El seguro frente al fraude informático

FERNANDO VILLAR MADERUELO

TELA IBÉRICA

Las organizaciones se encuentran ante un riesgo de fraudes informáticos, problema cuyas consecuencias económicas pueden dañar gravemente el desarrollo de las actividades empresariales, por tanto es imprescindible que, por un lado, tomen todas las medidas de seguridad a su alcance para impedir, o en todo caso dificultar las acciones delictivas, y, por otro, siguiendo una buena política de gerencia de riesgos, se protejan de una posible pérdida mediante los productos aseguradores que existen en el mercado.

Introducción

Si se busca en el Diccionario de la Lengua Española el verbo «defraudar», se encuentra como uno de sus significados el siguiente: «Privar a alguien, con abuso de su confianza o con infidelidad a las obligaciones propias, de lo que le toca de derecho». Si esto se hace utilizando los equipos informáticos como herramienta para cometer el delito, estamos ante lo que se puede llamar «Fraude o delito informático».

En este tipo de definición tan generalista se pueden incluir gran variedad de acciones delictivas o fraudulentas como puede ser el tan conocido problema de las copias «piratas» que tantos perjuicios económicos producen a los fabricantes de «software» y, en cuya utilización, España tiene el desgraciado «honor» de encontrarse a la cabeza de los países europeos. No se pueden olvidar los delitos contra la integridad de la información de la empresa, que pueden producir grandes pérdidas económicas indirectas, aunque el desarrollo del artículo se refiere más concretamente a los delitos de fraude que provocan una pérdida económica directa causada por la manipulación de ordenadores o programas de ordenador.

Tomando como referencia el ejemplo concreto de un país europeo altamente desarrolla-

do en sistemas de la información, las estadísticas elaboradas por la policía criminal alemana, demuestran que este tipo de delitos en general, está aumentando en los últimos años como se aprecia en la tabla 1.

No creo que estas estadísticas sorprendan a nadie, ya que por uno u otro medio seguro que todos hemos tenido noticias de hechos como los aquí nominados, lo que puede dar una idea de la gravedad del tema. Según publica la revista World Policy Guide (1) en su número de Marzo, refiriéndose a un reciente estudio realizado por Ernst & Young (2) a altos ejecutivos de compañías, «casi la mitad de los encuestados habían sido víctimas de fraude en más de una ocasión durante un período de 18 meses, sin embargo menos de una cuarta parte tienen una política por escrito de prevención del fraude».

Es evidente que el riesgo existe, pero sobre todo es preocupante constatar que en un gran número de empresas se considera como un mal inevitable o para el que no merece la pena invertir esfuerzos para implantar un control que consiga poder evitarlos en gran medida.

Los sectores de las empresas donde existe más vulnerabilidad suelen ser compras, informática y nóminas, aunque en entidades financieras, cualquier área donde sea posible el movimiento de dinero puede ser susceptible de generación de fraudes.

La clasificación de posibles defraudadores que Labodia (3) hace en su libro «Protección de activos informáticos», que se refleja en la tabla 2, da una idea de la facilidad con que este tipo de acciones pueden darse, ya que básicamente, y dejando a un lado el factor ético-moral que afortunadamente es favorable en la mayoría de las personas, es la «oportunidad» la que condiciona en muchas ocasiones la comisión o no de un determinado hecho fraudulento.

No se debe olvidar no obstante, que para realizar un fraude informático, es preciso disponer de unos conocimientos básicos, o en la mayoría de los casos ser un experto, por lo que la clasificación presentada quedaría, en ese sentido, bastante limitada.

Siguiendo los resultados del estudio de Ernst and Young, «en siete de cada diez casos los propios empleados estaban implicados en alguna medida. Los empleados fueron los únicos autores en el 49 por ciento de los casos y estaban en convivencia con otras personas en el 22 por ciento».

