risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido / Recibido: 15/1/2015
Aceitação /Aceptación: 1/6/2015

Selección de salvaguardas en gestión del riesgo en sistemas de la información: un enfoque borroso

Antonio Jiménez-Martín [1], Eloy Vicente, Alfonso Mateos [1]

{antonio.jimenez, e.vicentecestero, alfonso.mateos}@upm.es

[1] Grupo de Análisis de Decisiones y Estadística, Departamento de Inteligencia Artificial, Universidad Politécnica de Madrid, Campus de Montegancedo S/N, Boadilla del Monte, 28660, España.

DOI: 10.1013/risti.15.83-100

Resumen: En este trabajo nos centramos en la fase de selección de salvaguardas dentro del proceso de análisis y gestión del riesgo en sistemas de la información (SI) bajo un enfoque borroso. Para reducir el riesgo asociado a posibles amenazas en SI se pueden implementar salvaguardas preventivas, paliativas o salvaguardas que disminuyan la probabilidad de transmisión de fallos a través de la red de activos asociada al SI. Sin embargo, las salvaguardas tienen asociadas costes por lo que se debe realizar un proceso de selección de las mismas. En este trabajo describimos problemas de optimización asociados a distintas perspectivas en la selección de salvaguardas y proponemos técnicas de solución basadas en programación dinámica y el uso de metaheurísticas.

Palabras-clave: Análisis y gestión del riesgo; sistemas de información; selección de salvaguardas; lógica borrosa; optimización.

Safeguard selection for risk management in information systems: a fuzzy approach

Abstract: In this paper we focus on the safeguard selection within the risk analysis and management in information systems (IS) under a fuzzy perspective. Preventive safeguards can be implemented to reduce the risk associated with potential threats in IS, whereas palliative safeguards reduce the probability of failure transmission through the assets network. However, safeguards have associated costs and a selection process has then to be carried out. We describe optimization problems associated with different perspectives on the selection of safeguards and propose solution techniques based on dynamic programming and the use of metaheuristics.

Keywords*:* Risk analysis and management, information systems, safeguard selection, fuzzy logic, optimization.

1. Introducción

Existen numerosas metodologías para el análisis y gestión del riesgo en sistemas de la información (SI) ajustadas a los estándares ISO, específicamente a la familia de estándares ISO 27000 (ISO/IEC, 2011). Algunos ejemplos de dichas metodologías son MAGERIT (López Crespo, Amutio-Gómez, Candau & Mañas, 2006), del *Ministerio de Administraciones Públicas* (España); CRAMM (CCTA, 2003), de la *Central Computing and Telecommunications Agency* (Reino Unido); o NIST SP 800-30 (Stoneburner & Gougen, 2002), del *National Institute of Standard and Technology* (E.E.U.U.)

Sin embargo, las metodologías propuestas por las normas internacionales obvian la dificultad de asignar acertadamente las dependencias entre activos, así como el valor de los activos terminales o el impacto que provocaría sobre todo el sistema la materialización de una amenaza sobre un activo. Estas metodologías tampoco consideran la incertidumbre sobre estas valoraciones.

En (Vicente, Jiménez & Mateos, 2013; Vicente, Mateos & Jiménez, 2013a; Vicente, Mateos & Jiménez-Martín, 2014b) se propone el uso de la *lógica borrosa* (Zadeh, 1965) como solución a tales deficiencias. Se define una escala de términos lingüísticos, cada uno de los cuales tiene asociado un número borroso trapezoidal (Zadeh, 1975), véase la Figura 1. Los números borrosos trapezoidales asociados a los términos lingüísticos de esta escala son *Muy bajo* (VL): (0,0,0, 0.25), *Bajo* (L): (0,0.05,0.15,0.25), *Medio-bajo* (M-L): (0.15,0.25,0.35,0.45), *Medio* (M): (0.35, 0.45,0.55,0.65), Medio-alto (M-H): (0.55,0.65,0.75,0.85), *Alto* (H): (0.75,0.85, 0.95,1) y *Muy alto* (VH): (0.95,1,1,1).

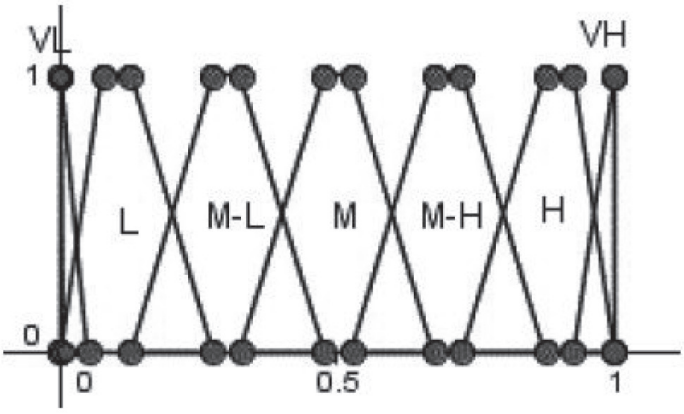

Figura 1 – Escala borrosa de términos lingüísticos

A continuación, se utiliza esta escala para incorporar la imprecisión a la hora de valorar los distintos elementos que forman parte del proceso de análisis y gestión del riesgo en los SI (Ramos, Rodrigues & Perna, 2008; Porta, Parapar, García, Fernández, Touriño, Ónega, Díaz, Miranda & Crecente, 2012), como la valoración de los activos terminales, la dependencia entre éstos, degradaciones y frecuencias asociados a las amenazas, o los efectos de las salvaguardas.

Todos los cálculos se realizan, por tanto, usando los valores borrosos trapezoidales asociados a los términos lingüísticos seleccionados, por lo que se hace necesaria la utilización de una aritmética adecuada, como la propuesta en (Xu, Shang, Qian & Shu, 2010). Denotaremos por $\oplus$, $\otimes$ y $\neg$, las operaciones suma, producto y resta entre números borrosos trapezoidales, respectivamente.

En la próxima sección hacemos un breve repaso de las etapas de las que consta el proceso de análisis y gestión del riesgo en SI. En la Sección 3 nos centramos en la selección de salvaguardas para la reducción del riesgo, presentando dos perspectivas distintas del problema, las técnicas de solución identificadas y ejemplos ilustrativos. Finalmente, en la Sección 4 presentamos las conclusiones del trabajo.

2. Análisis y gestión del riesgo en SI

El valor total de los *activos* de una organización se concentra generalmente en unos pocos elementos (activos *terminales*) que suelen ser de tipo "datos" o "servicios". El valor de estos activos se transmite al resto de activos (*de soporte*) a través de las relaciones de dependencia establecidas (que dan lugar a un grafo dirigido), de modo que los activos de soporte no tienen valor propio, sino que lo acumulan de los activos terminales.

