Aproximación @ los riesgos de Internet

MERCEDES MUÑOZ NUÑEZ
GONZALO FERNÁNDEZ ISLA
SUBDIRECCIÓN GENERAL DE RIESGOS, SEGUROS Y CONTINGENCIAS
TELEFÓNICA, S. A.

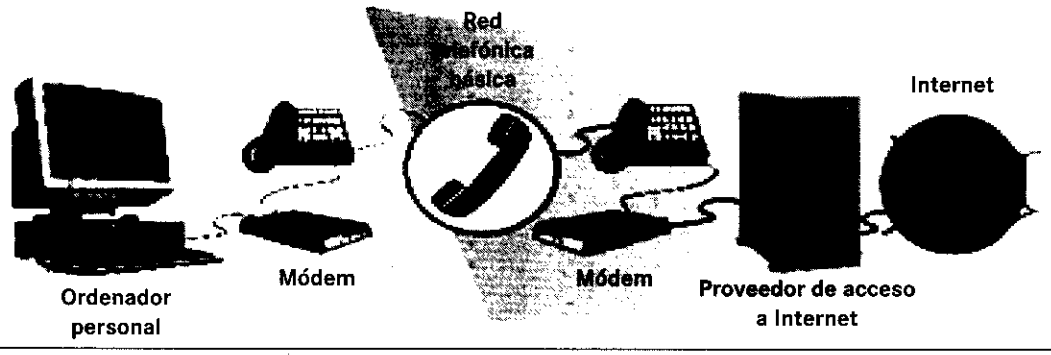
El progreso tecnológico, en los sectores de telecomunicaciones e informática y el rápido crecimiento y expansión de Internet, han propiciado cambios sustanciales en el desarrollo de las empresas (estrategia, imagen, gestión de marcas, productividad, gestión del conocimiento, nueva cadena de valor, nuevos servicios y productos, etc.) y de la estructura económica mundial (integración y/o convergencia sectorial, cambios en el entorno social, nuevas formas de negocio, globalización, etc.).
El objeto de este estudio es efectuar una primera aproximación a los riesgos derivados de la introducción de Internet en las empresas, su análisis e incidencias desde la perspectiva empresarial, así como las alternativas existentes para su reducción, control y financiación.

@ 1. INTERNET Y SUS PRINCIPALES CARACTERÍSTICAS

Internet es una interconexión de redes informáticas (públicas, privadas, empresariales, etc.), que permite a los ordenadores conectados comunicarse directamente. Es decir, es una gigantesca red de redes de ordenadores conectados entre sí (aunque cada uno de ellos funciona de forma autónoma), que les permite compartir información, programas, enviar mensajes etc, con independencia de dónde se encuentren físicamente los usuarios. Esta enorme retícula ya se extiende por el planeta.

También existen sistemas de redes más pequeñas, llamadas Intranet, generalmente destinadas para el uso exclusivo de una organización.

FIGURA 1. COMPONENTES DE LA RED



La facilidad en las **formas** de **comunicación** a través de la **red,** ha permitido el **desarrollo** de **servicios** que **comportan riesgos**, debido a las características de la misma.

- Intercambio de ficheros.
- Intercambio de información.
- Control remoto de otro ordenador-Telnet.
- Correo electrónico (e-mail).
- Grupos de noticias, foros de discusión (web).
- Tertulias escritas a tiempo real (chats).
- Video-conferencias.

Las principales **características** de **Internet,** que se deben **considerar** al realizar un **análisis** de **riesgos** son, *entre otras:*

- No es una red única, planificada como tal desde el principio.
- Es una red descentralizada que se distribuye por cada elemento de Red.
- Los mensajes o ficheros se trocean en paquetes, que se van enviando por las líneas menos usadas en cada momento.
- Se distribuye con una ausencia de jerarquía en la Red:
  - Organización caótica.
  - Organización anárquica.
- Es independiente del tipo de ordenador y de su lugar de ubicación.
- No es una red regulada sino autorregulada, aunque en Europa se está tratando de regular los aspectos relacionados con el Comercio Electrónico.
- No existe un catálogo o clasificación de la información aceptada por todos.

@ 2. IMPACTO DE INTERNET EN LA NUEVA ECONOMÍA

La interacción informática, ha cambiado espectacularmente el mundo en que vivimos, eliminando las barreras del tiempo y la distancia y permitiendo a la gente compartir información y trabajar en colaboración.

Internet por lo tanto, supone un **nuevo modo de hacer negocios** para la empresa, que comporta nuevos riesgos o modificaciones sustanciales en los riesgos existentes, que serán analizados más adelante.

Como señala Negroponte «En la nueva economía se **sustituye el átomo por el bit**», expresión suficientemente gráfica, que nos indica que el valor que circula por Internet es la información. No obstante, en muchos casos, **el átomo** es el elemento de **intercambio final, al menos de momento** (libros, c.d., bienes, alimentos, etc.).

En términos muy genéricos se puede esquematizar este sistema como se recoge en la figura 2, de la siguiente manera:

FIGURA 2. ELEMENTOS DE LA NUEVA ECONOMÍA

La nueva economía se sustenta en tres pilares básicos:

- El uso intensivo de la tecnología (telecomunicaciones, informática, etc.).
- La información y otros intangibles como elementos de valor.
- El ámbito mundial de actuación (Globalización).

a) Pilar tecnológico

En la nueva economía, se requieren capacidades tecnológicas de alcance global y al mismo

tiempo conocer con el máximo detalle, los aspectos más significativos del entorno local (cultura, política, hábitos, etc.), lo que requiere un aprendizaje y transferencia continua en toda la empresa, con las siguientes características:

- Mejorar productividad.
- Diferenciación de la competencia.
- Valor añadido a productos/servicios.
- Fácilmente aplicables y asumidas.
- Implantación en todas las áreas de la empresa.

