IV CONGRESO INTERNACIONAL DE GESTIÓN TECNOLÓGICA E INNOVACIÓN 2014
Gestión de la Innovación para el desarrollo territorial

COGESTEC

La mejora de la gestión de seguridad de la información desde las políticas: Caso Universidad Industrial de Santander

Leidy Johanna Cárdenas Solano

Estudiante segundo año de Maestría en Ingeniería Industrial, Universidad Industrial de Santander, Bucaramanga, Santander, Colombia. Investigadora Grupo de Investigación INNOTEC y Grupo de Investigación GIGIA. Docente Investigador Universidad Manuela Beltrán.
leidy.cardenas@docentes.umb.edu.co; lcardenas@uis.edu.co

Hugo Ernesto Martínez Ardila

Estudiante de doctorado en Ingeniería. Universidad Industrial de Santander, Bucaramanga, Santander, Colombia. Investigador Grupo de Investigación INNOTEC. hugo.martinez@correo.uis.edu.co.

Luis Eduardo Becerra Ardila

Profesor asociado Escuela de Estudios Industriales y Empresariales. Universidad Industrial de Santander, Bucaramanga, Santander, Colombia. Investigador principal Grupo de Investigación INNOTEC.
lbecerra@uis.edu.co, Correo e. personal: luchouis@gmail.com

Resumen

Garantizar la seguridad de la información corporativa, que es almacenada, procesada y difundida mediante el uso de tecnologías de información y comunicación [TIC], se ha convertido en una actividad sumamente compleja y desafiante. Esta es una preocupación muy importante para las organizaciones intensivas en conocimiento, como las universidades, en donde sus actividades de investigación, docencia y procesos administrativos demandan cada vez más de una gestión eficiente de conocimiento. Esta gestión depende de la disponibilidad, integridad y exactitud de los recursos de información. En este trabajo se evidencia explícitamente que uno de los puntos más importantes para definir controles de seguridad de la información, es instaurar políticas claras al respecto, que establezcan un marco regulatorio para las actividades que deben ser llevadas a cabo en este contexto, y es precisamente uno de los resultados más importantes del ejercicio de prospectiva realizado. Por tanto, se muestra el caso de la Universidad Industrial de Santander, una institución de educación superior, que tiene el reto de aplicar controles que aseguren la gestión de la información administrativa y académica sensible, y también, la información personal de los estudiantes y empleados.

Palabras clave

Seguridad de la información, Tecnologías de información y comunicación, Análisis Estructural, MICMAC, Universidad.

1 Introducción

Hoy en día son múltiples los riesgos asociados a que los equipos y sistemas de información y comunicaciones no cuenten con controles de seguridad, por lo que cada día, se desarrollan nuevos métodos que afectan a la seguridad de la información de las organizaciones, generándose la necesidad de una estrategia completa de seguridad que prevenga fugas y fallas en los sistemas. A lo antes expuesto se suman vulnerabilidades internas (misma organización), que son un factor de riesgo no menor, y por lo tanto, existe alta probabilidad de pérdida de dinero y repercusiones en la confiabilidad por parte de usuarios, clientes y socios de negocios.

El objetivo del presente artículo es por tanto mostrar los resultados de un estudio de prospectiva que prueba lo anteriormente expuesto, desarrollado en una universidad pública colombiana que durante los últimos tres años se ha mostrado desde la dirección de la misma muy interesada en fortalecer la seguridad de su información y conocimiento por ser principalmente una organización basada en conocimiento. Este estudio se realizó a través de la herramienta "análisis estructural" usando como software libre de soporte MICMAC® (Matriz de Impactos Cruzados Multiplicación Aplicada a una Clasificación)[1] , el cual evidencia la necesidad de una estrategia de seguridad en la información alineada con las iniciativas que tiene la universidad y el gobierno nacional en el tema. De acuerdo con un reporte de Deloitte (2007), el 54% de las empresas cuenta con una estrategia, el 20% planea hacerlo en los próximos dos años; en tanto, el 17% considera que la falta de esta estrategia es una de las principales barreras para lograr la seguridad en la información. Adicionalmente, se identificó también que una organización debe contar con un marco de gobernabilidad en relación a la seguridad de la información que pueda evitar una serie de riesgos de seguridad, entre los que incluyen robo de identidad, fuga de información, fraude y otros.