La dependencia entre activos no tiene por qué ser directa, sino que puede ser transitiva a lo largo del grafo. Es decir, la transmisión de un fallo entre dos activos puede pasar por activos intermedios. Denotaremos por $\tilde{d}(A_i, A_j)$ el grado de dependencia directo entre dos activos A_i *y* A_j, mientras que el grado de dependencia de A_i sobre A_k a través de activos intermedios lo denotamos por $\tilde{D}(A_i, A_k)$, pudiendo ser calculados mediante el método recursivo propuesto en (Vicente et al., 2013a; Vicente et al., 2014b).

Los activos terminales se pueden valorar en función de tres componentes: *confidencialidad*, daño que causaría que lo conociera quien no debe; *integridad*, perjuicio que causaría que estuviera dañado o corrupto; y *autenticidad*, perjuicio que causaría no saber exactamente quién hace o ha hecho cada cosa.

Si denotamos el valor propio en los activos terminales por $\tilde{v}_j = (\tilde{v}_{j_{(1)}}, \tilde{v}_{j_{(2)}}, \tilde{v}_{j_{(3)}})$, donde $\tilde{v}_{j_{(l)}}$ será un término lingüístico borroso asignado por un experto para el activo A_j, y por T el conjunto de activos terminales, el valor acumulado del activo A_j respecto de los activos terminales es:

$$\tilde{v}_{j_{(l)}} = \sum_{A_k \text{en } T} \tilde{D}(A_j, A_k)\tilde{v}_{k_{(l)}}, l = 1,2,3.$$

Una *amenaza* es un evento que puede producir daños materiales o pérdidas inmateriales en los activos de la organización. Para valorar las amenazas debemos tener en cuenta la *degradación*, perjuicio que la amenaza puede provocar sobre el activo en sus distintas componentes; y su *frecuencia*, es decir, el número de materializaciones por unidad de tiempo.

Una vez determinadas estas dos medidas se calculan los indicadores de impacto y riesgo. Si consideramos una amenaza sobre el activo A_j cuya degradación en cada componente viene dada por el vector $\tilde{\mathrm{d}} = (\tilde{d}_1, \tilde{d}_2, \tilde{d}_3)$, cuando la amenaza se materializa, el *impacto* de la misma en cada componente del activo será $\tilde{I}_{j_{(l)}} = \tilde{d}_l \otimes \tilde{v}_{j_{(l)}}$, l= 1,2,3. Para calcular el

riesgo sobre este activo podemos utilizar la expresión $\tilde{R}_{j_{(l)}} = \tilde{I}_{j_{(l)}} \otimes \tilde{f}$, *l*= 1,2,3.

Una vez calculado el impacto provocado por una amenaza materializada sobre un activo del sistema, podemos calcular el impacto transmitido a los activos que dependen del activo atacado. Si A_j es el activo sobre el que se ha materializado la amenaza y el grado de dependencia de A_j con respecto a A_k es $\tilde{D}(A_k, A_j)$, entonces la amenaza sobre el activo A_j provoca un impacto sobre A_k de $\tilde{I}_{k_{(l)}} = \tilde{D}(A_k, A_j) \otimes \tilde{d}_l \otimes \tilde{v}_{j_{(l)}}$, y el riesgo sobre el activo será $\tilde{R}_{k_{(l)}} = \tilde{I}_{k_{(l)}} \otimes \tilde{f}$, *l*= 1,2,3.

3. Selección de salvaguardas

Las *salvaguardas* consisten en medidas para tratar las posibles amenazas del sistema y reducir el riesgo total del mismo. Pueden ser procedimientos, como la documentación y gestión de incidentes, políticas de personal, soluciones técnicas; o medidas de seguridad física de las instalaciones.

Las salvaguardas pueden ser *preventivas*, si reducen la frecuencia de las amenazas, o *paliativas*, si reducen la degradación causada por las amenazas en los activos. Un caso especial de salvaguarda preventiva es aquélla que reduce la probabilidad de transmisión de fallos en la red de activos, disminuyendo la dependencia entre los activos terminales y los de soporte. Si el efecto de una salvaguarda es $\tilde{e}$%, entonces el parámetro correspondiente se reduce en la proporción $\tilde{1} - \tilde{e}\%$.

Denotaremos los conjuntos de salvaguardas disponibles de la siguiente forma:

- S:{ S_t^{ik}, i,k=1,...,n, t=1,...,m_{ik}}. Salvaguardas que reducen la probabilidad de transmisión de fallos, siendo S_t^{ik} la salvaguarda *t*-ésima que reduce la transmisión de fallos entre los activos A_i *y* A_k. Su efecto sobre $d(A_i,A_k)$ lo denotamos por $\tilde{e}^{S_t^{ik}}$.
- $S^{(pr)}$:{ $S_t^{(pr)T_{ij}}$, *i*=1,...,*n*, *j*=1,...,n_i, *t*=1,..., m_{ij}^{pr} }. Salvaguardas preventivas, siendo $S_t^{(pr)T_{ij}}$ la *t*-ésima salvaguarda preventiva para la amenaza *j*-ésima sobre el activo A_i. Su efecto sobre la frecuencia de la amenaza T_{ij} es $e^{S_t^{(pr)T_{ij}}}$.
- $S^{(pa)}$:{ $S_t^{(pa)T_{ij}}$, *i*=1,...,*n*, *j*=1,...,n_i, *t*=1,..., m_{ij}^{pa} }. Salvaguardas paliativas, siendo $S_t^{(pa)T_{ij}}$ la *t*-ésima salvaguarda paliativa para la amenaza *j*-ésima sobre el activo A_i. Su efecto sobre la componente l-ésima de la degradación causada por la amenaza T_{ij} es $e_l^{S_t^{(pa)T_{ij}}}$, *l*= 1,2,3.
- Podemos seleccionar distintos paquetes de salvaguardas para reducir el riesgo, que representaremos por los vectores binarios $x_{ik} = (x_t)_{t=1}^{m_{ik}}$, $x^{pr}_{ij} = (x_t)_{t=1}^{m_{ij}^{pr}}$ y $x^{pa}_{ij} = (x_t)_{t=1}^{m_{ij}^{pa}}$, respectivamente, siendo x_t=1 si la salvaguarda *t*-ésima es seleccionada.
- Dentro del proceso de selección de salvaguardas vamos a mostrar dos perspectivas distintas del problema, que estudiaremos en detalle en las dos próximas secciones.