La empresa, en los moementos iniciales en los que convivan tecnologías diferentes, se siente atrapada en la incertidumbre que romperá cuando la tecnología sea el factor clave en la competitividad.

Internet es un cambio revolucionario (virtual) para la comunicación en la era de los servicios, por los siguientes motivos:

- **Se pierde el control sobre la información.**
- **Es un acceso inmediato a todo tipo de información.**
- **Posibilita la comunicación con quién se quiere y cuando se quiere.**

Pero estos cambios, tienen sus barreras:

- **Capacidad.**
- **Sistemas de acceso.**
- **Coste.**

El objetivo de cualquier medio o red, es llegar a una masa crítica adecuada. Según la tecnología disponible en cada momento, dicho objetivo se reduce temporalmente de forma significativa con los nuevos avances tecnológicos, como se puede apreciar en el cuadro 1.

El acceso a Internet se establece de la forma siguiente:

ACTUAL: Ordenador (coste, complejidad instalación, dificultad de uso para ciertas personas), Teléfonos Móviles.

FUTURO: Múltiples accesos (ordenador, Teléfonos Fijos y Móviles, Televisión, Play Station, Integración de los diferentes sistemas...).

CUADRO 1. TIEMPO PRECISADO POR CADA TECNOLOGÍA PARA LA OBTENCIÓN DE 50 MILLONES DE CLIENTES

Tecnología	Años	Plazo
• Teléfono	25	1920-1945
• Radio	38	1922-1960
• TV	13	1951-1964
• Cable	10	1976-1986
• WWW	5	1993-1998

b) Pilares Intangibles

Se consideran como principales pilares intangibles, además de la información los siguientes:

- **Relaciones con los consumidores y proveedores.**
- **Marcas.**
- **Propiedad Intelectual.**

Dichos **pilares** nos ofrecen nuevos **activos y elementos** sobre los que centrar el **análisis de riesgos.**

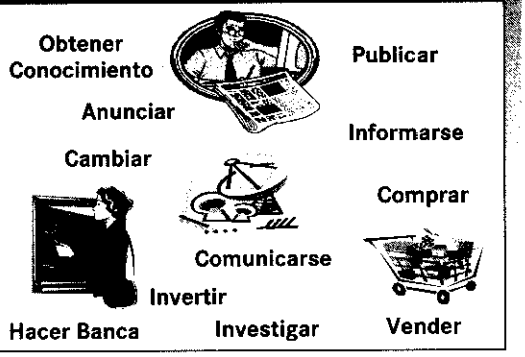
c) La Globalización

Es la posibilidad de interactuar simultáneamente en cualquier lugar del mundo, en cualquier mercado, esbleciendo relaciones complejas en los intercambios que comportan riesgos adicionales a tomar en consideración.

SERVICIOS DE INTERNET: E-BUSINESS/E-COMMERCE

Los servicios que se ofrecen en la Red son innumerables, entre empresas: compras virtuales (en supermercados, librerías, tiendas de informática, plataformas sectoriales verticales, etc.), visitas guiadas (a museos, reservas naturales, países...), acceso a la prensa diaria, televisiones, radios, agencias de noticias..., consultas (en bibliotecas, universidades, centros de investigación...), reservas (de billetes de avión, de tren, de autobús...), y prácticamente todo lo que se pueda imaginar.

FIGURA 3. INTERNET MÁXIMO EXPONENTE DE LA GLOBALIZACIÓN



La relación e intercambio con los clientes se realiza fundamentalmente a través de las websites, que se clasifican en:

- Pasiva = Información acerca de la empresa.
- Interactiva = El cliente puede intercambiar información.
- Activas = Cliente puede realizar servicios de compra/venta.

Se considera que **comercio electrónico** es cualquier tipo de transacción comercial, en la cual las contrapartes involucradas interactúan a través de medios electrónicos.

Los modelos básicos del Comercio Electrónico (E-commerce) son:

- **B2B = Business to business.**
- **B2C = Business to consumer.**
- **B2E = Business to employee.**
- **B2M = Business to mobile.**
- **C2C = Consumer to consumer.**
- **C2B = Consumer to business.**

FIGURA 3. IMPACTO DEL COMERCIO ELECTRÓNICO

La evolución y desarrollo de los intercambios en la red, se podrían resumir como sigue:

– SITUACIÓN ACTUAL

En la actualidad existen:

- **Más de 1.000 millones de páginas Web.**
- **15.719.462 sitios por dominio.**

Cada año:

- **Se envían 7 billones de correos electrónicos.**
- **Se conectan entre sí más de 275 millones de personas.**

– A CORTO Y MEDIO PLAZO

Perspectivas de futuro

2002 Previsión 490 millones de internautas y el volumen total de comercio en Internet alcance 215.000 millones de pesetas (1.200 millones de euros, 1,1 billones de $US).

2003 Previsión 795 millones de internautas.

2004 Según Gatner Consulting Group, se alcanzarán los 1,4 billones de pesetas (8.400 millones de euros, 7,29 billones de Dólares USA), de intercambio a través del comercio electrónico.

2005 Previsión 1.000 millones de internautas.

CADA **100 DÍAS** se dobla el número de internautas y se crean cada **HORA** 65 millones de páginas/web, si bien la previsión es que este crecimiento disminuirá paulatinamente.

