MAGERIT – versión 3.0
Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Libro III - Guía de Técnicas

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS
DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

TÍTULO: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
Libro III - Guía de Técnicas

Elaboración y coordinación de contenidos:
Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica

Equipo responsable del proyecto:
Director, Miguel Angel Amutio Gómez, Ministerio de Hacienda y Administraciones Públicas
Javier Candau, Centro Criptológico Nacional, Ministerio de la Presidencia
Consultor externo: José Antonio Mañas, Catedrático de la Universidad Politécnica de Madrid

Características: Adobe Acrobat 5.0
Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones
(Jesús González Barroso)

Madrid, octubre de 2012
Disponible esta publicación en el Portal de Administración Electrónica (PAe):
http://administracionelectronica.gob.es/

Edita:

Secretaría General Técnica
Subdirección General de Información,
Documentación y Publicaciones
Centro de Publicaciones

Colección: administración electrónica
NIPO: 630-12-171-8

Índice

1. Introducción

Este documento la guía metodológica Magerit. Se presume el conocimiento y comprensión de los conceptos de análisis y gestión de riesgos, según se exponen en la guía metodológica.

El objetivo de este documento es describir algunas técnicas utilizadas en análisis y gestión de riesgos. Se considera técnica a un conjunto de heurísticos y procedimientos que ayudan a alcanzar los objetivos propuestos.

Para cada una de las técnicas referenciadas:

- se explica brevemente el objetivo que se persigue al utilizarlas,
- se describen los elementos básicos asociados,
- se exponen los principios fundamentales de elaboración,
- se presenta una notación textual y/o gráfica y
- y se citan las fuentes bibliográficas que, sin ser exhaustivas, se han estimado de interés para que el lector profundice en cada materia.

Todas las técnicas de este libro pueden utilizarse sin ayudas automatizadas; pero su aplicación repetitiva o compleja recomienda el empleo de herramientas tan amplia y frecuentemente como sea posible.

Es importante resaltar que la notación que se propone en la aplicación de la técnica en ningún caso se considerará obligatoria. Cada organización podrá utilizar la notación que desee, la que suele utilizar o la que ofrecen sus herramientas de desarrollo, respetando las reglas y restricciones específicas de las distintas técnicas.

2. Técnicas específicas

En este capítulo nos centraremos en algunas técnicas muy específicas de los proyectos de análisis y gestión de riesgos, técnicas que no se utilizan en otros contextos de trabajo.

Se han considerado de especial interés:

1. uso de tablas para la obtención sencilla de resultados
2. técnicas algorítmicas para la obtención de resultados elaborados
3. árboles de ataque para complementar los razonamientos de qué amenazas se ciernen sobre un sistema de información

que se desarrollan en las siguientes secciones.

2.1. Análisis mediante tablas

Dícese análisis de la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos. En el análisis de riesgos hay que trabajar con múltiples elementos que hay que combinar en un sistema para ordenarlo por importancia sin que los detalles, muchos, perjudiquen la visión de conjunto.

La experiencia ha demostrado la utilidad de métodos simples de análisis llevados a cabo por medio de tablas que, sin ser muy precisas, sí aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas.

Sea la escala siguiente útil para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

- **MB:** muy bajo
- **B:** bajo
- **M:** medio
- **A:** alto
- **MA:** muy alto

Estimación del impacto

Se puede calcular el impacto en base a tablas sencillas de doble entrada:

impacto		***degradación***		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Aquellos activos que reciban una calificación de impacto muy alto (MA) deberían ser objeto de atención inmediata.

Estimación del riesgo

Por otra parte se modelan impacto, probabilidad y riesgo por medio de escalas cualitativas:

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Pudiendo combinarse impacto y frecuencia en una tabla para calcular el riesgo:

riesgo		***probabilidad***				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

2.1.1. Referencias

- ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk management.
- ISO 31010
  ISO/IEC 31010:2009, Risk management — Risk assessment techniques.
  UNE-ISO/IEC 31010:2010, Gestión del riesgo. Técnicas de apreciación del riesgo.

  B.29 Matriz de consecuencia / probabilidad

2.2. Análisis algorítmico.

Dícese análisis de la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos. En ciencias químicas, dícese análisis cualitativo del que tiene por objeto descubrir y aislar los elementos o ingredientes de un cuerpo compuesto. A diferencia del análisis cuantitativo que es el que se emplea para determinar la cantidad de cada elemento o ingrediente.

En las siguientes secciones se presentan dos enfoques algorítmicos. Primero, un modelo cualitativo que busca una valoración relativa del riesgo que corren los activos (¿qué es lo más frente a qué es lo menos?). Segundo, un modelo cuantitativo que ambiciona responder a la pregunta de cuánto más y cuánto menos. A continuación se presenta un modelo escalonado, típico del análisis de impacto sobre la disponibilidad de los sistemas de información. Por último se incluye un modelo para estimar la eficacia de un paquete de salvaguardas.

2.2.1. Un modelo cualitativo

En un análisis de riesgos cualitativo se busca saber qué es lo que hay, sin cuantificarlo con precisión más allá de relativizar los elementos del modelo.

En esta sección se presenta un modelo de cálculo que trabaja sobre una escala discreta de valores.

Valores.

En un análisis de riesgos es necesario poder valorar, al menos relativamente, los elementos involucrados. En particular, los activos, el impacto de las amenazas y el riesgo que se corre.

Para todo ello se usará una escala de niveles simbólicos:

$$V = \{ 0, ..., v_0, v_1, ..., v_i, ... \}$$

El valor 0 representa que no vale absolutamente nada.

Esta serie de niveles satisface las siguientes propiedades:

- elemento mínimo: $\forall$ i, $0 < v_i$
- orden total: $\forall$ i, $v_i < v_{i+1}$
- existe un elemento singular, *"v_0"*, que se denomina "despreciable"[1].

Informalmente, se dice que un activo tiene "i puntos" para indicar que su valoración es *"v_i"*[2].

El valor de los activos.

Cada activo, en cada dimensión, recibe un valor de la escala *V*.

Los activos reciben una valoración en cada una de las dimensiones de seguridad.

Las dependencias entre activos.

Sólo hay que preocuparse de si un activo A depende, significativamente, o no de otro activo B. Es decir, la dependencia entre activos es un valor booleano: sí o no.

$$A \rightarrow B$$

La dependencia puede ser transitiva:

$$(A \rightarrow B) \wedge (B \rightarrow C)$$

A depende de B; B depende de C.

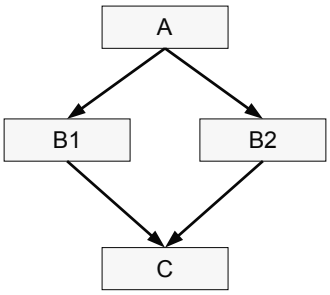
1 Este nivel despreciable establece una frontera, subjetiva, entre lo que es apreciable y debe preocupar, y lo que es despreciable y se puede obviar. Se despreciarán los valores por debajo de v_0.

2 Si el lector lo desea, en este sistema de valoración, puede interpretar los puntos como órdenes de magnitud; por ejemplo, interpretando v_x como 10^x.

E incluso puede dibujar figuras de diamante:

$$(A \rightarrow B_1) \wedge (A \rightarrow B_2) \wedge (B_1 \rightarrow C) \wedge (B_2 \rightarrow C)$$

A depende de B1 y B2; B1 y B2 dependen de C.



Interesa pues del cierre transitivo de las dependencias directas entre activos.

$$A \Rightarrow C \Leftrightarrow \exists\ B, (A \Rightarrow B) \wedge (B \rightarrow C)$$

A depende (indirectamente) de C sí y sólo si
existe algún activo B tal que A depende directa o indirectamente de B y
B depende directamente de C.

En lo que sigue no se distingue entre dependencias directas o indirectas.

El valor acumulado.

Sea SUP(B) el conjunto superiores de B, es decir el conjunto de activos que dependen directa o indirectamente de B:

$$SUP(B) = \{ A_i, A_i \Rightarrow B \}$$

Se define el valor acumulado sobre B como el mayor valor entre el propio y el de cualquiera de sus superiores:

$$valor\_acumulado(B) = \max (valor(B), \max_i \{valor(A_i)\})$$

La fórmula anterior dice que el valor acumulado sobre un activo es el mayor de los valores que soporta, bien propio, bien de alguno de sus superiores.

La degradación [del valor] de un activo.

Cuando un activo es víctima de una amenaza, una parte de su valor se pierde. Intuitivamente, se habla de un "porcentaje de degradación del activo", de forma que se puede perder entre un 0% y un 100%. Se recoge *"d"* como un valor real entre 0,0 (degradación del 0%) y 1,0 (degradación del 100%).

Impacto acumulado de una amenaza sobre un activo.

Es la medida de lo que implica una amenaza; es decir, la pérdida de valor acumulado. El impacto se mide en las mismas unidades que el valor.

Si un activo tiene un valor acumulado *"v"* y se degrada un porcentaje *"d",* el valor del impacto se calcula con alguna función que cumpla las siguientes condiciones de contorno

$$impacto(0, 0\%) = 0$$

$$impacto(v, 0\%) = 0$$

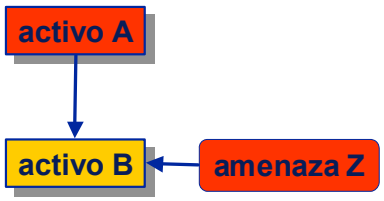
$$impacto(v, 100\%) = v$$

$$\forall\ d, v_i < v_j \Rightarrow impacto(v_i, d) < impacto(v_j, d)$$

$$\forall\ v, d_i < d_j \Rightarrow impacto(v, d_i) < impacto(v, d_j)$$

Cuando el impacto queda a *"v_0", o menos,* se dice que el impacto es despreciable.

Impacto repercutido de una amenaza sobre un activo.



Si el activo A depende del activo B, las amenazas sobre B repercuten sobre A. Si B sufre una degradación *"d",* eso mismo le ocurre a A, siendo el impacto sobre A la pérdida de su valor propio. Si A tiene un valor propio *"*v_A*"*, y B tiene un valor propio v_B, los impactos sobre A y B serán:

impacto sobre A = impacto(v_A, d)

impacto sobre B = impacto(v_B, d)

Cuando el impacto queda reducido a *"v_0",* se dice que el impacto es despreciable.

Probabilidad de una amenaza.

Para caracterizar la probabilidad de las amenazas se usará una escala de valores simbólicos:

$$P = \{ 0, ..., p_0, p_1, ..., p_i, \dots \}$$

El valor 0 refleja el suceso imposible. El valor p_0 refleja una probabilidad despreciable.

Es decir, una serie de niveles de probabilidad, que son los elementos o átomos de análisis.

Esta serie de niveles satisface las siguientes propiedades:

- orden total: $\forall\ j,\ p_j < p_{j+1}$
- existe un elemento singular, *"f_0",* que se denomina "probabilidad despreciable"

Riesgo.

El riesgo se mide por medio de la escala de valores, que es distinta de la escala de valores.

$$R = \{ 0, ..., r_0, r_1, ..., r_i, \dots \}$$

El valor 0 refleja el riesgo inexistente.

El riesgo es una función del impacto y la probabilidad:

riesgo = $\Re$(impacto, probabilidad)

función que hay que definir con los siguientes requisitos:

- $\Re(0, p) = 0$
- $\Re(v, 0) = 0$
- crece con el valor: $\forall\ f,\ v_i < v_j \Rightarrow \Re(v_i, p) < \Re(v_j , p)$
- crece con la probabilidad: $\forall\ v,\ p_i < p_j \Rightarrow \Re(v, p_i) < \Re(v , p_j)$

El riesgo puede tomar el valor *"r_0",* e incluso valores inferiores, en cuyo caso se entiende que el riesgo es "despreciable".

Habitualmente se emplea alguna función que de más peso al impacto que a la probabilidad. Ver "análisis tabular".

Riesgo acumulado.

En el cálculo del riesgo acumulado, se usará el impacto acumulado sobre el activo.

Riesgo repercutido.

En el cálculo del riesgo repercutido, se usará el impacto repercutido sobre el activo.

Paquete de salvaguardas.

Frente a una amenaza se desplegará una serie de salvaguardas, un paquete de salvaguardas, cuya eficacia, *"e",* se calcula según se indica más adelante. Baste adelantar que la eficacia es un valor real entre 0,0 (no protege nada) y 1,0 (salvaguarda plenamente eficaz), valor que se puede descomponer en una eficacia frente al impacto, *"e^i",* y una eficacia frente a la probabilidad *"e^p".*

Degradación residual.