3.1. Selección de salvaguardas que restringen las probabilidades de transmisión de fallos minimizando el coste.

En primer lugar, supongamos que solamente disponemos de salvaguardas que reducen las probabilidades de transmisión de fallos (o grados de dependencia) entre los activos

del SI, *S*. El problema consistirá en seleccionar aquellas salvaguardas que aseguran que no se sobrepasa un umbral en dichas probabilidades entre los activos de soporte y terminales minimizando el coste asociado. El problema de optimización asociado es:

$$\min z = \sum_{i=1}^{n}\sum_{k=1}^{n} \mathrm{c}_{ik}\mathrm{x}_{ik}$$
$$s.a \quad \tilde{D}'(A_u,A_v) \le \tilde{U} \ \ \forall u,v$$
$$\mathrm{x}_{ik} = (x_t)_{t=1}^{m_{ik}},\ x_t \in \{0,1\}\ \forall i,k,t$$

donde c_{ik} son los vectores de costes asociados a las salvaguardas, *u y v* en el primer conjunto de restricciones se refieren a activos de soporte y terminales, respectivamente; $\tilde{U}$ es el umbral marcado por los expertos para las probabilidad de transmisión de fallos; y $\tilde{D}'(A_u,A_v)$ se calcula reemplazando los valores de dependencia directa $\tilde{d}(A_i,A_k)$ por los valores obtenidos teniendo en cuenta las salvaguardas seleccionadas $\tilde{d}(A_i,A_k)\otimes\left[\otimes_{t=1}^{m_{ik}}(\tilde{1}\neg\tilde{e}^{s_t^{ik}})\right]$, donde A_i *y* A_k son dos activos consecutivos conectados por un arco en algún camino entre A_u y A_v.

Las restricciones $\tilde{D}'(A_u,A_v)\le\tilde{U}\ \forall u,v$ se pueden sustituir por $S(\tilde{D}'(A_u,A_v),\tilde{U})\ge\alpha$, dado un umbral $\alpha\in[0,1]$, siendo S una función de similitud de números borrosos trapezoidales normalizados, como las propuestas en (Chen, 1996; Vicente, Mateos & Jiménez, 2013b).

Teniendo en cuenta que las dependencias indirectas se pueden calcular mediante el algoritmo recursivo descrito en (Vicente et al., 2013a; Vicente et al., 2014b) a partir de las dependencias de los activos más cercanos, el problema de optimización anterior puede resolverse por etapas, al cumplir el *principio* de *optimalidad* requerido en *programación dinámica*, de la siguiente forma (Vicente et al., 2014b): Sea L_0 el conjunto de nodos terminales.

- Consideramos L_1, conjunto que incluye solo a los activos cuyos hijos pertenecen a L_0. Identificamos las salvaguardas que minimizan los costes manteniendo los grados de dependencia sobre L_0 en un nivel aceptable.
- Consideramos L_2, activos cuyos hijos pertenecen a $L_0\cup L_1$. De nuevo, identificamos las salvaguardas que minimizan los costes manteniendo los grados de dependencia sobre L_0 en un nivel aceptable. Nótese que los grados de dependencia indirecta entre los hijos de L_2 y los activos terminales se han calculado ya en la etapa anterior, por lo que simplemente necesitamos identificar los grados de dependencia directa sobre los activos en $L_0\cup L_1$.
- ...
- Consideramos L_i, activos cuyos hijos pertenecen a $L_0\cup L_1\cup\ldots\cup L_{i-1}$. De nuevo, identificamos las salvaguardas que minimizan los costes manteniendo los grados de dependencia sobre L_0 en un nivel aceptable. Una vez más, solo tendremos que identificar las dependencias directas sobre los activos en $L_0\cup\ldots\cup L_{i-1}$.

Debido al carácter combinatorio de los problemas de optimización identificados en cada una de las etapas de la programación dinámica, se ha decidido utilizar una *metaheurística* para su resolución, en concreto el enfriamiento simulado (Kirkpatrick, Gelatt & Vecchi, 1983).

El *enfriamiento simulado* es una *metaheurística trayectorial* que considera una solución en cada una de las etapas del proceso de búsqueda de la solución óptima. La idea básica es la siguiente: Partiendo de una solución inicial factible, en cada iteración se genera de forma aleatoria una solución del entorno de la actual. Si la nueva solución es mejor que la actual, entonces el algoritmo se mueve a dicha solución; en caso contrario, existe una cierta probabilidad de que nos movamos a esa solución peor.

La aceptación de movimientos hacia soluciones peores hace la búsqueda del óptimo más dispersa y evita que nos quedemos atrapados en un óptimo local.

La búsqueda se inicia de una forma muy diversificada, en la que prácticamente cualquier movimiento es aceptado. Según avanza, la probabilidad de movernos hacia soluciones peores disminuye haciendo que al final del proceso de búsqueda solo se permitan movimientos hacia soluciones mejores.

Para ilustrar el método de solución propuesto, consideremos el SI y valores de dependencia directa entre activos mostrados en la Figura 2, siendo A_6 el único activo terminal.

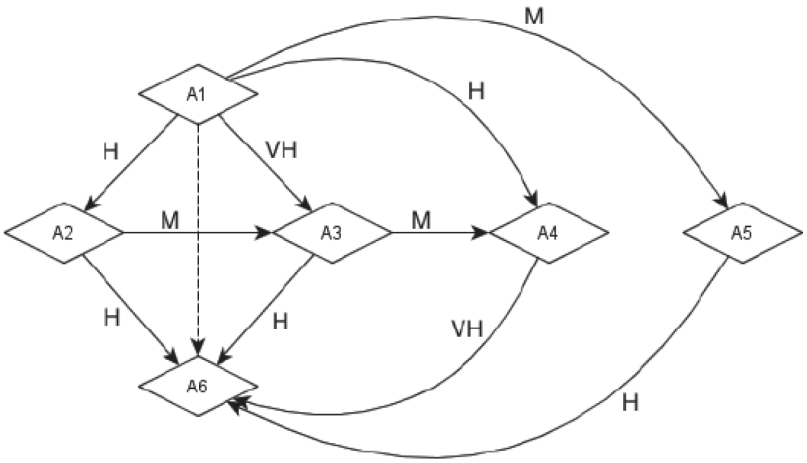

Figura 2 – Escala borrosa de términos

A continuación, se calculan las dependencias indirectas entre los activos de soporte y el terminal (A_6) (Vicente et al., 2013).

Consideremos una amenaza sobre el activo A_1 con frecuencia $\tilde{f} = \text{M}$ y degradación $\tilde{d} = (\text{H, H, H})$. Entonces, el riesgo sobre el activo A_1 es $\tilde{R}_{1_{(l)}} = (0.23, 0.415, 0.485, 0.675)$, $l = 1,2,3$.

Tomamos como umbral $\tilde{U} = (0,0,0.1,0.2)$, por debajo del cual el grado de dependencia o probabilidad de transmisión de fallos entre activos será aceptable, siendo $\alpha = 0.95$. Supongamos que el conjunto de salvaguardas disponibles es el que se muestra en la Tabla 1.

