EL RIESGO DE LAS ENTIDADES DE SEGUROS DESDE LA PERSPECTIVA DE LA AUDITORIA EXTERNA

JOSE LUIS DIEZ GARCÍA*

Para el auditor que analiza una empresa de seguros, el concepto de riesgo tiene varios significados que se derivan fundamentalmente del propio objetivo del trabajo a realizar, mas que de la actividad aseguradora propiamente dicha. En ese sentido, el concepto del riesgo tiene una doble vertiente:

- *Por un lado, examinar las áreas que desde el punto de vista del auditor presentan un especial riesgo en las compañías de seguros.*
- *Por otro, examinar brevemente el riesgo propio del auditor en el desarrollo de su trabajo.*

La auditoría financiera es aquélla que tiene por objeto principal emitir una opinión profesional sobre los estados financieros. Así, en la literatura profesional de los auditores suele definirse la auditoría como: «El examen de los estados financieros de una entidad realizado por profesionales cualificados e independientes, de acuerdo con normas de auditoría generalmente aceptadas, con el fin de expresar una opinión sobre la adecuación con que tales estados financieros presentan la información en ellos contenida, de acuerdo con principios y criterios contables generalmente aceptados que guardan uniformidad con los aplicados en el ejercicio anterior».

Partiendo de la base de que la auditoría externa lo que hace es «asegurar» el contenido de un balance y de una cuenta de resultados, es fácil concluir que el mayor riesgo con que se enfrenta el auditor es el de que el balance esté mal.

En otro orden de cosas, no cabe duda que la opinión del auditor independiente ayuda a establecer la credibilidad de los estados financieros. Sin embargo, es claro también que el balance refleja una acumulación de hechos históricos pero no garantiza una viabilidad futura de la entidad. Así, los auditores suelen incidir en que el usuario/lector de un informe de auditoría no debe asumir que la opinión del auditor es un seguro sobre la viabilidad futura de la entidad.

Del mismo modo, la misión del auditor no es juzgar sobre la eficacia con que la Dirección de una compañía ha gestionado los asuntos de la misma. Esta faceta sería propia de una auditoría de gestión, y no de una auditoría financiera. Lo mismo

* Socio-Director de Arthur Young, España.

sucede en lo que respecta a la detección de *fraudes* y otro tipo de irregularidades. Los procedimientos de trabajo no van orientados —por definición— a descubrir este tipo de aspectos y, sin embargo, están continuamente corriendo el riesgo de ser señalados con el dedo como auditores, por no haber identificado y denunciado una mala gestión o hechos irregulares.

El enfoque del trabajo de auditoría está orientado hacia el fin claro de reducir el riesgo de que el balance y demás estados financieros estén mal, y para ello se analizan con especial atención las áreas de mayor riesgo, entendiendo como tales aquéllas en las que existe una mayor probabilidad de que haya errores. El auditor no puede examinar todas las transacciones que han ocurrido durante un período de tiempo determinado. No sería posible. Tendría que tener un equipo tan numeroso como el propio de la compañía que contabilizó las transacciones.

Habida cuenta de la limitación de medios, el auditor habrá de obtener suficiente evidencia para concluir examinando solamente algunas transacciones y, sobre todo, apoyándose en los controles internos que tenga establecidos la gerencia de la Compañía. No sería posible trabajar de otra forma, especialmente en empresas que como las de seguros realizan un enorme número de transacciones. En la medida en que descanse en muestreos y en los controles internos del cliente, no cabe duda que el auditor asume un riesgo, pero su experiencia y buen criterio le ayudarán a determinar el grado de profundidad con que ha de realizar sus pruebas.

Si el objetivo básico de la auditoría son las cifras de la información financiera, el examinar como se construye esta información nos ayudará a conocer mejor el propio proceso de la auditoría.

Las cifras de los estados financieros provienen de la acumulación durante el año de una serie de datos procesados de una manera sistemática, periódicamente por unas aplicaciones y procesos **rutinarios.** Adicionalmente, se producen otros procesos denominados **no rutinarios** porque se realizan muy esporádicamente y que son puras **estimaciones,** o incluso decisiones con cierto grado de arbitrariedad (decisión de amortizar o no, actualizar el coste o no, etc.). Es decir, las cifras de los estados financieros se producen por acumulaciones originadas a través de tres fuentes principales:

- Procesos rutinarios.
- Procesos no rutinarios.
- Estimaciones y juicios de valor.