Si el activo, sin protección, podía sufrir una degradación "d", gracias a las salvaguardas la degradación se ve reducida a un valor residual "dr":

$dr(0, e^i) = 0$

$dr(d, 0) = d$

$dr(d, 1) = 0$

El impacto residual.

El impacto residual se calcula como el impacto, pero utilizando la degradación residual:

$impacto\_residual = impacto(v, dr)$

Un paquete de salvaguardas perfectamente eficaz reduce el impacto a un valor residual *"v_0",* es decir, al nivel de despreciable. Si las salvaguardas son insuficientes, el impacto seguirá siendo apreciable.

El impacto acumulado residual se calcula sobre el valor acumulado.

El impacto residual repercutido se calcula sobre el valor propio.

La probabilidad residual.

De forma similar al impacto, la probabilidad de la amenaza sobre el activo se ve reducida a un valor residual. Si la probabilidad era *"p",* ahora queda:

$pr(0, e^p) = 0$

$pr(p, 0) = p$

$pr(p, 1) = 0$

Siendo *"e^p"* la eficacia de las salvaguardas mitigando la probabilidad de ocurrencia de la amenaza. *"e^f"* es un valor entre 0,0 (0% de eficacia; o sea, inútil) y 1,0 (100% de eficacia; o sea, perfecta).

Riesgo residual.

Es el riesgo calculado a partir del impacto y frecuencia residuales:

$riesgo\_residual = \Re(impacto\_residual, frecuencia\_residual)$

El riesgo residual acumulado se calcula sobre el impacto residual acumulado.

El riesgo residual repercutido se calcula sobre el impacto residual repercutido.

Resumen

En este modelo, denominado cualitativo, se han posicionado los activos en una escala de valor relativo, definiendo arbitrariamente un valor *"v_0"* como frontera entre los valores que preocupan y los que son despreciables.

Sobre esta escala de valor se ha medido tanto el valor del activo, propio o acumulado, como el impacto de una amenaza cuando ocurra y el riesgo al que está expuesto.

Mientras el impacto mide el valor de la desgracia potencial, el riesgo pondera ese impacto con la frecuencia estimada de ocurrencia de la amenaza. El impacto es la medida del coste si ocurriera mientras que el riesgo mide la exposición en un determinado periodo de tiempo.

Las estimaciones de impacto y riesgo residual incorporan la eficacia de las salvaguardas para enfrentarse a la amenaza, bien limitando el impacto, *"e^i"*, bien reduciendo la probabilidad, *"e^p"*.

El modelo pues combina los siguientes parámetros de análisis:

- calibración del valor del activo por medio de una escala discreta
- calibración de la degradación que supone una amenaza como un porcentaje
- calibración de la probabilidad de ocurrencia de la amenaza por medio de una escala discreta
- vertebración de un paquete de salvaguardas
- calibración de la eficacia de las salvaguardas por medio de un porcentaje

Parámetros todos ellos que permiten moverse arriba y abajo por las escalas de valores.

2.2.2. Un modelo cuantitativo

En un análisis de riesgos cuantitativo se busca saber qué y cuánto hay, cuantificando todos los aspectos posibles.

El modelo que sigue no trabaja sobre una escala discreta de valores, sino con números reales (en el sentido matemático) positivos.

El valor de los activos.

El valor de un activo en una cierta dimensión es un valor real superior a cero.

Se determina que un cierto valor, *"v_0"*, representa la frontera entre los valores que son despreciables y los que son relevantes.

Las dependencias entre activos.

Interesa tanto de saber si un activo A depende o no de otro activo B, como de saber en qué grado. Se aplican los conceptos de dependencia directa o indirecta expuestos en el modelo cualitativo; pero ahora se calificará la dependencia por medio de un coeficiente entre 0,0 (activos independientes) y 1,0 (activos con dependencia absoluta). A este coeficiente se le denomina grado de dependencia.

Como la dependencia puede ser directa o indirecta, se calculará del cierre transitivo de las dependencias directas entre activos.

$$A \Rightarrow C \Leftrightarrow \exists\ B,\ (\ A \Rightarrow B\ ) \wedge (\ B \rightarrow C\ )$$

A depende (indirectamente) de C sí y sólo si existe algún activo B tal que A depende directa o indirectamente de B y B depende directamente de C.

Calculando el grado de dependencia como:

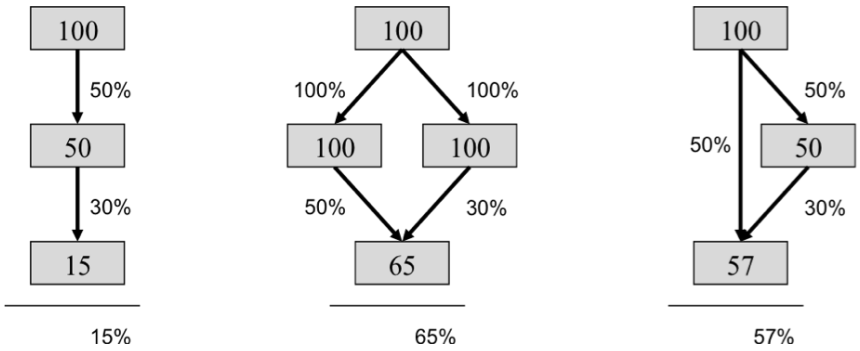
$$\text{grado}(A \Rightarrow C) = \sum_i \{\ \text{grado}(A \Rightarrow B_i) \times \text{grado}(B_i \rightarrow C)\ \}$$

Donde las sumas se realizan de acuerdo con esta fórmula:

$$a + b = 1 - (1 - a) \times (1 - b)^3$$

3 Esta manera de sumar satisface las propiedades conmutativa, asociativa y existencia de un elemento neutro, amén de acotar el resultado al rango [0..1] si los sumandos están dentro de dicho rango.
La elección de esta curiosa fórmula, tomada del cálculo de probabilidades de Bayes, deriva de la necesidad de reflejar el hecho de que si un activo depende de otro por varias vías (estructuras de diamante), la dependencia total no puede superar el 100%.

Ejemplos.



En lo que sigue no se distingue entre dependencias directas o indirectas.

El valor acumulado.

Sea SUP(B) el conjunto de superiores de B, es decir el conjunto de activos que dependen directa o indirectamente de B:

$$SUP(B) = \{ A_i, A_i \Rightarrow B \}$$

Se define el valor acumulado sobre B como la suma (tradicional) de valores de los activos superiores, ponderados por el grado de dependencia:

$$valor\_acumulado(B) = valor(B) + \sum_i \{ valor(A_i) \times grado(A_i \Rightarrow B) \}$$

La degradación [del valor] de un activo.

Cuando un activo es víctima de una amenaza, una parte de su valor se pierde. Intuitivamente, se habla de un "porcentaje de degradación del activo", de forma que se puede perder entre un 0% y un 100%. Se recogerá "d" como un valor real entre 0,0 (degradación del 0%) y 1,0 (degradación del 100%).

Impacto acumulado de una amenaza sobre un activo.

Es la pérdida de valor acumulado. Si un activo tiene un valor acumulado *"v"* y sufre una degradación *"d",* el impacto es

$$impacto = i = v \times d$$

Ejemplo.

Si un activo está valorado en 1.000.000 y sufre una degradación del 90%, el impacto acumulado es de cuantía 900.000.

Cuando el impacto queda reducido a *"v_0",* o menos, se dice que el impacto es despreciable.

Impacto repercutido de una amenaza sobre un activo.

Si el activo A depende del activo B, las amenazas sobre B repercuten sobre A. Si B sufre una degradación *"d",* A pierde en la proporción en que dependa de B. Si el activo A tiene un valor propio *"v",* el impacto es

$$impacto = v \times d \times grado(A \Rightarrow B)$$

Ejemplo.

Sea un activo A valorado en 1.000.000, que depende de otro activo B (cuyo valor no interesa aquí) en un 30%. Si B es víctima de una amenaza que lo degrada un 90%, A sufre un impacto repercutido de cuantía

1.000.000 x 90% x 30% = 270.000

Cuando el impacto queda reducido a *"v_0",* o menos, se dice que el impacto es despreciable.

Probabilidad de una amenaza.

Para medir la probabilidad utilizaremos la frecuencia esperada de ocurrencia (ARO – Annual Rate of Occurrence) .La frecuencia de una amenaza es un valor real superior a cero.

Se determina un valor *"f_0"* como frecuencia "despreciable", por debajo de la cual la amenaza no merece ser tomada en consideración.

Riesgo.

El riesgo se mide en las misma unidades que el valor.

El riesgo se calcula como

riesgo = impacto × frecuencia

Es un valor real, mayor que cero.

Ejemplo.

Sea un activo valorado en 1.000.000, que es víctima de una amenaza que lo degrada un 90%. El impacto es de cuantía

1.000.000 x 90% = 900.000

Si el activo está expuesto a la amenaza con una frecuencia estimada de 0,1, el riesgo estimado es de cuantía

900.000 x 0,1 = 90.000

Si los valores son euros y la frecuencia mide tasa anual (o sea, si 0,1 significa una vez cada 10 años), entonces la pérdida posible de valor es de 900.000 euros, mientras que la pérdida anual prevista es de 90.000 euros.

Riesgo acumulado.

En el cálculo del riesgo acumulado, se usará el impacto acumulado sobre el activo; es decir, la pérdida de valor acumulado por amenazas sobre el mismo.

Riesgo repercutido.

En el cálculo del riesgo repercutido, se usará el impacto repercutido sobre el activo; es decir, la pérdida de valor propio por amenazas en activos inferiores.

Paquete de salvaguardas.

Frente a una amenaza se despliega una serie de salvaguardas, un paquete de salvaguardas, cuya eficacia, *"e",* se calcula según se indica más adelante. Baste adelantar que la eficacia es un valor real entre 0,0 (no protege) y 1,0 (salvaguarda plenamente eficaz), valor que se puede descomponer en una eficacia frente al impacto, *"e^i",* y una eficacia frente a la frecuencia *"e^f",* de forma que

$$(1 - e^i) \times (1 - e^f) = 1 - e^4$$

4 La fórmula elegida disfruta de las siguientes propiedades. Si e^i= 0% y e^f= 0%, e= 0%. Si e^i= 0%, e= e^f. Si e^f= 0%, e= e^i. Si e^i o e^f= 100%, e= 100%. El resultado es pues creciente con los componentes e^i y e^f, estando al tiempo acotado al rango [0%..100%].

Degradación residual.

Es la parte de la degradación que no consigue contrarrestar la eficacia del paquete de salvaguardas aplicado.

El impacto residual.

Un sistema de salvaguardas absolutamente ineficaz ($e^i = 0$) deja el impacto donde estaba, mientras que un sistema de salvaguardas plenamente eficaz ($e^i = 1$) reduce el impacto a 0.

Ejemplo

Sea un activo valorado en 1.000.000, que es víctima de una amenaza que lo degrada un 90%. El impacto es de cuantía

1.000.000 x 90% = 900.000

Si las salvaguardas tienen un 90% de eficacia sobre el impacto, el impacto residual es

impacto residual = 900.000 * (1 – 0.9) = 90.000

El impacto acumulado se realiza con los datos de impacto acumulado sobre un activo y las salvaguardas adecuadas para las amenazas sobre dicho activo.

El impacto repercutido se realiza con los datos de impacto repercutido sobre el activo superior y las salvaguardas adecuadas para las amenazas del activo inferior.

La frecuencia residual.

Un sistema de salvaguardas absolutamente ineficaz ($e^f = 0$) deja la frecuencia donde estaba, mientras que un sistema de salvaguardas plenamente eficaz ($e^f = 1$) reduce la frecuencia a 0.

Al igual que para calcular el impacto residual, se suele emplear alguna función de tipo Pareto.

El riesgo residual.

Puede derivarse indirectamente como

riesgo_residual = impacto_residual x frecuencia residual

Ejemplo

Sea un activo valorado en 1.000.000, que es víctima de una amenaza que lo degrada un 90%. El impacto es de cuantía

impacto = 1.000.000 x 90% = 900.000

Si la frecuencia anual estimada es de 0,1, el riesgo es de cuantía

riesgo = 900.000 x 0,1 = 90.000 = pérdida anual estimada

Si las salvaguardas tienen un 90% de eficacia sobre el impacto, el impacto residual es

impacto residual = 900.000 x (1 – 90%) = 90.000

Si las salvaguardas tienen un 50% de eficacia sobre la frecuencia, la eficacia combinada de las salvaguardas es

frecuencia residual = 0,1 x (1 – 50%) = 0,05

y el riesgo residual es

riesgo residual = 90.000 * 0,05 = 4.500 (pérdida anual estimada)

Si las cantidades son euros y las frecuencias anuales, la pérdida posible es de 90.000 euros y la pérdida anual se estima en 4.500 euros.