«De los fraudes más graves sufridos entre enero de 1993 y julio de 1994, el 84 por ciento fueron denunciados a las autoridades por los en-

Tabla 1. Criminalidad informática. Número de casos denunciados a la policía en Alemania

Tipo de delito	1991	1992	1993
Fraude con tarjetas en cajeros automáticos	5.701	9.080	13.895
Piratería de software	1.046	572	501
Manipulación de datos y sabotaje informático	135	105	137
Falsificación de datos en comprobantes	106	118	156
Espionaje de información	61	75	103
Estafas	1.035	2.485	2.247
Total	8.084	12.435	17.042
Porcentaje de aclaración de los hechos	49,3%	45,3%	43,5%

Fuente: GDV 1995

Tabla 2. Clasificación del fraude informático

Defraudadores internos	**Elemento atacado**	**Tipo**
Trabajador manual	Mercancías Albaranes Facturas Registros	Alteración de datos físicos
Administrativos	Registros contables Listados	Manipulación de datos contables
Directivos	Registros contables generales	
Defraudadores externos	**Elemento atacado**	**Tipo**
Proveedores, clientes, representantes, etc.	Determinados bienes y documentos	Alteración de datos físicos
Resto de público	Fraudes descubiertos	
Delincuencia organizada	Extorsión a empleados	

cuestados. La razón más común dada para denunciar los fraudes era para disuadir a otros de cometer fraudes a la compañía en el futuro». Mi opinión es que el grado de denuncias varía mucho entre los diferentes países según su cultura empresarial y tradición judicial, y considero que el factor de posible pérdida de imagen, unido a la convicción muchas veces de la inutilidad de la denuncia por no poder recuperar lo defraudado, así como al coste en tiempo que conlleva el proceso de la denuncia, hacen desistir a una gran cantidad de empresas a acudir a las autoridades y por ello no pasan a engrosar las estadísticas a pesar de las pérdidas sufridas.

Las organizaciones se encuentran ante un riesgo de fraudes informáticos, problema cuyas consecuencias económicas pueden dañar gravemente el desarrollo de las actividades empresariales, por tanto es imprescindible que, por un lado, tomen todas las medidas de seguridad a su alcance para impedir, o en todo caso dificultar las acciones delictivas, y por otro, siguiendo una buena política de gerencia de riesgos, se protejan de una posible pérdida mediante los productos aseguradores que existen en el mercado.

La respuesta del seguro

Tradicionalmente han sido las entidades financieras las que han solicitado productos aseguradores destinados a paliar las pérdidas sufridas por los delitos de fraude en los que han sido utilizadas sus propias instalaciones de tratamiento de la información como herramientas para su comisión.

En la actualidad existen coberturas para cualquier tipo de entidad, financiera o no, que aseguran la restitución de las pérdidas o perjuicios económicos patrimoniales, originados por actos fraudulentos cometidos mediante la utilización de la informática.

Las coberturas de fraude informático pueden estar incluidas o ser un complemento de la póliza integral bancaria, o también puede ser una sección de una póliza de daños en equipos informáticos.

A continuación se describen los apartados más importantes que pueden incluir este tipo de pólizas.

Objeto de la cobertura

El objeto de la cobertura se define de forma general como la pérdida de valores patrimoniales, siendo normalmente cobertura estándar los valores monetarios gestionados por las instalaciones de tratamiento de la información y otorgando como coberturas opcionales las que se refieren a pérdidas de valores materiales, productos intelectuales o al perjuicio producido por la utilización no autorizada de la capacidad de cálculo de los equipos. Se aseguran los valores patrimoniales del tomador de seguro o los valores patrimoniales entregados en forma fiduciaria y de cuya pérdida tendrá que hacerse responsable.

Veamos a continuación que se entiende bajo cada uno de esos objetos asegurables.

Valores monetarios

Serán objeto de cobertura básica según las necesidades del asegurado, las siguientes modalidades:

- dinero en efectivo,
- dinero contable,
- títulos-valores,
- metales preciosos,
- piedras preciosas.

Un siniestro de esta categoría se puede producir, por ejemplo, con una modificación de facturas a pagar o con la ejecución falsa de transferencias bancarias.

El ejemplo más conocido es el de la técnica del redondeo o del «salami» que se produjo cuando un programador modificó un programa de transferencias bancarias de tal manera que los céntimos redondeados de los giros bancarios se traspasaban sistemáticamente a una cuenta especial, de la cual el programador retiró luego el dinero.

Valores materiales

Bajo este apartado se entienden las mercancías, instalaciones, materias primas, productos del tomador del seguro y bienes que se encuentran en producción con el tomador del seguro.

