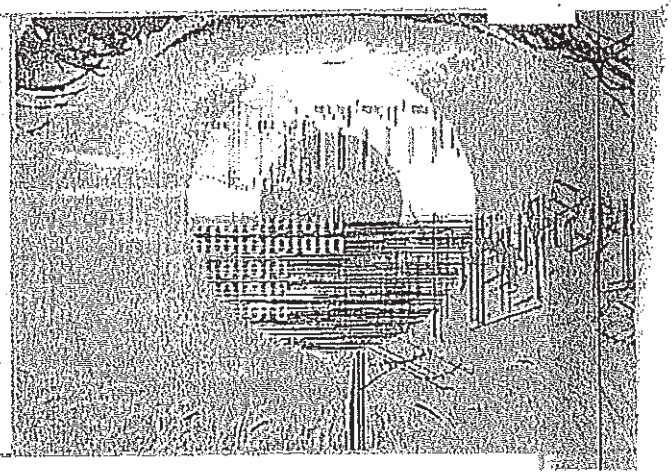
TOMO 5



DECISIONES ESTRATÉGICAS EN SISTEMAS DE INFORMACIÓN (Parte II)

CAPÍTULO 13

MANAGEMENT RESPONSABLE DE IS

Management responsable de IS

En este último capítulo, nos centraremos en cuestiones que se relacionan con el management de los IS de un modo "seguro". Cuando nos referimos a los IS seguros, hablamos de:

- "seguros" desde un punto de vista organizacional
- "seguros" desde un punto de vista social, es decir, ético
- "seguros" desde un punto de vista judicial, es decir, legal

Estos tres puntos –el ético, el legal y el que hace a la seguridad– se superponen. Es frecuente que existan obligaciones legales y morales en relación con la seguridad de la información y su almacenamiento, procesamiento y recuperación. El marco legislativo actual de los IS codifica una perspectiva social de lo que es correcto, es decir, de la ética. Mantener la seguridad de los IS puede plantear dilemas legales y éticos. Éstos son sólo algunos ejemplos de las complejas interrelaciones. Cada una de estas tres áreas constituye el ámbito de profesiones enteras, y cubrirlas en detalle excede el propósito de estas páginas. En el presente capítulo, sin embargo, realizaremos un bosquejo de los principales aspectos de management relacionados con cada área.

13.1 ◦ Manejo de la seguridad de los IS

Este aspecto se refiere a la visualización y el management de los riesgos en términos de las causas, los efectos y, por lo tanto, los costos que implica una pérdida de seguridad. Ésta puede definirse como:

La falla de los elementos de un sistema de información computarizado para realizar la función o brindar el o los servicios para los cuales estaba destinado.

Dicha falla puede referirse a la pérdida de uno de los siguientes aspectos (o de todos):

- Disponibilidad
- Integridad
- Confiabilidad = Confidencialidad

De esta definición se desprende la noción de que las organizaciones necesitan administrar el riesgo de exposición de cada uno de los elementos de los IS. Este management deberá considerar el equilibrio entre los costos resultantes de una falla en la seguridad y los costos resultantes de las medidas necesarias para aumentar la seguridad (ver **Figura 13.1**). El punto central de la presente sección es identificar el equilibrio óptimo. Cualquier cambio en la importancia relativa de los elementos del portfolio de IS o del entorno empresarial u operacional requerirá un revisión del enfoque de management del riesgo, ya que las consecuencias modificarán el punto de equilibrio óptimo.

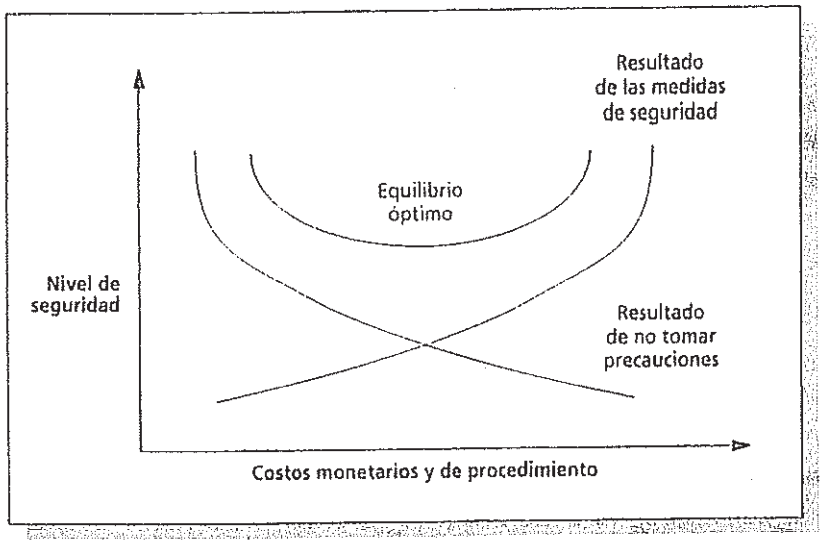


Figura 13.1. El equilibrio de los costos de seguridad.

Se ha vuelto imposible, y en gran medida irrelevante, cuestionarse si la mayoría de las empresas puede seguir existiendo después de una importante pérdida de seguridad; se trata simplemente de evaluar en cuánto tiempo dejarán de funcionar. Davis y Olson (1985) muestran cálculos de tiempos de supervivencia, ilustrados en la **Figura 13.2.**

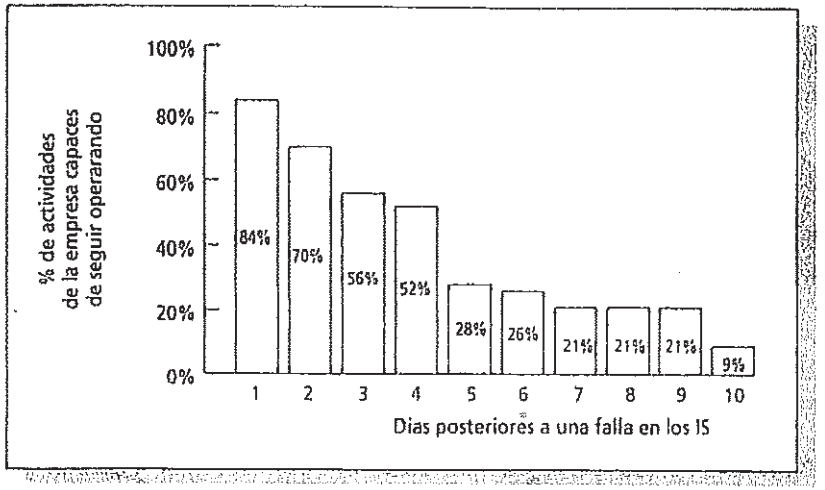


Figura 13.2. Supervivencia de una empresa después de un problema de seguridad (Davis y Olson, Management Information Systems, *1985. Adaptado con autorización de McGraw Hill).*

El costo de tener seguridad queda relativamente claro de antemano, mientras que el costo de no tener seguridad puede ser difícil de definir, aun cuando las fallas ocurran. El management del riesgo intenta reducir estas pérdidas. Un enfoque sistemático del management del riesgo permitirá que los IS de seguridad sean administrados de tal forma que reconozcan la vulnerabilidad y la sensibilidad de los sistemas de la empresa, y los datos que éstos contienen, pero también los costos, en términos sociales, financieros y técnicos, de los controles y las medidas para el manejo del riego. Ningún sistema puede ser completamente seguro. El management sistemático permite elegir e implementar

las contra medidas de una forma planeada y administrada, y no sobre una base *ad hoc*. Muchas de las metodologías del management de la seguridad utilizan básicamente un análisis *cualitativo*, aunque metodologías más formales intentan usar un análisis *cuantitativo* cuando es posible.

Existen varias metodologías de management del riesgo. Probablemente la más utilizada sea la Metodología de análisis y management del riesgo (CRAMM), producida por la CCTA y aprobada por el gobierno. Esta metodología sigue un patrón sistemático de identificación y análisis del riesgo, y una posterior enumeración de las contra medidas recomendadas. A fin de automatizar el proceso de management, esta metodología cuenta con un excelente software. Para obtener datos sobre los activos de IS y sobre las potenciales amenazas, se utilizan cuestionarios, y el software de CRAMM formula recomendaciones sobre el manejo del riesgo. A pesar de que este amplio enfoque goza de gran popularidad, tiene la desventaja de consumir demasiado tiempo. RiskPAC es un paquete norteamericano de management del riesgo basado en PC, MARION es su equivalente francés, y el Análisis de riesgo estructurado (SRA) es la metodología del Reino Unido. Todos estos métodos usan enfoques que son en gran medida similares a aquellos utilizados por CRAMM, y todos realizan un modelo de amenazas y consecuencias a fin de calcular la gravedad del riesgo y, por lo tanto, equilibrarlos con el costo de cualquier contra medida potencial.

Cualquiera sea la metodología que se siga, el management de la seguridad de los IS se reduce a cuatro etapas:

1. *Identificación del riesgo*: durante esta etapa, la organización busca identificar todos los riesgos a los que está potencialmente expuesta.

2. *Análisis del riesgo*: aquí la organización debe cuantificar la probabilidad y la frecuencia esperada de ocurrencia de cada riesgo identificado, y también evaluar la probable gravedad de las consecuencias.

3. *Manejo del riesgo*: una vez identificado y analizado el patrón de exposición al riesgo, la organización prosigue con la selección de controles y contra medidas a fin de alcanzar la posición de seguridad óptima.

4. *Recuperación del desastre*: ya que ningún proceso de management de seguridad puede ser absoluto, debería existir paralelamente a las otras tres etapas un planeamiento de contingencia para la recuperación después de un desastre. El plan de recuperación se controla, revisa y pone a prueba en forma continua.

13.1.1 • Identificación del riesgo

El primer paso en el management sistemático de seguridad es identificar "todos" los riesgos a los que es vulnerable un sistema particular, un conjunto de sistemas, una función o una empresa. Para realizar esta tarea, se necesitan dos cosas: un conocimiento bastante detallado del trabajo de la organización, más un reconocimiento de las áreas que tienden a la vulnerabilidad. Esta segunda parte, es decir la comprensión del riesgo probable, puede llevarse a cabo a través de consultores externos, pero la identificación de las amenazas específicas se realiza probablemente mejor mediante el personal o los consultores internos. Los consultores externos ofrecen un amplio conocimiento, mientras que el personal interno ofrece una profunda comprensión de la empresa. Pero ambas instancias hacen surgir la siguiente pregunta: ¿quién vigila a los que vigilan?

Una identificación completa del riesgo requiere, por lo general, reuniones iniciales para desarrollar ideas, y subsiguientes clasificaciones que conduzcan a un análisis sistemático de los riesgos. Se trata de encontrar los puntos débiles, un proceso organizado de identificación de:

- Fuentes de amenazas potenciales
- Activos que son vulnerables a la pérdida
- Ubicación de esos riesgos

Las listas de categorías del riesgo tratan de asegurar que, durante la etapa de exploración, las amenazas potenciales no se pasen por alto. La **Figura 13.3** ilustra una matriz útil de toma de conciencia, en la que los ejes nos recuerdan que existen categorías de *tipos* de amenazas, físicas y lógicas, deliberadas y accidentales.

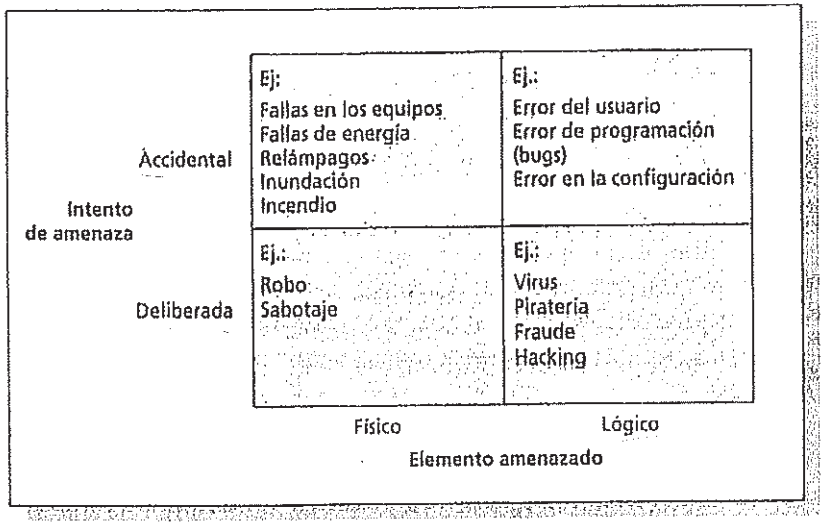


Figura 13.3. Lista de identificación de amenazas.