El gran **desafío** que en pocos años se verá cumplido es la **integración** de Internet con la **televisión**. Un solo monitor bastará para ver películas, hacer compras, trabajar en casa o realizar una llamada de teléfono viendo a nuestro interlocutor.

@ 3. VISIÓN GLOBAL DE LA GERENCIA DE RIESGOS

La Gerencia de Riesgos es la aplicación multidisciplinar del método científico, al espacio uni-

versal de los riesgos derivados del desarrollo de cualquier actividad por parte de las empresas, individuos y administraciones públicas, que se apoya como elemento fundamental en el **análisis de riesgos,** es decir, en la estimación y cuantificación de los riesgos implícitos en cualquiera de las actividades desarrolladas y en los recursos utilizados para llevar a cabo las mismas, considerando también su obtención, combinación, etc.

El Gerente de Riesgos, por tanto, deberá encontrarse siempre en disposición de dar respuesta inmediata a los problemas que la evolución de la sociedad trae consigo, como por ejemplo nuevos riesgos o un mayor número de riesgos a los que hacer frente, lo que obliga a su vez a estudiar nuevas formas de reducción, control y de financiación de los mismos, señalando en cada momento y en cada caso los instrumentos más adecuados desde su punto de vista, para ofrecer soluciones eficaces y oportunas en el tiempo.

Al gestionar los riesgos de una empresa, el Gerente de Riesgos deberá tender cada vez más hacia una gestión global, incluso a salirse de los límites clásicos, con el fin de establecer una política adecuada a cada una de las categorías del riesgo.

3.1. Identificación, análisis y evaluación de los riesgos

Cuando un empresario se enfrenta al estudio de los riesgos a los que está expuesta su empresa, debe tomar en consideración todas las fases de **identificación, análisis y cuantificación de las pérdidas** potenciales, que los distintos eventos pueden producir en su patrimonio, estableciendo medidas de control de los riesgos mediante **la implantación** de sistemas de **prevención y protección** para eliminar la causa productora del daño o al menos reducir sus consecuencias.

Si nos centramos en la identificación y análisis de riesgos de Internet, se deben acotar los Grupos de Riesgo (por su fuente de origen), Grupo de Sujetos y Efectos o Consecuencias, como se recoge en el cuadro 2.

Los riesgos vinculados a las **nuevas tecnologías,** se incluyen dentro de la categoría de los denominados **riesgos dinámicos,** caracterizados

CUADRO 2. GRUPOS DE ACTORES PROTAGONISTAS DE LOS RIESGOS

Grupos de riesgo	Grupos de sujetos	Consecuencias (pérdidas)
• Naturales • Humanos • Tecnológicos	• Personal propio • Activos materiales • Activos inmateriales • Personas y activos de terceros	• Producción • Ventas • Imagen • Cuota de mercado • Reclamaciones • Vidas • Activos

por obedecer a fenómenos que **evolucionan tan rápida e imprevisiblemente,** que hacen totalmente imposible su previsión, ya que en el instante cero **son casi inapreciables,** inexistentes y **cuando se manifiestan** al cabo del tiempo, **las pérdidas** ocasionadas por los mismos **son sumamente elevadas.**

Para **analizar** los **riesgos** vinculados con **Internet,** teniendo en cuenta lo antes señalado, es preciso considerar los **activos expuestos** (los que se quieren analizar: Home Pages, no disponibilidad de servicios, hardware, software, información, datos, otros activos físicos), **las amenazas** (ataques a los activos) y **las vulnerabilidades** (debilidades específicas), que se pueden dar en las actividades analizadas.

Todo ello nos ayudará a definir el nivel de riesgo o riesgos potenciales, además de determinar la no disponibilidad, destrucción, revelación y modificación de los activos antes señalados.

A partir de ese momento, habrá que actuar en dos sentidos: Adopción de medidas de **Prevención,** Detección o recuperación y **análisis coste beneficio** para definir si se **asume** o se **transfiere** el **riesgo,** tal y como veremos más adelante.

Además de los métodos más tradicionales de identificación, análisis y evaluación de riesgos, en

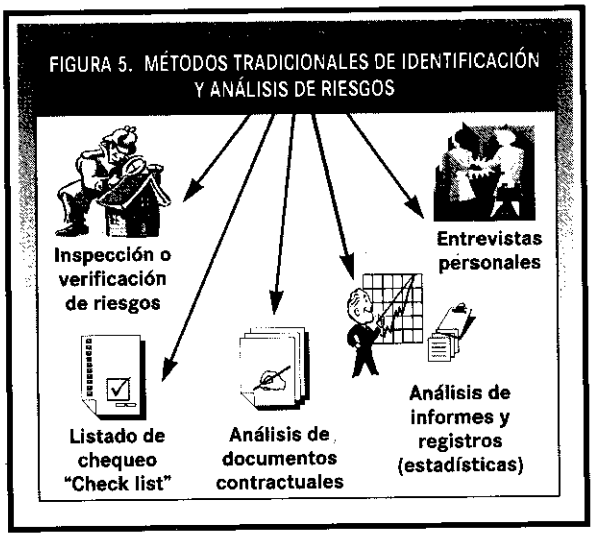


FIGURA 5. MÉTODOS TRADICIONALES DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

el ámbito informático y de Internet, se suele utilizar la **metodología CRAMM** (disponible en software), si bien es sumamente compleja y costosa, ya que establece **relaciones matriciales** entre los **activos** (para los que genera un cuestionario que se ha de superar positivamente), los diversos tipos de **amenazas** que pueden afectar a los mismos y las diferentes **vulnerabilidades** que puedan existir.