Por tanto, con el objetivo de entender una realidad o problema específico, y siendo interesante abordarlo, entendiéndolo como un sistema. Se crea entonces un modelo, en este caso, basado en conocimientos, en el que se "sintetiza en pocas variables el funcionamiento de un aspecto complejo". "La estructura de las variables en un sistema definido, conserva cierta permanencia, lo que varía son las relaciones entre ellas" (Garavito, 2012), su evolución y las nuevas maneras de medirlas. Todas estas características enmarcan el *análisis estructural*, y lo hacen ser una herramienta versátil, y por esta razón práctica para un estudio en el que se quiere conocer escenarios reales y potenciales, en el "corto" y "largo" plazo – Fotos instantáneas de la situación.

[1] Software desarrollado por el Laboratorio de Investigación en Prospectiva, Estrategia y Organización LIPSOR, el Instituto de Innovación Informática para la Empresa 3IE y la Escuela para la Informática y Técnicas Avanzadas EPITA.

2 Metodología

Para realizar el trabajo se realizó el análisis estructural, el cual es "una herramienta diseñada para el enlace de ideas", que se utiliza en la construcción de escenarios, principalmente con el fin de "encontrar las variables influyentes, dependientes y esenciales para entender la evolución del sistema y predecir su comportamiento futuro. Según Ballesteros (2008), el principal mérito de este método radica en la ayuda que presta a un grupo para plantearse las buenas preguntas y estructurar una reflexión colectiva" tal reflexión, debe ser lo suficientemente sencilla para apropiar fácilmente el proceso y los resultados asegura Godet (2000). Esta herramienta permite describir un sistema con la ayuda de una matriz en donde los diferentes actores del mismo, relacionan los elementos que lo constituyen. Su objetivo, afirma Godet (2000), es revelar las principales variables influyentes y dependientes y de esta manera los elementos esenciales entre aquellos constitutivos de un problema, para la evolución del sistema. En otras palabras, investigadores como Mojica (2005) sugieren que, permite "identificar el peso de los fenómenos y la gobernabilidad que se tiene sobre ellos dentro del sistema"; reduciendo de esta forma la complejidad del sistema de estudio.

En general, el proceso que se lleva a cabo en la realización de un análisis estructural consta de tres etapas (Arista, 1997): Elaboración del listado de variables, identificación de las interrelaciones por medio de la matriz de análisis estructural e identificación de las variables clave (Godet, 2000). A continuación se detallan las especificidades de cada una de ellas.

2.1 Definición del sistema y variables a evaluar

Como paso fundamental para la identificación de las variables que serán sujeto de evaluación es preciso especificar el sistema a analizar. En este sentido, se parte de la definición de sistema dada por O'Brien (1998), quien establece que un sistema es "un grupo de componentes interrelacionados que trabajan juntos hacia un fin común, aceptando inputs y produciendo outputs en un proceso de transformación organizado".

Un sistema es más complejo mientras más componentes y más interrelaciones existan entre estos. Como consecuencia, surgen propiedades o características nuevas que no pueden explicarse analizando de forma aislada cada elemento del sistema. En este caso, se considera como sistema de estudio, el sistema de seguridad de la información en grupos de investigación de la Facultad de Ingenierías Fisico-mecánicas de la Universidad Industrial de Santander, el cual está conformado por diferentes componentes, de tipo tecnológico o humano, que pueden aumentar o disminuir el nivel de seguridad en este tipo específico de organizaciones basadas en conocimiento.

Asimismo, se pueden establecer los factores en que se divide el sistema y en los cuales se deben clasificar las variables. Esta etapa, aunque es la menos formal, es crucial para el resto del proceso, ya que en ella se generan no solo las variables sino la estructura del sistema bajo

estudio; en el curso de esta fase conviene ser lo más exhaustivo posible y no excluir a priori ninguna pista de investigación[2].

Con base en el esquema general del sistema se realizó inicialmente una lluvia de ideas a fin de construir un listado inicial de variables que sirviera de soporte para la identificación final de las variables a analizar. Este listado se construyó previa revisión bibliográfica, estudiando diferentes documentos alusivos a la seguridad de la información, entre los que se encuentran, el libro "Information Security" de Layton; normas de referencia o metodologías para valoración de riesgos, como, OCTAVE[3], MAGERIT, e ISO/IEC 27002:2005; guías de seguridad de la información, como la proporcionada por NIST[4]; estudios institucionales y de organismos internacionales; entre otros. Luego de reuniones iniciales no estructuradas tipo tormenta de ideas en que emergieron más de 70 variables, la discusión se estructuró alrededor de una propuesta de 59 variables. Es importante aclarar que en este primer paso se eliminó cualquier tipo de restricción en la consideración de las variables, evitando la crítica de las mismas así como la exploración de las implicaciones de cada una, lo que generó una lista extensa y posiblemente redundante.