En este campo, los siniestros se producirán, por ejemplo, enviando estos productos a una dirección fingida o un testaferro que los venderá.

Otra posibilidad sería el sabotaje de las mercancías o productos por la producción de materias o productos incorrectos después de una modificación de datos de un sistema de diseño y fabricación automatizado asistido por ordenador CAD/CAM (Computer Aided Design/ Computer Aided Manufacturing).

También se puede predeterminar la autodestrucción de un robot industrial en caso de una modificación de los datos de operación, aunque normalmente este tipo de equipos, además de las seguridades lógicas que limitan sus movimientos, disponen de seguridades físicas, como pueden ser dispositivos de final de carrera, que evitan la ocurrencia de accidentes, por tanto, al sabotaje lógico de la programación del autómata habría que unir un sabotaje físico de anulación de seguridades.

Productos intelectuales

Esta opción irá destinada a cubrir la posible desaparición dolosa de planos, cálculos, estadísticas, listas de direcciones, programas, textos o resultados de investigaciones memorizados en un portador de datos.

No es objeto de cobertura la pérdida debida a eventos imprevisibles, que sería objeto de otro tipo de cobertura como puede ser el Seguro de Portadores de Datos, ni tampoco es objeto de cobertura, por no ser valorable, las pérdidas consecuenciales como podrían ser una pérdida de imagen o de clientes.

La pérdida de productos intelectuales ocurre, por ejemplo después de un borrado intencionado o una modificación de resultados de investigaciones o, por ejemplo, después de un borrado o modificación de la producción.

Capacidad de cálculo

Un siniestro de esta categoría afectaría a la parte del presupuesto informático que corresponde al uso no autorizado del sistema de tratamiento de la información.

Este uso no autorizado puede darse por la utilización con fines privados de los programas propios de la empresa, o por la utilización de juegos o por el aprovechamiento para el enriquecimiento personal, al margen de la empresa propietaria, de programas complejos de cálculo científico (p. ej., simulaciones técnicas o el cálculo de un boletín meteorológico).

Tras un siniestro de fraude que afecte a los objetos asegurables que se han detallado anteriormente, se suelen producir otro tipo de perjuicios para el asegurado como son:

- beneficios no obtenidos,
- pérdida de pedidos existentes,
- pérdida de la reputación o imagen,
- multas contractuales,
- gastos de prosecución legal,
- gastos por las disposiciones legales de responsabilidad profesional o de producto.

Esta clase de pérdidas quedan expresamente excluidas de este tipo de pólizas.

Hay todavía otra categoría de siniestros que no está cubierta, y es la que se refiere al espionaje de informaciones. Si un empleado vende estas informaciones a un competidor, el propietario de estas informaciones quizá sufre una pérdida en la cifra de ventas. Pero no se puede comprobar claramente si esta pérdida se debe directamente al espionaje o si tiene otras causas, como problemas organizativos o una estrategia inadecuada de venta.

Causante del daño

El segundo factor que se considera en este tipo de pólizas es el del autor del fraude, y en este sentido la cobertura básica indemniza las pérdidas producidas directamente por los propios empleados, y opcionalmente el asegurado puede cubrirse contra otro tipo de perpetradores del delito. Normalmente, por tanto, podremos encontrarnos cubiertos contra los siguientes causantes del daño:

a) Un empleado del tomador de seguro:

Es decir, una persona con la que existía un contrato de trabajo vigente en la fecha del acto delictivo y que trabaje en un lugar de producción asegurado.

No olvidemos que, como ya se ha mencionado, son los propios empleados los que perpetran más del 70 por ciento de los delitos de criminalidad informática.

b) Un servicio externo:

Es decir, una persona, representante o personal de una compañía que tiene un contrato de servicio o de obra con el tomador del seguro, por ejemplo, los empleados de un proveedor de software o un profesional libre.

c) Un tercero ajeno de la empresa:

Es decir, todas las personas no descritas bajo empleados o servicios externos.

Personas excluidas:

En todo caso quedan excluidas de estos contratos de seguro los daños causados por:

- El tomador del seguro, uno de sus representantes o una persona de su familia.
- Empleados del tomador del seguro que en el pasado cometieron hurto, estafa, fraude o un daño malintencionado.