Las ventajas que tiene, es que una vez que se ha introducido la información el software **facilita** el **nivel de riesgo por activo** y las **medidas óptimas** a implantar en **prevención, protección** y **seguridad,** además de facilitar un número significativo de **contramedidas.**

Los inconvenientes son: Alto coste de implantación y mantenimiento y gran esfuerzo para alcanzar los resultados.

Existen empresas como IBM Global Services que a través de su servicio «Internet Emergency Response Service», analiza tanto para Internet como para Intranet y Extranet, entre otros, lo siguiente:

- Protocolos no seguros accesibles por Internet (incluyendo sistema de archivo de red, protocolo de transferencia de activos, comandos «r» BERKLEY, etc.).
- Aplicaciones de Software accesibles vía Internet (versiones no actualizadas, versiones con «parches» de seguridad, etc.).
- Errores de configuración del servidor WORLD WIDE WEB (WWW), que permiten el acceso a archivos externos al servicio Web, el uso de passwords de administración, etc.
- Problemas con WWW Common Gateway Interface (CGI), por ejemplo: Uso de programas con reconocidos fallos de seguridad, errores de configuración, etc.

En **otros** casos el **análisis** se basa en la **definición** de **escenarios** de siniestros y la **aplicación** de **modelos** como los siguientes:

- What if?
- Causa-efecto.
- Análisis de fallos.
- Árboles de decisión.
- Etc...

Además sería **conveniente** disponer de los **informes** de las **auditorías** de **seguridad lógica** e **informática.**

En Internet y en otros entornos informáticos y de telecomunicaciones, se debe tener en cuenta también la **criticidad** de los **impactos** (consecuencias), desde el punto de vista de la:

- confidencialidad
- integridad
- disponibilidad
- fiabilidad
- acceso
- datos personales.

Aplicando la metodología antes expuesta a los diferentes servicios de Internet, se podría obtener una primera clasificación de los riesgos, pero que antes de exponerla, para una mejor visualización de los mismos, se caracterizarán previamente las principales amenazas de forma genérica.

3.2. Características de las principales amenazas en Internet

Sólo el 25 por ciento de las incidencias en la red se deben a:

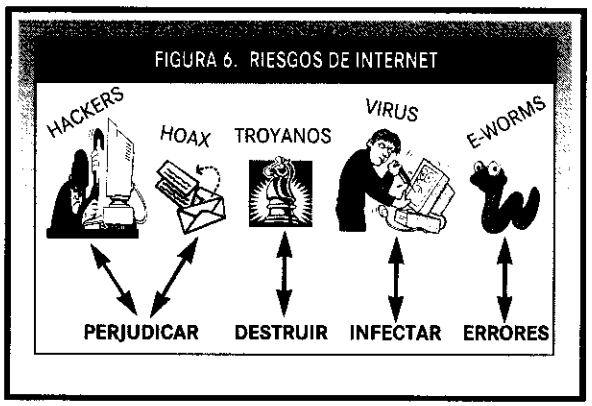
- Piratas informáticos (Hackers).

- Virus.
- e-worms.
- Troyanos.
- Hoax.

Más del 75 por ciento de las incidencias en la red se deben:

- Empleados/ex-empleados.
- Proveedores.
- Suministradores.
- Contratistas.
- Competidores.
- Clientes insatisfechos.

No se va a plasmar el análisis de los objetivos y fines del 75 por ciento de las incidencias en la red, por parecer casi obvios. Sin embargo, dado el carácter divulgativo del artículo, sí se efectuará una aproximación al 25 por ciento restante, que, desde una perspectiva externa no especializada, se identifica como si éstas fueran las amenazas más significativas, sobre todo gracias a la difusión que tienen a través de los medios de comunicación.



3.2.1. Hackers

Son individuos que dominan la tecnología informática y las comunicaciones utilizándola con diversos fines:

a) Aventura:

- Burla de sistemas de Seguridad.
- Juegos de inteligencia/Habilidad/conocimiento.

b) Perjudicar a terceros: sin o con beneficio propio.

- Mal uso o uso indebido de la red.
- Interrupción de negocios.
- Robos de datos.
- Realización de fraudes y otros delitos.
- Bombardeo a través de ordenadores esclavos.

c) ¿Cómo actúan?

Normalmente su acceso no autorizado a datos y la interrupción de mensajes y transacciones, suelen estar motivados por:

- Existencia de herramientas duales.
- Falta de encriptación o utilización de algoritmos no seguros.
- Presupuestos insuficientes para la seguridad lógica.
- Uso de hardware inadecuado o inexistencia de cortafuegos de seguridad.

3.2.2. Virus

Programa informático que se adhiere a otros programas provocando una serie de modificaciones:

a) Pueden infectar:

- Ficheros exe.
- Archivos DLL.
- Panel de Control CPL.
- Salvaportables SCR.
- Componentes del Hardware-BIOS.

Pueden:

- Residir en la memoria del sistema.
- Estar encriptados.
- Tener una activación espectacular.

b) Pueden ser:

- Macros: Secuencia de instrucciones para automatizar una serie de procesos en determinados programas de una aplicación.

3.2.3. e-Worms

Son programas que llegan como fichero adjunto a un e-mail que si se ejecuta da lugar a errores u otros problemas.