Las organizaciones deben reconocer que no todas las amenazas son el resultado de un abuso humano, deliberado, de los elementos físicos de los IS. Los riesgos accidentales incluyen factores como las inundaciones, los incendios y el daño producido por el humo, errores humanos que dañan los datos y los colapsos (*crashes*) del sistema. El abuso deliberado abarca robo, fraude, daño malicioso o acción industrial. En esta categoría, aquello que es menos común tiende a ser lo de consecuencias más notorias y, por lo tanto, lo que más atrae la atención. Así, mientras que los hackers y los fraudes bancarios son relativamente raros, se habla de ellos con mucha frecuencia. Los virus tienen un perfil alto, pero pueden causar

poco daño físico; su principal impacto recae sobre la confianza en los IS. La **Figura 13.4** muestra la importancia relativa de algunos de estos tipos de amenazas, según el informe de Lambeth (1996).

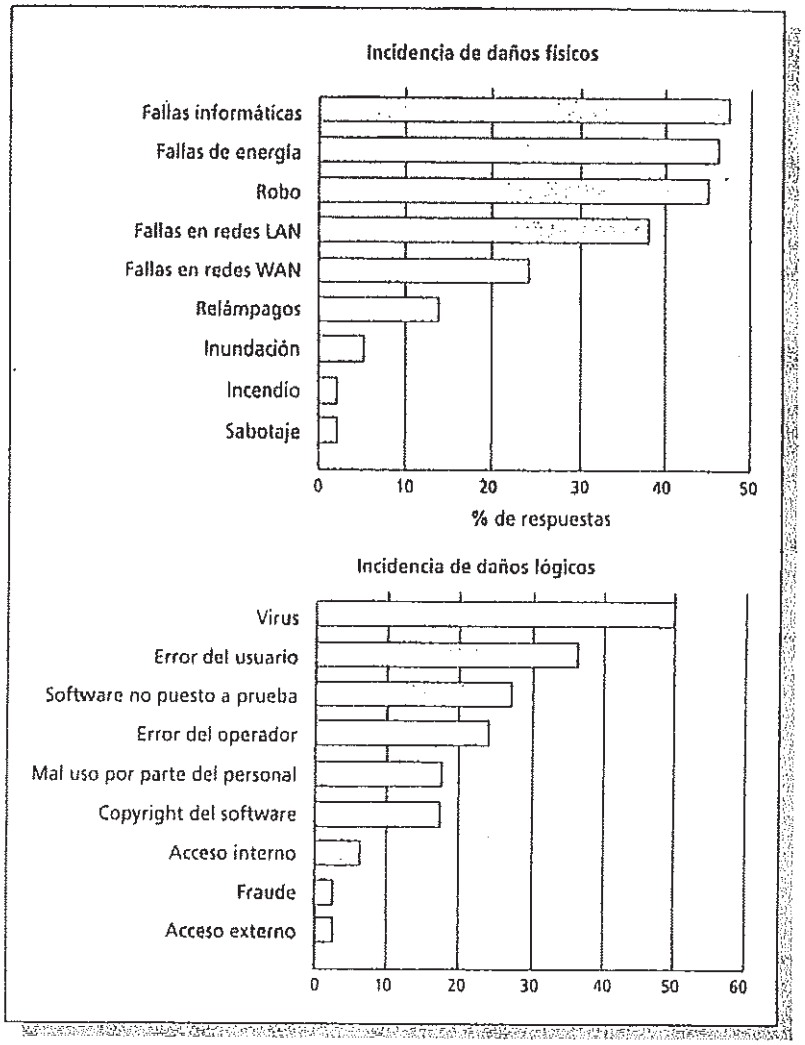


Figura 13.4. Importancia relativa de las amenazas de seguridad a los IS (basada en la información del National Computing Centre, 1996. Adaptada con autorización de Computer Weekly*).*

El robo ha sido siempre un gran problema en organizaciones importantes; esto se debe a que localizar datos, software y equipo es complicado por las dimensiones de la empresa. Una sociedad con más conocimientos de los IS hace más vendibles los datos, el software y los equipos, y por lo tanto, más fáciles de robar; los sistemas electrónicos de transferencia de fondos hacen que el dinero sea más accesible y, por lo tanto, más vulnerable.

Un método alternativo de identificación del riesgo es considerar las amenazas sistemáticamente a través de la vulnerabilidad de:

- Activos específicos
- Riesgo genérico

Cuando se evalúan los riesgos, un activo específico debe exponerse a ítems como redes de comunicación, datos y medios de almacenamiento, hardware y software, documentación y aptitudes de los empleados. La pregunta que se plantea es:

¿Qué le puede pasar a este activo en particular?

Por ejemplo, la vulnerabilidad de las redes –de acuerdo con Satya, 1988– puede incluir:

- Radiación que destruye las transmisiones de datos, en forma deliberada o accidental.
- Cruce de conversaciones que producen canales de comunicación ruidosos.
- Fallas en el hardware del emisor, del receptor o en algún elemento del circuito de comunicación. Las fallas en el hardware a menudo producen fallas en el software.
- Fallas del software en cualquier elemento de iniciación, control o recepción del mensaje. Como el software mantiene los controles de acceso, cualquier falla produce una importante pérdida de seguridad.

Las amenazas no se dirigen sólo a los elementos de "alta tecnología" de los IS. Por ejemplo, las máquinas de fax y otros elementos automáticos menos sofisticados están sujetos a toda clase de riesgos. Preocupado por esos bienes, el gobierno de Malasia implementó reglas estrictas de acceso a las máquinas de fax (menos seguras que la tradicional comunicación por correo), por miedo a que el uso indiscriminado produjera una filtración de datos confidenciales.

Además de concentrarse sobre activos específicos, la amenaza genérica puede ser el foco donde ciertos peligros, como los desastres naturales, el entorno físico, el robo o el sabotaje externo o interno, son objeto de una pregunta diferente:

¿Cómo somos vulnerables a este tipo de riesgo?

Por ejemplo, una categoría muy evaluada es el entorno físico de los IS; podríamos enumerar las amenazas potenciales de la provisión de energía, el aire acondicionado, las vibraciones o el acceso a los mismos sistemas de protección. Dichas amenazas también pueden abarcar niveles reducidos de energía, daños causados por el agua de los sistemas de suministro al personal, o por el calor y el polvo, debido a la inadecuada ubicación de las máquinas.

Los incendios son una amenaza siempre presente, no sólo con respecto a los IS, sino también respecto de muchas operaciones empresariales, y resulta esencial mantener este riesgo a niveles mínimos, ya que es factible que cada instancia de incendio produzca daños importantes, en especial físicos, en los IS. Si el daño no se produce por el fuego mismo, entonces puede provocarse por el humo y las emanaciones. Daños todavía mayores son causados por el agua y las sustancias químicas utilizadas para controlar el fuego. Por ejemplo, en Estados Unidos, un incendio mediano en una casilla pública de telecomunicaciones produjo una pérdida de hasta tres semanas en la conexión de datos. Esta experiencia hizo que muchas organizaciones construyeran redes que podían controlarse a través de intercambios centrales alternativos. De hecho, es probable

que –como informa Lambeth, 1996– recuperarse del daño causado por un incendio lleve más de una semana, mientras que la recuperación después de una falla de energía demora, por lo general, menos de una semana. La **Figura 13.5** ilustra los tiempos de recuperación según el tipo de amenaza.

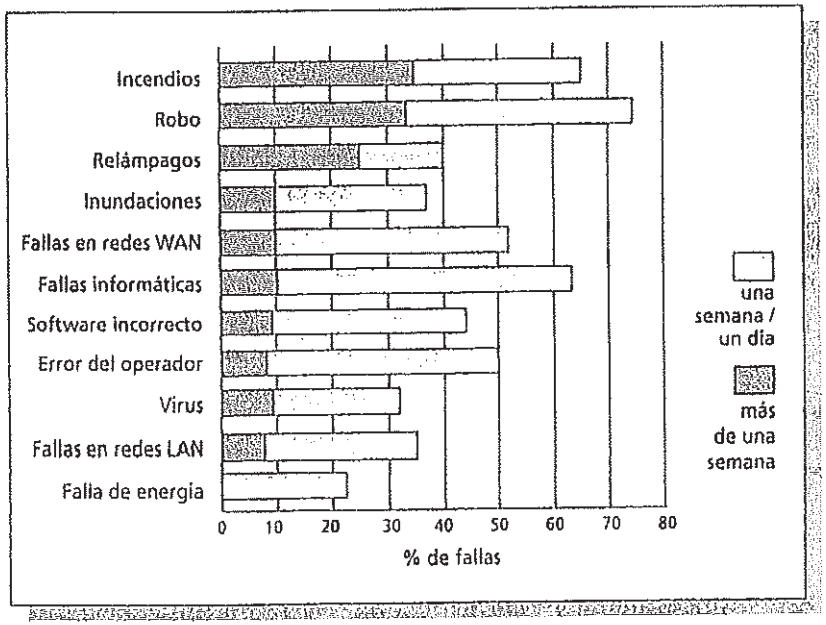


Figura 13.5. Tiempo de recuperación según el tipo de amenaza (basada en la información del National Computing Centre, 1996. Adaptada con autorización de Computer Weekly*).*

Los incendios constituyen una amenaza significativa para los IS por las siguientes razones:

- Es frecuente que las computadoras estén rodeadas de material inflamable, como papel y cajas de cartón.
- El fuego en los equipos de computación es difícil de extinguir porque hace que los componentes del hardware, las cintas magnéticas y la instalación de cables produzcan toxinas que obligan al personal a retirarse del lugar.
- Debido a razones de control de acceso, la mayoría de las oficinas donde se hallan las computadoras tienen una o, como máximo, dos salidas, lo cual constituye un peligro serio para el personal.
- Los sistemas para combatir el fuego pueden causar daños secundarios, como inundaciones, o pueden representar un peligro para el personal si se utilizan productos químicos.
- El fuego puede provocar la destrucción total de archivos de datos, programas y documentación. Las pérdidas que se originan son inconmensurables.
- Aunque las computadoras de escritorio no requieren aire acondicionado, muchas lugares de procesamiento sí lo necesitan. Los conductos de aire acondicionado pueden propagar el fuego, el calor y el humo de oficina en oficina, aunque éstas sean resistentes al fuego.
- A menudo, las áreas de computación tienen rejillas en el techo o en el suelo, en las que el fuego puede desarrollarse y propagarse. Las más peligrosas son aquéllas hechas de material inflamable, y las que no detienen el fuego y permiten que se extienda por las paredes.
- El interruptor del equipo de computación relacionado con la provisión de energía es una fuente perpetua de riesgo. Cuando los cables de plástico se encienden, aunque se queman lentamente, producen la liberación de compuestos tóxicos.

Muchas amenazas potenciales provienen de algún punto débil en una o en todas de las siguientes áreas:

- fabricación
- mantenimiento
- diseño
- capacitación del usuario
- procedimientos de operación

Una falla los mecanismos de seguridad proveniente de algún punto débil significa que, si se elimina ese punto débil, la amenaza puede reducirse. Un método de identificación de amenazas es la utilización de lo que los norteamericanos denominan "*tiger teams*". Estos equipos, compuestos de uno o varios expertos en el tema de seguridad, realizan deliberadamente una irrupción en los sistemas: roban, modifican o destruyen software, datos o equipos; en otras palabras, ponen al descubierto las áreas vulnerables de la organización. Como el propósito de estos equipos es exponer a críticas al personal, los sistemas y los procedimientos, originan consideraciones éticas y, en cualquier caso, lo que estos grupos hacen es poner de manifiesto las áreas vulnerables en relación con un abuso *deliberado*.