La gerencia de la Compañía está particularmente interesada en que haya un control férreo alrededor del proceso rutinario del día a día, y en ese sentido tendrá establecido casi con toda seguridad controles fuertes sobre dichos procesos rutinarios. Ejemplos de estos procesos serían la mayoría de las aplicaciones contables.

Las aplicaciones **no rutinarias,** como por ejemplo la determinación de las provisiones técnicas, los IBNR, o la provisión para anulación de recibos pendientes de cobro, al no realizarse tan a menudo, carecen muchas veces de controles adecuados sobre las mismas y, por tanto, en general no se puede hablar de fuertes controles internos.

Por último, las cifras que provienen de la tercera fuente, o sea, de estimaciones y/o juicios de valor, son en general decisiones tomadas a muy alto nivel en el seno de las compañías y, por consecuencia, bastante mal documentadas en cuanto al por qué de las mismas, a la vez que sujetas a decisiones políticas y, como no, con cierto grado de arbitrariedad.

Para el auditor, el riesgo de que se puedan producir errores en los estados financieros está asociado frecuentemente mucho con las estimaciones, algo con los procesos no rutinarios y muy poco con los procesos rutinarios (salvo la informática, como se indica más adelante). Normalmente, los errores que se han podido producir en los procesos más rutinarios habrán sido detectados por el propio sistema de control establecido en la compañía.

PROCESOS RUTINARIOS

Con frecuencia, el trabajo de auditoría comienza mediante un examen de los procesos rutinarios, es decir, de las principales aplicaciones contables al objeto de verificar que dichas aplicaciones cumplen y aseguran unos objetivos mínimos de control interno. Estos objetivos mínimos son los que se expresan en el Cuadro I.

Las principales aplicaciones que se revisan en una compañía de seguros son por tanto aquéllas relacionadas con:

- Emisión.
- Anulaciones.
- Cobros.
- Prestaciones.
- Pagos.

Cuadro I. Verificación por auditoría de las aplicaciones contables

1. Que todas las transacciones relativas a la aplicación son registradas, y
2. Que cada transacción registrada:
   - *a)* Es real (no existen transacciones ficticias o inexistentes).
   - *b)* Está correctamente valorada.
   - *c)* Se registra en el momento oportuno (período contable al que corresponde).
   - *d)* Está correctamente clasificada (cuenta adecuada del Libro Mayor y/o Auxiliares).
   - *e)* Está correctamente resumida (agrupada con transacciones homogéneas y bien sumarizados los totales por período).
   - *f)* Está correctamente registrada (adecuadamente traspasados los totales por período a los registros contables).

- Nóminas y comisiones.
- Reaseguro y coaseguro.

El riesgo existente en cada aplicación vendrá determinado por la posibilidad de que no se cumpla alguno de los objetivos mínimos de control interno enunciados anteriormente. La evaluación de este riesgo nos lleva necesariamente a tener que considerar aspectos operativos del propio negocio tales como:

- Definición técnica de los productos y adecuada tarificación de los mismos.
- Normas establecidas para selección de riesgos y cumplimentación de las mismas (supervisión).
- Definición adecuada de la estructura de gastos de la entidad para el correcto establecimiento de las bases técnicas.
- Vigilancia y controles establecidos sobre la aplicación adecuada de criterios contables.
- Definición del Plan de cuentas detallado aplicable por la entidad y su adecuación al Plan General de Seguros.
- Suficiencia y adecuación de los medios informáticos disponibles.
- Capacidad financiera de la entidad para asumir riesgos y política de reaseguro establecida acorde con dicha capacidad.
- Normas establecidas sobre declaración y seguimiento (control) de los siniestros.
- Normas establecidas para su valoración y posterior revisión (actualización).
- Política de inversiones acorde con la capacidad de la entidad y la necesidad de cobertura de provisiones técnicas.
- Sistemas de control y vigilancia de los saldos u operaciones de los agentes y/o delegaciones.
- Normas y controles establecidos sobre la tesorería y su rendimiento.

Todos estos aspectos definen el marco operativo de la entidad y permiten hacer una evaluación del riesgo que está asumiendo en sus operaciones, así como una identificación de las posibilidades de error (riesgo) existentes.