Teniendo en cuenta la lista mencionada en el párrafo anterior, y luego de un proceso de depuración, agrupación según relaciones y semejanzas existentes y un consenso entre los autores del estudio, se obtuvo como resultado una lista final de 11 variables a evaluar que logran explicar las 59 anteriores de una manera más general, que además no buscan describir con precisión el funcionamiento del sistema estudiado, sino destacar sus principales características (Godet, 2000).

2.2 Influencia entre las variables

La evaluación de la influencia que ejerce cada variable sobre las otras fue desarrollada por los evaluadores, los cuales fueron seleccionados de acuerdo a su trayectoria en la realización de actividades de investigación o administración en los grupos de investigación y Unidades Académico Administrativas de la UIS, y su conocimiento sobre el funcionamiento del sistema. La influencia entre las variables se presenta en alguno de los siguientes tipos:

- Real Directa: La variable A influye sobre B, por lo que los cambios en A modifican a B.
- Real Indirecta: Si la variable A influye sobre B y B influye sobre C, entonces A influye indirectamente sobre C.

[2] Prospectiva. Análisis Estructural, Mic Mac. Matriz de Impactos cruzados – Multiplicación Aplicada a una clasificación, p. 7. [Consultado 2 febrero de 2012] Disponible en: <http://www.ucol.mx/acerca/coordinaciones/cgic/cgic/Ejeinvestigacion/Bibliografia/Micmac_instrucciones.pdf>
[3] Operationally Critical Threat, Asset, and Vulnerability Evaluation.Ver Capitulo 3. Estado del Arte
[4] National Institute of Standards and Technology.Sitio web: http://www.nist.gov/index.html

- Potencial: Se da cuando la influencia de una variable sobre otra no acontece en el momento presente, pero se piensa que debería darse. Es decir, la influencia se sitúa no al nivel del ser sino del deber ser (Mojica, 2005).

De esta forma, se empleó una matriz de doble entrada en la que los evaluadores valoraron únicamente las influencias directas y potenciales entre variables. Finalmente la matriz fue diligenciada por los evaluadores empleando cualquiera de los símbolos de la Tabla 1 según la evaluación realizada.

Tabla 1. Simbología para el diligenciamiento de la matriz

Símbolo	Tipo de Influencia
1	Directa débil
2	Directa Moderada
3	Directa fuerte
4	Potencial.

Fuente: Autores con base en las instrucciones del software MIC MAC®

2.3 Identificación de las variables clave

A partir de las valoraciones dadas por los evaluadores, se aplicó una metodología propia de los autores con el fin de generar consenso entre las respuestas obtenidas, y así obtener la matriz de influencias directas que se introdujo en el software MICMAC® para ser procesada por el mismo. Para esta fase se empleó el software libre MICMAC® (Matriz de Impactos Cruzados Multiplicación Aplicada a una Clasificación)[5], a través del cual se realizó la jerarquización de las variables en términos de su influencia y dependencia. Para este fin, el software sitúa las variables en planos de Influencia/Motricidad -Dependencia de acuerdo al valor obtenido en los índices de estos dos criterios. El plano se encuentra explícitamente divido en cuatro zonas, sin embargo, se contempla la existencia de una quinta en la parte media del mismo; en éstas las variables son ubicadas de acuerdo a su relación de motricidad- dependencia, denotando con esto características especiales, las cuales son descritas en la Tabla 2 y la Figura 1.