Antes de la indemnización de un siniestro, el tomador del seguro tiene que formular la denuncia ante las autoridades competentes, aunque sea una denuncia contra persona desconocida.

El acto perjudicial

Es importante resaltar que sólo están cubiertos los actos y motivos mencionados en las pólizas.

Debemos distinguir entre:

- los motivos del causante del daño, y
- la forma del acto perjudicial, es decir, cómo ha cometido el acto de sabotaje o el fraude.

a) *Motivos del causante del daño*

Las pólizas suelen cubrir los siguientes motivos:

1. El enriquecimiento fraudulento a costa del patrimonio del tomador del seguro del propio defraudador o en favor de personas o instituciones por cuyo encargo actuó (también bajo presión)

2. El daño doloso al tomador del seguro.

b) *Tipos de acto perjudicial*

1. Borrado, modificación o entrada directa de datos en el sistema informático del tomador de seguro o en la transmisión de datos.

Las palabras «directo en el sistema informático» caracterizan la cobertura «criminalidad informática». Solamente quedan cubiertos los siniestros en los que la manipulación se efectúa directamente por medio de una unidad informática, por ejemplo, en el monitor, teclado, las unidades de disco o un aparato de registro de datos de operación.

Por el contrario, no se cubren los casos en que los comprobantes ya están falsificados en el momento de la entrada de los datos en el ordenador. Esto no constituye un acto perjudicial en el sentido de este seguro, sino un acto de infidelidad general o abuso de confianza.

2. El acto definido para la cobertura de la capacidad de cálculo es:

«El uso indebido de capacidad de cáiculo o tiempo de máquina».

3. Para la cobertura de los productos intelectuales el acto se define como:

«Daño, destrucción o hurto de portadores de datos». Con esta definición no se piensa en el espionaje de informaciones, sino en los casos de pérdida de datos debido al hurto del portador de datos.

Cuando tenemos en cuenta las definiciones anteriormente mencionadas, es evidente que la póliza no cubrirá, entre otros, los riesgos:

a) Negligencia

Por ejemplo, entrada errónea de datos por descuido o empleo equivocado de un programa.

b) Eventos accidentales, no causados por dolo.

Por ejemplo, caída de rayo, fallo de partes de la instalación, fluctuaciones de la tensión.

Otra exclusión muy importante, que no por obvia puedo dejar de mencionar, se aplica cuando el tomador del seguro ya tiene conocimiento o una sospecha concreta de la producción de un siniestro en el momento de contratar el seguro sin haberlo comunicado claramente al asegurador.

Gastos excluidos

Como ya he mencionado, hay gastos que no se incluyen en el Seguro de Criminalidad o Fraude Informático. Estos son, por ejemplo:

- daños materiales en el hardware o en los portadores de datos,
- el incremento en el costo de operación,
- gastos ocasionados por una interrupción del servicio,
- daños indirectos,
- multas contractuales,
- gastos jurídicos,
- gastos debidos a las disposiciones legales de responsabilidad profesional o de producto.

Los gastos de reconstrucción de datos se in-

demnizan solamente si con ellos se puede minimizar el daño de productos intelectuales.

Delimitaciones temporales de la cobertura

Hay tres condiciones temporales que tienen una influencia sobre la cobertura:

a) *La fecha del acto perjudicial*

El acto perjudicial se tiene que haber producido durante la vigencia del contrato de seguro.

Una cadena de actos perjudiciales que tienen una relación común, se considera como un solo siniestro, si bien como criterio para la indemnización se considera que habrá cobertura si el primero de esos actos encadenados se produjo dentro de la vigencia del contrato del seguro.

b) *El aviso del siniestro al asegurador*

No existe cobertura de seguro para siniestros que se avisen al asegurador después de haber transcurrido un período predeterminado en las pólizas tras la producción del primer acto perjudicial.

Esto es aplicable también a los siniestros que se descubren después de ese período preestablecido tras el primer acto perjudicial.

Lo importante es que esta condición se aplica también cuando la póliza está todavía vigente.