Las deficiencias existentes en cada uno de estos aspectos suponen la posibilidad de que la información generada por la aplicación contable a la que afecta sea errónea. Así, por ejemplo:

a) La ausencia de un adecuado sistema de tarificación supone la posibilidad de que las primas utilizadas por la entidad sean incorrectas.

b) La ausencia de una adecuada selección de riesgos o su incumplimiento supone la posibilidad de que la provisión para riesgos en curso o la provisión matemática (vida) constituidas no sean suficientes para cubrir el riesgo futuro de las pólizas.

c) La ausencia de normas sobre declaración, control y valoración de siniestros supone la posibilidad de que la provisión para prestaciones constituida sea errónea.

d) La ausencia o mal funcionamiento de un sistema de control de saldos u operaciones de agentes y/o delegaciones supone la posibilidad de errores en los saldos con agentes y/o asegurados (efectivo y recibos pendientes).

PROCESOS NO RUTINARIOS

Los procesos de información no rutinarios representan aquellos procedimientos que la entidad realiza de una forma no diaria o con relativa periodicidad. En las entidades de seguros existen algunos procesos no rutinarios que son más importantes que determinadas aplicaciones contables de las ya comentadas, tales como:

- Determinación de la provisión técnica para riesgos en curso.
- Determinación de la provisión para siniestros

pendientes incluidos los no declarados (I.B.N.R. Incurred but not reported).

- Determinación de las provisiones matemáticas (vida).
- Determinación de las provisiones técnicas relativas al reaseguro.
- Determinación de las provisiones para desviaciones en siniestralidad.
- Determinación de la provisión para anulación de recibos pendientes de cobro.
- Determinación de otras provisiones para insolvencias (coaseguradores, reaseguradores o agentes).
- Cálculo de las dotaciones a la amortización (inmovilizado material, inversiones materiales, comisiones descontadas, ...).
- Determinación de la valoración de la cartera de valores mobiliarios al cierre del ejercicio y cálculo de la provisión para depreciación de inversiones financieras, si es aplicable.
- Determinación de las deudas condicionadas (comisiones e impuestos sobre recibos pendientes de cobro).
- Cálculo de los ajustes de periodificación activos y pasivos.

El objetivo que se persigue al evaluar estos procesos es similar al ya comentado para las aplicaciones contables, por lo que el riesgo existente vendrá determinado por la posibilidad de que existan errores que puedan dar lugar a que el saldo de las cuentas afectas por estos procesos sea erróneo.

Los errores potenciales en estos procesos se encuentran en los siguientes aspectos:

a) Base de cálculo: utilización de una base de cálculo incorrecta o de una información estadística inapropiada. Por ejemplo, determinación de la provisión para anulación de recibos pendientes sobre la base de los recibos emitidos físicamente sin considerar la emisión fraccionada.

b) Factores o «inputs» para el cálculo: utilización de factores de cálculo erróneos o mal aplicados. Por ejemplo, valoración de los títulos de renta variable sin cotización en función de los balances de las sociedades de hace dos o tres años, o bien determinación de la provisión para riesgos en curso del reaseguro cedido aplicando porcentajes arbitrarios y sin correlación con los del seguro directo. También puede darse la utilización de información estadística mal elaborada para estimar evoluciones o proyectar datos, con lo que dichas estimaciones representan importes erróneos. Tal es el caso de utilizar información mal elaborada sobre evolución de recibos pendientes y anulaciones, sobre frecuencia de siniestros comunicados con posterioridad o sobre evolución de la provisión para prestaciones en función de los pagos y valoraciones posteriores.

c) Propio cálculo: errores en los cálculos aritméticos (manuales) o en las instrucciones de cálculo (mecanizado). Por ejemplo, en una instrucción del programa para sumar la provisión para prestaciones no se indica que reste los importes negativos, sino que sólo sume los positivos, o bien se indica que se sumen los importes.

LAS ESTIMACIONES Y JUICIOS DE VALOR

Este área es el de mayor riesgo desde el punto de vista del auditor.

Las estimaciones representan aquellas decisiones, selecciones o evaluaciones que la entidad toma o efectúa al preparar sus estados financieros. Tal es el caso, por ejemplo, de la selección de los criterios contables o de valoración que va a utilizar o de la determinación de revelaciones adecuadas en sus estados financieros.