Hacking

El hacking despierta temores en muchas organizaciones, que se ven a sí mismas en una situación de riesgo frente a agresores externos de mentalidad delictiva. Pero, de hecho, la mayoría del hacking (es decir, del acceso no autorizado a ciertas áreas) se realiza por personal interno (para consultar ejemplos, ver Alexander, 1995; Lynch, 1994, y Atkins, 1991). El hacking simplemente hace referencia a la entrada no autorizada, o a un intento de entrada, en un sistema y, sin duda, gran parte de estos intentos están impulsados por la curiosidad y carecen de una finalidad delictiva. Sin embargo, una vez dentro del sistema, el usuario no autorizado puede hacer cualquier cosa. Las actividades de los hackers van desde el robo hasta la modificación de resultados, la implantación de un virus o la alteración de datos. Durante la última elección general, un miembro del Parlamento inglés acusó al Partido Conservador de entrar en el sistema informático del Partido Laborista y robar datos secretos. La vulnerabilidad depende ampliamente de los siguientes factores:

- *El personal de la organización*: la protección del acceso puede ser quebrantada en cualquier elemento de la red.

- *El tamaño de la red*: mientras más amplia es la red, mayor será el potencial de riesgo. Las redes internacionales no suelen ser muy seguras.

- *La calidad de transmisión de datos*: mientras más alto es el valor de los datos que se transmiten, mayor será el riego de amenazas, ya que el valor obtenido por el abuso deliberado le justificará al hacker la inversión de tiempo y dinero.

Los aspectos legales se considerarán en detalle en la Sección 13.3.

Virus

En 1992, una encuesta de S&S International descubrió que el 61% de más de 1.000 organizaciones habían sido infectadas por virus. Aún más llamativo, el 28% de esas infecciones habían tenido lugar durante el mes anterior a la encuesta. Xephon, el consultor de IBM, calcula que más de la mitad de los desastres en los mainframe son infecciones de virus, pero hay que tener en cuenta que el delito es el desastre más costoso. Los establecimientos educativos son particularmente vulnerables a los virus, y CHEST calcula que el 4% de las compras de software que realizaron en 1991 tenían programas de protección contra virus, a diferencia del 0,5 % de 1989. No sólo los establecimientos educativos son vulnerables; de hecho a todas las organizaciones les resulta difícil convencer al personal de que no lleve software pirata, al que se relaciona no sólo con problemas de virus, sino también con problemas legales. Los virus son creados como un modo de abuso deliberado: la creación intencional de error de programación (*bug*) en el software (aunque a veces se denomina virus a cualquier error de programación). Desafortunada-

mente, los virus se propagan con más frecuencia como un ejemplo de abuso accidental por desconocimiento del peligro.

La disminución de incidentes de hacking y el aumento de la variedad de virus e infecciones indican que las tendencias delictivas relacionadas con los IS (en oposición a las tendencias delictivas que sólo explotan los IS para obtener ganancias monetarias) prefieren las tasas bajas de detección asociadas a la creación de virus. A la mayoría de las organizaciones les resulta difícil evaluar la realidad de una amenaza de virus. Los medios de comunicación exageraron el riesgo. Las infecciones están aumentando, probablemente porque una mayor cantidad de computadoras de escritorio significa una mayor utilización de discos, un mayor intercambio, y entonces un incremento de las infecciones causadas por virus. Aunque se presta más atención a los virus de las PCs, los mainframes también sufren infecciones. Los mainframes son máquina de múltiples usuarios y, a menudo, crean entornos con puntos de acceso ampliamente distribuidos.

El valor ínfimo de las infecciones de virus genera altos costos de prevención, pero muchos virus causan un daño evidente mínimo, y una vez que se los elimina, se regresa a la normalidad. Sin embargo, la interrupción del sistema, la pérdida de confianza en los IS y el daño a los datos causados por las reacciones de pánico del usuario generan costos serios. En el caso de los virus, la prevención puede no ser mejor que la cura, ya que los *backups* y los procedimientos de recuperación son una respuesta apropiada a un gran número de riesgos y pueden ser más efectivos en cuanto al costo que las onerosas medidas de prevención adoptadas como respuesta a un único riesgo.

13.1.2 • Análisis del riesgo

Una vez detectadas las amenazas, se puede proceder con el análisis de su *impacto* potencial. Si la etapa de identificación del riesgo constituye una forma de "pensamiento creativo y espontáneo", entonces la etapa del análisis del riesgo es un proceso más estructurado, aunque a menudo de una manera cualitativa y no cuantitativa. El análisis debe evaluar la pérdida esperada, producida por una amenaza particular, en donde:

Pérdida esperada = Pérdida potencial x Frecuencia de pérdida

Por lo tanto, el análisis del impacto potencial (es decir, por cada riesgo identificado, la probabilidad de ocurrencia y la gravedad de sus consecuencias) requiere de dos etapas. La primera evalúa los costos empresariales que surgen de una brecha en la seguridad. Esta evaluación debería incluir, al menos de un modo aproximado, cálculos financieros incluso para los costos conceptuales, como pérdida del buen nombre/de la clientela y daño de las expectativas del usuario. Existe un gran números de aspectos relacionados con las pérdidas potenciales provenientes de una falla de seguridad, y en la próxima sección los desarrollaremos en más detalle.

Debería utilizarse algún valor monetario o de otro tipo para cuantificar el efecto de la amenaza si ésta ocurre. A esto se le suma la posibilidad calculada de que suceda y entonces la segunda etapa del análisis de riesgo consiste en estimar la frecuencia de ocurrencia de cualquier falla de seguridad a través de la probabilidad de agresión y la probabilidad de que la agresión prospere. (En este contexto, la palabra "agresión" hace referencia a cualquier falla en la seguridad, no necesariamente a un deliberado abuso humano.) Estos cálculos pueden extraerse de :

- tablas de actuarios
- evidencia empírica
- cálculos razonados

Es difícil predecir de forma confiable la posibilidad de una amenaza a los IS; el uso y el management de los IS cambia con demasiada rapidez para que los datos anteriores se acomoden a cuadros de probabilidad precisos. En cualquier caso, debido al temor de dañar la reputación de la empresa, las agresiones exitosas *registradas* representan sólo un pequeñísimo número de las agresiones exitosas *reales*. Sin embargo, al utilizar medidas relativas (como muy alto, alto, mediano, etc.) y al asignar a cada medida relativa un valor numérico (por ejemplo, 90%, 70%, 50%, etc.), se puede realizar un cálculo aproximado. El uso de

estos cálculos aproximados es más efectivo que cualquier precisión espuria y engañosa. La **Figura 13.6** muestra algunos cálculos de frecuencia utilizando aproximaciones de probabilidad.

Amenaza	Probabilidad de agresión		x Probabilidad de éxito		= Frecuencia
Entrada de datos incorrecta	muy alta	90%	mediana	50%	45%
Incendio	mediana	50%	alta	70%	35%
Hacking	baja	20%	mediana	50%	10%

Nota: la reducción del riesgo discutida en la Sección 13.1.3 puede disminuir la probabilidad de agresión o la probabilidad de éxito a fin de reducir la frecuencia; puede también reducir los costos resultantes para disminuir la pérdida general.

Figura 13.6. Cálculos de frecuencia de amenazas.

El producto de costo y frecuencia da como resultado la pérdida anual esperada para cada amenaza :

Costo	x	Frecuencia	=	Exposición anual
(de las consecuencias)		(de los cálculos)		de pérdidas

Estas exposiciones de pérdida pueden estar tabuladas de varias formas; la **Figura 13.7** muestra un ejemplo de una tabla de pérdida anual (ALE), que debe desarrollarse en una escala pertinente al patrón de amenaza bajo análisis.

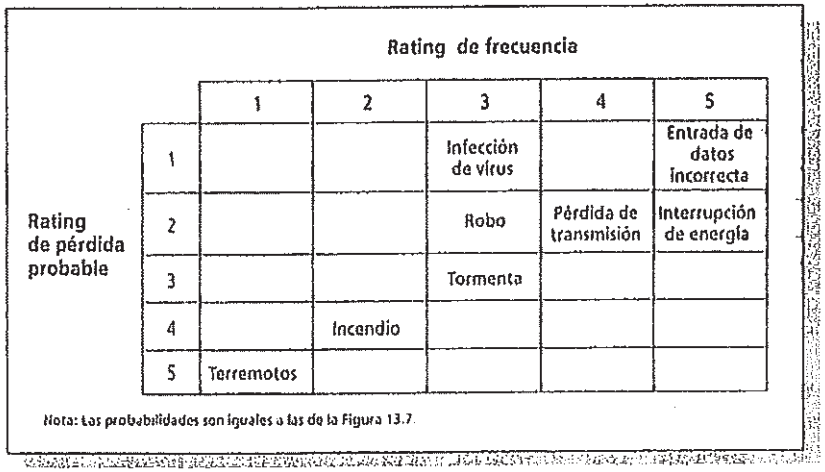
	Frecuencia (probabilidad de agresión x probabilidad de éxito) Tiempo medio entre eventos						
Pérdida (pesos)	300 años	20 años	3 años	100 días	10 días	1 día	1/10 días
10					300	3.000	30.000
100				300	3.000	30.000	300.000
1.000			300	3.000	30.000	300.000	3.000.000
10.000		300	3.000	30.000	300.000	3.000.000	30.000.000
100.000	300	3.000	30.000	300.000	3.000.000	30.000.000	
1.000.000	3.000	30.000	300.000	3.000.000	30.000.000		
10.000.000	30.000	300.000	3.000.000	30.000.000			

Figura 13.7. Pérdidas anuales.

Esta tabla permite entonces calcular la *verdadera* exposición anual. Por ejemplo, una reducción de energía que causa una pérdida de 100 pesos cada vez que ocurre y, tal vez debido a fallas en el cableado ocurre una vez al día en algún lugar del edificio, ocasiona una pérdida anual de 30.000 pesos. El método ALE cuantifica la gravedad de la amenaza y permite la implementación de un conjunto de contra medidas efectivas con respecto al costo, es decir medidas cuyo costo anual sea menor que 30.000 pesos.

Las cuantificaciones de la tabla de ALE en términos monetarios tal vez no sean fáciles, en cuyo caso puede utilizarse una tabla de ranking cualitativo, la matriz de *gravedad* de la amenaza. Ésta utiliza una escala simple, a menudo de logaritmos, para representar la magnitud de las pérdidas y la probabilidad de ocurrencia. La **Figura 13.8** muestra una matriz, parcialmente completa, de gravedad de la amenaza. Los riesgos que suceden con frecuencia se encuentran en el extremo derecho y los eventos que raramente ocurren están sobre el extremo izquierdo, en tanto que el costo del evento se lee de arriba hacia abajo. Por lo general, el manejo del riesgo (ver Sección 13.1.3) se concentra en dos categorías: los que ocurren frecuentemente, ya que las contra medidas tienden a dar un rédito neto alto, y las catástrofes absolutas, que, aunque infrecuentes, provocarían el cierre del negocio.

El análisis del riesgo establece un lado del punto de equilibrio óptimo entre el costo de pérdidas y el costo de medidas de seguridad. El manejo del riesgo identifica contra medidas posibles y luego elige el conjunto adecuado para ese trueque óptimo. La respuesta clásica a las amenazas de baja frecuencia, pero de un costo potencial alto, es el seguro, y así los controles y las contra medidas elegidas que constituyen la política de seguridad de una organización serán orientadas generalmente a aquellos eventos con una frecuencia alta aunque con costo bajo.



Rating de frecuencia

Rating de pérdida probable	1	2	3	4	5
1			Infección de virus		Entrada de datos incorrecta
2			Robo	Pérdida de transmisión	Interrupción de energía
3			Tormenta		
4		Incendio			
5	Terremotos				

Nota: Las probabilidades son iguales a las de la Figura 13.7.

Figura 13.8. Un ejemplo de matriz de gravedad de la amenaza.

Un análisis de riesgo efectivo requiere una apreciación de la verdadera magnitud de las pérdidas resultantes de cada amenaza, lo cual resulta difícil. El management efectivo del riesgo también requiere una valoración realista de la posibilidad de que la amenaza se convierta en realidad. Las investigaciones de Loch et al. (1992) indican que muchas organizaciones están ciegas, no ante las amenazas en sí mismas, o a sus costos potenciales, sino a la probabilidad de que suceda un evento a su organización.