Tabla 1 – Salvaguardas disponibles

A_i	Arco	Conjunto de salvaguardas
A_1	(A_1,A_2)	{($S_1^{1,2}$,L,100),($S_2^{1,2}$,M,300),(^{1,2} ,MH,550),($S_4^{1,2}$,M,430),($S_5^{1,2}$,ML,125),($S_6^{1,2}$,L,240), ($S_7^{1,2}$,VL,100), ($S_8^{1,2}$,MH,324),($S_9^{1,2}$,VH,570)}
	(A_1,A_3)	{($S_1^{1,3}$,MH,356),($S_2^{1,3}$,H,324),($S_3^{1,3}$,L,110),($S_4^{1,3}$,ML,345),($S_5^{1,3}$,VL,87),($S_6^{1,3}$,MH,345), ($S_7^{1,3}$,M,200)}
	(A_1,A_4)	{($S_1^{1,4}$,M,209),($S_2^{1,4}$,M,267),($S_3^{1,4}$,MH,342),($S_4^{1,4}$,VH,789),($S_5^{1,4}$,M,234),($S_6^{1,4}$,M,356), ($S_7^{1,4}$,M,276),($S_8^{1,4}$, M,200),($S_9^{1,4}$,H,467),($S_{10}^{1,4}$,H,342),($S_{11}^{1,4}$,L,127),($S_{12}^{1,4}$,M,207)}
	(A_1,A_5)	{($S_1^{1,5}$,M,230),($S_2^{1,5}$,M,345),($S_3^{1,5}$,L,187),($S_4^{1,5}$,M, 321),($S_5^{1,5}$,MH,345),($S_6^{1,5}$,H,543), ($S_7^{1,5}$,MH,356),($S_8^{1,5}$, M,206),($S_9^{1,5}$,M,342)}
A_2	(A_2,A_3)	{($S_1^{2,3}$,M,356),($S_2^{2,3}$,L,87),($S_3^{2,3}$,ML,267),($S_4^{2,3}$,M, 320),($S_5^{2,3}$,ML,156),($S_6^{2,3}$,M,320), ($S_7^{2,3}$,M,256), ($S_8^{2,3}$,M, 300),($S_9^{2,3}$,L,200)}
	(A_2,A_6)	{($S_1^{2,6}$,M,348),($S_2^{2,6}$,L,187),($S_3^{2,6}$,ML,254),($S_4^{2,6}$,ML,367),($S_5^{2,6}$,ML,567),($S_6^{2,6}$,M,390), ($S_7^{2,6}$,ML,256),($S_8^{2,6}$,M,307),($S_9^{2,6}$,L,235), ($S_{10}^{2,6}$,ML,124), ($S_{11}^{2,6}$,M,400),($S_{12}^{2,6}$,L,278), ($S_{13}^{2,6}$,ML,260)}
A_3	(A_3,A_4)	{($S_1^{3,4}$,M,345),($S_2^{3,4}$,H,650),($S_3^{3,4}$,M,200),($S_4^{3,4}$,M, 367),($S_5^{3,4}$,M,388),($S_6^{3,4}$,H,453), ($S_7^{3,4}$,L,189), ($S_8^{3,4}$, L,256),($S_9^{3,4}$,M,345)}
	(A_3,A_6)	{($S_1^{3,6}$,M,267),($S_2^{3,6}$,M,356),($S_3^{3,6}$,M,378),($S_4^{3,6}$,M,324), ($S_5^{3,6}$,M,345), ($S_6^{3,6}$,M,231), ($S_7^{3,6}$,MH,453)}
A_4	(A_4,A_6)	{($S_1^{4,6}$,M,260),($S_2^{4,6}$,M,245),($S_3^{4,6}$,ML,170),($S_4^{4,6}$,M,256),($S_5^{4,6}$,M,367),($S_6^{4,6}$,M,289), ($S_7^{4,6}$,M,278), ($S_8^{4,6}$,M, 345),($S_9^{4,6}$,M,240),($S_{10}^{4,6}$,MH,435)}
A_5	(A_5,A_6)	{($S_1^{5,6}$,M,200),($S_2^{5,6}$,M,210),($S_3^{5,6}$,L,120),($S_4^{5,6}$,ML,234),(^{5,6} ,M,267),($S_6^{5,6}$,MH,367), ($S_7^{5,6}$,MH,366), ($S_8^{5,6}$, M,254),($S_9^{5,6}$,ML,145),($S_{10}^{5,6}$,L,206),($S_{11}^{5,6}$,M,306),($S_{12}^{5,6}$,M,345), ($S_{13}^{5,6}$,M,280),($S_{14}^{5,6}$,L,178),($S_{15}^{5,6}$,MH,377)}

Aplicamos la técnica de solución propuesta para la selección de salvaguardas. Inicialmente $L_0=\{A_6\}$.

- $L_1=\{A_4, A_5\}$. Debemos ajustar los grados de dependencia

$$\tilde{D}'(A_4,A_6)=\tilde{d}(A_4,A_6)\otimes\left(\otimes_{t=0}^{10}(\tilde{1}\neg\tilde{e}^{S_t^{46}}x_{46}(t))\right) \text{ y}$$

$$\tilde{D}'(A_5,A_6)=\tilde{d}(A_5,A_6)\otimes\left(\otimes_{t=0}^{15}(\tilde{1}\neg\tilde{e}^{S_t^{56}}x_{56}(t))\right),$$

tales que $S'(\tilde{D}(A_4,A_6),\tilde{U})\geq 0.95$ y $S'(\tilde{D}(A_5,A_6),\tilde{U})\geq 0.95$, en función de las salvaguardas que se seleccionen.

Como L_1 contiene dos elementos, se deben resolver dos problemas de optimización.

$$\begin{array}{ll}\min z=c_{46}x_{46} & \\ s.a & \text{y} \\ S(\tilde{D}'(A_4,A_6),\tilde{U})\geq 0.95 & \\ x_{46}=(x_t)_{t=1}^{10},\ x_t\in\{0,1\} & \end{array}\qquad \begin{array}{ll}\min z=c_{56}x_{56} & \\ s.a & , \\ S(\tilde{D}'(A_5,A_6),\tilde{U})\geq 0.95 & \\ x_{56}=(x_t)_{t=1}^{15},\ x_t\in\{0,1\} & \end{array}$$

que utilizando enfriamiento simulado nos proporcionan la selección óptima de salvaguardas $x_{46}^*=(0,1,1,1,0,0,0,0,1,0)$ y $x_{56}^*=(1,0,0,0,0,0,1,0,1,0,\ 0,0,0,0,0)$.