Como comentario a esta limitación convendría indicar que habrá que contar con la jurisprudencia de cada país en este tipo de situaciones.

c) *Garantía del asegurador después de la vigencia del contrato*

La garantía del asegurador puede prorrogarse unos meses después de la vigencia del contrato –independientemente de las causas para su cancelación– terminando la cobertura tras ese plazo posterior a la fecha de cancelación de la póliza. Para los siniestros avisados al asegurador después de este plazo ya no existe cobertura de seguro.

Determinación de la suma del siniestro

En caso de daños materiales es bastante fácil calcular la suma del siniestro, pero en la categoría de los siniestros en valores patrimoniales hay que definir claramente cómo se fija la cuantía de un siniestro.

Valores monetarios

Los valores monetarios se fijan en base al tipo de cambio del día de la producción del siniestro que causó la pérdida. El valor de cualquier título o divisa o lingote o metal precioso por cuya pérdida se interpone una reclamación, se determinará de acuerdo con su precio al cerrar el mercado o valor en la fecha en que se descubrió la pérdida.

Valores materiales

En instalaciones, mercancías y materias primas se toma el valor registrado en la contabilidad o bien el valor no amortizado según las leyes fiscales.

En mercancías producidas por el tomador del seguro o en estado de producción, se toma el precio de compra de la materia prima empleada más los gastos de producción correspondientes hasta la fecha de ocurrencia del siniestro.

Productos intelectuales

Aquí, se suelen indemnizar los gastos de reproducción de los productos intelectuales, hasta un determinado porcentaje de los gastos originales de desarrollo comprobados, gastos directos de material, tiempo de máquina y laboral, pero no los gastos generales.

El desarrollo nuevo de un proyecto que fue destruido por un acto perjudicial no requiere

tanto tiempo como el desarrollo original. Por eso, la indemnización no es el cien por cien de los gastos del desarrollo original.

En caso de que los productos intelectuales hubieran sido comprobados a terceros, se suele indemnizar como máximo el precio original de compra.

Capacidad de cálculo

Se indemnizará como máximo el número de minutos del uso no autorizado multiplicado por el «presupuesto informático por minuto job». Esta cifra corresponde al importe de los gastos informáticos por minuto de operación del ordenador.

Para finalizar me gustaría comentar que existen otro tipo de delitos informáticos como puede ser la destrucción de la información de forma dolosa, que no causa una pérdida directa pero que requiere de una aportación por parte del afectado para devolver sus sistemas al estado original, antes del acto doloso. Son siniestros que se separan de la definición de fraude informático para acercarse a los delitos de sabotaje. Se debe destacar que también en estos casos, el sector asegurador dispone de productos específicos que asumen los costes de reposición de la información perdida tras un evento como el mencionado.

Conclusiones

Los desarrollos tecnológicos plantean siempre un reto para los aseguradores por la aparición de riesgos que anteriormente no se consideraban. Particularmente el desarrollo de la informática ha obligado a evolucionar al ramo que hace años se llamaba de Corriente Débil, y que actualmente se conoce como de Equipos Electrónicos. En este sentido, las pólizas actuales incorporan coberturas que posibilitan al asegurado recuperar sus pérdidas en caso de ser afectado por los delitos que se han descrito.

Para la contratación de este tipo de seguros se requiere un gran conocimiento de la empresa a asegurar, su organización y concienciación tanto en seguridad física como sobre todo en la seguridad lógica de sus instalaciones informáticas. Cada vez existe más conciencia de los riesgos asociados a la informática por parte de los directivos de las empresas bien asesorados por gerentes de riesgos, y es por ello que ya no sólo las entidades financieras, con sus coberturas asociadas a la póliza integral bancaria, son las que se preocupan de contratar un seguro apropiado, cualquier empresa es vulnerable a estos peligros por lo que este tipo de productos aseguradores está desarrollándose positivamente. ■

Bibliografía

(1) *Seguro de Infidelidad y Fraude Informático.* Newsletters-Seguros-World Policy Guide nº 10. Editorial Recoletos.

(2) *Fraude - El riesgo no gestionado.* Informe publicado por el Grupo de Investigación de Fraude y Gestión de Riesgos de Ernst & Young.

(3) Labodia Bonastre, José Antonio: *Protección de activos informáticos.* Editorial MAPFRE S. A. Madrid, 1994.