Las estimaciones más representativas que se producen en las entidades de seguros son las siguientes:

- Determinación de la provisión complementaria para desviaciones en la valoración de siniestros (I.B.N.R.).
- Selección de criterios para distribuir los gastos por ramos.
- Decisión sobre activación de comisiones (vida) y política de amortización.
- Decisión sobre contabilización de las obligaciones por jubilación y determinación del criterio de cálculo.
- Decisión sobre la distribución del resultado del ejercicio.

El riesgo o errores potenciales que pueden generar estos procesos de estimaciones se encuentra tanto en el origen (toma de decisiones errónea) como en el desarrollo del proceso. El riesgo en origen

significa que los responsables de la entidad pueden tomar una decisión errónea respecto a alguna de sus estimaciones como, por ejemplo, decidir distribuir el resultado total del ejercicio, sin considerar las posibles obligaciones legales o estatutarias para constituir una provisión o una reserva.

El riesgo o la posibilidad de errores existente en el proceso estaría en alguno de los siguientes aspectos:

- Identificación de factores que se espera puedan incidir sobre el valor resultante. Por ejemplo, al determinar una provisión para desviaciones en valoraciones de siniestros habrá que determinar los factores que pueden afectarla (velocidad de liquidación, condiciones generales de inflación, cambios de reglamentación previsibles, ...) con la consiguiente posibilidad de no considerar factores relevantes.
- Desarrollo de las suposiciones con respecto a tales factores. Por ejemplo, una vez identificados los factores anteriores se desarrollan las suposiciones, tales como que la velocidad de liquidación se mantendrá como hasta ahora, o que se prevé que los cambios en la reglamentación harán que el coste de los siniestros aumente en un 10%. En estas suposiciones existirá también una probabilidad de error.
- Elaboración del cálculo basado en las suposiciones efectuadas. Por ejemplo, en la situación mencionada la entidad establecerá el valor de la provisión utilizando la suposición sobre velocidad de liquidación constante y aumento esperado del coste en un 10% y la base de expedientes que se encuentren afectados por estas suposiciones.

EL RIESGO INFORMATICO

Se ha separado este apartado como un aspecto concreto de evaluación el riesgo, debido a que a pesar de estar directamente relacionado con los aspectos anteriormente mencionados (aplicaciones contables y procesos no rutinarios) por ser la base para el desarrollo de los subsistemas y de las suposiciones, merece un tratamiento diferenciado debido a su singular importancia en el entorno general de la actividad y a su particular complejidad para el personal profano en temas informáticos.

Sin entrar a analizar el tipo de riesgo que supone la posible pérdida de información muy valiosa, el análisis del sistema informático cubre, generalmente, desde el punto de vista de la auditoría, dos bloques fundamentales como son los controles generales establecidos para el proceso electrónico de datos (PED) y los controles específicos en cada aplicación diferenciada.

Este análisis sirve para identificar aquellas áreas del tratamiento informático de los datos donde presumiblemente pueden existir errores, con el objeto de efectuar posteriormente simulaciones para verificar si tales errores se producen. Asimismo, el conocimiento del sistema informático permite la aplicación de paquetes de auditoría adaptados para obtener información y desarrollar determinados procedimientos de comprobación que manualmente sería imposible efectuar.

El enfoque de la revisión que se da en la auditoría permite identificar debilidades, pero no sirve mucho para determinar su impacto en el negocio. Para esto existen algunos servicios diferenciados como es el método SSARA (System Security and Risk Assesment) desarrollado por Arthur Young que considera la seguridad en un entorno informatizado desde la perspectiva de la Dirección y tiene en cuenta las amenazas (riesgos) a las que está sometida una empresa en términos de riesgo para su negocio. Su metodología está pues basada en la determinación de los riesgos existentes en cada área de negocio y en la búsqueda de las soluciones apropiadas para evitarlos. En el Cuadro II se exponen algunos detalles más concretos en relación con las posibilidades y objetivos de este método.

CONCLUSIONES

El mayor riesgo del auditor ante una compañía de seguros, lo mismo que ante cualquier otro tipo de compañías, reside en el hecho de que pueda opinar favorablemente sobre unos estados financieros que esten mal.

La experiencia demuestra que las áreas en las que potencialmente existen situaciones que generan errores, intencionados o no, en las compañías de seguros son las siguientes:

- Estimaciones sobre las provisiones técnicas de todo tipo:
  - Siniestros.
  - Riesgos en curso.
  - Matemáticas ...