3.2.4. Troyallos (Caballo de Troya)

Son aplicaciones Kits de control remoto destinadas a:

- Destruir información (tradicionales).
- Robar contraseñas.
- Sustraer datos confidenciales.
- *Ejecutar o borrar programas.*
- Controlar otros ordenadores.
- Enviar y recibir archivos.
- Volcar contenidos.
- Colgar el ordenador.
- Colgar conexión a Internet.

3.2.5. Hoax

Son mensajes que se envían a través de Internet, utilizando terminología técnica para así *mejor difundir y extender falsos rumores* que pueden causar graves perjuicios.

@ 4. PRINCIPALES RIESGOS QUE SE PUEDEN PRODUCIR A TRAVÉS DE INTERNET

Una primera relación de los riesgos, que previamente se han identificado, analizado y evaluado podría ser la siguiente:

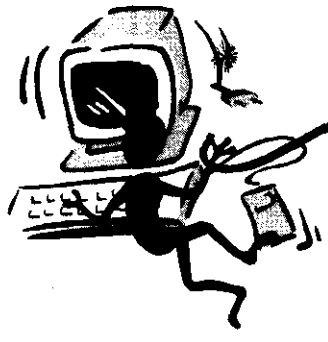
4.1. Infracciones y/o violaciones:

- Derechos de autor.
- Propiedad intelectual (Registros de Dominio, software, etc.).
- Marca comercial.
- Patente.
- Difamación (libelo o calumnia).
- Publicidad engañosa.
- Competencia desleal.
- Inclusión en la web de sentencias judiciales no autorizadas.

CUADRO 3. INCIDENCIA CUANTITATIVA DE ALGUNOS DE ESTOS RIESGOS

INTENSIDAD O CUANTÍA DEL RIESGO

* **„I-Love-You-Virus" causó daños > 1 bln. U$ en los E.E.U.U. y > 50 Mio U$ en Alemania**
* **Una compañía Aseguradora pagó 250.000 U$ por el análisis interno „anti-virus" por causa del „I-Love-You-Virus"**
* **gastos de reposición por megabite de datos están estimados en 5.000 U$**
* **gastos promedio de infección de virus: 8.000 U$ (KPMG análisis 9/98)**



DoS (Denial Of Service) ataques han bloqueado CNN, Yahoo y Amazon durante horas y han reducido la cotización de acciones en un 15%

El servicio de teléfono no funcionó durante horas para 2 millones de clientes en París

- Violación de la privacidad (Espionaje a través de la red, cookies, marketing no consentido, bases de datos, correo electrónico en la empresa, etc.).
- Acceso no autorizado.
- Extorsión basada en acceso no autorizado.
- Robo de propiedad intelectual.
- Falsa información.
- Falta de pago de impuestos derivados de ventas en la red.
- Regulaciones legales, en relación con la venta de productos.
- Transacciones vinculadas con las regulaciones de las bolsas.
- Fraude o fallos en certificados digitales o firma electrónica.
- Fraude o estafa al consumidor.
- Anulación, cancelación, rechazo o denegación de acceso.
- Destrucción, retirada o alteración de cualquier publicidad o dato.
- Uso indebido o no autorizado de caracteres y objetos de productos.
- Por falta de licencia.
- Plagio.
- Negligent statement.
- Apropiación indebida de datos.
- Errores en el manejo de sistemas de información.
- Errores en el manejo o diseño del software empleado.
- Captura indebida de literales.
- Uso de metatags y Links que perjudican los intereses de los propietarios de marcas.
- Secretos comerciales.
- Acuerdos comerciales.
- Acuerdos de confidencialidad.
- Realización de actividades ilegales y/o ilícitas.
- Fraude en ordenadores.

4.2. Pérdidas de:

- Fondos.
- Ingresos.
- Cuota de mercado.
- Imagen.
- Oportunidades.

Por:

- Fraude o error.
- Extorsión.
- Caídas de red.
- Falta de suministro eléctrico.
- Incapacidad de realizar el proceso o atender pedidos.
- Incapacidad para verificar o realizar cobros.
- Impago de los bienes comprados/vendidos.
- Uso fraudulento de tarjetas.
- Captura y/o uso no autorizado de tarjetas y otra información.
- Errores en los servicios o productos prestados o suministrados.
- Realización de actos vandálicos.
- Infidelidad de empleados.

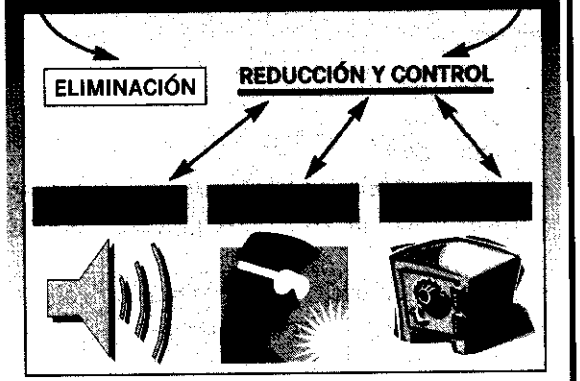
5.3. Aumento de costes o gastos

- Reobtención/recuperación.
- Sanciones.
- Reemprender actividad.
- Por responsabilidad frente a terceros.
- Publicidad defensiva.
- Devoluciones de bienes dentro de los 15 días de aceptación del consumidor.
- Otras.

@ 5. REDUCCIÓN Y CONTROL DE RIESGOS

La relación de riesgos antes señalada en el punto 5, puede ver eliminados ciertos riesgos y/o reducir su frecuencia e intensidad, si se aplica un correcto tratamiento de los mismos, tanto desde el punto de vista organizativo como preventivo y de gestión de crisis. En el caso de Internet y teniendo en cuenta las características de la Red, sería conveniente distinguir los aspectos legales del resto de medidas de prevención, protección y seguridad.

