientos y tratamiento de errores para prevenir los fraudes en los programas, exigiendo un tratamiento de control sistemático estrechamente vigilado, así como la instauración de un procedimiento de acceso por código y clave y número de secuencia del mensaje; los códigos de habilitación deben guardarse en un lugar seguro.

También se debe llevar un procedimiento de criptaje antes de la transmisión, para lo cual se requiere de operadores y técnicos altamente capacitados.

El asegurador debe conocer toda la documentación, catálogos, manuales, contratos y garantías que dé el proveedor al asegurado.

En algunos países como Francia existe un controlador, quien se encarga, entre otras cosas, de evaluar los proyectos y verificar los programas, estructura e instalación de archivos y acceso a la información. Labor sumamente importante antes de que la aseguradora tome un riesgo. El objetivo de esta persona es atenuar los riesgos hasta los límites de lo accidental o de lo imprevisible y que cuando ocurra un siniestro sea él quien inspeccione y ajuste, y en caso de salvamento se encargue de ellos a nombre y cuenta de la aseguradora.

Las prevenciones de todo tipo limitan los riesgos, no los evitan; por ello es necesario instalar un plan de reinicio de actividades después de un siniestro, así como los medios de indemnización correspondientes.

El plan de reinicio de actividades debe incluir el establecimiento y actualización de una lista de centros informáticos periféricos que ocupa-

dos similarmente puedan permitir la ejecución de los procesamientos. La lista de estos centros puede completarse por el conocimiento de las adaptaciones del *software* empleado en las configuraciones de apoyo, las horas disponibles en los equipos de estos centros y la adaptación de la planeación de la empresa a esos horarios, el volumen y disposición de los locales que podrían obtenerse en préstamo, personal que podría disponerse, tarifas de renta así como de las cláusulas de los seguros.

Después de un siniestro hay que proceder al reemplazo de los equipos parcial o totalmente destruidos y a la reconstitución de las herramientas de trabajo (*software,* archivos, etcétera). El plazo de reemplazo de los equipos debe ser objeto de una cláusula específica en el contrato de compra o de renta suscrito con el proveedor. La reconstitución de las herramientas de trabajo debe permitir la construcción de los programas y los archivos de todos los niveles. Sin las debidas precauciones esta reconstrucción es difícil y por momentos imposible, por lo cual es indispensable duplicar los archivos y almacenar los duplicados en locales alejados del centro de procesamiento; sin embargo, se requieren de elementos aún más consolidados, según veremos a continuación.