Pérdida

En un análisis de riesgo de los IS, debe encontrarse algún método de cuantificación de las pérdidas resultantes de una falla en la seguridad. Algunos elementos de los IS están sujetos a pérdidas que deben clasificarse de algún modo. Estos elementos de IS incluyen:

- *Hardware:* la pérdida es relativamente fácil de evaluar y estos elementos están a menudo asegurados; de hecho, el seguro puede ser un requerimiento de un acuerdo de alquiler o *leasing*. Estos ítems pueden ser valuados en su costo de reposición más una suma adicional que representa el costo de repetir el proceso de adquisición.

- *Datos e información:* es la pérdida más seria y la más difícil de cuantificar. La pérdida total de datos de venta dejaría a una organización en un estado de desconocimiento sobre sus deudores, que en la mayoría de los casos representan un 20% de su movimiento total. Las pérdidas de datos de producción pueden detener la operación de la empresa. Las pérdidas parciales causan, por cierto, un daño menor a la habilidad general para comercializar, pero los costos de recuperación dependen de las precauciones que se hayan tomado.

- *Software:* la principal complicación cuando se evalúa la pérdida de software es que el valor intrínseco, o costo de reemplazo, del software no tiene relación con el costo original de desarrollo. Para sumar complicaciones, la pérdida de software genera una pérdida de la capacidad de procesamiento y, entonces, el factor debe incluirse en la cuantificación de pérdida del software.

- *Capacidad de procesamiento:* la duración de la interrupción es la variable clave al determinar el valor de la pérdida. Definir franjas de tiempo apropiadas a la organización permite calcular los costos para cada franja, que variarán significativamente. Los sistemas complejos de tiempo real pueden generar costos enormes luego de unos pocos segundos, mientras que las organizaciones de baja dependencia tal vez sólo necesiten asegurarse un procesamiento periódico.

- *Personal:* quizás el costo que se pasa por alto con mayor frecuencia es el de la pérdida de personal clave, que puede ser significativa ya sea por su conocimiento teórico o por su competencia práctica. El costo de pérdida de personal varía constantemente según las actividades que realiza ese personal y, entonces, los cálculos de pérdida deben efectuarse con frecuencia.

- *Fondos*: la cantidad de fondos que se pierden depende del tipo de negocio. Las pérdidas accidentales o fraudulentas deben dividirse en franjas relacionadas con diferentes tipos de fallas en la seguridad, para que así la pérdida de fondos pueda cuantificarse. Distintas anécdotas señalan que los fraudes a menudo se originan en errores accidentales en los movimientos de efectivo que no se detectan.

Todas las pérdidas que resultan de una falla en la seguridad se relacionan con los atributos de valor agregado de la información y se las puede dividir en tres categorías:

- *Pérdida de disponibilidad*: la pérdida de seguridad destruye, total o parcialmente, la habilidad de la empresa para acceder a datos e información.

- *Falla en la integridad/precisión*: la pérdida de seguridad destruye la capacidad de una empresa para confiar en sus datos, o aún peor, de contar con datos de precisión incierta.

- *Pérdida de confidencialidad/seguridad*: la pérdida de seguridad destruye la posesión exclusiva de datos, lo que provoca que la organización pierda poder y confianza. Una vez más, el peor caso es el de incertidumbre.

El primer paso al evaluar la magnitud de la pérdida resultante de una falla en la seguridad es considerar las consecuencias primarias, es decir, aquellas cosas que se desprenden directamente, y por lo general en forma inmediata, de un problema en la seguridad. La **Figura 13.9** muestra algunos ejemplos de consecuencias primarias.

Ejemplos de pérdida directa:

- Interrupción del procesamiento a corto o largo plazo.
- Corrupción de los registros de datos, que a menudo incluyen material de backup; el peor caso es cuando la corrupción no se detecta o cuando su alcance es incierto.
- Destrucción de los medios de almacenamiento.
- Uso de software no autorizado; en el mejor de los casos, atasca las redes y reduce la capacidad de procesamiento; en el peor de los casos, los sistemas se destruyen y los fondos son mal dirigidos.
- Revelación de información confidencial.
- Desaparición de equipos, datos o software; el robo o la piratería son difíciles de reconocer.
- Pérdida de los registros de contabilidad u otros; en el mejor de los casos, esto perjudica el análisis histórico; en el peor de los casos, significa el detenimiento de los recibos de efectivo.

Figura 13.9. Consecuencias primarias de una falla en la seguridad.

No todas las pérdidas empresariales representan el resultado directo de una falla en la seguridad. Las pérdidas secundarias (que surgen como consecuencia de las pérdidas primarias, y no de una falla en sí misma) revisten gran importancia en los cálculos de pérdidas. La **Figura 13.10** muestra las relaciones entre la pérdida de seguridad, las pérdidas primarias y las consecuencias secundarias. Lo que esa figura no muestra es que muchas pérdidas primarias producen pérdidas similares secundarias y, aunque los riesgos de seguridad sean muy diferentes, si las pérdidas son similares, los costos también lo serán. La similitud es muy importante en lo que hace a las decisiones del manejo de riesgo, dado que es probable que el costo para evitar el riesgo sea muy diferente a pesar de que las pérdidas secundarias sean comparables.

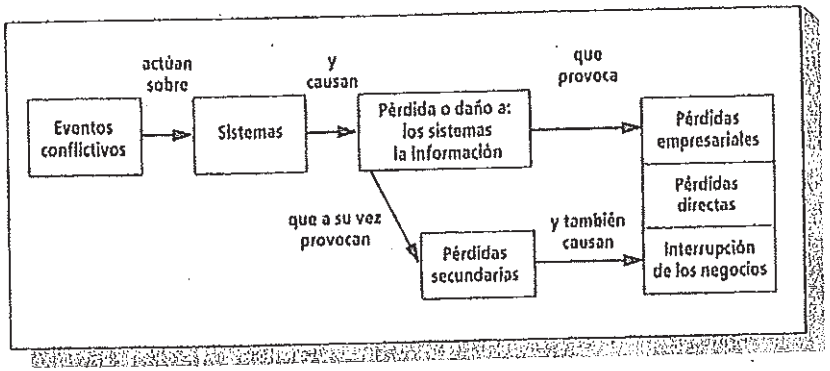


Figura 13.10. Pérdidas resultantes de una falla en la seguridad.

Si las consecuencias primarias son difíciles de cuantificar, es aún más difícil evaluar las consecuencias secundarias, que tienden a ser más costosas que las pérdidas directas y, como son costos empresariales, por lo general surgen después de un largo tiempo. Pocas veces resulta práctico vincular valores monetarios detallados a las consecuencias secundarias; se utilizan, en cambio, clasificaciones cualitativas. La **Figura 13.11** da algunos ejemplos de posibles pérdidas secundarias.

Ejemplos de pérdidas secundarias:

- Pérdida en la producción
- Retraso en las entregas
- Problemas de flujo de efectivo
- Pérdida de confianza del cliente
- Declaraciones de impuesto imprecisas
- Información gerencial inútil, imprecisa e inoportuna
- Sanciones por incumplimiento de obligaciones legales
- Incapacidad de continuar la función del sistema
- Pérdida de una posición competitiva
- Incapacidad de continuar con el negocio

Figura 13.11. Consecuencias secundarias de una falla en la seguridad.

La magnitud de la pérdida total de una falla en la seguridad es la suma de las consecuencias primarias y secundarias. En el caso de que las consecuencias primarias puedan ser minimizadas (y eso es lo que se intenta con una buena recuperación ante el desastre, ver Sección 13.1.4), entonces habría una doble ganancia, porque si se reducen las pérdidas primarias, entonces las secundarias también se minimizan. Por ejemplo, si una falla del software daña datos, la magnitud potencial de la pérdida podría ser extensiva. Sin embargo, el *backup* efectivo y los procedimientos de reparación minimizarán la pérdida primaria y, debido a esas imprecisiones y retrasos mínimos, la pérdida secundaria también se reducirá.

13.1.3 • Manejo del riesgo

La identificación y el análisis de la amenaza se realizan con el objetivo de seleccionar las estrategias de manejo del riesgo que ofrezcan la mejor efectividad neta, es decir, que mantengan el equilibrio óptimo deseado. El manejo del riesgo consiste en la aplicación de controles y contra medidas apropiadas para el riesgo, de acuerdo con el tiempo, el dinero y otros límites. Los pasos previos de:

1- Enumeración de amenazas potenciales
2- Cuantificación de pérdidas que surgen como consecuencia de las amenazas exitosas
3- Determinación de ALE o alguna otra medida de probabilidad o gravedad de la ocurrencia.

constituyen un proceso valioso pero sólo como un medio para alcanzar un fin. El propósito es identificar el "mejor" método de manejo del riesgo, en donde "mejor" se define como un management de fallas potenciales de seguridad que sea efectivo en cuanto al costo. Existen cuatro estrategias genéricas para el manejo del riesgo:

- *Prevenir el riesgo*: si es posible evitar la amenaza, entonces la organización puede tomar los recaudos necesarios. Por ejemplo, colocar los sistemas lejos de las áreas peligrosas, ubicar los datos delicados en áreas bien protegidas, no descentralizar, alterar los métodos del trabajo y prescindir de

los aspectos que amenazan a la seguridad, como alojar el sistema de cómputos en un sótano.

- *Asumir el riesgo*: si las pérdidas netas son tales que una organización no pueda tolerar la pérdida esperada sin excesiva incomodidad, entonces puede adoptar la estrategia de "sonreír y soportar". Este enfoque se aplica generalmente a los riesgos relacionados con bajos costos porque las consecuencias son menores. Los costos "verdaderos" dependen del valor de utilidad del capital, en cuyo caso la exposición de pérdida anual puede ser una medida excesivamente agregada. A menudo se pasa por alto la verdadera exposición total, y asumir el riesgo puede ser una estrategia de seguridad que se adopta en forma inadvertida.

- *Reducir el riesgo*: ésta es la estrategia de manejo del riesgo más común por razones obvias. Resulta muy difícil evitar por completo una amenaza y a menudo es inadecuado ignorarla. Entonces, la reducción del riesgo es un compromiso conveniente, y consiste en la introducción de controles y contra medidas para reducir la probabilidad de ocurrencia y/o para reducir las pérdidas resultantes de una falla en la seguridad. El portfolio de controles y contra medidas es sólo efectivo económicamente si provoca en la tabla de ALE una reducción mayor que el aumento anual del costo (de todo tipo) originado por la implementación de medidas. Todas las contra medidas suman costos a:

  - el desarrollo
  - la operación
  - el mantenimiento
  - la flexibilidad

Entonces, para calcular la efectividad neta, la ecuación de la reducción del riesgo equilibra los costos completos de las consecuencias primarias y secundarias con los costos completos de las medidas de seguridad. Como la empresa está buscando minimizar la suma de costos adicionales y los costos negativos pronosticados, la pregunta clave es:

¿Hasta qué grado se reducirá el costo?

- *Transferir el riesgo*: esta cuarta estrategia de manejo del riesgo transfiere los costos resultantes de una falla en la seguridad a un tercero, que en general implica pólizas de seguros o contratos de mantenimiento. Cabe señalar que las cláusulas de cualquier póliza de seguro, o las reglas de operación y servicio dentro de los acuerdos de mantenimiento, definen el grado de riesgo que se asume, que puede entonces estar sujeto a una estrategia de prevención.

Identificar un portfolio de management de riesgo significa seleccionar un conjunto heterogéneo de estrategias de manejo del riesgo que dependen de la aplicación sistemática de la identificación y el análisis del riesgo. La organización, entonces, enumera los riesgos en orden descendente de la tabla de ALE para considerar en forma prioritaria las contra medidas. Sin embargo, los desastres potenciales son tratados como un ítem de alta prioridad. Esta lista de prioridades permite concentrar los esfuerzos a fin de alcanzar la mejor posición neta. La mayoría de las organizaciones utilizan la estrategia de prevención del riesgo y la de transferencia del riesgo para calamidades totales; la de asumir el riesgo para amenazas con pérdidas muy bajas, a menudo independientemente de la frecuencia, a menos que los controles posibles sean baratos y no obstaculicen la flexibilidad; y una mezcla de la estrategia de reducción del riesgo y la de transferencia para las amenazas restantes.