- Cuentas con agentes o delegaciones y primas pendientes de cobro.
- Coaseguro y reaseguro (aceptado y cedido).

Si bien el trabajo de auditoría está referido a hechos ya ocurridos que determinan un resultado y una situación patrimonial, no se puede hacer abstracción de la realidad de cada compañía y, por consiguiente, se debe tener siempre presente para enfocar el trabajo y cumplir los objetivos adecuadamente, sin olvidar que los estados financieros sobre los que opina el auditor son reflejo de lo que cada compañía es. Al evaluar su operativa, se están identificando áreas de riesgo con una cierta perspectiva que puede permitir la identificación de problemas de gestión que, en cualquier caso, se pondría de manifiesto ante el cliente sugiriéndole las posibles actuaciones para su corrección.

Por otro lado, a modo de reflexión, cabe comentar que no sería demasiado aventurado que en el futuro seamos socios en este oficio que es la auditoría. Cada vez toma más fuerza la idea de que el auditor «asegura» el contenido de la información financiera que audita y que su opinión ante terceros es casi equivalente a una garantía bancaria. En este contexto, ¿por qué no presentar simplemente el balance, en vez de auditado, asegurado por una compañía de seguros?

Cuadro II. Seguridad en la informática

Las posibilidades de que se produzcan brechas en el sistema de seguridad del ordenador han aumentado considerablemente en los últimos años, paralelamente al desarrollo espectacular de la informática.

Las compañías han dejado de tener los clásicos sistemas en «batch» centralizados. Ahora cuentan con sofisticadas redes de proceso distribuido con un gran número de miniordenadores y microordenadores conectados entre sí, funcionando, bien independientemente o bien accediendo en tiempo real a los sistemas de la compañía. El control de acceso deja de ser una simple cuestión de proteger la entrada al ordenador para extenderse al control de la utilización de terminales tanto locales como remotos. Los terminales remotos, conectados vía telecomunicaciones, introducen un nuevo peligro, el acceso no autorizado de los llamados «hackers», que parecen capacitados para interferir en cualquier sistema. Ejemplos de ellos los tenemos a diario en las revistas especializadas.

Si el espionaje industrial es un tema preocupante, la demostración realizada en el programa «Tomorrow's World» de la BBC habría helado la sangre a cualquiera. El programa mostraba como las ondas producidas por las palabras que aparecen en la pantalla de un terminal, podrían ser utilizadas para reproducir dichas palabras en una pantalla de televisión situada en un vehículo aparcado en la calle, a unos cientos de metros. El equipo necesario para llevarlo a cabo cuesta aproximadamente 100 libras.

Un estudio de IBM muestra que las principales funciones de una compañía se paralizan entre 2 y 6 días después de la pérdida de su Departamento de Proceso de Datos.

A medida que el coste de los sistemas informáticos se reduce, las compañías continúan mecanizando partes importantes de su negocio y aumenta su dependencia en los resultados obtenidos por ordenador. Muchos de estos sistemas informáticos, sobre todo los utilizados por compañías de tamaño mediano, se venden llave en mano y son utilizados por personas con unos conocimientos de informática limitados. Esto ahorra dinero, pero tiene desventajas en lo que a seguridad se refiere, ya que se produce una falta de concienciación en cuanto a las medidas de control que un sistema informático requiere.

Dejando a un lado los costes y los daños que en un negocio puede ocasionar la falta de seguridad, debería recordarse que la Dirección tiene la obligación de asegurar que los libros, registros y activos de la compañía se protejan de daños, pérdidas e incorrecciones.

UN NUEVO ENFOQUE DE REVISION DE LA SEGURIDAD EN EPD

En el pasado, el enfoque de la revisión de seguridad se centraba únicamente en el Departamento de Proceso de Datos. Se identificaban las debilidades pero no se hacía mucho para determinar su impacto sobre el negocio. Ello complicaba la tarea de la Dirección en cuanto a encontrar suficientes controles compensatorios para equilibrar las variables coste-eficacia. Como resultado, muchas empresas han gastado unas veces demasiado y otras veces mucho menos de lo necesario en medidas de seguridad.