Resumen

En este modelo, denominado cuantitativo, se trabaja con valores que son números reales, siempre superiores a cero.

Se modela el grado de dependencia entre activos como un continuo entre 0,0 (activos independientes) y 1,0 (activos absolutamente dependientes; lo que ocurre sobre el inferior repercute contundentemente sobre el superior).

Se mide tanto el valor del activo, propio o acumulado, como el impacto de una amenaza cuando ocurra y el riesgo que supone.

Mientras el impacto mide el valor de la desgracia potencial, el riesgo pondera ese impacto con la frecuencia estimada de ocurrencia de la amenaza. El impacto mide el coste si ocurriera mientras que el riesgo es la medida de la exposición en un periodo de tiempo.

Si la valoración del activo es económica (coste monetario que significaría su pérdida total y absoluta), el impacto calculado es el coste inducido por la amenaza y el riesgo calculado es la cantidad que hay que prever como pérdidas anuales. El modelo cuantitativo permite pues comparar el gasto en salvaguardas con la disminución de pérdidas.

Las estimaciones de impacto y riesgo residual incorporan la eficacia de las salvaguardas para enfrentarse a la amenaza.

Si la valoración del activo es económica, el modelo cuantitativo permite comparar el gasto en salvaguardas con la disminución de pérdidas.

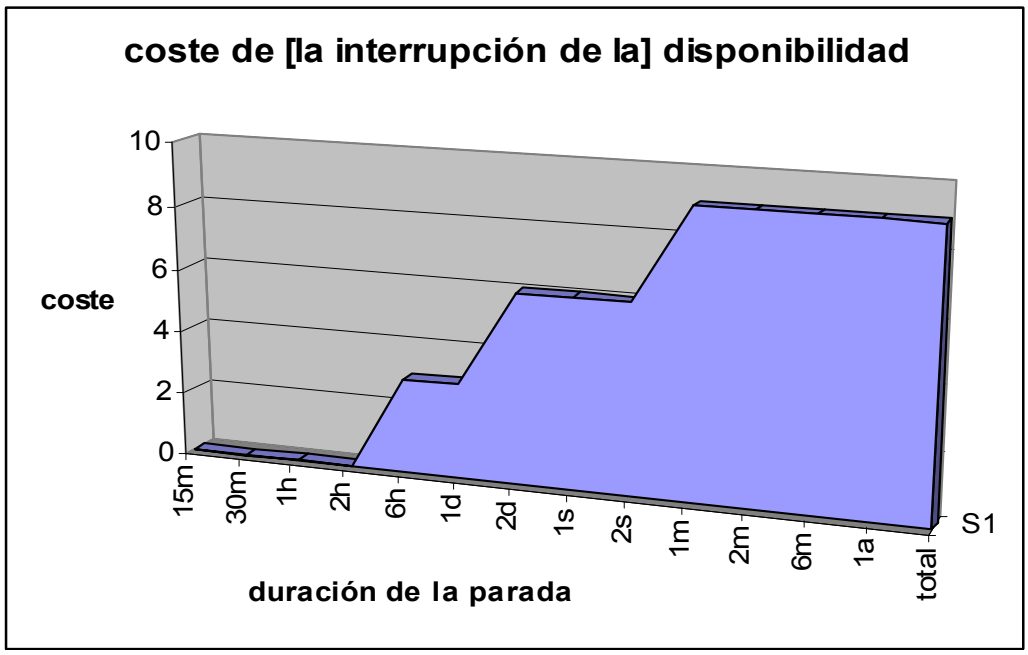
El modelo pues combina los siguientes parámetros de análisis:

- calibración del valor del activo por medio de una cantidad numérica
- calibración de la dependencia entre activos por medio de un porcentaje
- calibración de la degradación que supone una amenaza por medio de un porcentaje
- calibración de la frecuencia de ocurrencia de la amenaza por medio de una frecuencia
- vertebración de un paquete de salvaguardas
- calibración de la eficacia de las salvaguardas por medio de un porcentaje

Parámetros todos ellos que permiten moverse arriba y abajo por la escala de valores.

2.2.3. Un modelo escalonado

Ciertas dimensiones de degradación de un activo se modelan más adecuadamente como escalones de valor. El caso típico es la interrupción del servicio, que responde a esquemas como el siguiente



donde se observa una serie de escalones de interrupción que terminan con la destrucción total o permanente del activo.

En los párrafos siguientes se indica como analizar este tipo de dimensiones, bien sea de forma cualitativa (escala discreta de niveles de valor) o cuantitativa (valor continuo).

Los escalones.

Se determina una serie, ordenada, de escalones de valoración:

$$E = \{ e_1, e_2, ..., e_n \}, \text{ donde } e_1 < e_2 < ... < e_n$$

Cada escalón refleja un tiempo de parada (ver gráfica ilustrativa anterior).

El valor de los activos.

El activo recibe un valor para cada uno de los escalones

$$v[e_i]$$

valor que puede ser cualitativo o cuantitativo, según el tipo de análisis de interés; pero siempre con la condición de que la serie sea monótona creciente:

$$v[e_1] \leq v[e_2] \leq \ldots \leq v[e_n]$$

Las dependencias entre activos.

Se usará el tratamiento cualitativo (binario: sí o no) o el cuantitativo (grado) según corresponda.

El valor acumulado.

Se calculará independientemente (en paralelo) para cada escalón.

Es decir, para cada activo se estima un valor propio y un valor acumulado en cada escalón.

Ejemplo.

Una unidad administrativa proporciona un servicio de reclamaciones que, tradicionalmente, se ha prestado de forma escrita: el afectado reclama por carta y se le responde en el plazo máximo de 1 semana. Actualmente ha introducido una ventanilla electrónica alternativa en la que se ha considerado excelente una respuesta en menos de 1 hora (en horario de atención al público). A partir de una hora, la imagen ofrecida a los ciudadanos empieza a resentirse. Si el servicio se demora más de un día, se considera inútil, aunque de una gravedad relativa pues siempre queda la opción de la reclamación por escrito.

Ambos servicios dependen de un equipamiento informático que hereda las valoraciones de ambos servicios:

activo	*1h*	*1d*	*1s*
escrito	[0]	[0]	[8]
web	[3]	[5]	[5]
servidor	[3]	[5]	[8]

acumulado

Degradación [del valor] de un activo.

Se indicará como el escalón *"e_i"* al que conduce la materialización de la amenaza.

Así, si la consecuencia de una amenaza Z es una parada de 2 horas, se tomará el escalón correspondiente, cuyo valor económico se valoró anteriormente.

El impacto de una amenaza sobre un activo.

Es el valor correspondiente al escalón de degradación, *"v[e_i]"*.

El impacto acumulado empleará en valor acumulado sobre el activo que es víctima de la amenaza.

El impacto repercutido empleará el valor propio del activo superior en el escalón de degradación del impacto inferior que es víctima de la amenaza. Si el análisis es cuantitativo, se multiplica el valor propio por el grado de dependencia.

Ejemplo.

En el ejemplo anterior, un virus informático provoca una detención de unas 48 horas. El impacto en el servidor es [5], lo mismo que en el servicio web. El impacto repercutido en el servicio escrito es [0].

La frecuencia de una amenaza.

Se empleará el modelo cualitativo o cuantitativo, según corresponda.

El riesgo que supone una amenaza para un activo.

Se empleará el modelo cualitativo o cuantitativo, según corresponda.

La eficacia de una salvaguarda frente al impacto.

Una salvaguarda frente a la interrupción del servicio se caracteriza por un tiempo de reacción: lo que tarde en reponer el servicio.

A fin de calificar la eficacia de la salvaguarda, se toma el escalón correspondiente a dicho tiempo de "respuesta garantizada"[5].

Ejemplo.

En el caso anterior, se puede desplegar un sistema antivirus que permite reactivar el servicio en 6 horas. Se dice que su eficacia está en el escalón de las 6 horas.

5 El razonamiento es como sigue. Si una parada superior a x1 horas supone un perjuicio v1, y una parada superior a x2 horas, un perjuicio v2; entonces, una parada de x horas, siendo x1 …≤ x < x2, supone un perjuicio v1, dado que no ha llegado al nivel x2.

Este escalón de eficacia puede ser e_0, si la salvaguarda es tan contundente que no deja lugar ni al primer escalón valorado, e_1.

Este escalón de eficacia es el mismo que la degradación cuando la salvaguarda es incapaz de reducir el impacto[6].

Este escalón de eficacia nunca puede ser superior al escalón de degradación, pues una salvaguarda no puede empeorar la situación de un activo frente a una amenaza.

Además del escalón de eficacia, las salvaguardas que se consideran aplicables al caso constituyen un paquete que se puede caracterizar por su eficacia reduciendo el impacto, e^i, y su eficacia reduciendo la frecuencia, e^f. El cálculo de estos coeficientes se describe más adelante.

Lo que sí hay que indicar es cómo calcular el escalón de efectividad de un paquete de salvaguardas:

escalón(ps)=	escalón(s)	si s es singular
	$\max_k$ { escalón(ps_k) }	si ps= todas (ps_k)
	$\min_k$ { escalón(ps_k) }	si ps= algunas (ps_k)
	$\min_k$ { escalón(ps_k) }	si ps= una (ps_k)

Donde el valor especial *"na"*[7] se comporta como elemento neutro en las operaciones.

De forma que, de un conjunto de salvaguardas alternativas se requiere al menos una que sea efectiva. Y que, de un conjunto de salvaguardas concurrentes, la eficacia la marca la peor de ellas.

La degradación residual.

Si el activo, sin protección, se posicionada en el escalón *"e_d"* de degradación, gracias a las salvaguardas se colocará en el escalón propuesto como escalón de eficacia, *"e_s";* pero modulado por la eficacia *"e^i"* frente al impacto, resultado en un escalón residual *"e_r":*

$$r = \lfloor d - ((d - s) \times e^i) \rfloor$$ [8]

Donde el valor especial "na" se valora como 0.

El impacto residual.

Es el valor correspondiente al escalón residual:

$$impacto\_residual = valor[e_r]$$

Ejemplo.

En el caso anterior, si se despliega un sistema antivirus que permite reactivar el servicio en 6 horas, el impacto residual en servidor y servicio web quedan en [3].

Si se desplegara un sistema antivirus que garantizase la reposición del servicio en 30 minutos, el impacto residual sería [0].

La frecuencia residual.

Se empleará el modelo cualitativo o cuantitativo, según corresponda.

6 Un centro de respaldo que empieza a funcionar en 48 horas es inútil frente a amenazas que detienen el servicio durante 6 horas.
7 na: no aplica.
8 La notación $\lfloor v \rfloor$ indica el entero que resulta de un redondeo por defecto.

El riesgo residual.

En base al impacto residual y la frecuencia residual, se empleará el modelo cualitativo o cuantitativo, según corresponda.

2.2.4. Sobre la eficacia de las salvaguardas

Todos los modelos requieren una evaluación de la eficacia de las salvaguardas que se despliegan para proteger a un activo de una amenaza. Se describe a continuación un modelo común para evaluar la eficacia de un conjunto de salvaguardas aplicadas sobre un activo.

Paquete de salvaguardas.

Frente a una amenaza se despliega un paquete de salvaguardas que no es sino un conjunto de salvaguardas singulares acumuladas sobre un activo. Las diferentes salvaguardas se pueden acumular de forma concurrente (todas son necesarias para surtir efecto), de forma excluyente (sólo tiene efecto una de un conjunto) o de forma aditiva (cuantas más, mejor).

```
ps::= salvaguarda
    | todas(ps0, ps1, ...)
    | algunas (ps0, ps1, ...)
    | una (ps0, ps1, ...)
```

La eficacia de una salvaguarda.

Cada salvaguarda se valora según su eficacia reduciendo el riesgo del activo que protege. La eficacia de un paquete de salvaguardas es un número real entre 0,0 y 1,0:

e	**razonamiento**
e = 1	si una salvaguarda es idónea (100% eficaz)
0 < e < 1	si una salvaguarda es insuficiente
e = 0	si una salvaguarda no sirve para nada
e = na	i una salvaguarda no tiene sentido en este contexto

La eficacia de la salvaguarda depende tanto de su capacidad natural para proteger el activo como de la calidad de su despliegue. El valor de la eficacia recoge ambos aspectos en un único parámetro.