- $L_2=\{A_3\}$. Ahora, ajustamos el grado de dependencia

$$\tilde{D}'(A_3,A_6)=\left[\tilde{d}(A_3,A_6)\otimes\left(\otimes_{t=0}^{7}(\tilde{1}\neg\tilde{e}^{S_t^{36}}x_{36}(t))\right)\right]\oplus$$
$$\left[\tilde{d}(A_3,A_4)\otimes\left(\otimes_{t=0}^{9}(\tilde{1}\neg\tilde{e}^{S_t^{34}}x_{34}(t))\right)\otimes\tilde{D}'(A_4,A_6)\right]$$

tal que $S'(\tilde{D}(A_3,A_6),\tilde{U})\geq 0.95$, en función de las salvaguardas que se seleccionen. Nótese que el valor $\tilde{D}'(A_4,A_6)$ ya se obtuvo al resolver el problema de optimización de la etapa anterior, (0.016,0.072,0.104,0.269).

El problema de optimización a resolver es:

$$\begin{array}{ll}\min z= & c_{36}x_{36}+c_{34}x_{34} \\ s.a & S(\tilde{D}'(A_3,A_6),\tilde{U})\geq 0.95 \\ & x_{36}=(x_t)_{t=1}^{7}\ x_{34}=(x_t)_{t=1}^{9},\ x_t\in\{0,1\}\end{array},$$

cuya solución óptima es $x_{36}^*=(1,0,0,1,0,1,1)$ y $x_{34}^*=0$.

- L_3={A_2}. Ajustamos el grado de dependencia

$$\tilde{D}'(A_2,A_6)=\left[\tilde{d}(A_2,A_6)\otimes\left(\otimes_{t=0}^{13}(\tilde{1}\neg\tilde{e}^{S_t^{26}}x_{26}(t))\right)\right]\oplus$$
$$\left[\tilde{d}(A_2,A_3)\otimes\left(\otimes_{t=0}^{7}(\tilde{1}\neg\tilde{e}^{S_t^{23}}x_{23}(t))\right)\otimes\tilde{D}'(A_3,A_6)\right],$$

siendo $\tilde{D}'(A_3,A_6)$ =(0.008,0.059,0.096,0.301), obtenido de la etapa anterior. El problema de optimización a resolver es:

$$\begin{array}{rc}\min z = & c_{23}x_{23}+c_{26}x_{26}\\ s.a & S(\tilde{D}'(A_2,A_6),\tilde{U})\geq 0.95\\ & x_{23}=(x_t)_{t=1}^{9}\ \mathrm{x}_{26}=(x_t)_{t=1}^{13},\ x_t\in\{0,1\}\end{array},$$

que proporciona la selección óptima x_{23}^{*}=(0,0,0,0,0,0,1,0,0) y x_{26}^{*}=(1,0,0, 0,1,0,1,0,0,1,0,0,0).

Finalmente, L_4={A_1}. Ajustamos

$$\tilde{D}'(A_1,A_6)=\begin{array}{l}[\tilde{d}(A_1,A_2)\otimes(\otimes_{t=0}^{9}(\tilde{1}\neg\tilde{e}^{S_t^{12}}x_{12}(t)))\otimes\tilde{D}'(A_2,A_6)]\oplus\\ [\tilde{d}(A_1,A_3)\otimes(\otimes_{t=0}^{7}(\tilde{1}\neg\tilde{e}^{S_t^{13}}x_{13}(t)))\otimes\tilde{D}'(A_3,A_6)]\oplus\\ [\tilde{d}(A_1,A_4)\otimes(\otimes_{t=0}^{12}(\tilde{1}\neg\tilde{e}^{S_t^{14}}x_{14}(t)))\otimes\tilde{D}'(A_4,A_6)]\oplus\\ [\tilde{d}(A_1,A_5)\otimes(\otimes_{t=0}^{9}(\tilde{1}\neg\tilde{e}^{S_t^{15}}x_{15}(t)))\otimes\tilde{D}'(A_5,A_6)].\end{array}$$

Ahora, resolvemos el problema de optimización:

$$\begin{array}{rc}\min z = & c_{12}x_{12}+c_{13}x_{13}+c_{14}x_{14}+c_{15}x_{15}\\ & S(\tilde{D}'(A_1,A_6),\tilde{U})\geq 0.95\\ s.a & x_{12}=(x_t)_{t=1}^{9}\ x_{13}=(x_t)_{t=1}^{7},\ x_t\in\{0,1\}\\ & x_{14}=(x_t)_{t=1}^{12}\ x_{15}=(x_t)_{t=1}^{9},\ x_t\in\{0,1\}\end{array},$$

que nos proporciona la selección óptima de salvaguardas x_{12}^{*} =(1,0,0,0,0, 0,0,0,0), x_{13}^{*} =(0,1,0,0,0,0,0,0), x_{14}^{*} = (0,0,0,0,0,0,0,0,0,0,1,0,0) y x_{15}^{*}=0

Tras la implementación de las salvaguardas seleccionadas, el riesgo sobre el activo A_1 es $\tilde{R}_{1_{(l)}}$ = (0.001,0.018,0.039,0.22), l=1,2,3.

En la Figura 3 se puede comparar el riesgo sobre el activo A_1 antes y después de la aplicación de las salvaguardas.

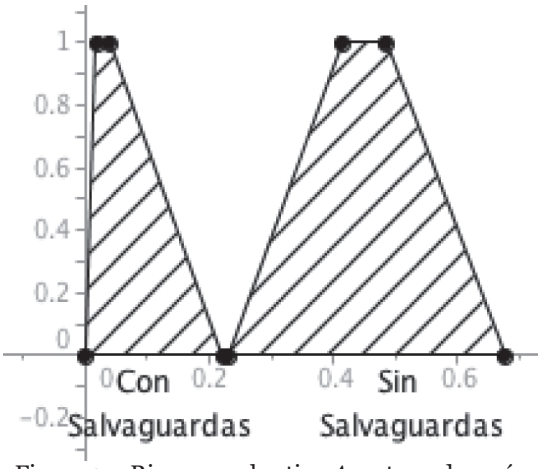

Figura 3 – Riesgo en el activo A_1 antes y después de la aplicación de salvaguardas

3.2. Selección de salvaguardas que minimizan el riesgo del sistema para un presupuesto disponible.

Consideremos ahora de forma adicional los conjuntos de salvaguardas preventivas, $S^{(pr)}$, y salvaguardas paliativas, $S^{(pa)}$, y deseamos seleccionar aquellas salvaguardas que minimizan el riesgo del sistema dado un presupuesto.

El problema de optimización a resolver es, por tanto, el siguiente (Vicente, Mateos, & Jiménez-Martín, 2014a):

$$\min z = \max_{i,j,l}\{\tilde{R}_l^{T_j^i}\}$$

$$s.a \quad \sum_{i=1}^{n}\sum_{k=1}^{m_{ik}} x_{ik}c_{ik} + \sum_{i=1}^{n}\sum_{j=1}^{n_i} x^{pr}c_{ij}^{pr} + \sum_{i=1}^{n}\sum_{j=1}^{n_i} x^{pa}c_{ij}^{pa} \leq c$$

donde c_{ik}, c_{ij}^{pr} y c_{ij}^{pa} son los vectores de costes de las salvaguardas y c es el presupuesto disponible.