Una vez se ha tomado la decisión de explorar y conocer las condiciones de un sistema en el presente y en el futuro una vez se intervenga, la primera acción que se debe efectuar es la determinación de los elementos que serán fundamentales en el futuro de la organización o sistema tomado (De Jouvenel, 1993), entendiendo esto como la identificación de las variables clave. Esta fase consiste en la identificación de variables esenciales a la evolución del sistema,

[5] Software desarrollado por el Laboratorio de Investigación en Prospectiva, Estrategia y Organización LIPSOR, el Instituto de Innovación Informática para la Empresa 3IE y la Escuela para la Informática y Técnicas Avanzadas EPITA.

en primer lugar mediante una clasificación directa (de realización fácil, mediante simples sumas de valores de motricidad/influencia y de dependencia para cada una de las variables), y posteriormente por una clasificación indirecta (llamada MICMAC® para matrices de impactos cruzados Multiplicación Aplicada para una Clasificación). Esta clasificación indirecta se obtiene después de la elevación en potencia de la matriz. La comparación de la jerarquización de las variables en las diferentes clasificación (directa, indirecta y potencial) es un proceso rico en enseñanzas. Ello permite confirmar la importancia de ciertas variables, pero de igual manera permite desvelar ciertas variables que en razón de sus acciones indirectas juegan un papel principal (y que la clasificación directa no ponía de manifiesto)[6].

[6] Prospectiva. Análisis Estructural, Mic Mac. Matriz de Impactos cruzados – Multiplicación Aplicada a una clasificación, p. 7. [Consultado 2 febrero de 2012] Disponible en: <http://www.ucol.mx/acerca/coordinaciones/cgic/cgic/Ejeinvestigacion/Bibliografia/Micmac_instrucciones.pdf>

Tabla 2. Zonas en los planos Motricidad/Influencia – Dependencia

Zona	Motricidad	Dependencia	Característica de las variables
Poder	Alta	Baja	Sus modificaciones repercuten en todo el sistema.
Conflicto/ Trabajo	Alta	Alta	Las variaciones sobre ellas tienen efecto en sí mismas y en la zona de salida.
Salida	Baja	Alta	Son producto de las variables de las zonas anteriores.
Autónoma	Baja	Baja	No constituyen parte determinante para el futuro del sistema.
Pelotón	Media	Media	No se puede decir nada *a priori* sobre estas variables.

Fuente: Elaboración a partir de Flórez y Serrano, 2011

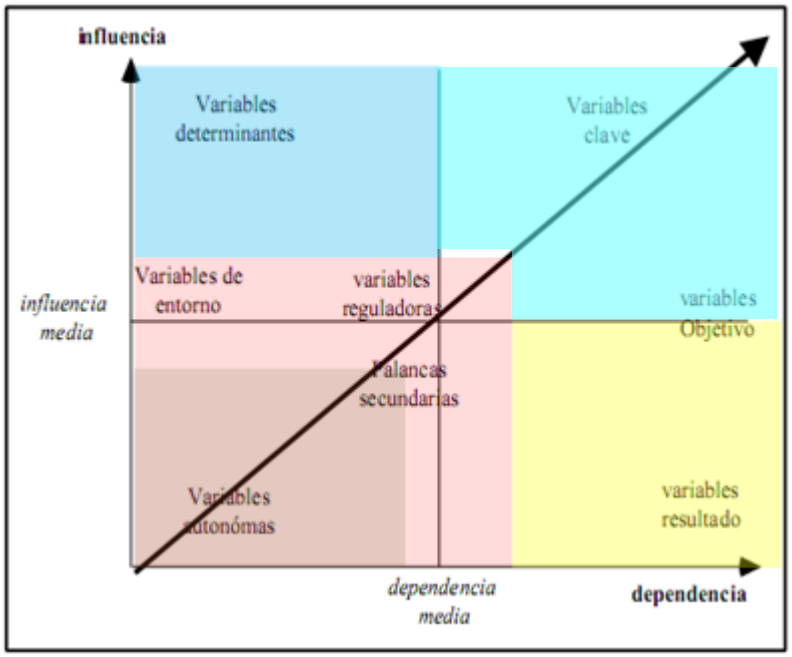

Figura 1. Plano Motricidad/Influencia - Dependencia MICMAC

3 Presentación de los resultados

El análisis preliminar del sistema partió del *plano de influencia/dependencia indirecto* (Figura 2), que permite apreciar las influencias ocultas entre las variables, revelando la influencia que se puede ejercer sobre una variable a través de terceros, es decir que se puede modificar el estado de una variable de interés a través de la acción sobre otra sin atacarla directamente, dándole a quienes toman las decisiones (actores) la posibilidad de diversificar sus opciones para influenciar el sistema.