La eficacia de un paquete de salvaguardas.

$$
e(ps) = \begin{cases} e(s) & \text{si s es singular} \\ \text{media}_k \{ e(ps_k) \}\ ^{9} & \text{si ps= todas } (ps_k) \\ \min \{ 1{,}0, \sum_k e(ps_k) \} & \text{si ps= algunas } (ps_k) \\ \max_k \{ e(ps_k) \} & \text{si ps= una } (ps_k) \end{cases}
$$

Donde el valor especial *"na"* se comporta como elemento neutro en las operaciones de cálculo del máximo, producto o suma.

De forma que, de un conjunto de salvaguardas concurrentes, la eficacia es la media de ellas; de un conjunto de salvaguardas aditivas, la eficacia de las salvaguardas se acumula, con un límite del 100%; y de un conjunto de salvaguardas alternativas, la eficacia la marca la mejor.

9 El valor medio se calcula de la forma habitual: se suman las eficacias diferentes de NA y se divide por el número de sumandos.

Eficacia ponderada de un paquete de salvaguardas

Como eficacia de un paquete de salvaguardas se ha tomado el valor medio de las eficacias de los componentes. Este cálculo puede modularse si se tiene en cuenta que no todas las salvaguardas son de la misma naturaleza, introduciendo una ponderación *"p":*

$$e(ps) = \sum_k e(ps_k) \times p_k \ / \sum_k p_k$$

El caso particular de que todas las salvaguardas sean igual de importantes, se consigue tomando *"p = 1".*

La eficacia frente al impacto y la frecuencia de una amenaza.

El riesgo combina impacto y frecuencia. Una salvaguarda puede reducir el impacto, o la frecuencia, o ambas facetas. Depende de la naturaleza de la salvaguarda el que actúe sobre el impacto o sobre la frecuencia.

Así, en los párrafos anteriores, se puede diferenciar entre la eficacia reduciendo el impacto, *"e^i",* y la eficacia reduciendo la frecuencia *"e^f",* Ambas eficacias se estiman con el mismo criterio: satisfacción de su cometido. Por último se puede calcular la eficacia reduciendo el riesgo, *"e",* como

$$(1 - e^i) \times (1 - e^f) = 1 - e$$

2.3. Árboles de ataque

Los árboles de ataque son una técnica para modelar las diferentes formas de alcanzar un objetivo. Aunque han existido durante años con diferentes nombres, se hicieron famosos a partir de los trabajos de B. Schneier que propuso sus sistematización en el área de los sistemas de información.

El objetivo del atacante se usa como raíz del árbol. A partir de este objetivo, de forma iterativa e incremental se van detallando como ramas del árbol las diferentes formas de alcanzar aquel objetivo, convirtiéndose las ramas en objetivos intermedios que a su vez pueden refinarse. Los posibles ataques a un sistema se acaban modelando como un bosque de árboles de ataque.

Un árbol de ataque pasa revista a cómo se puede atacar un sistema y por tanto permite identificar qué salvaguardas se necesita desplegar para impedirlo. También permiten estudiar la actividad del atacante y por tanto lo que necesita saber y lo que necesita tener para realizar el ataque; de esta forma es posible refinar las posibilidades de que el ataque se produzca si se sabe a quién pudiera interesar el sistema y/o la información y se cruza esta información con la habilidades que se requieren.

Veamos un ejemplo ilustrativo sobre como usar fraudulentamente (sin pagar) un servicio de pago:

1. **Objetivo**: usar sin pagar (OR)
    1. suplantar la identidad de un usuario legítimo
    2. soslayar la identificación de acceso al servicio
    3. abusar del contrato (AND)
        1. ser un usuario legítimo
        2. conseguir que no se facture el servicio (OR)
            1. que no queden trazas de uso
            2. que se destruyan las trazas antes de facturación (OR)
                1. las destruyo yo
                2. engaño al operador para que las borre
                3. manipulo del sw para que no las sume
            3. repudiar las trazas
            4. dar datos de cargo falsos

Lo más habitual para alcanzar un objetivo o subobjetivo es que se disponga de varias maneras alternativas (nodos OR); aunque en ocasiones se requiere la concurrencia de varias actividades (nodos AND). En conjunto, se consigue un esquema de las diferentes maneras en las que un usuario podría usarlo sin pagar por ello.

2.3.1. Nodos con atributos

Identificadas las diferentes maneras de alcanzar un objetivo, los nodos del árbol se pueden enriquecer con información de detalle, que puede ser de muy diferentes tipos; por ejemplo:

- conocimientos que se requieren del atacante: cualquiera, alguna experiencia, un ingeniero, un *hacker* profesional, etc.
- inversión del atacante: cantidad de dinero y tiempo que tendría que desembolsar para realizar la acción
- riesgo para el atacante: si es capturado, ¿qué consecuencias afrontaría?

Si la información del árbol con estos atributos se procesa automáticamente, podemos obtener escenarios simplificados de ataque:

- usuarios inexpertos pero con bastante dinero
- atacantes profesionales pero sin capacidad de inversión (o sin necesidad de realizar una inversión adicional para perpetrar este ataque)

- atacantes que quedarían impunes
- etc.

Para alcanzar estos escenarios especializados basta eliminar del árbol las ramas que no satisfagan una condición cualitativa o cuantitativa[10].

Sobre un árbol con atributos es posible determinar el ataque más probable, simplemente extrayendo aquel ataque que requiere menos medios y menos conocimiento por parte del atacante. También es posible determinar cuál será la línea de acción de un posible perfil de atacante (que se determina en base al tipo de servicio o información que estamos protegiendo): aquel que con menos coste satisfaga los conocimientos mínimos para realizar el ataque.

2.3.2. Riesgo residual

Cuando se han desplegado salvaguardas, su efecto puede reflejarse sobre el árbol de ataque:

- incrementando el conocimiento que el atacante necesitaría para alcanzar su objetivo pese a las salvaguardas desplegadas: idealmente debería ser imposible por mucho que supiera
- incrementando el desembolso que el atacante tendría que realizar para alcanzar su objetivo a la vista de las salvaguardas desplegadas: idealmente el coste debería ser superior al beneficio para el atacante

Un sistema ideal de salvaguardas eliminaría todas las ramas del árbol. Un sistema real suele llevar los atributos a niveles elevados de conocimiento e inversión que reducen la posibilidad de que el ataque se materialice a un nivel residual aceptado por la Dirección.

2.3.3. Construcción del árbol

La construcción del árbol es laboriosa. Marcar el objetivo final requiere un conocimiento de dónde está el valor en la Organización y cual puede ser el objetivo del atacante respecto del mismo. El enriquecimiento en forma de ramas debería ser exhaustivo; pero está limitado por la imaginación del analista; si el atacante es “más listo” tiene una oportunidad para utilizar una vía imprevista. La experiencia permite ir enriqueciendo el árbol con nuevos ataques realmente perpetrados o simplemente detectados en el perímetro con un buen sistema de monitorización.

Puede encontrarse ayuda a la construcción del árbol en

- la experiencia propia o ajena en sistemas similares
- grupos de reflexión (*brain storming meetings*) en los que de forma informal se van exponiendo cosas que posiblemente pensarían los atacantes; estas sesiones suelen generar mucho material en bruto que hay que organizar y estructurar para ser utilizado como herramienta de análisis
- herramientas que sugieran ataques en base a la naturaleza de los activos presentes en el sistema

Si se dispone de un modelo de valor como el desarrollado en las actividades de la metodología Magerit, es posible utilizar éste para determinar la naturaleza de los activos y las dependencias entre ellos, de forma que podemos elaborar el árbol de ataques en base al conocimiento de los activos inferiores que constituyen la vía de ataque para alcanzar los activos superiores en los que suele residir el valor para la Organización.

Resumen

Los árboles de ataque son una herramienta gráfica para analizar y presentar qué puede pasar y cómo lo prevenimos. Capturan de alguna forma el razonamiento del atacante y permiten anticiparse a lo que pudiera ocurrir.

10 Los cálculos suelen ser sencillos y permiten trabajar con diferentes niveles de refinamiento. Los nodos OR cuestan lo que el más barato de sus hijos. Los nodos AND suman los costes. En el caso de analizar conocimientos, los nodos OR requieren en conocimiento más bajo, mientras que los nodos AND requieren el conocimiento del hijo más sofisticado. Nótese que para tomar decisiones combinadas hay que ir al último nodo de detalle, pues frecuentemente lo más barato y lo más sofisticado son condiciones contradictorias.

Aunque es difícil construir árboles exhaustivos en el primer intento, sí son un buen soporte para ir incorporando la experiencia acumulada y recopilar en cada momento el mejor conocimiento de que se dispone. De esta forma es posible realizar simulaciones:

- ¿qué pasaría si introducimos nuevos activos?
- ¿qué pasaría si cambiamos las salvaguardas?
- ¿cómo lo enfocaría un atacante de perfil X?

Nótese que los árboles de ataque constituyen una documentación extremadamente valiosa para un atacante, especialmente cuando incorporan el estado actual de salvaguardas, pues facilitan en extremo su trabajo. Por ello deberán extremarse las medidas de protección de su confidencialidad.

Su principal inconveniente se encuentra en que es explosivo por la cantidad de árboles y detalle que pueden ser necesarios para recopilar todas las amenazas posibles sobre un sistema medianamente complejo. Por ello cabe esperar su uso como complemento a un análisis de riesgos, permitiendo profundizar en algunas líneas de ataque y dramatizar sus consecuencias.

2.3.4. Referencias

- J. Viega et al., “Risk Analysis: Attack Trees and Other Tricks”, Software Development Magazine, August 2002.
- A.P. Moore et al., “Attack Modeling for Information Security and Survivability”, Software Engineering Institute, Carnegie Mellon University, Technical Note CMU/SEI-2001-TN-001, 2001.
- B. Schneier, “Secrets and Lies: Digital Security in a Networked World”, John Wiley & Sons, 2000.
- B. Schneier, “Attack Trees: Modeling Security Threats”, Dr. Dobb's Journal, December 1999.

ISO 31010
ISO/IEC 31010:2009, Risk management — Risk assessment techniques.
UNE-ISO/IEC 31010:2010, Gestión del riesgo. Técnicas de apreciación del riesgo.

Esta norma introduce, a título informativo, multitud de técnicas para valorar diferentes magnitudes para analizar riesgos. Aunque los árboles de ataque no aparecen como tales, hay varias técnicas cercanas que analizan secuencias de ataque:

B.5 Análisis preliminar de peligros (PHA)

B.7 Análisis de riesgos y puntos de control críticos (HACCP)

B.14 Análisis de árbol de fallos (FTA)

B.15 Análisis del árbol de sucesos (ETA)

B.16 Análisis de causa-consecuencia

B.17 Análisis de causa-y-efecto

B.18 Análisis de capas de protección (LOPA)

B.19 Análisis de árbol de decisiones

B.21 Análisis de pajarita

B.26 Estadísticas y redes Bayesianas

3. Técnicas generales

En este capítulo nos referiremos a técnicas generales que, entre otros casos, son de utilizad en el desarrollo de un proyecto de análisis y gestión de riesgos. No obstante su generalidad, cuando procede se ha indicado cómo se aplican en el contexto del análisis y gestión de riesgos. Las indicaciones dadas en este libro complementan a las presentadas a lo largo de la metodología.

Se han considerado de especial interés:

1. técnicas gráficas: histogramas, diagramas de Pareto y de tarta
2. sesiones de trabajo: entrevistas, reuniones y presentaciones
3. valoraciones Delphi

que se desarrollan en las siguientes secciones.

3.4. Técnicas gráficas

Esta sección se centra en cómo algunas representaciones gráficas de los elementos de un proyecto AGR pueden apoyar a dicho proyecto, tanto como soporte a presentaciones, como en la toma de decisiones.

Se presentan:

- Gráficas para presentar resultados
  - puntos
  - barras
  - radar
- Diagramas de Pareto, para priorización de acciones
- Diagramas de tarta

3.4.2. Por puntos y líneas

Es la forma más clásica de presentación de resultados. Se limita a usar los ejes cartesianos usando las abscisas para recoger los datos y las ordenadas para mostrar su valor.

