

IMPLANTACION ORGANIZACIONAL DE ICT'S: NUEVOS FACTORES DE RIESGO TECNOLÓGICO.

M^a Teresa Areitio
Dpto. de Economía Industrial
Universidad del País Vasco. UPV/EHU.

ABSTRACT

En esta ponencia, ante la situación actual y futura que se está gestando en los entornos empresariales, se pretende abordar frontalmente el problema fundamental de la aplicación incontrolada (en sus aspectos de seguridad, confidencialidad, integridad, etc.,) de las herramientas informáticas a nivel empresarial, el rechazo a cuestionar la orientación de la utilización de tales nuevas tecnologías y su importancia como factor de transformación socio-económica.

PLANTEAMIENTOS INICIALES.

Actualmente el progreso de las tecnologías de la información y las comunicaciones (ICT) puede considerarse como uno de los grandes factores de innovación a nivel organizacional. Se han creado potentes sistemas capaces de almacenar, procesar y transmitir a gran velocidad enormes cantidades de información. La introducción masiva de los sistemas de información en el mundo de los negocios, la industria, el comercio y la Administración, hace posible una mayor velocidad en las transacciones bancarias (uso de tarjetas de crédito, servicios bancarios desde el domicilio, consultas a voluminosos bancos de datos donde pueden obtenerse datos casi instantáneamente,...), la resolución de complejos problemas estadísticos de análisis de mercados, control de inventarios, la emulación del análisis que realizan los expertos ante problemas determinados (sistemas expertos) y un sinnúmero de tratamientos que no por ser cotidianos dejan de ser complejos.

La naturaleza de este progreso tecnológico es, por tanto, uno de los mayores desafíos actuales, pero también del mañana. Vemos, como diversas acciones colectivas testimonian el agravamiento de las exigencias que pesan sobre la vida económica; el llamado "chantaje tecnológico", la pretendida imposibilidad técnica de garantizar la seguridad; y más allá, el cuestionamiento creciente del trabajo parcelario, del denominado "imperialismo" de la telemática y del peligro aparente que hace correr a las libertades individuales y colectivas.

Como cualquier otra nueva tecnología, los computadores dentro del ámbito empresarial están suscitando cuestiones importantes sobre el nivel al que se debería controlar a la tecnología y por parte de quién debería realizarse dicho control. Incluso las más recientes tecnologías, por ejemplo los sistemas de imágenes, pueden tener consecuencias sobre la integridad de los documentos legales y financieros, y sin duda, están provocando los mismos tipos de cuestiones complejas.

La información debe verse como un recurso más de la empresa y como tal debe administrarse y gestionarse. Es un hecho que estamos ante una nueva etapa de la evolución de la Economía mundial en la que, potencialmente,

las actividades relacionadas con la información van a ser uno de los motores principales de la generación de riqueza y empleo. La información atraviesa horizontal y verticalmente a toda Organización y por tanto es una cuestión clave establecer las normas de fiabilidad de la información, máxime si está siendo o va a ser almacenada, procesada o modificada por medios informáticos.

Gasto per capita en ICT

	1991	1992	1993	1994
Austria	635	678	721	760
Belgica/Luxemburgo	627	653	677	711
Dinamarca	902	917	959	1.019
Finlandia	566	553	583	613
Francia	722	750	773	813
Alemania	845	914	935	964
Grecia	142	152	169	188
Irlanda	483	501	523	549
Italia	436	460	470	490
Holanda	759	776	803	842
Noruega	994	1.024	1.089	1.149
Portugal	214	246	275	309
España	332	333	332	341
Suecia	986	979	1.025	1.076
Suiza	1.545	1.590	1.608	1.673
Reino Unido	704	719	748	787
UE + EFTA	652	682	703	735
EEUU	1.086	1.124	1.165	1.217
Japon	1.010	1.106	1.102	1.152

Fuente: Computing España (Sep 95)

(Cifras en ecus)