Cada vez más, la seguridad de los IS debe ser considerada como un tema estratégico, y toda empresa debería invertir en seguridad, hasta donde el dinero gastado contribuya con las metas globales de los IS. Si el resultado de las pérdidas prevenidas o reducidas es mayor que el costo de seguridad, entonces existe una contribución neta a las ganancias. Reconocer

este hecho puede superar parte de la imagen negativa asociada a los gastos de seguridad. Si seguimos esta línea de razonamiento, es importante mencionar la ley de disminución de ganancias. Esto significa que mientras más alto sea el nivel *actual* de seguridad, más costará el próximo paso. El foco debe estar puesto sobre el equilibrio neto, para cuestionar no sólo qué medidas podrían ser utilizadas, sino qué medidas deben ser utilizadas.

Smith (1993) explora esta ley de disminución de ganancias aplicada a las medidas de seguridad de las PCs, y llega a la conclusión de que no sólo es más caro elevar el nivel de seguridad, sino que las medidas de seguridad adicionales tienen un efecto *perjudicial* en la utilidad global. Sugiere que se "filtre" la lista de todas las posibles defensas para asegurarse de que el conjunto utilizado es beneficioso y no perjudicial. Dichos filtros pueden determinarse por un test objetivo, cuyas instancias incluyen:

- *La interconexión de la PC a otras PCs*: Smith sugiere tres categorías: PC sola, PC conectada a un servidor de datos, PC conectada a un servidor de programa. Mientras mayor sea la interconexión, más posibilidades de amenaza existirán.

- *El número de usuarios*: muchas PCs constituyen un recurso compartido, y mientras más personas compartan el acceso, más posibilidades de amenaza existirán.

Estos filtros eliminan objetivamente las medidas que no ofrecen beneficios. Las opciones restantes deben ser priorizadas hasta el punto en que la utilidad marginal llegue a cero. Como la seguridad efectiva de las computadoras trata básicamente sobre la motivación del personal, la cultura y el estilo corporativo siempre tendrán un fuerte impacto en el momento de seleccionar un conjunto de estrategias de management óptimo del riesgo, y adoptar las contra medidas y los controles adecuados.

Cuando el control o la contra medida introduce riesgos adicionales, entonces la evaluación costo-beneficio utilizada debe ser rigurosa. Las medidas baratas aplicadas con un espectro amplio son por lo general más efectivas que las medidas costosas aplicadas con un espectro restringido. Por ejemplo, utilizar una contraseña de verificación relativamente barata en todos los sistemas resulta más efectivo que usar una firma de verificación costosa en sólo algunos sistemas.

La transferencia de riesgo, por lo general a través de la contratación de un seguro, resulta apropiada para las amenazas de alto costo y baja probabilidad, y en las que la recuperación completa es imposible. El seguro extiende el costo de esos eventos de alto costo y baja frecuencia a través del tiempo y de muchas organizaciones. Los principales problemas relacionados con dicha estrategia son la elección del tipo de seguro y el hecho de que las aseguradoras exigen algunos procedimientos de reducción de la amenaza antes de asegurar el riesgo. El seguro de los equipos por lo general no presenta complicaciones, pero el seguro de datos y pérdidas secundarias es necesario para transferir el riesgo; de lo contrario, la empresa deja de funcionar pero los liquidadores pueden recuperar, de los aseguradores, los costos de reemplazo del equipo. Las primas del seguro del equipo son a menudo del 1% del monto asegurado si el equipo tiene mantenimiento, y del 6% si no lo tiene. Lloyds ofrece un seguro de pérdidas secundarias pero sólo si las políticas de manejo del riesgo son consistentes. Tanto la pérdida del rédito bruto como los costos de operación pueden reembolsarse, y el seguro puede incluso cubrir las oportunidades empresariales perdidas, resultantes de la pérdida de datos.

Una política de seguridad define el nivel de seguridad que se ajusta al valor de lo que se debe proteger y al gasto e inconveniencia de las medidas de protección. Esas políticas documentan el resultado de la identificación y el análisis del riesgo, y de las estrategias elegidas para manejarlo. Saunders (1989) sugiere que el documento cubra por lo menos:

- *La protección de la información*: dado que la naturaleza de la información determina su atractivo externo y su importancia interna.
- *El valor de la información*: ya que cuantifica las pérdidas potenciales.
- *El acceso a la información*: porque define quién está autorizado para ver, modificar, cargar o bajar los datos.
- *La recuperación de la información*: porque define cómo los datos perdidos o dañados pueden recuperarse y luego utilizarse.

Los documentos de las políticas de seguridad normalmente incluyen tablas explicativas de la estrategia de manejo del riesgo para cada una de las amenazas consideradas. La Figura 13.12 muestra un ejemplo de esas tablas.

Controles y contra medidas

Las estrategias de manejo del riesgo se implementan a través de controles y contra medidas. La elección del conjunto que, de un modo efectivo con respecto al costo, evita, reduce o transfiere el impacto del riesgo es obviamente un aspecto del management del riesgo. Es también obvio que los controles y las contra medidas se relacionan básicamente con las estrategias de prevención y reducción. Las medidas de seguridad y control deben ser consideradas en términos de los costos netos y de los nuevos riesgos potenciales resultantes de su adopción.

Existen fundamentalmente dos tipos de control: las contra medidas generales que se introducen para reducir la amenaza de todas las actividades de los IS dentro de una organización; y los controles de aplicación diseñados para proteger de amenazas a un área específica. Hasta cierto punto, los controles de aplicación son un subconjunto de controles generales y, para la mayoría de las empresas, un gran número de medidas generales se aplican a todas las áreas de los IS tomando precauciones adicionales para las áreas específicas. Un punto débil en los controles generales podría provocar una pérdida de seguridad en cualquier sistema y así, el costo de estas medidas debería considerarse "compartido" por todas las áreas protegidas.

Riesgo	Pérdida potencial	Probabilidad	Contra medidas	Costo
Oficina de cómputos destruida por incendio	Capacidad de procesamiento para la planificación de la producción, el pago de sueldos y el procesamiento de pedidos. Reemplazo de equipos. Reconstrucción del lugar.	Baja	Backups Sistemas de resguardo Seguro Prevención de incendios	$ 30 000
Pérdida completa de los registros	Incapacidad para cobrar a los clientes. Paro de la línea de producción durante cuatro días. Incapacidad para seguir con la comercialización durante cuatro semanas.	Acción mandatoria	Copias remotas de todos los archivos vitales. Seguro contra pérdidas secundarias durante la recuperación	$ 10 000
Robo de información para uso de los competidores	Pérdida de posición en el mercado	Baja	Control estricto de acceso a los archivos vitales. Control del personal	Sistema para autentificar al usuario. Fortalecer los procedimientos de incorporación de personal.
Uso ilegal de la capacidad de procesamiento	Aumento mínimo de los costos de procesamiento. Posible efecto adverso en el propio procesamiento.	Baja	Detección de controles/ obstáculos	Ninguna acción: riesgo bajo/pérdida pequeña contrapesados con consideraciones sobre la moral del personal.
La lista muestra qué corre peligro pero, al ser expresado a través del cómo, permite que las acciones sean claras	En secuencia, por prioridad de esfuerzo	La política debe explicar el espectro de la amenaza utilizado. Son preferibles las probabilidades relativas a las absolutas y espurias.	Si hay demasiadas entradas, entonces el riesgo definido no fue lo suficientemente específico	Cada acción requiere su costo correspondiente identificado

Figura 13.12. Ejemplo de tabla de manejo de riesgo.

Los controles y las contra medidas no son un único conjunto homogéneo. Para dar como resultado una "buena" seguridad, las diversas amenazas deben ser combatidas por capas de controles dirigidos a diferentes aspectos del uso y management de los IS. La naturaleza precisa de las instancias de cada capa de control dependerá de la naturaleza de la organización, del entorno de los IS y del valor de su información. En el caso de los IS, los factores determinantes son:

- *La plataforma de hardware*: que ejerce influencia en el tipo y la *cantidad* de controles disponibles.
- *El grado de distribución*: que influye en el énfasis de los controles requeridos.
- *La integración de la infraestructura*: que influye en la naturaleza de las amenazas.

Cualquier cambio en este entorno de los IS significa que las consecuencias de seguridad se extienden por todas las capas de control. Por ejemplo, una iniciativa de *downsizing* altera sin duda la plataforma de hardware y probablemente altere el grado de distribución y el grado de integración. Por lo tanto, exige un reajuste de la posición neta con respecto a los controles y las contra medidas.

Aun dentro de cada capa de control existen diferentes intenciones relacionadas con cada medida específica. La intención puede ser la de prevenir, detectar o reducir el impacto de las amenazas anticipadas. La **Figura 13.13** ilustra los vínculos entre las etapas de control, mientras que la **Figura 13.14** indica dónde se encuentran estos controles en relación con las pérdidas empresariales experimentadas como resultado de una pérdida de seguridad (ilustrada en la Figura 13.10). Estas tres etapas se aplican a la mayoría de las capas de control. Por ejemplo, el software de autorización puede tratar de prevenir el uso no autorizado, pero también registra los ingresos fallidos a fin de detectar los ataques y luego utiliza la encriptación de la segunda etapa para minimizar el daño causado por la entrada ilegal al sistema.

Primera línea de defensa	**Prevención**	Prevenir amenazas; por ej., prohibir que se fume en el centro de datos.
Segunda línea de defensa	**Detección**	Detectar fallas de seguridad a pesar de la primera línea de defensa, por ej., un detector de humo.
Tercera línea de defensa	**Recuperación**	Recuperarse de una falla de seguridad con pérdidas mínimas; por ej., backups de datos off-site.

Figura 13.13. Tres etapas de controles y contra medidas.

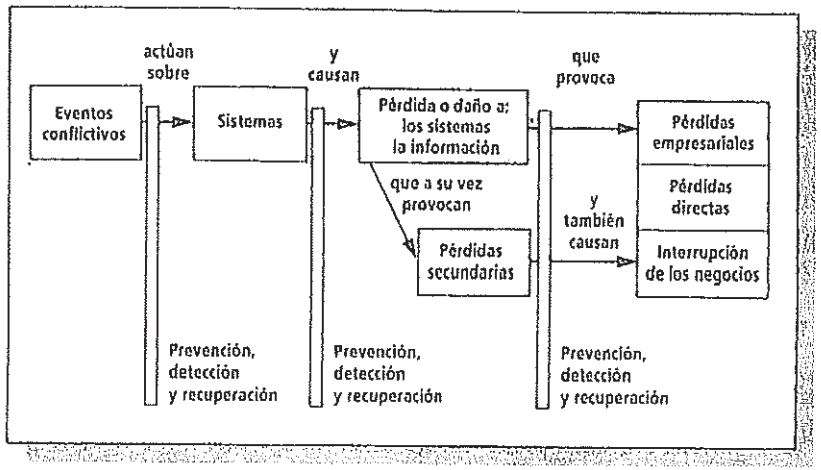


Figura 13.14. Los controles bloquean los efectos de la amenaza.

El principal objetivo cuando se seleccionan controles y contra medidas y, por lo tanto, cuando se define la política de seguridad, es crear una situación equilibrada entre los costos de riesgo y los costos de control. El problema surge cuando las organizaciones no equilibran eficazmente las amenazas con los controles y las contra medidas. La **Figura 13.15** muestra cómo los niveles de control y de medidas de seguridad aplicados a algunos de los elementos de IS son fuertes mientras que otros son débiles. Esto no representaría un problema si no

fuera porque las áreas de control débil son áreas de alto riesgo. Si la amenaza y los controles no se ajusten nivel por nivel, entonces la política de seguridad es ineficaz.