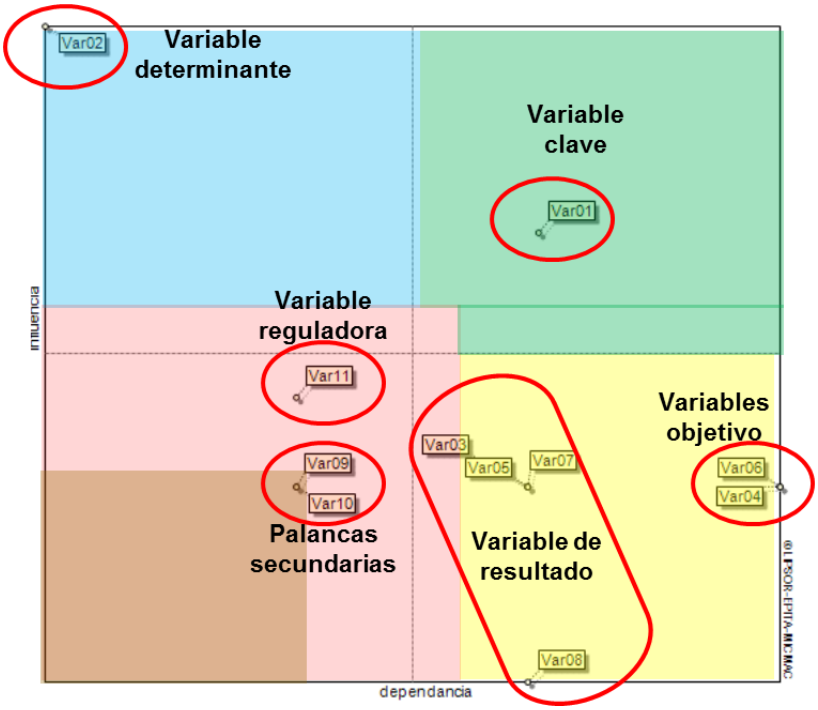

Figura 2. Plano de influencias / dependencias indirectas

Fuente: Software MicMAc®

Se observa, que la variable 2, es decir, la organización de seguridad de la información, ubicada en una posición completamente influyente e independiente del resto de variables, se puede entender como una variable de gran poder, y corresponde al área en la que se pueden realizar acciones que afecten todo el sistema, es decir, variables de entrada, fuertemente motrices. Según la perspectiva de los evaluadores, la seguridad en los grupos de investigación depende de la presencia de una estructura que gestione en diferentes niveles (estratégico, táctico y operativo). Es decir, se requiere que se definan directrices y se apoye activamente desde la dirección de los grupos de investigación, la gestión de la seguridad de la información, este compromiso debe verse reflejado a través de un comité encargado del área, la asignación de responsabilidades, la aprobación de un documento de políticas de seguridad de la información,

la exigencia del cumplimiento de dichas políticas, la revisión periódica y monitoreo del estado general de la seguridad de la información, entre otras actividades de alto nivel relacionadas con la seguridad de la información[7]. En conclusión, esta variable determina el sistema en un inicio, es decir, cuando se quiere dar los primeros pasos de implementación de seguridad en toda la organización; es a través de esta primera gestión que se debe fomentar la cooperación y la colaboración de todos los integrantes del grupo de investigación[8], y con esta variable se puede por tanto, influenciar y afectar todas las demás variables.

Sin embargo, a la hora de definir las variables estratégicas del sistema de investigación en el área de seguridad de la información, el plano de influencias/dependencias indirectas no es contundente; por tanto, es indispensable incluir el efecto de las relaciones potenciales definidas por los evaluadores que darán como resultado un estado de evolución del sistema en un contexto futuro, lo que puede implicar un desplazamiento de cada variable respecto a su posición inicial. De esta forma se obtiene el plano de influencias/dependencias indirectas potenciales, visible en la Figura 3.