Arthur Young ha desarrollado un método de revisión, el cual contempla tanto las necesidades del negocio como los aspectos técnicos y que se orienta a la Dirección en vez de centrarse sola-

Cuadro II. *(continuación)*

mente en el Departamento Técnico de EPD. El resultado final del trabajo, que recoge la experiencia de nuestras oficinas en los Estados Unidos, Canadá y Europa, se plasma en una metodología bautizada con el nombre de SSARA (Systems Security and Risk Assessment).

SSARA considera la seguridad en un entorno informatizado desde la perspectiva de la Dirección y tiene en cuenta las amenazas a las que está sometida una empresa en términos de riesgo para el negocio. Una revisión utilizando SSARA incluye el examen de los trabajos más complejos del Departamento de Proceso de Datos, pero además, y esto es lo más importante, se centra en los sistemas críticos para el negocio, de los cuales el proceso mecanizado es solamente una parte.

Con este método se han llevado a cabo revisiones de seguridad en materia informática en un gran número de empresas de diversos tamaños y pertenecientes a diferentes sectores de la actividad económica. Por ejemplo, se han realizado revisiones utilizando la metodología SSARA en una gran cadena de almacenes de venta al público, en una compañía de transportes de viajeros de tamaño medio, en una gran compañía de ingeniería que realiza proyectos para el Sector Público, etc.

En una investigación realizada en 1981 sobre 319 empresas en Inglaterra, el 80% admitió que fueron víctimas de fraudes en un período de cinco años atrás.

PRINCIPALES RIESGOS

El objetivo de una revisión bajo la metodología SSARA es «emitir un dictamen comprensible sobre el riesgo relativo a los sistemas informáticos de una empresa, que puede derivar, directa o indirectamente, en una pérdida financiera significativa».

Comenzamos acordando con la Dirección qué sistemas son críticos para la compañía y qué riesgos concretos son importantes para la empresa. Estos riesgos, claro está, difieren de unos tipos de negocios a otros, pero se ha podido observar que las principales áreas de preocupación son:

1. Pérdidas debidas a errores.

   Por ejemplo, pueden cometerse errores en las facturas por un diseño deficiente de los programas o por no haber sido éstos suficientemente probados. ¿Detectaría este tipo de error su Departamento de Ventas, o por el contrario las facturas se ponen directamente en el correo? ¿Están actualizados los precios del fichero maestro? ¿Cómo puede estar usted seguro de ello?

2. Sustracción de bienes o de dinero interfiriendo en el sistema informático.

   ¿Cuántas personas tienen la oportunidad de interferir en los sistemas informáticos?

   ¿En qué extensión se prueban los programas? ¿Qué posibilidades tiene el personal de grabación de introducir transacciones falsas? ¿Y el personal de almacén o el jefe de contabilidad? ¿Se podría perder un terminal o una impresora?

3. Pérdidas por destrucción de los medios informáticos.

   ¿Están sus sistemas a salvo de daños por agua, fuego o sabotaje?

   ¿Qué daños podría producir alguien ajeno que irrumpiera en los sistemas de la compañía?

4. Filtración a terceros de información confidencial.

   Las fórmulas o los procesos que se hallan en la base de datos de fabricación, ¿son críticos para su negocio? ¿Qué sucedería si alguien ajeno conociese su relación de clientes o sus costes estándar o sus márgenes de beneficio? ¿Tendría importancia que la nómina del Director General fuese a parar a manos del encargado de la nómina en el almacén?

   Obviamente algunos de los hechos utilizados como ejemplos son más importantes que otros, y en todo caso el orden de importancia variará de una compañía a otra.

PROBLEMAS FRECUENTES

La utilización de la metodología SSARA ha revelado algunas áreas en las que suelen producirse problemas con cierta frecuencia.

1. Plan de contingencias.
   En muchas empresas, los objetivos que se pretenden conseguir en este área adolecen de no haber sido establecidos y documentados adecuadamente, o bien no han sido considerados en absoluto. En muchas instalaciones que cuentan con un plan de contingencias, se ha podido observar que estaba desactualizado. Areas importantes como la identificación de sistemas críticos y las acciones a tomar en las interrupciones más frecuentes han sido muchas veces ignoradas o tratadas superficialmente.
2. Insuficiente back-up de datos y programas.
   Las normas para la creación y mantenimiento de copias de seguridad, a menudo no distinguen entre datos y programas, con el resultado de que la copia de seguridad de un programa puede ser la de la semana anterior o la del año anterior, aunque dicho programa haya sido mo-

Cuadro II. *(continuación)*

dificado varias veces durante el ejercicio. Algunas empresas solamente hacen copias de seguridad cuando disponen de tiempo libre, lo que no parece muy razonable en algo tan vital. Además, a veces se obtienen copias de seguridad de la documentación de programas y procedimientos, aunque su creación haya supuesto una inversión importante para la compañía.