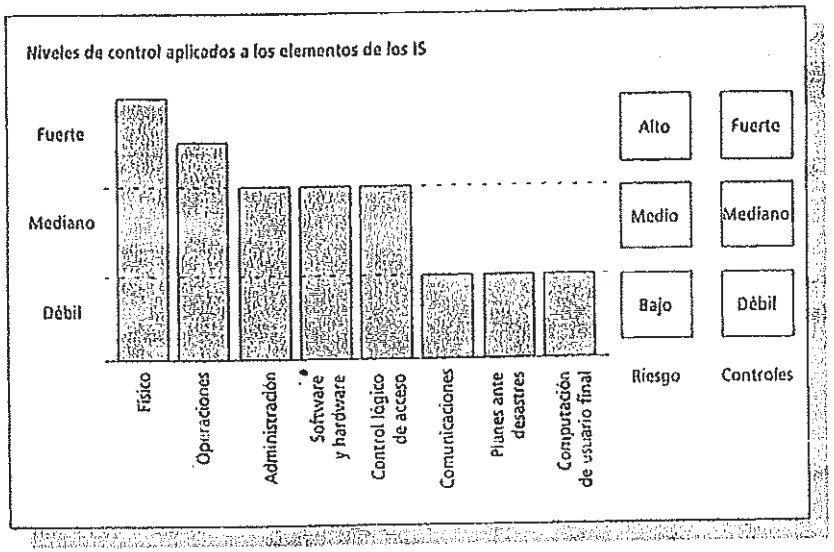


Figura 13.15. Niveles de control no ajustados a los niveles de las amenazas.

Las medidas para combatir las amenazas a los IS no siempre requieren acciones relacionadas con los IS. Por ejemplo, el trabajo de Courtney (1989) indica que los delitos relacionados con los IS están estrechamente vinculados a los niveles de salarios y, por lo tanto, el ajuste de tasas de pago podría conformar una medida de reducción del riesgo, efectiva en cuanto al costo. La división entre riesgo y contra medidas hace surgir un problema espinoso: ¿quién se encargará de seleccionar el conjunto de acciones que previenen la amenaza? Por ejemplo, la sección de IS puede hacerse responsable de mantener la seguridad de los IS y, sin embargo, no es libre de responsabilizarse por los salarios. Esto deja en claro que la seguridad de los IS es un tema estratégico que atañe a toda la organización y que requiere participación activa de la gerencia senior.

Al igual que con las amenazas, las contra medidas seleccionadas pueden ser *lógicas* o *físicas*. Los controles lógicos son las medidas adoptadas para asegurarse de que el desarrollo, la integridad de los datos y las operaciones continúen sin tropiezos. Dichos controles podrían incluir diccionarios de datos (que son una excelente forma de implementar, de una sola vez, toda una serie de controles de datos), claves de usuario, estándares de desarrollo y evaluación, reglas de management, controles de ingreso fallido, software de control y claves de acceso. Una de las medidas de control lógico más comunes, y a menudo inadecuadas, es la identificación del usuario y los sistemas de contraseñas para restringir el acceso a los sistemas. Estos controles lógicos protegen los datos asegurando que no se tendrá acceso a ellos o que, si se accede, es porque los datos carecen de importancia. Las medidas físicas de seguridad generan más costos, son menos efectivas y más propensas a producir resentimiento y, por lo tanto, su uso debe ser cuidadosamente evaluado. Tienen como propósito minimizar el riesgo de acceso no autorizado que conduzca en forma deliberada o accidental a:

- La revelación de información
- La modificación o destrucción de datos, software o equipos
- El uso no autorizado de las capacidades de los IS
- El robo de datos, software o equipos

Los controles físicos de seguridad pueden incluir el uso de personal de seguridad, sistemas de vigilancia, cerraduras, tarjetas con clave y otros métodos de acceso. Estas medidas filtran el acceso físico a la utilización de elementos de IS. Un ejemplo simple es la decisión de dónde ubicar el equipo, ya que no es aconsejable dejarlo cerca de áreas públicas o en centros de procesamiento ubicados en áreas físicamente amenazadas, como sótanos (por las inundaciones) o cerca de las paredes (por las escuchas furtivas).

Cuando se elige un conjunto de contra medidas, las organizaciones suelen preferir los controles físicos a los lógicos.

Además debe reconocerse que, a medida que las capacidades de procesamiento se vuelven más portátiles, son también más vulnerables, y mientras que en términos del hardware constituyen un ítem de bajo costo tan fácil de poner bajo llave y asegurar como una bicicleta, el software que contienen es menos fácil de reemplazar y los datos son tan valiosos como los almacenados en otro lugar. En el resto de la sección, examinaremos con más detalle algunas de las contra medidas y de los controles lógicos y físicos.

Estándares de operatividad

Al parecer, es verdad que una empresa siempre paga por los estándares, ya sea en el presente, al desarrollarlos, o en el futuro, por no tenerlos. Los estándares proveen el marco dentro del cual los IS pueden funcionar segura y eficazmente, y brindan además dos beneficios:

- La racionalización de las prácticas a fin de facilitar la comunicación y el management, y de simplificar la educación y la capacitación.

- La compatibilidad de software, hardware, datos, personal y canales de comunicación, y su posibilidad de volverse portátiles. Por lo tanto, en esta instancia, los controles también generan amenazas; por ejemplo, la interfase estándar y los mecanismos de acceso facilitan la entrada del personal en áreas no autorizadas.

A pesar de que los estándares operativos generan amenazas en ciertas áreas, ofrecen además los siguientes beneficios:

- *Management de proyectos*: dado que el *quién*, el *qué* y el *cuándo* están definidos

- *Desarrollos*: ya que los enfoques pueden estar estructurados y la producción, orientada

- *Operaciones*: tanto los procedimientos lógicos como las acciones físicas se vuelven más claros y menos susceptibles a errores a través de la ambigüedad

- *Calidad y documentación*: pueden ser mejorados si se utilizan los sistemas adecuados

El mantenimiento de los estándares es en sí mismo una gran responsabilidad que conduce a una definición de los estándares de performance mínimos para que así "la falla de seguridad" se pueda medir con más facilidad.

División de responsabilidades

Un control de seguridad tradicional debe asegurar que no haya instancias en las que un *único* individuo sea el responsable de configurar, implementar y vigilar los controles, y que sea, al mismo tiempo, responsable del uso de los sistemas. La participación de varias personas, cada una responsable de alguna parte de los controles y de la operación de los IS, permite la vigilancia mutua. Como ningún empleado realiza todos los pasos en una única transacción, los demás participantes pueden estar atentos a accidentes y conductas delictivas. Los IS podrían agruparse de un modo lógico en las siguientes actividades:

- Desarrollar sistemas
- Administrar medios de entrada (*input media*)
- Operar el sistema
- Administrar los documentos y los archivos
- Distribuir las salidas (*outputs*)

A fin de dividir por completo las responsabilidades, ninguna persona, siempre y cuando sea posible, debe transponer los límites de su tarea. Este tipo de control de seguridad se relaciona con la rotación de obligaciones y con las auditorías sorpresivas. Tales medidas corresponden a un estilo de management basado en la desconfianza hacia el personal, y pue-

den resultar inadecuadas dentro de un enfoque moderno de management. Sin embargo, Hinde (1993) analiza la película *Jurassic Park* como un ejemplo perfecto de desastre en los IS originado precisamente en la no división de tareas. Resulta evidente que la naturaleza de algunos desarrollos de IS (por ejemplo, las computadoras controladas por los usuarios) no se presta a esas medidas, y una contra medida más efectiva, basada en el personal, establece un clima de honestidad e incentiva a los empleados para que participen personalmente en el mantenimiento de la seguridad de los IS.

Medidas de seguridad de la red

El primer paso para seleccionar medidas de seguridad de la red consiste en realizar un diagrama que indique los puntos de acceso potenciales. El diagrama también contribuye a la capacidad de planificación y, así, los costos operacionales ahorrados pueden "pagar" por las medidas de seguridad de la red. Toda actividad de la red abarca tres elementos:

- La terminal de inicio
- La terminal de recepción
- El canal de transmisión

Para lograr una adecuada seguridad de la red, deben existir medidas confiables en las terminales de inicio y de recepción, y durante la transmisión de datos, que incluyan el uso de:

- El saludo: ésta es una señal predeterminada que debe ser recibida desde una terminal válida.
- Los módems de rediscado, que llaman al supuesto usuario a un número predeterminado.
- La identificación del usuario y las contraseñas, que dan validez a la persona que opera la terminal de inicio o de recepción.

- La encriptación de datos para protegerlos durante su transmisión o para cubrir las instancias en las que otras medidas fallan o son evitadas.

Hay que recordar que los objetivos de las medidas de seguridad son la prevención, la detección y la recuperación, y deberían aplicarse a cada uno de los elementos de la red.

Contraseñas

Un método a menudo utilizado para reducir la amenaza del hacking interno o externo, y para disminuir la posibilidad de daño accidental, es la implementación de la contraseña. Existen tres dimensiones para utilizar los sistemas de contraseña:

- Identidad individual del usuario, en cuyo caso la contraseña es privada y "demuestra" la identidad de la persona.
- Acceso grupal, en cuyo caso la contraseña "demuestra" la pertenencia del usuario al grupo, y cada uno de los miembros debe tener acceso a ella.
- Utilización de contraseñas como la "clave" para decodificar los datos encriptados.

En cualquiera de estos casos, la persona que selecciona la contraseña y el modo en que lo hace son de vital importancia.

Las contraseñas pueden generarse de dos formas. El sistema de contraseñas las puede crear de modo automático, y esto cuenta con la ventaja de que la contraseña se cambie regularmente y de que no utilice palabras. Las contraseñas sin palabras son, sin lugar a dudas, más seguras, a menos que su forma confusa obligue a escribirlas. Para reducir las posibilidades de que los usuarios las escriban, y que de esta forma comprometan la seguridad, las contraseñas que se crean en forma automática tienden a ser cortas. La segunda alternativa es la clave seleccionada por el usuario. Esto cuenta con la ventaja de que no sea necesario escribirla para recordarla, y la desventaja de

que la mayoría de los usuarios eligen palabras fáciles de adivinar y se niegan a cambiarlas. La posibilidad de adivinar las contraseñas disminuye si ésta no contiene palabras. Una alternativa son las secuencias con letras y números que sean fáciles de recordar por el usuario, y *nunca* deben escribirse.

Debido a que la detección, y no la prevención, constituye un objetivo de los controles de seguridad, entonces el sistema de contraseñas debe mantener un registro del número de entradas infructuosas mediante contraseñas. El hecho de que las entradas mediante contraseña sean múltiples puede implicar que el sistema de configuración de contraseñas es inadecuado, por lo que el usuario legítimo se ve obligado a hacer varios intentos; en este caso, la empresa debe revisar su proceso de configuración de contraseñas.

Las contraseñas son útiles sólo si se administran de forma correcta y, por eso, es necesario que todo el personal conozca los peligros que amenazan a la seguridad si éstas se "prestan", se escriben o se revelan. Aún más, debe incentivarse a los usuarios a que ingresen su contraseña sólo cuando nadie los pueda ver. Como éstas se transmiten mediante los sistemas de software, cualquier daño que se produzca en él reduce la eficiencia de la contraseña y, entonces, compromete la seguridad. Esto significa que los costos de las contra medidas adoptadas para proteger al software también protegerán los sistemas de contraseña y, por lo tanto, serán "compartidos".

Encriptación de datos

En los sistemas de red, el canal de comunicación es a menudo el vínculo más débil y, entonces, los datos que viajan a través de él pueden ser encriptados. Cuando se roban los medios de almacenamiento de datos, si éstos se encuentran codificados, carecen de valor; de la misma forma, cuando se accede ilegalmente a los sistemas, la encriptación protege los datos. En todos los sistemas, los archivos en los que las contraseñas se almacenan deben estar encriptados y, por lo general, las mismas técnicas de encriptación están protegidas. Los tres casos en los que se indica el uso de la encriptación son:

- La transmisión de datos de un punto a otro: encriptación de la comunicación.
- La protección de contraseñas o claves utilizadas para restringir el acceso: encriptación de la contraseña o de la clave.
- Almacenamiento de datos en bases de datos y archivos: encriptación de archivos.

Las técnicas de encriptación transforman el material legible en un texto cifrado con un formato ininteligible y, al hacerlo, cumplen con tres principios de seguridad:

1. Identificación: ayuda a identificar a los emisores y a los receptores autorizados.
2. Control: ayuda a prevenir la modificación de mensajes.
3. Privacidad: ayuda a proteger las intromisiones.