FIGURA 7. TRATAMIENTO DE LOS RIESGOS



5.1. Aspectos legales

Los negocios de Internet pueden estar sujetos a **múltiples jurisdicciones** y uno de los aspectos más complejos, es qué legislación procede aplicar en cada caso; normalmente la jurisdicción se determina en función de la interactividad y de la naturaleza del intercambio comercial.

Internet no está regulada salvo por las asociaciones de internautas en Estados Unidos, que propugnan la autorregulación como la Federal Trade Comisión, etc. Otras reconocen las firmas y los certificados electrónicos, cuyo alcance difiere de unos estados a otros. No obstante, existen regulaciones sobre: Patentes, Marcas, Privacidad (reciente), etc. En la Unión Europea existe una mayor regulación.

Por su posible interés, se señala a continuación los aspectos más significativos de la Directiva sobre Comercio Electrónico.

CUADRO 4. MARCO LEGAL EN LA UNIÓN EUROPEA

• Patentes - Marcas	• Certificación electrónica
• Derechos de Autor	• Comercio electrónico *(Directiva 2000/31/CE 8 de junio)*
• Protección datos personales	
• Consumidores y usuarios	• Contratos de venta a distancia
• Firma electrónica	• Advertising (Publicidad)

- **Objetivo:**

Contribuir al correcto funcionamiento del mercado interior, garantizando la libre circulación de los servicios en la Economía Virtual (Sociedad de la Información).

- **Regulará:**
  - Establecimiento de los Proveedores de Servicios (ISP).
  - Las Comunicaciones Comerciales.
  - La Responsabilidad de los Intermediarios.
  - Los Acuerdos Extrajudiciales.
  - Los Recursos Judiciales.
- **No se aplicará en:**
  - Materia de Fiscalidad.
  - Actividades de Notarios.
  - Juegos de Azar.
  - Derechos de Autor, etc.

5.2. Elementos preventivos

Los principales elementos preventivos a considerar los siguientes:

- Uso de contraseñas, cortafuegos.
- Encriptación de la información.
- Evaluaciones regulares de Seguridad lógica, Informática y Física.
- Pautas de actuación ante extorsiones.
- Criterios de actuación para uso de Internet y correo electrónico.
- Procedimientos antipiratería.
- Revisión periódica de datos.
- Formación de empleados.
- Control de noticias e imagen de marca.
- Aplicación de métodos casuísticos (árboles de decisión).
- Plan de contingencias global.
- Solicitud de derechos de uso de propiedad intelectual (contenidos).
- Actuaciones previas antes de registrar cualquier marca o patente.

Además de las medidas tradicionales de Prevención, Protección y Seguridad, se pueden o deben llevar a cabo otras actuaciones de carácter

preventivo, además de las meramente organizativas, que pueden ayudar a aminorar las consecuencias, reclamaciones y/o pérdidas para la empresa. Así se podrían aplicar por ejemplo:

- Transferencia contractual de riesgos.
- Establecer «disclaimers» o elusiones de responsabilidad, etc.

5.3. Otros aspectos a considerar:

La pérdida de empleados, sobre todo de aquéllos que se marchan a la competencia, divulgando los conocimientos que ellos han desarrollado o contribuido a desarrollar, puede ser muy crítica para la empresa, puesto que pueden conocer las vulnerabilidades de la misma.

También se deben tener en cuenta las actuaciones preventivas, a implementar ante situaciones cómo: Imposibilidad de acceso a los datos por no poder descifrar el código o la clave, por olvido o por actos intencionados, que impedirían el normal desenvolvimiento de la actividad de la empresa.

@ 6. FINANCIACIÓN DEL RIESGO

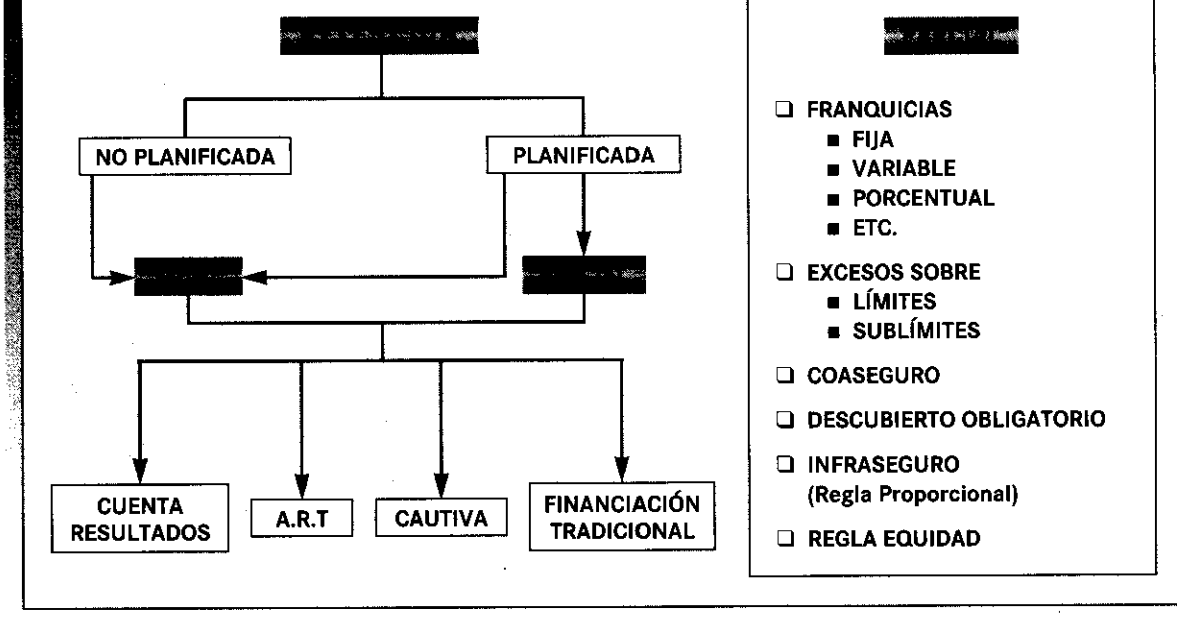
A pesar de realizar correctamente las fases anteriores, en ciertas ocasiones resultará imposible eliminar o controlar (reducir frecuencia y/o intensidad) las causas que pueden originar un siniestro.