3. Controles de acceso inadecuados a datos y programas.
   Continúan abundando las clásicas historias de horror, tales como dejar el terminal conectado todo el día sin utilizarlo, filtraciones de «passwords», así como la no modificación periódica de las mismas. No obstante, hay un gran número de sistemas que no cuentan con protección contra accesos no autorizados.
4. Seguridad física ineficaz.
   En un gran número de empresas se prohíbe el acceso al ordenador a las personas no autorizadas, pero no se define qué empleados concretos tienen acceso al mismo. Otro problema típico es el de instalar medidas de seguridad que impresionan por su aspecto, pero que en la práctica son ineficaces. Con demasiada frecuencia una persona bien vestida y de carácter decidido puede entrar en las instalaciones del ordenador, aunque no haya obtenido previamente la autorización oportuna. Comúnmente hechos como los mencionados se mezclan con otros menos frecuentes, pero asimismo preocupantes. En una compañía, por ejemplo, los listados de programas en producción y los resultados de las pruebas con datos reales, que fueron arrojados a la papelera en el Departamento de Desarrollo, se vendían intactos al chatarrero.

ES MEJOR ASEGURARSE QUE LAMENTARSE

Como puede verse por los ejemplos antes mencionados, la seguridad en los sistemas informáticos no es una consideración teórica que solamente afecta a los demás. Casi todas las revisiones efectuadas utilizando la metodología SSARA han detectado al menos un problema importante de seguridad en las empresas examinadas.

Es importante recordar que la seguridad de los sistemas informáticos no cubre solamente las posibles catástrofes físicas o el espionaje industrial. También cubre aspectos como errores en programación, distribución inadecuada de listados de salida o incluso deficiencias en la cobertura de los seguros.

La seguridad en los sistemas informáticos no solamente se aplica a grandes empresas con grandes ordenadores. Existe una tendencia creciente entre empresas de tipo medio a mecanizar sus sistemas. Se podría decir que normalmente están corriendo mayores riesgos que las grandes empresas.

¿Está usted seguro de que cuenta con unas adecuadas medidas de protección en sus sistemas informáticos? ¿Cómo se vería afectado su negocio en caso de que alguien interfiriera en sus medidas de seguridad? Si le preocupan las respuestas a estas preguntas, debería considerar el realizar una revisión formal de la seguridad de sus sistemas informáticos. Esta revisión no sólo le proporcionará tranquilidad sino también la seguridad de que ha seguido el camino adecuado para proveerse de medidas de protección para el tipo de riesgo que usted está corriendo en concreto.

¿PODRIA PASARLE A USTED ESTO?

Una gran empresa, dedicada a la distribución y a la venta al por menor, invirtió en una sofisticada red de teleproceso para conectar terminales en puntos de venta con su sistema de distribución en doce almacenes.

La red se controlaba por un sofisticado ordenador central, y la compañía tuvo la precaución de separarlo del controlador de comunicaciones, colocando éste en una habitación al otro extremo del edificio.

Desgraciadamente, la compañía infravaloró el hecho de que esta habitación estaba situada debajo del servicio de caballeros.

Después de una noche especialmente fría, a principios de diciembre, la tubería principal que pasaba por el techo reventó. El agua cayó sobre el controlador dejándolo inservible. Como consecuencia, la compañía no pudo comunicarse con ninguno de sus terminales remotos.

En plena temporada de ventas, la compañía fue incapaz de registrar qué mercancías fueron vendidas, qué tiendas se quedaron sin stocks ni qué suministros eran necesarios. ¿Pudo sobrevivir esta compañía? Por suerte se pudo encontrar otro controlador de comunicaciones en un par de días.

La conexión y la distribución de los terminales y de la velocidad de transmisión consumió otros tres días.

Incluso así, la compañía perdió completamente las ventas de una semana. Debido a que esto ocurría en el mes de mayor venta, el efecto en sus resultados fue enorme.

Costó casi seis meses arreglar los efectos y la confusión causada por este simple incidente.