Es importante destacar que las amenazas deben ser consideradas de forma secuencial para computar el riesgo en el SI en lugar de considerar que todas ellas se producen simultáneamente. Como consecuencia, tenemos un problema de optimización borroso multiobjetivo cuyas funciones objetivo representan nuevos riesgos (reducidos) como resultado de la aplicación de las salvaguardas. Por lo tanto, dichos riesgos no deben ser sumados y, por ello, hemos decidido minimizar el máximo de los mismos.

La función objetivo necesita de un orden total en su argumento del cuál carecen los números borrosos trapezoidales. Se han propuesto más de 30 métodos para ordenar números borrosos trapezoidales (Bortolan & Degani, 1985; Wang & Kerre, 2001a-b;

Brunelli & Mezei, 2013). En este trabajo usamos el índice de Murakami (Murakami, Maeda & Imamura, 1983), que calcula el centroide de los números borrosos comparados: Si $\tilde{A}=(a_1,a_2,a_3,a_4)$, entonces su centroide es $(\tilde{X}_{\tilde{A}},\tilde{Y}_{\tilde{A}})$, con $\tilde{Y}_A=\left(\frac{a_3-a_2}{a_4-a_1}+2\right)/6$ y $\tilde{X}_A=\tilde{Y}_A(a_3-a_2)+(1-\tilde{Y}_A)(a_4-a_1)$.

El índice compara primero las abscisas de los centroides de forma que los números borrosos con mejor abscisa son ordenados mejor. Si las abscisas son iguales, entonces aquél con mayor ordenada es el mejor.

Como ejemplo ilustrativo, consideremos ahora el SI y valores de dependencia directa entre activos mostrados en la Figura 4, siendo A_5 el único activo terminal.

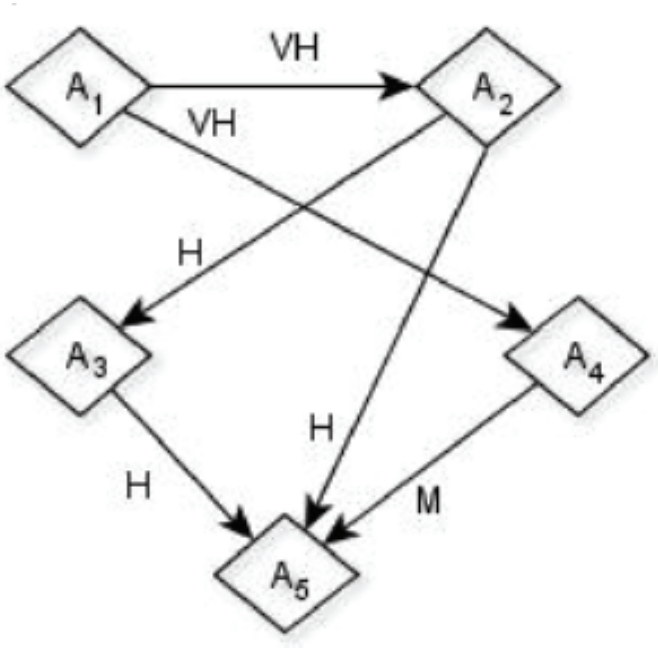

Figura 4 – Segundo ejemplo de SI

El valor monetario (en cientos de unidades) del activo terminal es $\tilde{v}_5=((10,15,20,25),(18,20,23,30),(12,15,26,30))$. Las dependencias indirectas entre los activos no terminales y el terminal (A_5) son $\tilde{D}(A_4,A_5)=\text{M}$, $\tilde{D}(A_3,A_5)=\text{H}$, $\tilde{D}(A_2,A_5)=(0.93,0.97,0.99,1)$ y $\tilde{D}(A_1,A_5)=(0.92,0.98,0.99,1)$, véase (Vicente et al., 2014a).

Si consideramos las 5 amenazas mostradas en la Tabla 2, los riesgos inducidos por cada amenaza individual se muestran en la Tabla 3.

Tabla 2 – Amenazas en los activos

Activo	Amenaza	Frecuencia	Degradación
A_1	T_{11}	H	(M,H,MH)
A_2	T_{12}	M	(H,M,MH)
A_2	T_{22}	H	(M,M,M)
A_3	T_{13}	MH	(H,H,M)
A_4	T_{14}	H	(H,MH,M)

Tabla 3 – Riesgos en A_5 antes de la aplicación de las salvaguardas

Amenaza	Confidencialidad	Integridad	Autenticidad
T_{11}	(2898, 5622.7, 13449, 19500)	(6210, 10620.7, 23230, 30000)	(4554, 8121.7, 18339.7, 25500)
T_{12}	(2929.5, 5565.4, 13449, 19500)	(1367.1, 2946.4, 7786, 12675)	(2148.3, 4255.9, 10617.7, 16575)
T_{22}	(2929.5, 5565.4, 13449, 19500)	(2929.5, 5565.4, 13449, 19500)	(2929.5, 5565.4, 13449.1, 19500)
T_{13}	(3712.5, 7044.4, 17599, 25500)	(3712.5, 7044.4, 17599, 25500)	(1732.5, 3729.4, 10188.7, 16575)
T_{14}	(2362.5, 4876.9, 12906, 19500)	(1732.5, 3729.4, 10189, 16575)	(1102.5, 2581.9, 7471.7, 12675)

Si ahora consideramos las salvaguardas mostradas en las Tablas 4, 5 y 6, y disponemos de un presupuesto de 5000 unidades, el problema de optimización a resolver es:

$$\min z = \max_l\{\tilde{R}_l^{T_1^1}, \tilde{R}_l^{T_1^2}, \tilde{R}_l^{T_2^2}, \tilde{R}_l^{T_2^3}, \tilde{R}_l^{T_1^4}\}$$

$$s.a \quad \sum_{i=1}^{n}\sum_{k=1}^{n} c_{ik}x_{ik} + \sum_{i=1}^{n}\sum_{j=1}^{n_i} c_{ij}^{pr}x^{pr} + \sum_{i=1}^{n}\sum_{j=1}^{n_i} c_{ij}^{pa}x^{pa} \leq 5000 \text{ ,}$$

donde, por ejemplo, el primer y último término de la función objetivoson:

$$\tilde{D}'(A_1,A_5)\otimes\tilde{f}^{T_1^1}\otimes\left(\otimes_{t=1}^{4}(\tilde{1}\neg e^{S_t^{(pr)T_1^1}})\right)\otimes d_l^{T_1^4}\otimes\left(\otimes_{t=1}^{6}(\tilde{1}\neg e^{S_t^{(pa)T_1^1}})\right) \text{ y}$$

$$\tilde{D}'(A_4,A_5)\otimes\tilde{f}^{T_1^4}\otimes\left(\otimes_{t=1}^{4}(\tilde{1}\neg e^{S_t^{(pr)T_1^4}})\right)\otimes d_l^{T_1^4}\otimes\left(\otimes_{t=1}^{5}(\tilde{1}\neg e^{S_t^{(pa)T_1^4}})\right),$$

y $\tilde{D}'(A_i,A_5)$ se obtiene de $\tilde{D}(A_i,A_5)$ multiplicando el valor inicial de cada arco por la reducción causada por el efecto de las salvaguardas de transmisión de fallos en dicho arco.