Conforme los actuales sistemas informáticos han ido aumentando en complejidad, han puesto de manifiesto una mayor cantidad de elementos vulnerables desde el punto de vista de la Seguridad de la Información. Es un hecho, que hoy en día, existen más puntos vulnerables y mayor facilidad para llevar adelante un ataque contra ellos. Existen varias razones para ello, entre otras:

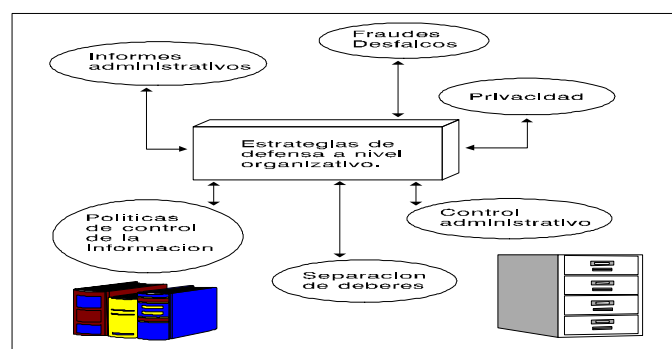
- * El enorme aliciente que supone la posibilidad de obtener a corto plazo grandes beneficios (económicos, de mercado,...), vulnerando la información de todo tipo que circula por una Organización (espionaje industrial, ataques a redes bancarias,...).
- * El hecho de existir medios disponibles para llevar a cabo tales acciones, medios éstos tan sofisticados como los propios sistemas, ya que tienen en muchos casos el mismo origen tecnológico.

LA SEGURIDAD DE LA INFORMACION Y LAS ORGANIZACIONES.

El uso de las tecnologías de la información y de las comunicaciones (ICT) está creando, por tanto, un riesgo que hay que gestionar y controlar dentro de las organizaciones empresariales, del mismo modo que la eficiencia en el cumplimiento de los objetivos, por los que son aplicadas. Esto equivale a afirmar que tanto la seguridad como la eficiencia deben ser objetivos inseparables y que es obligación de los responsables organizativos implantar ambos (eficiencia y control) y exigirlos al personal informático del mismo modo que a los demás recursos humanos de la Empresa, a pesar de que la seguridad en muchos casos pueda parecer prescindible por razones económicas o por el propio interés del personal involucrado, en no ser controlado.

La necesidad de proteger la información parece, por tanto, evidente. Sin embargo, en ciertos momentos puede resultar un problema extraordinariamente difícil de resolver, el delimitar lo que hay que proteger y cómo debe hacerse. Así mismo, el concepto de Seguridad de la Información se confunde, muchas veces aplicando criterios muy simplistas, con el de seguridad informática, o incluso con el uso de software de seguridad. Nada más lejos de la realidad. La auténtica Seguridad de la Información en una Organización, debe abordar aspectos de seguridad física y lógica de la información. Será la seguridad lógica la relacionada con el nivel de control de los riesgos informáticos y éste a su vez con el nivel de medidas para reducir estos riesgos y no sólo los que puedan afectar a la confidencialidad y a la integridad de la información, sino también los económicos, financieros y legales.

Según lo anterior, puede considerarse acertadamente, a la Seguridad de la Información como un problema de gestión, en el que se trata de alcanzar unos objetivos concretos por medio de la adecuada asignación de recursos, tales como recursos humanos, técnicos, distribución del tiempo, etc. La Seguridad debería ser por todo ello, cuidadosamente planificada y presupuestada, estableciendo el nivel de seguridad que sea aceptable para cada Organización y los medios más adecuados para alcanzarla. De hecho será preciso establecer una política de seguridad por parte de los gestores empresariales. Dicha política de seguridad deberá realizar un exhaustivo análisis de riesgos y a partir de él, incluir un conjunto completo de mecanismos y servicios de seguridad, que permitan conseguir la seguridad de la información que la Organización precisa, a un coste proporcional a lo que se pretende salvaguardar.



Deberá establecerse dentro de la Organización, un compromiso equilibrado entre los tres factores siguientes:

- * La operatividad de todo el sistema que sea necesaria, frente a los diferentes riesgos potenciales que puedan definirse.
- * Los mecanismos y técnicas que puedan reducir la probabilidad de aparición de riesgos e incidentes, así como disminuir sus efectos.
- * Los costos (directos y no directos) derivados de la utilización de dichas técnicas.