Los datos en ordenadas se pueden representar en escala lineal o en escala logarítmica. La escala lineal es razonable cuando el rango de valores es reducido, imponiéndose la escala logarítmica cuando el rango es grande (órdenes de magnitud). No obstante, el principal criterio para elegir el tipo de escala debería ser la naturaleza del valor que se quiere representar. Una escala lineal es adecuada cuando importa transmitir la diferencia absoluta entre valores

$$x_i - x_j$$

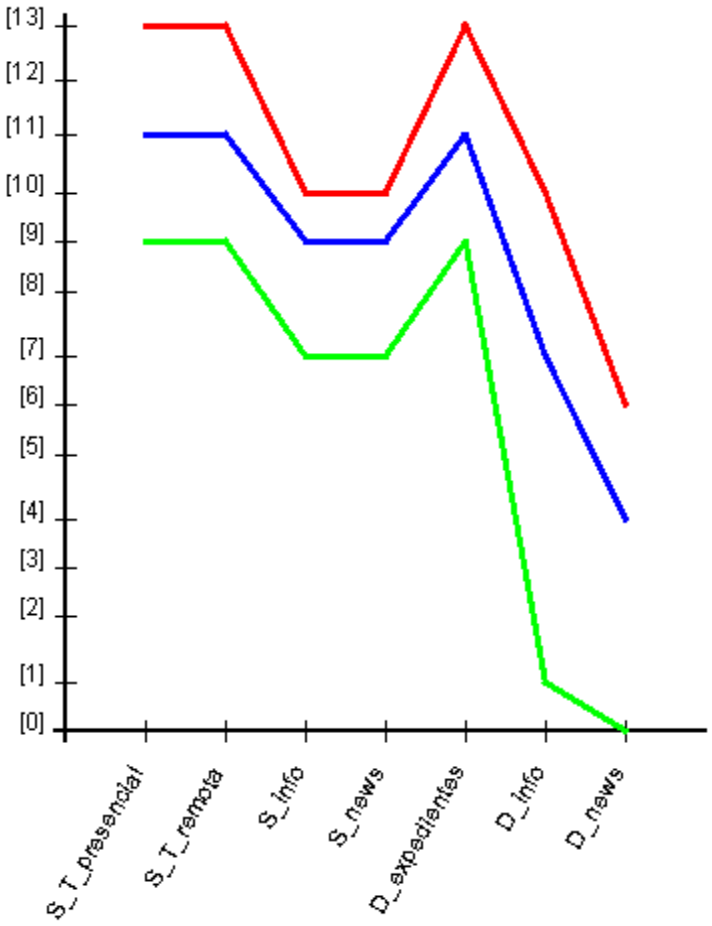
Por el contrario, una escala logarítmica es adecuada cuando importa transmitir la diferencia relativa entre valores:

$$\frac{x_i - x_j}{x_i}$$

En proyectos de análisis y gestión de riesgos se trabaja con múltiples magnitudes que son percepciones de valor que se ajustan naturalmente a escalas logarítmicas.

A veces se pintan las líneas que unen los puntos correspondientes a cada valor en el eje Y para cada dato en el eje X. Otras veces sólo se pintan los puntos. A veces se introducen líneas horizontales de nivel para marcan umbrales: valores mínimos o máximos para alguna toma de decisiones.

Como ejemplo, se presenta el resultado de cálculo de riesgo en un sistema de información, a lo largo de varias fases del proyecto:



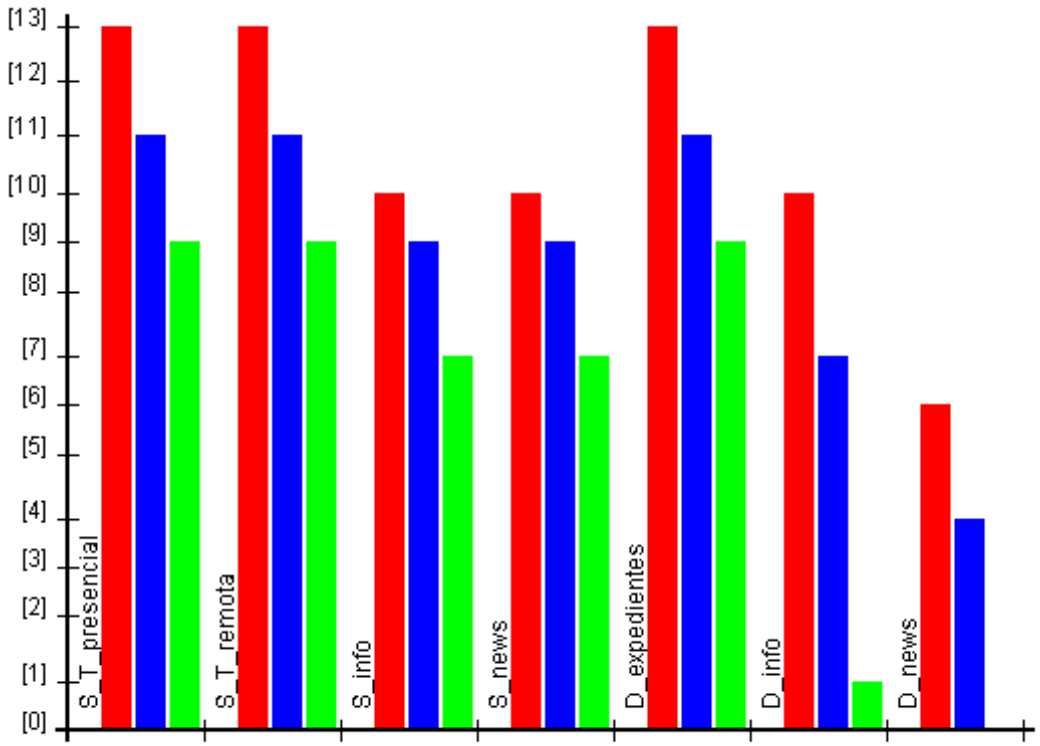
Estas gráficas permiten acumular gran cantidad de información. Informalmente, se puede decir que son más apreciadas por personas con perfil técnico.

3.4.3. Por barras

Los diagramas de barras disponen los elementos en unas coordenadas cartesianas convencionales: los elementos a considerar en un eje y los valores en el otro eje. Son muy similares a las presentaciones por puntos y líneas, aunque permiten menos resultados (dado que las barras ocupan más espacio que los puntos).

El eje Y puede disfrutar de una escala lineal o logarítmica. Ver consideraciones expuestas en la sección anterior.

Como ejemplo, se presenta el resultado de cálculo de riesgo en un sistema de información, a lo largo de varias fases del proyecto:



En este tipo de diagramas es fácil recopilar todos los valores. A veces se introducen líneas horizontales de nivel para marcan umbrales: valores mínimos o máximos para alguna toma de decisiones.

Informalmente, se puede decir que son presentaciones apreciadas por personas con perfil técnico.

3.4.4. Gráficos de 'radar'

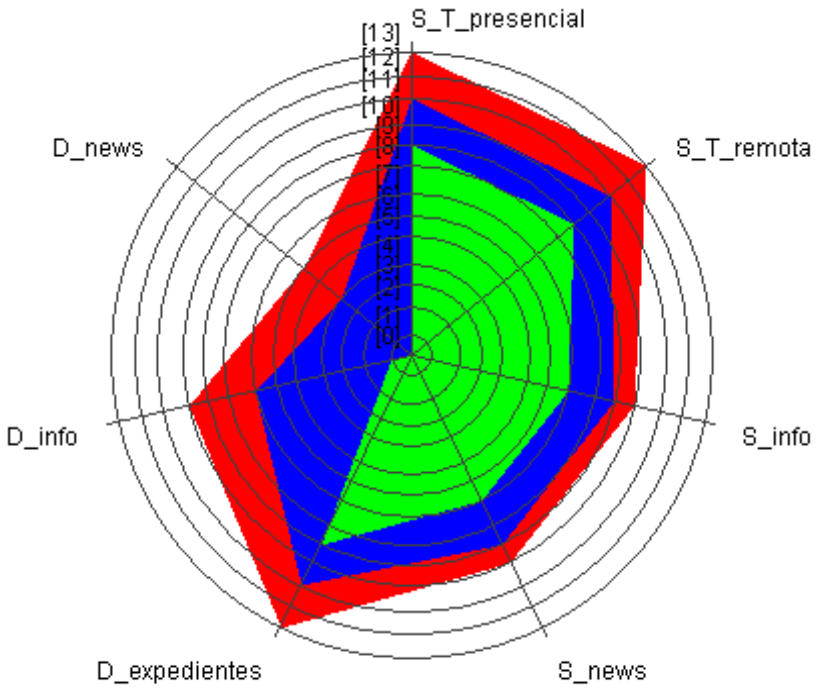
Estos gráficos representan las distintas variables o factores del fenómeno en estudio sobre semiejes o radios que parten de un centro. Estos radios, tantos como factores, se gradúan para representar sus niveles y posibles umbrales en escala normal o logarítmica, según convenga.

El valor alcanzado por cada factor o variable se marca en su radio respectivo (el centro representa el valor cero). Se unen por segmentos los puntos consecutivos así marcados, correspondientes a los valores de las variables definidas en los semiejes, obteniendo un polígono irregular 'estrellado' denominado gráfico de 'radar' o 'rosa de los vientos'.

Todos ellos ofrecen una visión sintética del fenómeno que permite estudiarlo globalmente, facilitando la observación de sus características y tendencias así como el balance entre sus distintos factores o elementos. Esta visión sintética es especialmente importante en el análisis y gestión de riesgos, donde se busca cierto equilibrio entre factores complementarios. La seguridad procede más de una cobertura homogénea sin fisuras que de una cobertura muy alta en ciertos aspectos frente a claras deficiencias en otros buscando una cierta compensación.

El gráfico de 'radar' básico exige empezar por decidir qué factores o variables se van a incluir. Así, si se busca representar el estado global de seguridad de una Organización, los factores serán los diferentes servicios. Tras obtener, calcular, clasificar y tabular los valores de cada factor, se dibujan las escalas como radios (dentro de un círculo máximo cuyo radio sea el valor más alto normalizado en cada semieje). Hay que cuidar siempre que exista la misma distancia angular entre los semiejes (es decir que éstos dividan el círculo máximo en arcos iguales).

El siguiente ejemplo muestra la evolución del riesgo sobre los activos de tipo servicio y datos:



A veces se marcan algunos niveles (circunferencias) con valores especiales tales como umbrales mínimos o cotas máximas. A veces se rellena la superficie abarcada, aunque otras veces se pintan sólo las líneas del perímetro. Las superficies son útiles cuando no se da el caso de que un área “tape” a otra. Las líneas siempre son utilizables.

Este tipo de diagramas permiten:

- sintetizar gráficamente el equilibrio o desequilibrio en varios ejes
- acumular perfiles de máximos o de mínimos
- mostrar la evolución temporal

Informalmente, se puede decir que son presentaciones apreciadas por personas con perfil gerencial o de dirección.

3.4.5. Diagramas de Pareto

Vilfredo Pareto (1848-1923) fue economista italiano estudioso de la distribución de la riqueza. Descubrió que la minoría de la población poseía la mayor parte de la riqueza y la mayoría de la población poseía la menor parte de la riqueza. Con esto estableció la llamada "Ley de Pareto" según la cual la desigualdad económica es inevitable en cualquier sociedad.

Posteriormente, se aplicó este concepto a la calidad, obteniéndose lo que hoy se conoce como la regla 80/20. Según este concepto, si se tiene un problema con muchas causas, se puede decir que el 20% de las causas resuelven el 80% del problema y el 80% de las causas solo resuelven el 20% del problema.

El análisis de Pareto es una técnica que separa los “pocos vitales” de los “muchos normales”. Una gráfica de Pareto es utilizada para separar gráficamente los aspectos más significativos de un problema que el equipo sepa dónde dirigir sus esfuerzos para mejorar. Reducir los problemas más significativos (las barras más largas en una gráfica Pareto) servirá más para una mejora general que reducir los más pequeños. Con frecuencia, un aspecto tendrá el 80% de los problemas. En el resto de los casos, entre 2 y 3 aspectos serán responsables por el 80% de los problemas.

La minoría vital aparece a la izquierda de la gráfica y la mayoría normal a la derecha. Hay veces que es necesario combinar elementos de la mayoría normal en una sola clasificación denominada otros, la cual siempre deberá ser colocada en el extremo derecho. La escala vertical es para el costo en unidades monetarias, frecuencia o porcentaje.

La gráfica es muy útil al permitir identificar visualmente en una sola revisión tales minorías de características vitales a las que es importante prestar atención y de esta manera utilizar todos los recursos necesarios para llevar acabo una acción correctiva sin malgastar esfuerzos.

Algunos ejemplos de tales minorías vitales podrían ser:

- La minoría de clientes que representen la mayoría de las ventas.
- La minoría de productos, procesos, o características de la calidad causantes del grueso de desperdicio o de los costos de reelaboración.
- La minoría de rechazos que representa la mayoría de quejas de la clientela.
- La minoría de vendedores que esta vinculada a la mayoría de partes rechazadas.
- La minoría de problemas causantes del grueso del retraso de un proceso.
- La minoría de productos que representan la mayoría de las ganancias obtenidas.
- La minoría de elementos que representan al grueso del costo de un inventarios.