En una red, la encriptación puede aplicarse de dos modos: como una encriptación de un extremo a otro, en la que sólo la terminal de inicio y la de recepción deben descifrar los datos codificados; o como la encriptación de enlace a enlace, más segura pero más lenta, en la que los datos son descifrados y vueltos a cifrar en cada una de las etapas de transmisión. Los métodos de encriptación exceden el presente trabajo, pero señalaremos que el proceso de decodificación requiere autorización y entonces los beneficios de la encriptación dependen de la protección otorgada a la clave para descifrar los datos. En relación con estos métodos, se encuentra la noción de *ocultamiento* de datos: muchos sistemas de software esconden los archivos o elementos dentro de una configuración de archivos. Mientras que estas configuraciones a menudo son revertidas con facilidad, las medidas de encriptación no son para nada costosas, tanto en la compra como en los términos de procedimiento y, entonces, pueden tener una alta eficacia neta.

Antivirus

Todas las formas de management de los IS necesitan de los antivirus. Estas medidas de seguridad se dividen inevitablemente en etapas, que son las siguientes:

- Prevenir la infección del virus, si es posible, mediante el uso de sistemas de monitoreo de virus.

- Detectar la infección tan pronto como sea posible, mediante el uso de sistemas de escaneo de los medios de almacenamiento, con lo cual se reducen los costos de "limpieza" y la gravedad de las pérdidas secundarias.

- Eliminar los efectos de la infección tan económica y rápidamente como sea posible, mediante buenos procedimientos de *backup* para acelerar el proceso de recuperación.

Las medidas adoptadas para proteger los sistemas contra el acceso ilegal actúan obviamente en la prevención de infecciones deliberadas causadas por virus. Sin embargo, estas infecciones son infrecuentes en comparación con las infecciones accidentales ocasionadas porque el personal autorizado utiliza discos y software no autorizados. Los programas educativos constituyen la medida más efectiva para combatir estas acciones involuntarias, ya que no sólo reducen el peligro de una infección de virus, sino también los riesgos provenientes de muchas otras fallas en la seguridad, y proveen una base para procedimientos adecuados de recuperación.

Detección y prevención de incendios

Una evaluación de los riesgos y de los costos de los incendios muestra que tanto los costos como la probabilidad de ocurrencia son altos. Debido a eso, resulta efectivo desde el punto de vista de los costos emplear un gran número de medidas de seguridad. Éstas podrían incluir la restricción del acceso no autorizado, a fin de reducir el riesgo de incendios

premeditados, pero por lo general, implican el uso de sistemas generales de prevención y detección del fuego.

Cabe señalar que *todas* las computadoras, incluso las *desktop*, son particularmente vulnerables a los daños causados por el humo y diferentes emanaciones, al igual que por el agua y los productos químicos de los sistemas de extinción. La **Figura 13.16** muestra varios agentes contaminantes, incluyendo las partículas de humo, y los compara con el *espacio libre del disco.* La tendencia a utilizar computadoras *desktop* provoca la necesidad de ajustar los mecanismos de prevención y detección de incendios en toda la empresa y no sólo en la oficina de cómputos. Durante este reajuste, deben considerarse los efectos que tienen los sistemas de extinción "más baratos", y que causan contaminación, sobre el almacenamiento de datos distribuidos. La información creada por los datos es valiosa, independientemente de dónde esté almacenada, y así las PCs exigen sistemas costosos y no contaminantes.

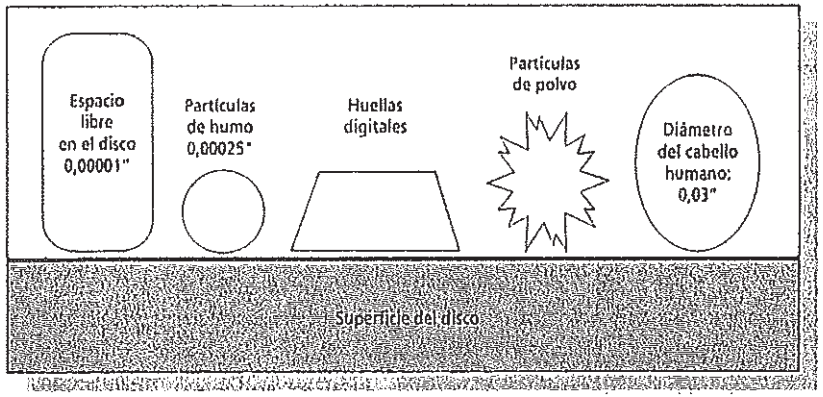


Figura 13.16. Efectos potenciales de agentes contaminantes sobre los medios de almacenamiento de datos.

Las medidas de seguridad elegidas por lo general disminuyen la productividad global ya que reducen la flexibilidad y la velocidad del acceso a la información. Por este motivo, es importante asegurarse de que el conjunto seleccionado de con-

tra medidas reduzca, prevenga o transfiera los riesgos identificados de un modo efectivo en cuanto al costo, porque:

- Un conjunto que es demasiado "pesado" desperdicia dinero y reduce de forma innecesaria la flexibilidad.

- Un conjunto que es demasiado "liviano" deja un nivel inaceptable de riesgo.

La empresa debe recordar que *todos* los cambios del entorno de los IS implican que el conjunto óptimo de contra medidas debe estar sujeto a un reajuste. Mientras que se busca un equilibrio de las medidas de seguridad que sea efectivo en cuanto al costo, algunos requisitos legales pueden anular las decisiones basadas exclusivamente en los costos. Por ejemplo, la *Data Protection Act* de 1984 (Ley de Protección de Datos del Reino Unido) hace de la seguridad de datos un requisito legal y, en teoría, la *Data Protection Office* (Oficina de Protección de Datos) podría obligar a cumplir las medidas de seguridad.

13.1.4. • Planificación de contingencias y recuperación ante el desastre

El cuarto y último elemento de los procesos de management de seguridad de los IS asume que la prevención *total* del riesgo es poco práctica o imposible y que, por lo tanto, la empresa debe planificar cómo enfrentarse a las inevitable rupturas de seguridad y cómo recuperarse de ellas. Esto es lo que se denomina planificación de contingencias, e incluye planes para métodos de trabajo que permitan que la empresa sobreviva al desastre, y para procesos a largo plazo a fin de que la organización se recupere. La primera etapa consiste en incrementar la seguridad, minimizar los daños y facilitar el regreso al trabajo. En la segunda etapa, se minimizan los efectos secundarios del desastre. Los términos relacionados con estas etapas son los siguientes:

- Tiempo de inhabilitación: cantidad de tiempo antes de que las operaciones vuelvan a funcionar parcial o completamente.

- Respaldo o mantenimiento: mantener el funcionamiento de la empresa a través de los sistemas clave hasta volver a la normalidad.

- Reinstalación: sistemas de actualización con todos los datos generados durante el tiempo de inhabilitación.

Por supuesto que el management de riesgo busca prevenir en los casos en que esto es posible, pero también debe prepararse para los desastres. La recuperación ante desastres debe llevarse a cabo con rapidez a fin de estar listo para cualquier falla en la prevención del riesgo y, de hecho, una estrategia de reducción del riesgo reconoce que existe la probabilidad residual de una falla en la seguridad. En algunos casos, cuando las consecuencias del riesgo son bajas, la prevención *no* es mejor que la cura y, entonces, la recuperación en sí misma puede ser una estrategia adecuada para el manejo del riesgo.

No es sorprendente que una encuesta de MSA, 1990, llegara a la conclusión de que la sofisticación de los esfuerzos de recuperación de una empresa se relacionaban con el grado en que los IT eran considerados críticos. Cuando se evaluaba que la confianza era total, entonces se realizaban disposiciones de recuperación, que incluían los preparativos para ubicar los IS en el estacionamiento de automóviles utilizando construcciones prefabricadas y un tendido de cables subterráneo. Es difícil de definir el grado de semejante confianza, con tantas empresas que confían en los IS no sólo para alcanzar eficiencia operacional, sino también practicidad operacional. A pesar del término "recuperación ante *desastres*" y de que la publicidad a menudo se preocupe por las respuestas ante bombas terroristas, incendios, inundaciones y terremotos, gran parte de la planificación de contingencias ofrece respuestas para causas menos dramáticas. Las pérdidas empresariales resultantes de datos perdidos por la destrucción de un disco revisten la mis-

ma importancia que aquéllas provocadas por las inundaciones. En una organización dependiente de los IS, un desperfecto importante en las máquinas puede constituir el "desastre". Gran parte del proceso de planificación de contingencias se ve obstaculizado por el miedo al ridículo relacionado con la recuperación. Este miedo llega hasta el punto de que un proveedor de servicios de recuperación se promociona ofreciendo rapidez, eficiencia y apoyo *discreto* durante la crisis, de lo cual se desprende que la discreción tiene la misma importancia que el servicio efectivo. Sin embargo, el volumen de desastres naturales y deliberados que han ocurrido durante los años noventa ha facilitado que la planificación de contingencias se incluyera en los programas de estrategia.

Para la mayoría de las organizaciones, el primer paso de toda planificación de contingencias consiste en clasificar los sistemas y las aplicaciones de acuerdo con la necesidad de las operaciones empresariales. Esta clasificación le permite a la compañía establecer un "cronograma de prioridades" que muestra cuándo cada elemento de los IS debe volver a funcionar para que la empresa sobreviva. Este cronograma facilita, entonces, que los esfuerzos se canalicen del modo más productivo. Por lo general, el *elemento de standby* del plan sólo cubre los sistemas críticos, pero el plan de recuperación debe cubrir *todos* los aspectos del uso y del management de los IS. El cronograma debería estar basado en la importancia del negocio (no en la dificultad técnica) y en general es similar al de la Figura 13.2, pero con descripciones del sistema adjuntas, cuya función es identificar qué aspectos de la funcionalidad se necesitan y cuándo. Un informe de Green Armytage (1995) señala que para el 78% de las empresas encuestadas, la disponibilidad de los sistemas era superior a las actividades empresariales. Como muestra la Figura 13.2, puede haber una meseta en el proceso de recuperación. Habrá también un grupo de elementos operativos de los IS que debe funcionar "inmediatamente", pero habrá otros para los cuales el tiempo de recuperación puede ser de unos pocos días, tres o cuatro, y un último conjunto para el que se dispone de alre-

dedor de una semana; los restantes serán tratados sin prisa. Para que sea conveniente, el cronograma de prioridades se establece presuponiendo una falta completa de la capacidad de operatividad en cualquier función dada.

Como la planificación de contingencias es parte del management estratégico de los IS, no se la puede separar de otros aspectos de gerenciamiento del uso de los IS y debe ser considerada junto con otros temas de la selección y la implementación de estrategias. Existe una clara distinción entre la tradicional recuperación ante desastres, que asegura básicamente la reconstrucción de la oficina de cómputos, y la necesidad de planificar el mantenimiento de la continuidad del negocio. La adecuación de la disponibilidad de datos, y no el funcionamiento de la ubicación del *mainframe*, es el factor de éxito más importante a fin de mantener la continuidad de la empresa después de un desastre de los IS y, por lo tanto, los *backups* de datos constituyen un pilar fundamental en cualquier proceso de recuperación. Pero a pesar de que los *backups* son muy importantes, a menudo no se realizan; cuando sí se los hace, no se los pone a prueba, y cuando sí se ponen a prueban, no se almacenan.

Muchos planes de contingencias tratan sólo con un subconjunto de los elementos de IS (a menudo con los sistemas basados en los *mainframes*) y entonces, pocos pueden definirse como planes de "continuidad del negocio". Una de las causas es que el proceso de planificación se delega al especialista de IS, que no se encuentra en posición de juzgar los cronogramas reales. El 80% de los planes de recuperación de desastres fallan la primera vez que se los pone a prueba, y esto a menudo sucede porque se desconocen las interdependencias empresariales. Pero tampoco es únicamente este desconocimiento lo que reduce la efectividad del plan de recuperación. La comercialización electrónica, cada vez mayor, hace que una organización sea vulnerable a los desastres experimentados por los flujos ascendentes y descendentes de la cadena de valor.

Existen dos problemas importantes en la planificación ante desastres: la dificultad de mantenerse actualizado con los ti-

pos de desastre, y la dificultad de mantenerse actualizado con los cronogramas de prioridades. En el Reino Unido, la planificación de la recuperación en cuanto a la continuidad / desastre es bastante pobre y quizás la mayoría de las organizaciones no tengan ningún plan o, si lo tienen, estará desactualizado, no habrá sido puesto a prueba o tendrá un campo de acción limitado. Esta situación se ilustra en la **Figura 13.17**.