Los sistemas informáticos pueden ser diseñados conforme a una serie de criterios de economía, eficiencia, etc., ya que para dichos criterios se conocen parámetros que maximizándose ó minimizándose, pueden dar lugar a diseños óptimos. Sin embargo, cuando se trata del criterio de seguridad el problema se vuelve mucho más complejo y en muchos casos difícilmente resoluble. Es en estos casos, en los que la puesta en práctica de la teoría matemática de los juegos (juegos de suma no nula), pueda ser el punto de vista bajo el que haya que estudiar el problema de la seguridad.

En el convencimiento de que establecer medidas de seguridad en el ámbito empresarial es un problema en muchos casos muy complejo, lo más importante es que los responsables organizacionales tomen conciencia de que son medidas que llevan un coste asociado en su implantación y que pueden obligar a subordinar algunas ventajas de los sistemas tradicionales de tratamiento de la información.

IMPLANTACION PRACTICA DE LA SEGURIDAD DENTRO DE LAS ORGANIZACIONES.

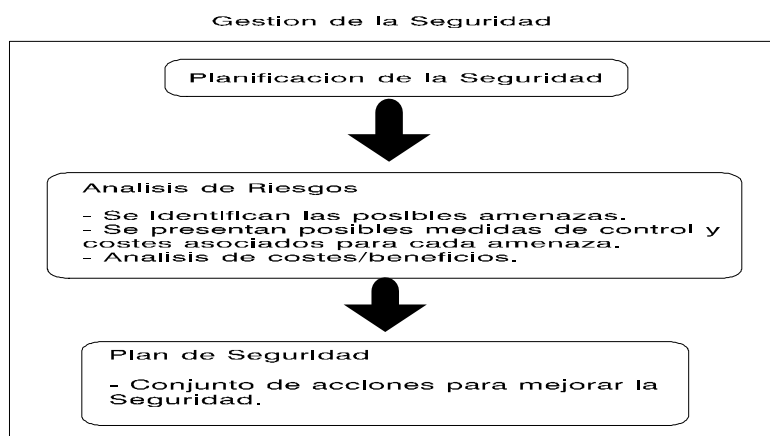
El análisis de la rentabilidad de la aplicación de la Seguridad en una Organización pese a su indudable interés e importancia práctica presenta ciertas limitaciones en ciertos entornos o tipos de Organización. En el caso del control de la Seguridad de la Información, es preciso acometer un ambicioso proyecto, que aparte de los beneficios económicos que pueda reportar el hecho de prevenir y evitar graves problemas para la Organización, tiene de hecho otros objetivos, incluso más trascendentales, como son: mejora de la información existente, mejora de la imagen de la Organización frente a sus clientes, adquisición de una cierta posición ventajosa estratégicamente, instauración de un clima humano interno mejor definido y favorable, etc.. Es decir, en este caso no se persigue tanto una rentabilidad económica inmediata y directa, sino que existen otras metas de naturaleza inmateral pero que sin duda pueden llegar a ser tanto ó más importantes que el objetivo de la rentabilidad económica.

Desde esta perspectiva, las técnicas de análisis coste/eficacia o de coste/beneficio, tradicionalmente aplicadas en otros ámbitos del conocimiento, pueden en el ámbito de la Seguridad de la Información, proporcionar una valiosa ayuda, orientando por ejemplo, la toma de decisiones en relación a si es conveniente o no instaurar una

cierta contramedida, ante alguna categoría de amenaza, y propiciar la utilización de criterios de racionalidad para elegir entre diversas alternativas posibles. En concreto, puede servir para orientar una adecuada planificación de Seguridad hacia tareas o actividades de mayor interés y repercusión económica o de mercado.