Un equipo puede utilizar la Gráfica de Pareto para varios propósitos durante un proyecto para lograr mejoras:

- Para analizar las causas
- Para estudiar los resultados
- Para planear una mejora continua
- Para comparar fotos de “antes y después” y estudiar qué progreso se ha logrado.

Aplicado a proyectos análisis y gestión de riesgos, cabe citar los siguientes usos

- riesgo del sistema en función de los activos, quizás para cierta dimensión de seguridad, permitiendo detectar qué activos contribuyen fundamentalmente al riesgo del sistema
- riesgo del sistema en función de las amenazas, quizás para cierta dimensión de seguridad, permitiendo detectar qué amenazas contribuyen fundamentalmente al riesgo del sistema

3.4.5.1. Construcción

1. Seleccionar las categorías lógicas
2. Reunir datos: valor para cada categoría
3. Ordenar los datos de mayor a menor a menor valor
   - a menudo conviene introducir una nueva categoría “otros” para agrupar los datos de menor valor para los que no se requiere detalle; esta categoría siempre es la última
   4. Calcular el valor agregado para cada categoría
   - y calcular el porcentaje del total que cada categoría representa
5. Trazar los ejes:
   - eje horizontal (x) para las categorías
   - eje vertical (Y) primario, para la magnitud propia del valor a representar; puede ser lineal o logarítmica, según convenga
   - eje vertical (Y) secundario, para el porcentaje del total: lineal
6. De izquierda a derecha trazar las barras para cada categoría. Si existe una categoría “otros”, debe ser colocada al final, sin importar su valor. Es decir, que no debe tenerse en cuenta al momento de ordenar de mayor a menor la frecuencia de las categorías.
7. Trazar el gráfico para el porcentaje agregado
8. Analizar la gráfica para determinar los “pocos vitales”

3.4.5.2. Ejemplo práctico

Se aplican los pasos anteriores a un caso práctico, a título de ilustración.

Pasos 1 y 2: seleccionar categorías y recopilar valores

Como resultado del análisis de riesgos, se dispone de la siguiente tabla que resume el riesgo en los diferentes servicios y datos del sistema de información

activos	*riesgo*
[S] Servicios	
[S_T_remota] tramitación vía www	132.400
[S_T_presencial] tramitación presencial	99.300
[S_notificación] notificación telemática	83.400
[S_info] información de normativa	40.400
[S_news] noticias y modificaciones	5.300
[D] Datos / información	
[D_ciudadanos] identificación de usuarios	7.300
[D_económicos] datos económicos	120.600
[D_expedientes] estado de la tramitación	45.000
[D_normativa] normativa legal	55.100
[D_histórico] de cambios	12.200

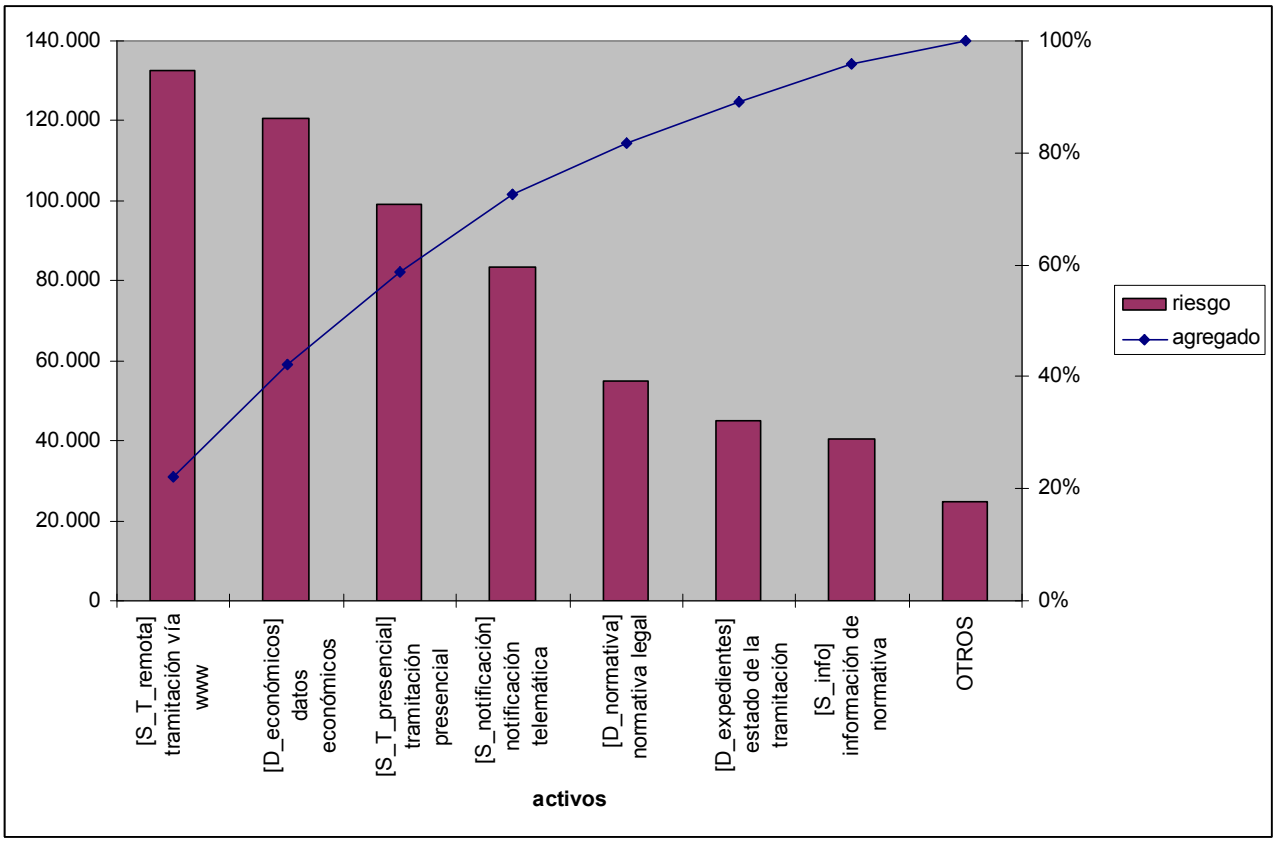
Paso 3: ordenar los datos e introducir "otros"

activos	*riesgo*
[S_T_remota] tramitación vía www	132.400
[D_económicos] datos económicos	120.600
[S_T_presencial] tramitación presencial	99.300
[S_notificación] notificación telemática	83.400
[D_normativa] normativa legal	55.100
[D_expedientes] estado de la tramitación	45.000
[S_info] información de normativa	40.400
OTROS	*24.800*

Paso 4: agregar datos y calcular porcentajes

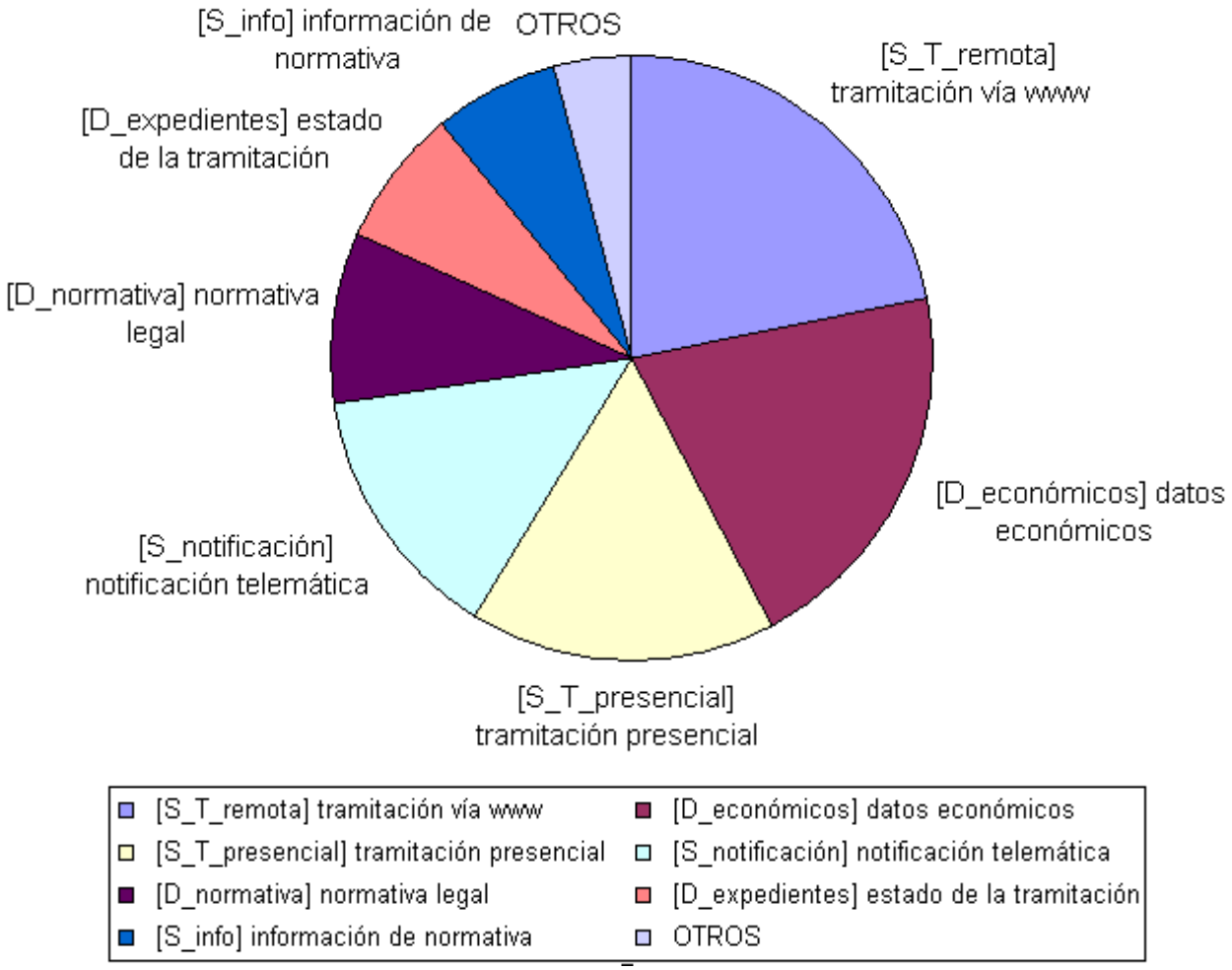
activos	*riesgo*	*agregado*	
[S_T_remota] tramitación vía www	132.400	132.400	22%
[D_económicos] datos económicos	120.600	253.000	42%
[S_T_presencial] tramitación presencial	99.300	352.300	59%
[S_notificación] notificación telemática	83.400	435.700	72%
[D_normativa] normativa legal	55.100	490.800	82%
[D_expedientes] estado de la tramitación	45.000	535.800	89%
[S_info] información de normativa	40.400	576.200	96%
OTROS	24.800	601.000	100%
	601.000		

Pasos 5, 6 y 7: dibujar la gráfica



3.4.6. Diagramas de tarta

Estos diagramas presentan los datos como fracciones de un círculo, distribuidos los 360º de éste en proporción al valor que es representado en cada sección. La proporción suele ser lineal; rara vez logarítmica.



Aunque los datos pueden ordenarse de la forma que más interese en cada momento, es frecuente usar una ordenación de valor decreciente (siguiendo el procedimiento indicado para los diagramas de Pareto).

Los diagramas de tarta no permiten presentar muchos datos simultáneamente; pero si son una indicación muy gráfica de cómo las diferentes partes contribuyen al total.

3.6. Sesiones de trabajo

Las sesiones de trabajo tienen diversos objetivos. Dependiendo del tipo de sesión que se realice, los objetivos pueden ser: obtener información, comunicar resultados, reducir el tiempo de desarrollo, activar la participación de usuarios y directivos o aumentar la calidad de los resultados. Las sesiones de trabajo pueden ser de varios tipos en función de las personas que participen en ellas, el objetivo que se persiga y el modo de llevarlas a cabo.

Las **entrevistas** son un tipo de sesiones de trabajo dirigidas a obtener la información de una forma individual dónde aparecen los perfiles de entrevistado y entrevistador.

Las **reuniones** pueden tener el mismo objetivo, pero la información está dispersa entre varias personas y únicamente trabajando en grupo, se conseguirá extraer y depurar toda la información de forma global.