En este caso, nos encontraremos ante la **dicotomía** de **cómo financiar** las **pérdidas** potenciales, que se puede resolver efectuando un análisis coste/beneficio sobre las siguientes alternativas:

6.1. Retención de riesgos

El riesgo residual de pérdidas, resultante una vez adoptadas las medidas de control y/o eliminación de riesgos, puede ser atendido con las capacidades financieras propias de la empresa (Cash Flow, etc.), decisión conocida como Retención (Asunción) de Riesgos, de la que sólo se expone el esquema de la figura 8, sin entrar en un análisis más pormenorizado.

FIGURA 8. FUNDAMENTOS Y FORMULAS DE RETENCIÓN



6.2. Transferencia del riesgo

Consiste en transmitir el riesgo, normalmente a una compañía aseguradora. Desde un punto de vista general, el Seguro es una actividad económico-financiera que presta el servicio de transformación de los riesgos de diversa naturaleza, (situación de incertidumbre), en un gasto periódico presupuestable (pérdida cierta).

FIGURA 9. TRANSFERENCIA DE RIESGOS

Existen diversas alternativas para transferir al mercado asegurador los riesgos que se pueden producir a través de Internet, con diferentes matizaciones según la segmentación geográfica de los mercados.

En términos generales el sector asegurador da diversas respuestas:

- Para algunos de los tipos de RIESGOS vistos anteriormente, existe cobertura en las pólizas estándar de **Responsabilidad Civil General,** aunque ésta puede ser limitada –derechos de autor, violación del derecho de privacidad de las personas, difamación a personas, bienes o servicios (oral o escrito, si existe publicación material que la recoge)–.
- Otras tipologías de riesgos se cubren a través **de pólizas Multimedia** o de pólizas de Responsabilidad Civil Profesional para Grupos Media –derechos de autor, patentes, marcas, plagio, uso no autorizado de: títulos, formatos, ideas, caracteres, presentaciones artísticas, programas, inversión de la privacidad, libelo, calumnia y otras formas de difamación–.
- En otros casos a través de las pólizas específicas de **comercio electrónico** (e-commerce) o cyberlialility de **Propiedad Intelectual** (derechos de autor, patentes, marcas, etc.).
- Otras coberturas se pueden encontrar en pólizas **E&O** (Errores y Omisiones).
- Otras son específicas de **Daños Materiales y Pérdida de Beneficios.**
- Otras garantías se recogen en pólizas de Fraude de Transferencia de Fondos o las pólizas CRIME (fraude e infidelidad).

No obstante, sería conveniente que cada empresa efectuara su análisis de riesgos específico y una vez reducido y/o eliminado el riesgo, definiera su esquema de financiación de pérdidas y, en su caso, si decide transferir el riesgo, que diseñe el producto que precisa o al menos defina claramente sus necesidades, apoyándose en asesores externos, si es preciso, y contando con los principales actores del mercado (aseguradores y mediadores). Solo así la empresa podrá gestionar de forma eficiente sus recursos, añadiendo valor a sus accionistas presentes y futuros y garantizar la continuidad de la gestión.

@ 7. ADMINISTRACIÓN Y POLÍTICA DE RIESGOS

No sería prudente concluir este estudio, sin hacer referencia a dos elementos de singular importancia en la Gerencia de Riesgos: Administración y Política.

Estas fases, por sus características, son independientes de la vinculación del riesgo a Internet o no, su aplicación a la Red es válida e imprescindible para adaptar el modelo de gestión en cada momento según los resultados deseados de la organización.

La administración de riesgos, estará vinculada con la definición de:

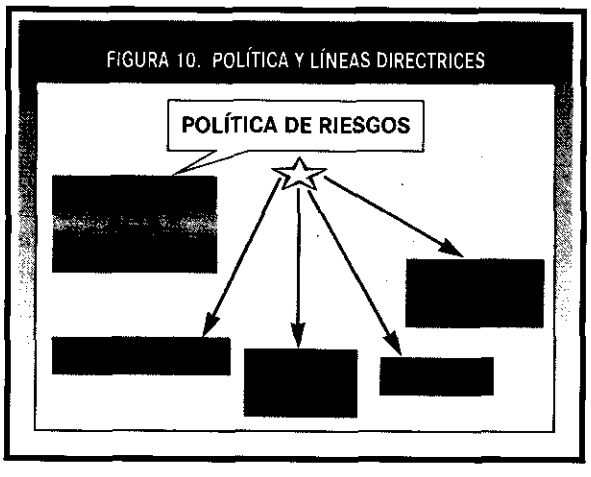
- Canales de comunicación.
- Procedimientos de actuación (Normativas).
- Sistemas de información.
- Medición de resultados.
- Elaboración de estadísticas e informes.
- Proceso de Toma de Decisiones.