Las ventajas que pueden aportar estas técnicas a la planificación de la Seguridad de la Información, dentro de una Organización, pueden resumirse en las siguientes:

- 1.- Facilitan la elaboración de Planes de Seguridad de la Información específicos.
- 2.- Permiten la comparación de Subtareas entre sí y el establecimiento de prioridades entre ellas, dentro de un Plan de Seguridad global.
- 3.- Incluyen la posibilidad de establecer una planificación de seguridad detallada y convenientemente presupuestada, para una determinada Organización en cualquier periodo específico.
- 4.- Hacen posible el seguimiento y control "a posteriori", de los resultados parciales y globales de los Planes establecidos.



Antes de aplicar propiamente un análisis costes/beneficios, será imprescindible como pasos previos llevar a cabo:

(1) **Una definición expresa de objetivos, incluidos los de naturaleza inmaterial, que el Plan de Seguridad de la Información pretende conseguir, con indicación precisa de todas aquellas posibles amenazas a la Información contra las que se desea actuar.** Cuanto más concreta sea la descripción de estos objetivos y amenazas, y más explícita su formulación, menor será el riesgo de acometer un Plan de Seguridad que a posteriori resulte injustificado o inoportuno y será más sencillo controlar si se alcanzan o no los objetivos perseguidos.

La mayoría de las amenazas a la Seguridad de la Información, que los gestores/administradores de las distintas Organizaciones deberían considerar no son, aunque a primera vista pueda parecer lo contrario, de carácter tecnológico. Esta parte del proceso de análisis de riesgos deberá requerir la utilización de tests y cuestionarios, que interroguen al responsable de la Organización sobre las amenazas probables. Una lista de posibles objetos sobre los que debe aplicarse la Seguridad de la Información, es la siguiente:

- Edificios.
- Personal de limpieza y mantenimiento de edificios.
- Personal administrativo.
- Operadores.
- Personal de programación.
- Personal en general.
- Documentos y volúmenes de biblioteca.
- Documentos de Auditoría.
- Programas de test.
- Programas de aplicación.
- Librerías de ficheros.
- Dispositivos de almacenamiento de información (discos, cartridges, cintas magnéticas,...).
- Impresoras e impresos.
- Líneas de comunicación (modems, multiplexores, routers, gateways, bridges,...).
- Otros dispositivos de E/S.
-

Además, será necesario clasificar siempre las amenazas potenciales en base a su "importancia" relativa para la Organización en estudio. Para poder hacer una valoración adecuada de los riesgos, deberán asignarse prioridades a cada uno de ellos de acuerdo a diversos criterios. Por ejemplo, se pueden considerar como posibles factores de decisión:

- 1) La frecuencia potencial de la incidencia.
- 2) Las dimensiones de la pérdida.
- 3) La facilidad/coste de las medidas de protección.
- 4) La facilidad en que la amenaza sea perpetrada.
- 5) El número de intrusos potenciales.

(2) Una estimación de los costes asociados a cada una de las amenazas encontradas en la fase anterior, así como la identificación de las posibles contramedidas o medidas de control, más adecuadas previstas para cada tipo de amenaza. Básicamente hay dos elementos principales que debieran intervenir en la estimación de los costes de los riesgos o amenazas organizacionales: F, la frecuencia con la que una determinada amenaza puede llegar a producirse, durante un periodo de tiempo prefijado y C, el costo ó pérdida atribuido a tal amenaza., en términos de pérdida económica por año. Sin embargo, en muchas situaciones de amenaza no es fácil determinar estos valores. Es en estos casos, en los que el coste de un riesgo o amenaza debe interpretarse en sentido amplio, pudiendo estar

definido en términos no necesariamente económicos. Esta circunstancia puede variar en función de las características propias de los recursos afectados, cuantificándose por ejemplo en unidades más clarificadoras y tan diversas como: el número de empleados y/o máquinas por unidad de tiempo, credibilidad, horas, desplazamientos, tiempo de proceso informático, tiempo de proceso manual, etc.