El objetivo de las **presentaciones** es la comunicación de avances, conclusiones y resultados por parte del equipo de trabajo al auditorio que corresponda. Se llevan a cabo con el fin de informar sobre el estado de un proyecto en su totalidad o de alguno de los procesos, o exponer uno o varios productos finales de un proceso para su aprobación.

3.6.1. Entrevistas

Las entrevistas son reuniones con una persona o un grupo de personas con el objetivo de recabar cierta información. Las entrevistas se dicen estructuradas cuando se atiene a una serie de preguntas planificadas sin margen para la improvisación. Las entrevistas se dicen libres cuando, existiendo un objetivo claro, no existe un formulario rígido.

En proyectos de análisis y gestión de riesgos suelen practicarse entrevistas semi-estructuradas en las que, existiendo un guión preestablecido de preguntas, el entrevistado tiene margen para extenderse en puntos no previstos o, más frecuentemente, responderlas en un orden diferente al previsto. En cualquier caso el guión se emplea para no olvidar nada.

Por ser más precisos, en las primeras tareas (T1.1.1, Determinar la oportunidad) es casi imposible disponer de un cuestionario rígido, y el entrevistado debe disfrutar de una elevada flexibilidad. En las tareas de descubrimiento (como, por ejemplo, T2.1.1, Identificación de activos) las entrevistas son semi-estructuradas, usando el cuestionario como guía que hay que adaptar. En las tareas de detalle (como, por ejemplo, T2.1.3, Valoración de activos), el margen de maniobra está fuertemente pautado, usándose entrevistas estructuradas.

El mayor volumen de entrevistas en un proyecto AGR se encuentra en las tareas del proceso P2, Análisis de riesgos, en el que hay que centrarse especialmente.

Las actividades A2.1 (caracterización de los activos), A2.2 (caracterización de las amenazas) y A2.3 (caracterización de las salvaguardas) del proceso P2 (análisis de riesgos), permiten conocer los elementos objeto del análisis de riesgos, identificándolos, valorándolos y relacionándolos. Para capturar este conocimiento se procede por medio de una serie de entrevistas con los participantes, según se determinó en la tarea T1.3.2 (organizar a los participantes) y de acuerdo al plan del proyecto (T1.3.3). Estas entrevistas tienen una importancia crucial porque la información a recoger condiciona el conocimiento del equipo del proyecto (ajeno en parte al funcionamiento del dominio o sea dependiente de los conocedores de su comportamiento cotidiano). La recogida de información es una operación delicada que exige una buena sintonía entre los participantes para no que no quede oculta (ni voluntaria ni involuntariamente) alguna información que posteriormente pudiera revelarse importante y, al tiempo, no caer en un excesivo nivel de detalle que impida separar lo esencial de lo accesorio.

Por todo ello es necesario:

Durante la preparación de la entrevista:

1. Recopilar los cuestionarios personalizados distribuidos en la tarea T1.4.1.
2. Disponer del documento acreditativo de la Dirección.
3. Ubicar y localizar a los entrevistados, para optimizar la realización de las entrevistas, tanto espacial como temporalmente.

4. Confirmar cada entrevista, informando de los documentos que se van a requerir durante la entrevista, para facilitar su disponibilidad.

Durante la entrevista

5. Informar al entrevistado de los principales conceptos relacionados con la seguridad y la de los sistemas de información, en un grado que depende de su información y experiencia en la materia.
6. Recordar los objetivos de cada entrevista al entrevistado.
7. Perfilar el entorno de trabajo del entrevistado.
8. Recabar las funciones y objetivos del entrevistado.
9. Recabar el modo de actuación del entrevistado.
10. Identificar los medios de que dispone para realizar las funciones y del personal a su cargo.
11. Identificar los procesos realizados y de la información manejada.
12. Identificar posibles situaciones conflictivas (internas o externas, accidentales o provocadas).

Para la adquisición de este conocimiento puede ser necesario entrevistar a diferentes colectivos dentro de la Organización:

- dirección o gerencia, que conocen las consecuencias que para la misión de la Organización tendrían los incidentes
- responsables de los servicios, que conocen los servicios que se manejan y las consecuencias de la no prestación del servicio o de su prestación degradada
- responsables de los datos, que conocen los datos que se manejan, su valor y las consecuencias de los incidentes que pudieran afectarles
- responsables de sistemas de información y responsables de operación, que:
  - conocen qué sistemas hay en operación
  - tienen el conocimiento histórico de lo que ha pasado anteriormente
  - conocen las consecuencias de un incidente
  - conocen las salvaguardas técnicas implantadas
  - conocen las actividades en curso relacionadas con la seguridad de los sistemas

3.6.2. Reuniones

Las reuniones tienen como objetivo obtener información que se encuentra repartida entre varias personas, tomar decisiones estratégicas, tácticas u operativas, transmitir ideas sobre un determinado tema, analizar nuevas necesidades de información, así como comunicar los resultados obtenidos como consecuencia de un estudio.

Para realizar una reunión es necesario designar a las personas que deben participar en ella y determinar el lugar en el que poder llevarla a cabo. Las directrices básicas de una reunión son:

- Preparar y convocar la reunión (orden del día)
- Realizar la reunión
- Consolidar el resultado de la reunión
- Elaborar el acta de reunión

Previamente a la convocatoria de la reunión, se definen los objetivos, se planifica el método de trabajo que se va a seguir y el tiempo del que se dispone, se eligen los participantes y se prepara el material necesario.

Después de la preparación, es imprescindible enviar al usuario la convocatoria con el orden del día de la reunión. Este orden incluye la fecha, hora de inicio, hora de finalización prevista, lugar,

asistentes y los puntos a tratar, detallando, entre otros, el tiempo que se dedicará a cada tema y la persona responsable de exponerlo. Dicha convocatoria se envía con antelación suficiente para que los asistentes puedan organizar su agenda y prepararse para la reunión con tiempo.

Al inicio de la reunión, es importante hacer un resumen general de los temas a tratar, los objetivos que se persiguen, el método de trabajo y la agenda de la reunión. Si se considera oportuno se puede utilizar la técnica de presentación. Desde su inicio se debe crear un clima de confianza entre los asistentes. La persona responsable de la reunión ejercita la dinámica de dirección de grupos, estimulando la participación, controlando el ritmo de la sesión y centrando o clarificando el tema cuando sea necesario. Al finalizar, se sintetizan las conclusiones, se comprueba si hay acuerdo o si quedan puntos pendientes de reflexión y se propone fechas para próximas reuniones.

El responsable de tomar las notas en la reunión, levanta el acta y la remite a los asistentes que deben confirmar su recepción.

3.6.3. Presentaciones

El objetivo de las presentaciones es la comunicación de avances, conclusiones y resultados por parte del equipo de trabajo al auditorio que corresponda. Se llevan a cabo con el fin de informar sobre el estado de un proyecto en su totalidad o de alguno de los procesos, o exponer uno o varios productos finales de un proceso para su aprobación.

En primer lugar se establece el alcance de la presentación, determinando cuál es el objetivo principal y qué contenido general se quiere comunicar.

Una vez que están claros estos puntos, se inicia la preparación de la presentación considerando quién es el ponente, qué tema se va a exponer, cuál va ser la duración estimada y a qué tipo de audiencia o auditorio va dirigida la presentación considerando, a su vez, el nivel de decisión que tengan sus componentes. Todos estos factores van a influir en el tono más o menos formal de la presentación, en el nivel de detalle que requiere la presentación y en los medios a utilizar.

La eficacia de una presentación está directamente relacionada con el conocimiento que posea el ponente sobre el tema a exponer, así como de la audiencia a quién va dirigido.

Las cuestiones que guían esta preparación responden a las preguntas, a quién se dirige, qué se espera conseguir, de cuánto tiempo se dispone, dónde se va exponer y con qué medios.

Una vez analizados todos estos aspectos, se estructura el mensaje que se quiere transmitir a la audiencia de forma que sea significativo y esté bien organizado. Su estructura se apoya en los objetivos y en el concepto esencial que se está tratando y se divide en una apertura o introducción, una visión previa, el cuerpo del tema, una revisión y la conclusión final. Previamente, el ponente debe decidir cuál es el enfoque más eficaz que le quiere dar al tema que va a exponer en función de la audiencia a quien va dirigido.

Para conseguir el objetivo de una presentación no es suficiente preparar de una forma estructurada el mensaje, sino que además, el contenido se debe exponer de una forma convincente, utilizando pruebas o materiales de apoyo que refuercen la credibilidad a la audiencia.

Por este motivo es importante seleccionar cuidadosamente el material de apoyo que se va a utilizar como pueden ser datos estadísticos, análisis de resultados, etc.

También tiene especial relevancia escoger los apoyos audiovisuales oportunos que aclaren conceptos o datos difíciles de captar, resaltar puntos significativos, reforzar la comunicación verbal, despertar interés, cambiar el ritmo de la presentación, etc. Habrá que seleccionar los temas que requieren mayor soporte audiovisual.

Conviene señalar que no se debe utilizar un número excesivo de medios ya que no son un fin en sí mismos y podrían dispersar la atención de la audiencia convirtiéndose en fuente de posibles imprevistos por fallos técnicos y repercutiendo negativamente en el ritmo de la presentación. Por este motivo, es importante conocer las ventajas e inconvenientes de cada medio como son pizarras, transparencias, diapositivas, vídeos, ayudas informatizadas, etc., para seleccionar el más apropiado y garantizar el éxito de la presentación.

Antes de iniciar la exposición, habrá que asegurar la disponibilidad de todos los recursos materiales necesarios que se hayan considerado oportunos en la preparación de la presentación.

Durante el desarrollo, es fundamental que el ponente hable con el ritmo adecuado y con un estilo verbal claro, correcto y conciso, y que cuide los aspectos formales. También debe mantener centrado el tema objeto de la presentación, resaltando los puntos más importantes y utilizando el material de soporte de forma adecuada y en el momento preciso, con el fin de captar la atención del auditorio.

Conviene prestar atención a la corrección con que el ponente se relaciona con la audiencia. Debe intentar mantener una actitud positiva y abierta ante las posibles preguntas o comentarios.

El estilo no verbal es la suma de todas las claves vocales (tono, voz, etc.) y visuales (expresión facial, gestos, movimiento, etc.) que el ponente transmite a la audiencia y es especialmente importante, ya que con él se puede ejercer un impacto significativo sobre la percepción y respuesta de la audiencia.

Al finalizar la presentación, puede ser conveniente realizar una evaluación en la que se recojan las capacidades del ponente, el modo en que se llevó a cabo, las características del contenido, material utilizado, etc. y con esta información valorar el grado de satisfacción de la audiencia y tomar las medidas que se consideren oportunas.

3.6.4. Referencias

- “Managing Information Security Risks: The OCTAVE Approach”, C.J. Alberts and A.J. Dorofee, Addison-Wesley Pub Co; 1st edition (July 9, 2002)
  http://www.cert.org/octave/
- Magerit, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, MAP, versión 1.0, 1997
  http://www.csi.map.es/csi/pg5m20.htm
- ISO 31010
  ISO/IEC 31010:2009, Risk management — Risk assessment techniques.
  UNE-ISO/IEC 31010:2010, Gestión del riesgo. Técnicas de apreciación del riesgo.

  B.2 Entrevistas estructuradas y semiestructuradas

3.7. Valoración Delphi

La técnica o método Delphi[11], original de la Rand Corporation (Research ANd Development), comenzó a aplicarse desde 1948 en un proyecto avanzado de las Fuerzas Aéreas de los Estados Unidos y la Compañía Douglas de Aviación, orientándose desde entonces a los estudios prospectivos de investigación espacial. De forma paulatina la técnica diseñada por la Rand Corporation ha ido ampliando sus campos de aplicación: así esta "reflexión intuitiva de expertos" (como algún autor denomina al método Delphi), puede ser utilizada con éxito en multitud de campos y sectores. Delphi es especialmente adecuada para Magerit por las razones siguientes:

- Es una técnica netamente cualitativa que relativamente permite tratar con alta precisión problemas técnicamente complejos.
- Está planteada como una reflexión organizada de expertos sobre un tema concreto, reflexión que permite recoger las ideas y opiniones más cualificadas en el ámbito de la seguridad (valoración de activos e identificación de amenazas e impactos).
- Se desarrolla a partir de un cierto 'escenario inicial' de modo que permita una adecuada recapitulación e identificación de los problemas que ya existen actualmente.
- Desarrolla una prospectiva mucho más rica que la mera identificación de la opinión mayoritaria, por medio de un proceso de convergencia de opiniones que se consigue mediante rondas sucesivas de entrevistas.
- Garantiza satisfactoriamente la 'limpieza' de la investigación, impidiendo el predominio de unos expertos sobre otros por razones ajenas a la calidad de sus opiniones.