Tabla 4 – Salvaguardas sobre la transmisión de fallos

Activo	**Salvaguardas (Identificador, Efecto, Coste)**
A_4	S^{45}={(S_1^{45},M,205),(S_2^{45},L,124), (S_3^{45},ML,230), (S_4^{45},M,189), (S_5^{45},L,104), (S_6^{45},M,167),(S_7^{45},M,178),(S_8^{45} L,98)}
A_3	S^{35}={(S_1^{35},M,198),(S_2^{35},L,100),(S_3^{35},M,123),(S_4^{35},M,167),(S_5^{35},L,89), (S_6^{35},M,178), (S_7^{35},M,209),(S_8^{35} L,100)}
A_2	S^{25}={(S_1^{25},M,203),(S_2^{25},M,198), (S_3^{25},L,170)} S^{23}={(S_1^{23},L,143),(S_2^{23},M,178), (S_3^{23},M,154), (S_4^{23},M,190), (S_5^{23},L,102)}
A_1	S^{14}={(S_1^{14},M,178),(S_2^{14},M,160), (S_3^{14},L,120), (S_4^{14},L,105)} S^{12}={(S_1^{12},L,120),(S_2^{12},M,180), (S_3^{12},L,104), (S_4^{12},M,200)}

Tabla 5 – Salvaguardas paliativas disponibles

	Salvaguardas (Identificador, Efecto (C,I,A), Coste)
$S^{(pa)T_{11}}$	{($S_1^{(pa)T_{11}}$,(H,H,H),520), ($S_2^{(pa)T_{11}}$,(M,L,M), 250),($S_3^{(pa)T_{11}}$,(L, L,VL), 100), ($S_4^{(pa)T_{11}}$, (ML, VL, L),96), ($S_5^{(pa)T_{11}}$,(VL,L,ML),110), ($S_6^{(pa)T_{11}}$,(ML,M,L),78)}
$S^{(pa)T_{13}}$	{($^{(pa)T_{13}}$,(H,H,H),535), ($S_2^{(pa)T_{13}}$,(L,L,VL),89), ($S_3^{(pa)T_{13}}$,(H, H,H), 670), ($^{(pa)T_{13}}$, (ML, H,L),537), ($S_5^{(pa)T_{13}}$,(H,L,ML),477)}
$S^{(pa)T_{12}}$	{($S_1^{(pa)T_{13}}$,(H,H,H),496), ($S_2^{(pa)T_{13}}$,(VL,L,ML), 110), ($S_3^{(pa)T_{13}}$,(ML,M,L), 78)}
$S^{(pa)T_{22}}$	{($S_1^{(pa)T_{13}}$,(M,L,M),195), ($S_2^{(pa)T_{13}}$,(L,L,VL),89), ($S_3^{(pa)T_{13}}$,(ML,VL,L), 56)}
$S^{(pa)T_{14}}$	{($S_1^{(pa)T_{13}}$,(H,H,H),539), ($S_2^{(pa)T_{13}}$,(L,L,VL),110), ($S_3^{(pa)T_{13}}$,(ML,H,L),478), ($S_4^{(pa)T_{13}}$, (ML, H,L),495), ($S_5^{(pa)T_{13}}$,(H,H,H),689)}

Tabla 6 – Salvaguardas preventivas disponibles

	Salvaguardas (Identificador, Efecto, Coste)
$S^{(pr)T_{11}}$	={($S_1^{(pr)T_{11}}$,H,367), ($S_2^{(pr)T_{11}}$,H, 485), ($S_3^{(pr)T_{11}}$,ML, 100), ($S_4^{(pr)T_{11}}$,ML,120)}
$S^{(pr)T_{13}}$	={($S_1^{(pr)T_{13}}$,M,198), ($S_2^{(pr)T_{13}}$,L, 100), ($S_3^{(pr)T_{13}}$,M, 123), ($S_4^{(pr)T_{13}}$,M,167)}
$S^{(pr)T_{12}}$	={($S_1^{(pr)T_{12}}$,M,203), ($S_2^{(pr)T_{12}}$,M, 198)}
$S^{(pr)T_{22}}$	={($S_1^{(pr)T_{22}}$,M,178), ($S_2^{(pr)T_{22}}$,M, 160)}
$S^{(pr)T_{14}}$	={($S_1^{(pr)T_{14}}$,M,178), ($S_2^{(pr)T_{14}}$,M, 160), ($S_3^{(pr)T_{14}}$,L, 120),($S_4^{(pr)T_{14}}$,L,105)}

En la Tabla 7 se muestra la solución obtenida utilizando el enfriamiento simulado, con un coste asociado de 4850 unidades, mientras que la Tabla 8 muestra los nuevos valores de riesgo en el activo terminal A_5 una vez que las salvaguardas han sido implementadas.

Si comparamos los riesgos mostrados en las Tablas 3 y 8, antes y después de la implementación de salvaguardas, podemos apreciar que la reducción del riesgo es significativa.

Tabla 7 – Selección final de salvaguardas

Arco	Salv. trans. fallos	Amenaza	Salv. preventiva	Salv. paliativa
(A_4, A_5)	(10100111)	T_{11}	(0011)	(000011)
(A_3, A_5)	(10111110)	T_{12}	(00)	(110)
(A_2, A_5)	(110)	T_{22}	(00)	(101)
(A_2, A_3)	(01111)	T_{13}	(0010)	(00000)
(A_1, A_4)	(0100)	T_{14}	(0100)	(00000)
(A_1, A_2)	(0101)			

Tabla 8 – Riesgos en A_5 tras la aplicación de las salvaguardas

Amenaza	Confidencialidad	Integridad	Autenticidad
T_{11}	(16.9, 161.7, 936, 3681.5)	(32.7, 239.7, 1295.6, 5197.4)	(25.1, 198.6, 1576.7, 5777)
T_{12}	(0, 49.6, 458.1, 1791.2)	(0, 29.7, 289.7, 1397.1)	(0, 24.6, 352.6, 1552.9)
T_{22}	(0, 49.6, 458.1, 1791.2)	(0, 29.7, 289.7, 1397.1)	(76, 379.3, 2074, 5588.4)
T_{13}	(12.2, 110.5, 647, 2465.6)	(21.9, 147.3, 744.3, 2958.7)	(6.8, 58.5, 487.1, 1923.2)
T_{14}	(34.8, 245.5, 1177, 3793)	(62.7, 327.4, 1353.3, 4551.9)	(19.5, 130, 885.7, 2958.7)

4. Conclusiones

En este trabajo se han analizado los problemas de selección de salvaguardas en la gestión del riesgo en sistemas de la información (SI) desde dos perspectivas. En la primera, únicamente hemos considerado salvaguardas que disminuyen la probabilidad de transmisión de fallos en la red de activos y el problema de optimización planteado minimiza los costes asociados a las salvaguardas seleccionadas que mantienen dichas probabilidades de transmisión de fallos entre activos de soporte y terminales en unos niveles aceptables.