Siempre que nos decanemos por una valoración de las amenazas puramente económica, deberemos tener en cuenta que el coste material del recurso no suele ser el criterio más apropiado. Por ejemplo, si una caja de 10 discos magnéticos cuesta en el mercado 2.000 pesetas, pero la información que contiene cada disco puede ser de valor superior a 35.000 ptas.; el coste más apropiado será de 35.000 ptas./disco si la pérdida afectara a sólo una caja de discos. Esto, demuestra que las amenazas deben estar definidas específicamente, antes de realizar cualquier asignación de coste (pérdidas previsibles).

Tras el análisis de algunas complejas alternativas para la selección del coste más apropiado para cada amenaza definida, una alternativa conceptualmente válida y algo más sencilla desde el punto de vista de la complejidad del calculo matemático necesario, consistiría en preguntarse cuál de los siguientes seis tipos de coste conviene aplicar a la amenaza definida:

1. El coste material del activo.
2. El coste para reparar el activo (daños, menos seguro).
3. El coste para colocar el activo (incluyendo pedidos, portes e instalación).
4. El coste para operar sin el activo (incluyendo pérdida general, pérdida aplazada, etc.).
5. El coste de la capacidad de retroceso/recuperación.
6. El coste de los seguros.

De manera que pueda estimarse cuantitativamente el coste de una amenaza por medio de la siguiente expresión matemática (en Ptas./año): $E = ((10^{F+C-3})/4)$

Donde, F representa la frecuencia con la que una determinada amenaza puede llegar a producirse y C, el coste atribuido a tal amenaza, en términos de pérdida económica. Suponiendo conocidas las siguientes tablas:

- TABLA de F:

- 0 - Virtualmente imposible.
- 1 - Puede que suceda una vez en 400 años.
- 2 - Puede que suceda una vez en 40 años.
- 3 - Puede que suceda una vez en 4 años (1.000 días de trabajo).
- 4 - Puede que suceda una vez en 100 días de trabajo.
- 5 - Puede que suceda una vez en 10 días de trabajo.
- 6 - Puede que suceda una vez cada día.
- 7 - Puede que suceda 10 veces al día.

- TABLA de C:

- 0 - Despreciable (alrededor de 100 Ptas.).
- 1 - Del orden de 1.000 Ptas.
- 2 - Del orden de 10.000 Ptas.
- 3 - Del orden de 100.000 Ptas.
- 4 - Del orden de 1.000.000 Ptas.
- 5 - Del orden de 10.000.000 Ptas.
- 6 - Del orden de 100.000.000 Ptas.
- 7 - Del orden de 1.000.000.000 Ptas.

Si un cierto tipo de amenaza se estima que puede provocar una pérdida por valor de 100.000 Ptas. y tiene una frecuencia probable de que suceda una vez cada 100 días de trabajo, entonces: $F= 4$, $C= 3$; siendo el coste de la amenaza E de 2.500 Ptas/año. Si por el contrario, un incendio en el Centro de Proceso de Datos de una Organización causara un daño calculado en 100.000.000 de Ptas., pero fuera improbable que ésto sucediera más de una vez cada 400 años, el costo de tal amenaza sería de: $E = (10^{(1+6-3)})/4 = 2.500$ Ptas/año.

Un problema que afecte a una determinada Organización, cuyo coste sea de 1.000 Ptas. y que ocurra 10 veces al día, supondría: $E = 25.000$ Ptas/año, con lo que, por ejemplo, merecería la pena invertir 10 veces más en esta amenaza que en las dos anteriores.

Obviamente, pueden definirse otras fórmulas más precisas para calcular la importancia de una amenaza, pero se corre el riesgo en su definición, de convertirlas en una herramienta de uso restringido, difícilmente generalizable para cualquier amenaza y/o Organización. Pudieran ser admisibles en aquellos estudios en los que se desee emplear más tiempo y dinero ó en aquellos que se realicen para refinar aproximaciones anteriores de ciertas amenazas más costosas o más frecuentes. Por ejemplo, en algunos casos cuando exista cierta experiencia previa sobre amenazas y su ocurrencia práctica en la Organización en estudio, puede interesar calcular el costo correspondiente a una amenaza, de una forma más precisa, aplicándose en este caso la siguiente expresión alternativa:

$$E = F/(\text{Tiempo medio que transcurre entre ocurrencias de una amenaza (en años)}).$$