La técnica Delphi es un instrumento de uso múltiple que se utiliza con muy variados objetivos:

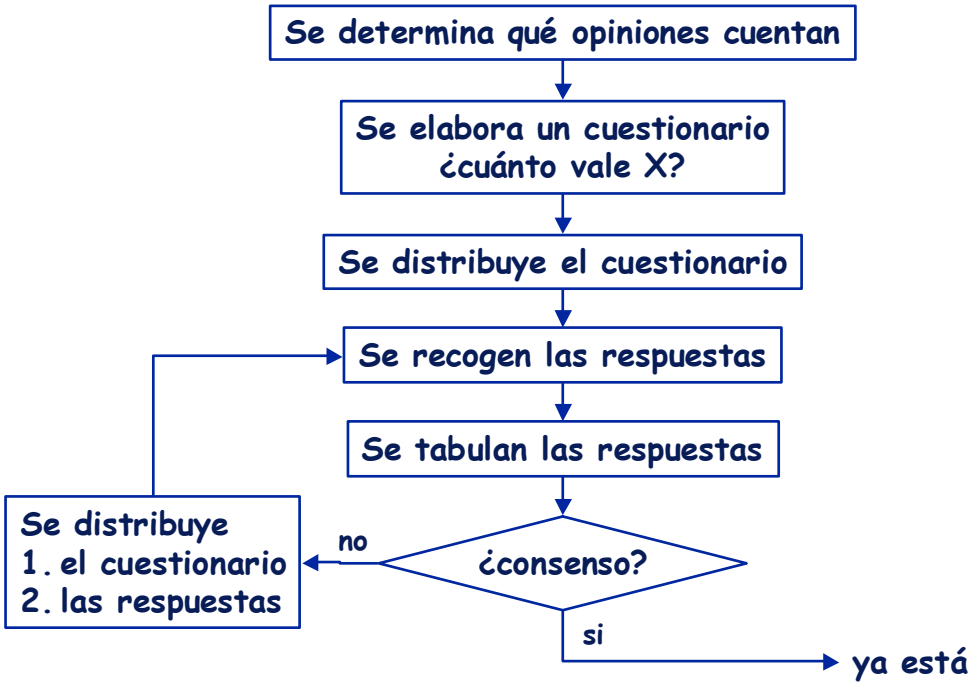
- Identificar problemas.
- Desarrollar estrategias para la solución de problemas, fijando un rango de alternativas posibles.
- Identificar factores de resistencia en el proceso de cambio.
- Establecer previsiones de futuro sobre la evolución de las tendencias que se observan en un determinado campo o sector.
- Contrastar opiniones en un tema abarcando un amplio campo de disciplinas o sectores.

3.7.1. Resumen ejecutivo

1. Se prepara un cuestionario con los temas cuya valoración se desea conocer. Este punto es crítico para el éxito de los siguientes pasos. Para la elaboración de un buen cuestionario se requiere experiencia y conocimiento del tema que se desea investigar.
2. Se distribuye entre los sujetos que tienen una opinión relevante en el tema a investigar: los expertos.
3. Con las respuestas recibidas, se prepara un histograma indicando cuántos entrevistados se decantan por cada nivel de valoración.
4. Si hay una clara concentración de respuestas en torno a un único valor, el proceso ha acabado: hay un claro consenso en el valor buscado.
5. Si hay diferencias importantes de opinión, se remite de nuevo el mismo cuestionario; pero esta vez acompañado del histograma. Si se han apreciado ambigüedades en el primer cuestionario, deben aclararse en esta segunda ronda. A los entrevistados se les inquiere sobre si consideran que deben mantener su primera opinión o prefieren modificarla.

11 "Delphi" es la forma inglesa de pronunciar Delfos, población griega famosa por su oráculo. Pese al origen fonético, el método usado por el Oráculo de Delphos (adivinación) no tenía nada que ver con el usado con el método Delphi (consenso de opinión entre expertos). Delphi basa la calidad de sus resultados en la hipótesis de que cuando no existe un conocimiento preciso de la realidad, lo mejor que se puede hacer es recoger la opinión, consensuada, de un grupo lo más amplio posible de expertos en la materia.

6. Si el histograma de esta segunda ronda sigue sin mostrar una respuesta clara, se pueden realizar nuevas rondas o convocar a los entrevistados en una reunión conjunta para llegar a un consenso.
7. Ante un histograma disperso, siempre hay que preguntarse si se ha hecho la pregunta correcta a las personas correctas, si la pregunta estaba claramente expresada o si, por el contrario se debe volver a empezar con nuevas preguntas y/o nuevos entrevistados.



En sentido estricto, Delphi no es tanto un método como un conjunto de técnicas que se aplican según las circunstancias. Algunos aspectos hay que determinarlos en cada caso:

Número de participantes.

Se estima que el número ideal se encuentra entre 15 y 35 expertos. Aplicado al análisis de riesgos, se pueden establecer grupos amplios en temas generales (por ejemplo, frecuencia típica de una amenaza o idoneidad de una salvaguarda para un riesgo); pero en temas puntuales es difícil pasar de unos pocos participantes (por ejemplo, para valorar un activo).

Número de rondas.

La segunda ronda es necesaria salvo que haya un consenso suficiente en la primera. Sucesivas rondas pueden dar una opinión más refinada; pero no esto no siempre se consigue por diferentes motivos:

- los expertos muestran rápidamente síntomas de agotamiento, disminuyendo su disposición a colaborar
- probablemente lo que está mal es el diseño del cuestionario y más vale revisarlo que insistir en el error

Como recomendación general para proyectos de análisis y gestión de riesgos, se puede centrar en número estándar en dos rondas.

3.7.2. Aspectos sociológicos

Delphi permite que un grupo trabaje aisladamente y de forma anónima. Es un instrumento que agrupa sistemáticamente las opiniones de un grupo y evita el excesivo protagonismo que pueden ejercer algunas personas, además de cualidades como éstas:

- La generación de ideas de forma aislada produce una mayor cantidad de éstas en el conjunto del grupo seleccionado.

- El proceso de respuestas escritas a las preguntas formuladas obliga a los que responden a pensar en toda la complejidad del problema y a proponer, por tanto, ideas de gran calidad.
- La conducta del grupo es proactiva, puesto que los que responden no pueden reaccionar ante las ideas expresadas por los otros, eliminando posibles excesos de protagonismo que se manifiestan cuando se expresan opiniones de forma directa y simultánea.
- El anonimato y el aislamiento entre los que responden proporciona una gran libertad frente a la presión hacia el conformismo en las opiniones.
- La técnica es válida para obtener opiniones de expertos que se encuentren físicamente alejados.
- Se puede comprobar que el error de predicción de un conjunto de expertos en un tema es siempre menor que la media de los errores de las opiniones individuales de las personas que lo integran.

3.7.3. Análisis de las respuestas

Delphi implica un análisis estadístico del producto de cada una de las rondas de cuestionarios. El análisis debe garantizar que la opinión de cada uno de los expertos se encuentre representada en la respuesta final.

Para determinar si hay consenso se necesita una medida de la dispersión de las respuestas. Para determinar cual es el consenso se necesita un punto de convergencia.

El análisis es diferente si se busca un valor en una escala continua de valoración (por ejemplo, intentando determinar el valor de un activo para la Organización) o si se intenta identificar elementos a considerar (por ejemplo, activos que deben incluirse en el análisis). En el caso de opiniones de valor, se recurre a estimaciones estadísticas. En el caso de opiniones, se recurre a esquemas de votación.

3.7.3.1. Análisis estadístico

Las respuestas se ubican sobre una escala de valores, lineal o logarítmica según la naturaleza del problema que se esté analizando. En aspectos de percepción subjetiva de valor, las escalas logarítmicas suelen ser las más adecuadas.

Dados n valores, $x_1, x_2, \cdots, x_n$ se definen los siguientes estadísticos:

Media o valor medio

$$\overline{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$$

Mediana

Habiendo ordenado los valores x_i en orden ascendente (de menor a mayor), se denomina **mediana** al primer valor que deja por debajo al 50% de los datos; es decir al valor en la posición $\lceil n/2 \rceil$

Desviación estándar o típica

$$\sigma = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n} (x_i - \overline{x})^2}$$

Desviación media

$$desviación\ media = \frac{1}{n}\sum_{i=1}^{n} |x_i - \overline{x}|$$

Cuartiles. Habiendo ordenado los valores en orden ascendente, se definen 3 puntos de interés

Q1: primer valor que deja por debajo al 25% de los datos

Q2: primer valor que deja por debajo al 50% de los datos (la mediana)

Q3: primer valor que deja por debajo al 75% de los datos

Recorrido intercuartílico

Se define como la distancia Q3 – Q1.

Es el rango que recoge las opiniones del 50% de los expertos más “centrados”.

Para determinar el valor de consenso se pueden utilizar la media o la mediana, si bien esta última es habitualmente más adecuada por ser inmune a las opiniones más extremas.

Para determinar la dispersión se puede utilizar la desviación estándar, la media o el recorrido intercuartílico. La desviación estándar da una importancia mayor a la existencia de respuestas muy alejadas de la media, lo que suele considerarse mala idea. El recorrido intercuartílico es el más adecuado para desechar opiniones extremas.

En cualquier caso, cuando se remiten los resultados de una ronda para la siguiente ronda, conviene acompañar los estadísticos de un histograma o diagrama de frecuencia de las respuestas agrupadas en intervalos. Sobre este histograma conviene indicar algunos los valores importantes:

- la mediana o cuartil Q3
- la media
- el cuartil Q1
- el cuartil Q3
- los valores extremos: los más alejados por arriba y por abajo

3.7.3.2. Votaciones

Cuando las respuestas no se pueden asociar a un valor numérico sobre una escala continua de valores, hay que recurrir a técnicas de votación.

Sea una pregunta con N posibles respuestas, de las que hay que determinar cual es más adecuada.

Una opción es pedirle al experto que valore de 0 a 10 la conveniencia de cada una de las posibles respuestas. En el análisis se puede determinar la valoración media recibida por cada respuesta. En la siguiente ronda, el experto puede estar de acuerdo con la puntuación de consenso, o seguir insistiendo en su opinión divergente.

La valoración de consenso y la medida de dispersión se pueden estimar estadísticamente (ver sección anterior).

Otra opción es pedirle al experto que seleccione las 5 mejores respuestas y les asigne 5 puntos a la mejor, 4 a la segunda mejor, 3 a la tercera, 2 a la cuarta y uno a la quinta[12]. En el análisis se suman los puntos recibidos por cada respuesta para determinar su posición relativa en la ordenación de consenso. En la siguiente ronda, el experto puede estar de acuerdo en la ordenación de consenso, o seguir insistiendo en su opinión divergente.

3.7.4. Resumen

Se pueden resumir los rasgos esenciales de un proceso Delphi en los siguientes puntos:

- Anonimato de respuestas, que reduce las distorsiones de personalidades dominantes que pudieran producirse en reuniones o comités de expertos.
- *‘Feedback’* o realimentación controlada por medio de interacciones sucesivas de modo que en cada una el experto posee la información que se refiere a la interacción previa.
- Análisis estadístico de las respuestas del grupo, que permite ir consiguiendo el acuerdo razonado de los expertos evitando cualquier modo de presión para obtener modificaciones en sus puntos de vista.
- Énfasis puesto en la opinión informada, que en ocasiones puede ser contraria a la más común o generalizada en la sociedad.

12 Obviamente, hay que adecuar estos números a cada caso concreto.

3.7.5. Referencias

- ISO 31010
  ISO/IEC 31010:2009, Risk management — Risk assessment techniques.
  UNE-ISO/IEC 31010:2010, Gestión del riesgo. Técnicas de apreciación del riesgo.

  B.3 Técnica Delphi

- J. Fowles, “Handbook of Futures Research. Westport, Greenwood Press, 1978.
- H.A. Linstone and M. Turoff (eds), “The Delphi Method: Techniques and Applications”, Reading, MA: Addison-Wesley Publishing Company, 1975.
- N.C. Dalkey, “The Delphi Method: An Experimental Study of Group Opinion”, RAND Corporation, RM-5888-PR, 1969.
- O. Helmer, “Analysis of the Future: The Delphi Method”. RAND Corporation Technical Report, P-3558, March 1967.
- N. Dalkey and O. Helmer, “An Experimental Application of the Delphi Method to the Use of Experts”. Management Science, vol. 9, no. 3, April 1963.
- M. Girshick, A. Kaplan and A. Skogstad, “The Prediction of Social and Technological Events”. Public Opinion Quarterly, Spring 1950.