En el segundo enfoque, se disponen tanto de salvaguardas preventivas y paliativas, como de salvaguardas que disminuyen la probabilidad de transmisión de fallos y se seleccionan las salvaguardas que minimicen el riesgo del sistema sin sobrepasar un presupuesto disponible.

Ambos problemas de optimización se han resuelto de una manera eficiente. En el primer caso, mediante el uso de programación dinámica y enfriamiento simulado para resolver los problemas asociados a cada una de sus fases; y en el segundo, mediante el uso directamente de la metaheurística.

Agradecimientos

El trabajo ha sido financiado por el proyecto del Ministerio de Ciencia (España) MTM2011-28983-CO-03 y el Ministerio de Economía y Competitividad MTM2014-56949-C3-2-R.

Referencias bibliográficas

Bortolan, G., & Degani, R. (1985). A review of some methods for ranking subsets. *Fuzzy Sets and Systems*, *15*, 1-19. doi: http://dx.doi.org/10.1016/0165-0114(85)90012-0

Brunelli, M., & Mezei, J. (2013). How different are ranking methods for fuzzy numbers? A numerical study. *International Journal of Approximate Reasoning*, *54*, 627-639. doi: http://dx.doi.org/10.1016/j.ijar.2013.01.009

Central Computing and Telecommunications Agency (2003). *Risk analysis and management method* (CRAMM), V5.0. London.

Chen, S. M. (1996). New Methods for subjective mental workload assessment and fuzzy risk analysis. *Cybernetics Systems*, *27*, 449-472. doi: http://dx.doi.org/10.1080/019697296126417

International Organization for Standardization (2011). *ISO/IEC 27005:2011 Information technology – security techniques – information security risk management*. Geneva.

Kirkpatrick, S., Gelatt, D. C., & Vecchi, C. D. (1983). Optimization by simulated annealing. *Science*, *220*, 671-680. doi: http://dx.doi.org/10.1126/science.220.4598.671

López Crespo, F., Amutio-Gómez, M. A., Candau, J., & Mañas, J. A. (2006). *Methodology for information systems risk. Analysis and management (MAGERIT version 2). Books I, II and III*, Madrid, Spain: Ministerio de Administraciones Públicas.

Murakami, S., Maeda, S., & Imamura, S. (1983). Fuzzy decision analysis on the development of centralized regional energy control system. *IFAC Symposium on Fuzzy Information Knowledge Representation and Decision Analysis*, 363-368.

Porta, J., Parapar, J., García, P., Fernández, G., Touriño, J., Ónega, F., Díaz, P., Miranda, D., & Crecente, R. (2012). Sistema de información del banco de tierras de Galicia, *Revista Ibérica de Sistemas y Tecnologías de la Información, 9*, 27-41. doi: http://dx.doi.org/10.4304/risti.9.27-41

Ramos, C., Rodrigues, P. M. M., & Perna, F. (2008). Sistemas de Informaçao para apoio ao turismo, o caso dos dynamic packaking, *Revista Ibérica de Sistemas y Tecnologías de la Información, 2*, 25-35.

Stoneburner, G., & Gougen, A. (2002). *NIST 800-30 risk management. Guide for information technology systems*, Gaithersburg, USA: National Institute of Standard and Technology.

Vicente, E., Jiménez, A., & Mateos, A. (2013). A Fuzzy Approach to Risk Analysis in Information Systems. *Proceedings of the 2nd International Conference on Operations Research and Enterprise Systems*, 130-133.

Vicente, E., Mateos, A., & Jiménez, A. (2013a). A Fuzzy Extension of MAGERIT Methodology for Risk Analysis in Information Systems. *Proceedings of the IADIS Information Systems Conference*, 39-46.

Vicente, E., Mateos, A., & Jiménez, A. (2013b). A New Similarity Function for Generalized Trapezoidal Fuzzy Numbers. In L. Rutkowski, M. Korykowski, R. Scherer, R. Tadeusiewizc, L. Zadeh & J. Zurada (Eds.), *Lecture Notes on Computer Science: Vol. 7894*. (pp. 400-411). Berlin: Germany, Springer. doi: http://dx.doi.org/10.1007/978-3-642-38658-9_36

Vicente, E., Mateos, A., & Jiménez-Martín, A. (2014a). Selection of Safeguards for Fuzzified Risk Management in Information Systems. In A. Rocha, A. M. Correira, F. B Tan & K. A. Stroetmann (Eds.), *Advances in Intelligent Systems and Computing: Vol. 275. New Perspectives in Information Systems and Technologies* (pp. 267-276). Berlin: Germany, Springer. doi: http://dx.doi.org/10.1007/978-3-319-05951-8_26

Vicente, E., Mateos, A., & Jiménez-Martín, A. (2014b). Risk analysis in information systems: a fuzzification of the MAGERIT methodology. *Knowledge-Based Systems*, *66*, 1-12. doi: http://dx.doi.org/10.1016/j.knosys.2014.02.018

Wang, X., & Kerre, E. E. (2001a). Reasonable properties for the ordering of fuzzy quantities (I). *Fuzzy Sets and Systems, 118*, 375-385. doi: http://dx.doi.org/10.1016/S0165-0114(99)00062-7

Wang, X., & Kerre, E. E. (2001b). Reasonable properties for the ordering of fuzzy quantities (II). *Fuzzy Sets and Systems*, *118*, 387-405. doi: http://dx.doi.org/10.1016/S0165-0114(99)00063-9

Xu, Z., Shang, S., Qian, W., & Shu, W. (2010). A Method for fuzzy risk analysis based on the new similarity of trapezoidal fuzzy numbers. *Expert Systems and Applications*, *37*, 1920-1927. doi: http://dx.doi.org/10.1016/j.eswa.2009.07.015

Zadeh, L. A. (1965). Fuzzy sets. *Information and Control*, *8*, 338-353. doi: http://dx.doi.org/10.1016/S0019-9958(65)90241-X

Zadeh, L. A. (1975). The Concept of a linguistic variable and its application to approximate reasoning. Parts 1, 2 and 3. *Information Sciences*, *8*, 199-249. doi: http://dx.doi.org/10.1016/0020-0255(75)90036-5