Probabilidad de que la organización tenga		Probabilidad de que la organización (con un plan ya probado y efectivo) siga las pruebas iniciales	
• Ningún plan de continuidad	40%	• Nunca	15%
• Un plan vago / irreal	15	• Dentro de 1-2 años	15
• Un plan no puesto a prueba	20	• Entre 6 meses y 1 año	30
• Un plan probado y efectivo	25	• Dentro de los 6 meses	40

Figura 13.17. Perfil de una plan de recuperación empresarial del Reino Unido.

Merry (1992) cita un trabajo de investigación en el que se descubrió que el 84% de las empresas encuenstadas afirmaba tener un plan de recuperación ante desastres, pero sólo el 64% pudo sostener que tenía un plan de recuperación de *oficinas*. Son únicamente estos últimos planes los que incluyen computadoras *desktop*, conexiones de teléfono y de red, y otros servicios relacionados con la computadora. La oficina, y no la sala de cómputos, constituye hoy en día el lugar crítico. Muchas estrategias de recuperación ante desastres y de prevención ignoran este desplazamiento de ubicación. Por ejemplo, el 90% de los *mainframes* se encuentran protegidos por sistemas UPS, pero esta protección sólo alcanza el 6% de las LANs. Para un gran número de organizaciones, la bomba del IRA de abril de 1992 sobre Londres puso en evidencia el valor de los datos almacenados en las computadoras de escritorio. Las máquinas en sí mismas son cada vez más económicas, pero el valor de los sistemas y los datos está en relación con las operaciones "reales" que se realizan basándose en ellos.

Si la empresa no se mantiene operando a corto plazo, la recuperación a largo plazo será, entonces, irrelevante y, por lo tanto, las soluciones inmediatas son críticas para las posibilidades de supervivencia y para los costos generales. Algunos de los distintos tipos de soluciones de mantenimiento son:

- *Instalaciones de emergencia*: en las que todo lo que posibilita el funcionamiento de los IS ya está instalado; permiten una operatividad inmediata, siempre y cuando los backups de datos estén disponibles.

- *Instalaciones intermedias*: un centro de datos, vacío pero equipado, se encuentra disponible. Se utilizan para propósitos generales y, por lo tanto, son menos costosas que las anteriores, pero son más lentas en el funcionamiento de las operaciones, porque necesitan la preparación adecuada *después* del desastre.

- *Instalaciones móviles*: la provisión se realiza desde vehículos o desde edificaciones prefabricadas, semi-móviles. Representan una opción muy aceptada porque pueden ser rápidamente compartidas.

La ola de atentados terroristas durante 1992 modificó no sólo las *percepciones* de valor, sino también la naturaleza de las recuperaciones de emergencia requeridas: de un abastecimiento de *mainframes* a un abastecimiento garantizado de PCs con un software de administración de redes y un software adecuado preinstalado. Los acuerdos de mantenimiento constituyen una estrategia exitosa para las divisiones dentro de un mismo grupo, pero raramente funcionan entre organizaciones independientes porque el socio operante tal vez no está dispuesto a dejar libre las instalaciones o porque él también está afectado. Los desastres importantes siempre representan un problema para los acuerdos de mantenimiento cuando los suscriptores al servicio se ven afectados al mismo tiempo. En los casos en que se realiza un acuerdo de este tipo, la recupera-

ción ante desastres requiere la provisión de un concentrador de comunicación, ya que gran parte del personal depende de sistemas computarizados, portátiles y manuales.

Aunque muchas organizaciones se enfrenten con problemas en el momento de determinar cómo se establecen los planes de contingencia, Bolton (1992), citando a Lloyds, afirma que resulta "evidente" qué es lo que una organización debería hacer. El autor considera que esta lista "evidente" es obligatoria antes de que la organización firme un seguro. Por lo tanto, requiere:

- Defensas y detectores físicos de primera línea
- Backups de datos, software y documentación en un lugar separado
- Hardware de respaldo
- Contratos de mantenimiento completos y confiables
- Reglas para el desarrollo del software y aceptación
- Buenos procedimientos del personal

La planificación de contingencias no puede ser algo que se agrega "después del hecho" y entonces, *todos* los enfoques de desarrollo de los IS deben ofrecer puntos de recuperación. Por ejemplo, los elementos de los IS pueden parcelarse en cajas negras con entradas identificadas que, luego de una falla en la seguridad, puedan reunirse por medios alternativos incluso en forma manual. Este proceso de separación en módulos permite que cualquier elemento de los IS que todavía funcione pueda seguir operando lo mejor posible. Los requisitos de la recuperación presionan a la empresa a fin de lograr la división en módulos, la reestructuación y el *outsourcing* o, por lo menos, el uso de paquetes de software de fácil reemplazo para aplicaciones no críticas. La planificación de contingencias debe considerar detenidamente la naturaleza de todo servicio de respaldo y de su potencial efecto sobre las aplicaciones. La recuperación efectiva planea por adelantado cómo enfrentarse con las incompatibilidades y, una vez más, existe una presión para utilizar los elementos de los IS que se ajusten a los estándares de la industria a fin de reducir la escala de posibles incompatibilidades.

Durante la fase de respaldo, es probable que desaparezcan muchos rasgos del control de la seguridad y de las contra medidas, ya sea porque las operaciones están en una instalación de respaldo en una ubicación diferente o porque el nivel de stress humano es alto. Esto significa que una parte crítica de la planificación de contingencia implica detectar las amenazas que surgen como resultado del mismo proceso de recuperación ante desastres. Por ejemplo, la agrupación manual de datos es más susceptible a errores que la captura de datos automática, y el uso compartido de una instalación de respaldo aumenta la amenaza del acceso no autorizado a los datos. Incluso durante este período de dislocación, deben conservarse la seguridad de los datos requerida legalmente y los procedimientos de auditoría.

La planificación de recuperación ante desastres debe acordar medidas de seguridad adecuadas para todos los elementos fuera del lugar, ya que es probable que el plan de contingencias requiera un uso extensivo de todos los almacenamientos *off-site*, y es imprescindible que el plan en sí mismo esté protegido. Muchos intentos de recuperación han fracasado porque todas las copias del plan de desastres se incendiaron durante el "desastre" o porque las llaves para la caja fuerte a prueba de fuego estaban incineradas al haber sido guardadas en escritorios comunes.

Por su misma naturaleza, el documento del plan de recuperación es específico para cada organización. La mayoría se ocupará en primer lugar de la planificación de respaldo, en donde el énfasis se pone en obtener un método alternativo de operación durante el ínterin. Luego vendrá la planificación de la recuperación, en la que el énfasis estará sobre el modo de recobrarse completamente de una pérdida de seguridad. Hill (1992) ofrece una descripción detallada de diez secciones que, a su criterio, debe contener todo documento para la recuperación (ver **Figura 13.18**).

- **Introducción o índice:** incluyen una breve descripción y resumen del manual: cómo está estructurado, quién posee copias, cómo utilizar el plan, etc.
- **Definición de un desastre informático:** aquí se define con exactitud qué es lo que la empresa denomina desastre, por ejemplo, una pérdida de servicio o una pérdida de ingresos. También se incluye en este capítulo la política de la compañía sobre la planificación ante desastres. El documento debería además definir los niveles de desastre, ya que para cada uno existirá una estrategia de recuperación diferente. Será suficiente identificar cinco niveles, el primero de los cuales puede ser un incendio pequeño, que causa poco daño, mientras que el nivel cinco representará el caso más grave, un incendio que destruya por completo el área de datos.
- **Supuestos:** los planes estarán basados en supuestos que deben ser explicados. Un supuesto puede ser, por ejemplo, que un centro de operaciones apoye, durante un tiempo específico, a todas las aplicaciones críticas, y que todo el personal se encuentre disponible. Estos supuestos deben ponerse a prueba con regularidad.
- **Exclusión de desastre:** pueden existir ciertos tipos de desastres que, debido a su magnitud, no quedan cubiertos por el manual, por ejemplo, un holocausto nuclear. Aun así, las exclusiones deberían estar enumeradas para que no haya dudas sobre los desastres que cubre el plan.
- **Inventarios:** esta sección o capítulo detallará todo el software y el hardware, incluyendo los datos y los equipos de comunicación por voz, que se encuentran cubiertos por el manual de recuperación. Además hay que incluir diagramas de organización del personal, planos de los pisos, vías de entrada y salida, etc. Los niveles de servicio también tienen que figurar en el inventario. En esta sección, se identificarán y enumerarán las aplicaciones críticas, y debe además declararse cuándo los servicios comienzan a recuperarse. Se subrayará también la disponibilidad de sistemas de respaldo, acuerdos contractuales y provisión de equipos de reemplazo. Si la organización necesita satisfacer algún requerimiento legal, aquí debe figurar una sección al respecto.
- **Presupuestos de emergencia:** este capítulo o sección debe detallar con qué urgencia se generarán los flujos de efectivo. Los códigos especiales de presupuesto deben ser identificados de antemano, con auditorías adecuadas para los análisis posteriores al desastre.
- **Alarma:** aquí se especificará cuándo hay que dar la alarma y poner en marcha el plan. En relación con el tipo de desastre, puede haber varios métodos para dar la alarma y para conectarse con el personal clave. Deben definirse los equipos de administración de desastres y además tiene que figurar la estructura organizacional de todos los equipos de recuperación, cuyos planes de acción deben estar presentados con un nivel adecuado de detalles. Estos planes pueden representarse a través de un diagrama que muestre la secuencia lógica de actividades, interdependencias, punto de controles y cronograma.
- **Logística:** sin la planificación logística adecuada existe un alto grado de riesgo de que falle el plan de recuperación ante desastres. Los ejemplos de planificación logística incluyen las secciones de transporte, personal, provisiones, medios, comunicación, acceso y acuerdos de seguridad, servicios, etc.
- **Mantenimiento y puesta a prueba:** aquí se definirá el modo en que el plan será puesto a prueba y mantenido. Este capítulo reviste una vital importancia para cualquier organización que opera en un medio de IS dinámico en donde se realizan cambios continuos del hardware, software y línea de productos. Debe mostrar toda documentación de control del cambio, agendas de mantenimiento, resultados de las pruebas, etc.
- **Apéndices:** el área en la que se deben archivar copias de:
  - Pólizas de seguros
  - Contratos de servicio de terceros
  - Acuerdos con los vendedores
  - Correspondencia importante o útil
  - Resultados del análisis del riesgo

Figura 13.18. Estructura sugerida para el documento de planificación ante desastres.

No sólo los equipos, el software o los datos son los que se pierden en la mayoría de los desastres. Por lo general, todo desastre también incluye los edificios y el personal, y entonces los planes deben identificar el personal clave, a quién contactar durante qué circunstancias, cuáles son los ítems bien almacenados, cuáles son los acuerdos de seguro; en suma, cómo manejar la situación. Independientemente de los aspectos que abarque el plan, el proceso de planificación de contingencias debe brindar una puesta a prueba, un monitoreo y una actualización regular del plan. Esto asegura que éste funcione de acuerdo con los cronogramas de prioridades presentes, y no pasados. Sólo así permitirá el mantenimiento de la continuidad de la empresa.

13.2 • Management y ética de los sistemas de información

En la sección 13.1 hemos considerado de qué forma el management de los IS puede asegurar que dichos sistemas sean seguros. La seguridad de los IS se refiere a mantener su disponibilidad, integridad y confidencialidad. En esta sección se analizarán las responsabilidades legales del manejo de los IS. Sin embargo, el management de los sistemas de información va mucho más allá de la seguridad y las leyes; también es una cuestión de ética. En la sección 13.3 veremos que existe legislación específica que pena determinados comportamientos, como la *Computer Misuse Act* en el Reino Unido (Ley del mal uso de las computadoras). Esto hace que algunos usos de los IS sean delictivos, con lo que se plantea la pregunta de si está "bien" generar un nuevo tipo de delincuente. Como vimos en la sección 13.1, muchos bancos y entidades financieras son renuentes a dar a conocer sus problemas de seguridad por temor a perder la confianza de los clientes. ¿Es "correcto" engañar al público de esta forma? ¿Qué obligaciones tienen las empresas para evitar este tipo de hechos? Estas preguntas se relacionan con la seguridad de los sistemas de información y con las leyes correspondientes, pero son, en primer lugar, cuestiones de ética.