En definitiva, en los ejemplos anteriores, se ha establecido como indicador de gestión, para cuantificar los distintos factores de coste, las Ptas/año que supone cada amenaza, de modo que el peso a dar a cada factor (0, 1, 2,..., 7), viene dado por el valor que adquiere el indicador que hemos establecido. El disponer de otros criterios de coste (incluso menos objetivos y cuantificables), acompañados de sus pertinentes indicadores (indicadores de coste o eficiencia alternativos), será un punto esencial para poder elegir entre diversas alternativas y para evaluar posteriormente la calidad de los resultados obtenidos, ya que permitirían integrar las prioridades o directrices que toda Organización debe tener.

Así mismo, sería conveniente asignar diversas ponderaciones, a cada uno de los criterios seleccionados, pues es lógico pensar que todos ellos no son igualmente relevantes. Esta asignación de carácter subjetivo permitiría sin embargo considerar otros factores de relevancia, como por ejemplo, preferencias otorgadas en función de las directrices políticas de la Empresa y del grado de contribución de cada factor a los objetivos de la Seguridad de la Información. La consideración de los dos factores anteriores: indicadores y su ponderación relativa, nos permitiría confeccionar finalmente cuadros que cuantifiquen globalmente el Plan de Seguridad de la Información.

CONCLUSIONES.

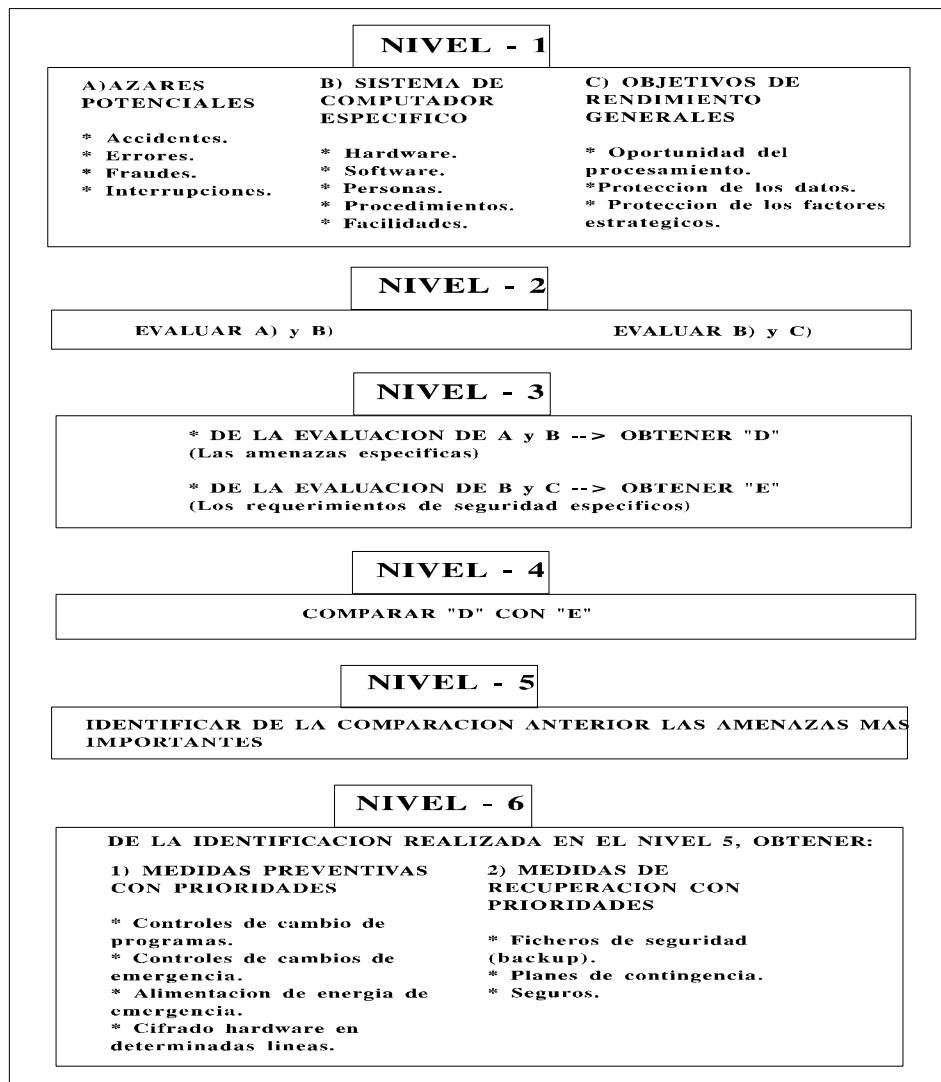
A la hora de llevar a cabo la gestión de la Seguridad de la Información en una Organización se debe realizar un análisis de riesgos, que permita descubrir lo amenazado que se encuentra dicho sistema. Los principales objetivos que con ello se obtienen serían:

1. Ayudar a la identificación de amenazas potenciales contra el buen funcionamiento de la Organización, desde la perspectiva de su Información.
2. Ayudar en la cuantificación de las pérdidas ocasionadas por dichas amenazas a la Seguridad de la Información.
3. Permitir una ordenación de las amenazas en base a un sistema de prioridades.
4. Servir como base sólida para el análisis y obtención de una Plan de Seguridad ajustado y rentable para la Organización.

Normalmente, una sencilla valoración de los riesgos, suele considerar los puntos anteriores 1 y 2. Sin embargo, un auténtico análisis de riesgos organizacional, debe ser más amplio y su finalidad debe abarcar los cuatro objetivos señalados. Según esto, el análisis de riesgos puede considerarse como un planteamiento sistemático, enormemente útil para caracterizar las amenazas que existen sobre los datos y/o computadores dentro de las Organizaciones actuales, para así poder establecer contramedidas a dichas amenazas y para decidir en definitiva, un Plan de acción, que invertirá los máximos recursos (técnicos, humanos,...) contra los riesgos más probables y/o los que pueden suponer mayores pérdidas. El proceso de análisis de riesgos, desde el punto de vista de la información como valor incuestionable en las Organizaciones actuales, puede expresarse, a modo de resumen, según el esquema multinivel de la figura adjunta.

Como puede observarse, en el nivel 6, los planes de acción se consignan con prioridades. De este modo, no tiene sentido trabajar contra todos aquellos riesgos relativamente improbables, a pesar de lo interesante que pueda ser la implementación de sus contramedidas, hasta que no hayan sido tratados todos los riesgos potencialmente más costosos para la Organización.

También es importante destacar que el procedimiento de análisis de riesgos descrito, no pretende ofrecer un Plan de seguridad absoluta. De hecho, la seguridad absoluta es un concepto prácticamente inalcanzable en los cada vez más complejos, sistemas reales de tratamiento automatizado de la Información, al servicio de las Organizaciones actuales. Más bien, el análisis de riesgos permite alcanzar un cierto grado de Seguridad en la Información, que estará en función de la naturaleza de los datos que deban protegerse y de la cantidad de recursos que esté previsto invertir en tal Seguridad.



REFERENCIAS.

- ALVAREZ, C. et al. *Papeles de Avila: Reunión de Expertos sobre Auditoría Informática*. Centro Regional del IBI para la Enseñanza de la Informática. 1986, Avila (España).
- AREITIO, J y AREITIO, M.T.- "A New Protection Mechanism for Computer Networks". *Proceeding del 8th European Conference on Information Systems Security, Control and Audit*. Pag. 71-77. 1993, Stockholm (Suecia).
- CASTELLOTE, A. "Telecomunicaciones, de la liberalización a la globalización". *Computing España*. Business Publications España. Nº 21, pag. 16-18. 1995, Barcelona (España).
- CRESSON, C. *Effective Information Security Management*. Elsevier Advanced Technology. 1992, UK.
- INOSE, H, y PIERCE, J. *Tecnología de la información y civilización*. Labor. 1985, Barcelona (España).