En base a lo antes señalado, podremos definir o realimentar la «Política de Riesgos» de la empresa, en relación a sus pérdidas potenciales (operativas, financieras, comerciales, accidentales, etc.), es decir:

- Sus líneas generales de actuación para desarrollar la estrategia y alcanzar la meta fijada.
- Los objetivos o fines hacia los que la empresa dirige sus actividades.
- Los planes y presupuestos para alcanzar los objetivos.
- La asignación de los deberes y responsabilidades específicos para llevarla a cabo.
- Las pautas sobre el nivel de riesgo asumible y la medición del grado de cumplimiento y su revisión.
- La responsabilidad final del C.R.O. (Chief Risk Officer).

Las relaciones de interdependencia existentes en el sistema empresa, se manifiestan también en la Gerencia de Riesgos; cualquier cambio en la empresa (recursos, procesos, tecnologías, etc.), repercuten en sus fines y objetivos y en su pérdidas potenciales, sólo la actuación global y coordinada, garantizará para sus accionistas, empleados, clientes, proveedores, etc., su patrimonio, su cuenta de resultados y en su caso su continuidad.

FIGURA 10. POLÍTICA Y LÍNEAS DIRECTRICES



@ 8. CONCLUSIONES

- Las nuevas tecnologías son un motor de competitividad y aumento de la productividad para las empresas.
- Determinadas nuevas tecnologías, difuminan las diferenciaciones entre ciertos sectores y mercados, haciéndoles converger.
- Aplicaciones concretas de la tecnología, como Internet, comportan riesgos, cuyo análisis requiere un estudio profundo según el negocio o negocios que aborde la empresa y cómo los lleve a cabo.
- El mundo está inmerso en el desarrollo de una nueva economía basada en mercados virtuales desarrollados a través de Internet.
- Internet es una red no regulada de intercambios, creciendo éstos exponencialmente, que puede ayudar a aumentar la competitividad de las empresas y su productividad.
- El desarrollo del mercado virtual requiere conocer el medio y los riesgos vinculados al mismo.
- Tan importante como la identificación, análisis y evaluación de riesgos en Internet, es la adopción de medidas de prevención, protección y seguridad en los aspectos relacionados con la misma.
- El mercado de seguros ofrece alternativas para la transferencia de riesgos.
- Se prevé un favorable desarrollo de nuevos seguros que atiendan a las necesidades reales de las empresas, supeditado a un mejor conocimiento del comportamiento de los riesgos.

- El establecimiento de un sistema de gestión e información global, es imprescindible para que la empresa adopte decisiones coherentes con su situación, meta y objetivos.
- La definición y difusión de la Política de Riesgos de la empresa o Grupo de empresas, con unos objetivos claros y precisos es el elemento que permitirá alcanzar las metas establecidas por la organización.

Estamos construyendo y regulando en algunos casos, nuestro futuro ya presente. Todos debemos aportar nuestro esfuerzo para que sea positivo y fructífero.

@ 9. BIBLIOGRAFÍA

Aon Gil y Carvajal: *Seguro de Actividades Electrónicas*, febrero 2001.

Carpio, Manuel: «¿Es posible la gestión de e-riesgos?», *AGERS* 12°, Madrid, 2000.

Enciclopledia Microsoft - Encarta 2000.

«Encuesta de empresas de EE.UU. y Europa», The St. Paul, Marzo, 2001.

Ernest & Young: «Responsabilidad de los empresarios en la nueva economía», *Expansión* 12, 2000.

Fernández Isla, Gonzalo: *Nuevas Tecnologías, Nuevos Riesgos*, Madrid, abril de 2000.

–: *Visión Global de la Gerencia de Riesgos*, Tenerife, mayo 2000.

–: *Internet Visión Global*, Italia, junio 2000.

–: *Regulación, Riesgos y Transferencia*, Madrid, noviembre de 2000.

Iturmendi Morales, Gonzalo: «Riesgos de Responsabilidad Civil en Internet», *AGERS* 12°, 2000.

«La Cautela de las aseguradoras», *Actualidad Económica*, marzo de 2001.

«La RC. del E-business», *Actualidad Aseguradora*, noviembre de 2000.

Lucas, José A.: *Internet desde el punto de vista Jurídico*, Madrid, noviembre de 2000.

Manso Colomo, Emilio: *El Seguro ante las nuevas tecnologías*, Madrid, noviembre de 2000.

Reed, Michael: «Comercio electrónico», *AGERS* 12°, Madrid, 2000.

«Seguro contra hackers de Itaú», *BDS*, América Latina, octubre 2000.

Seminario Gerencia de Riesgos y Seguros, MAPFRE, Cursos 2000/2001.

Settembrino, F.: «Cyber-Risk», *AGERS* 12°, Madrid, 2000.

TELA, «Virus Informáticos; Seguro de Equipos Electrónicos», Madrid, junio 2000.

Villar Maderuelo, Fernando: *Counterpane Internet Security*, junio 2000.

Webs especializadas en ciber-riesgos consultadas:

www.ssbb.com/control.html
www.mcm.com/views/oellrich.shtml
www.cybercrimes.net
www.calco.com/html/cyberliability.htm
www.upside.com/Upside Counsel/39452f350.html
www.marshweb.com
www.isn.ethz.ch/crn/issueareas/index.cfm