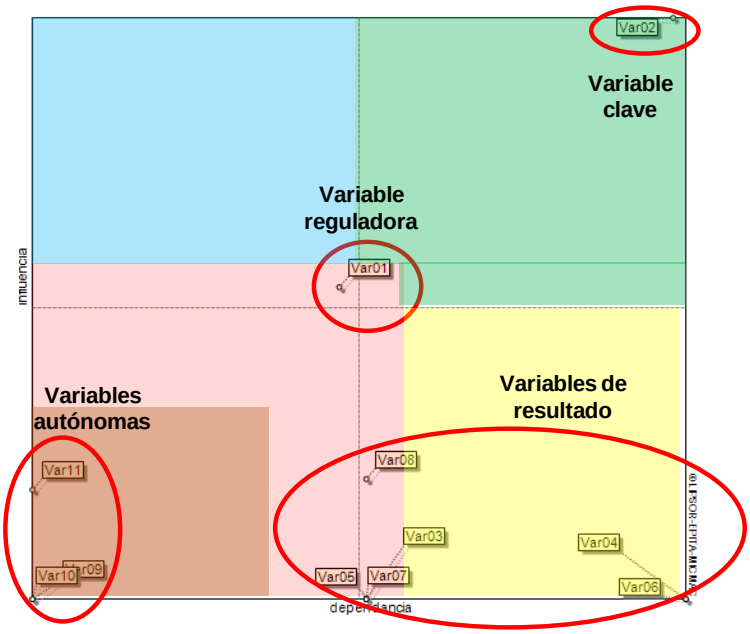

Figura 3. Plano de influencias / dependencias indirectas potenciales
Fuente: Software MicMAc®

[7] SISTESEG. Organización de la Seguridad de la Información. [en línea] [consultado 15 agosto 2012]. Disponible en: <http://www.sisteseg.com/files/Microsoft_Word_-_Organizaci_n_de_la_seguridad_de_la_informaci_n.pdf>

[8] PORTAL DE SOLUCIONES TÉCNICAS Y ORGANIZATIVAS A LOS CONTROLES DE ISO/IEC 27002. Capítulo 6: Organización de la seguridad de la información. [en línea]. [consultado 15 agosto 2012]. Disponible en: <http://iso27002.wiki.zoho.com/6-1-Organizaci%C3%B3n-Interna.html>

Como panorama inicial, se observa que todas las variables se han movido a través del plano, donde algunas conservan su zona mientras que otras cambian radicalmente de posición, lo que puede justificarse dadas las influencias indirectas, es decir, la existencia de una "tercera variable" afectando a través de otra. Según su distribución en el plano, las variables reguladoras situadas en la zona central del plano, se convierten en "llave de paso" para alcanzar el cumplimiento de las variables-clave y que estas vayan evolucionando tal y como conviene para la consecución de los objetivos del sistema. Corresponde a esta denominación la Política de Seguridad de la Información; la cual en todos los planos de influencia dependencia analizados (directo, potencial, indirecto, e indirecto potencial), siempre conserva el segundo lugar más influyente después de la organización de la seguridad de la información**.** Su ubicación en la zona de poder se justifica al tratarse de una variable netamente de gobierno, pues es en la política donde se definen los lineamientos de actuación para todas las demás dimensiones de seguridad de la información. Además, expresa las intenciones y objetivos de la alta dirección respecto a la protección de los activos de información y conocimiento, que son áreas resultado en el sistema.

4 Conclusiones

Finalmente, el análisis estructural es aprovechado como una herramienta para identificar o describir el funcionamiento del sistema de seguridad de la información, mediante las relaciones de influencia y dependencia entre las variables o dimensiones incluidas. Por tanto, más allá de identificar las variables estratégicas futuras, se logró identificar que variables determinan el sistema, que causas, efectos o impactos generan y de qué forma se deben controlar.

Todo lo anterior basado en el conocimiento tácito de los evaluadores que fueron encuestados a nivel institucional como muestra representativa de la UIS. Ahora se verá materializado el conocimiento y los criterios de evaluación recolectados mediante la matriz de impactos.

Los resultados obtenidos se detallan en el plano de desplazamientos (ver Figura 4), que permite ver el comportamiento de las variables a través del tiempo mientras el sistema se estabiliza. Allí se observa que la variable "Política de Seguridad de la Información", en el plano directo se encontraba en la zona de poder y en el plano indirecto potencial se desplazó a la zona de conflicto. Dados estos comportamientos, se puede pensar hipotéticamente que en una organización, y en este caso un grupo de investigación de una universidad pública, donde el conocimiento es el activo más importante, no puede abordarse asuntos específicos de seguridad de la información sin antes implementar una política que permita tener una aproximación holística de los riesgos, puesto que la política ayudará a escoger los controles adecuados para disminuir los riesgos identificados, y tener una priorización clara de los asuntos de seguridad a tratar para que los controles implementados sean coherentes con los requerimientos de seguridad del grupo.

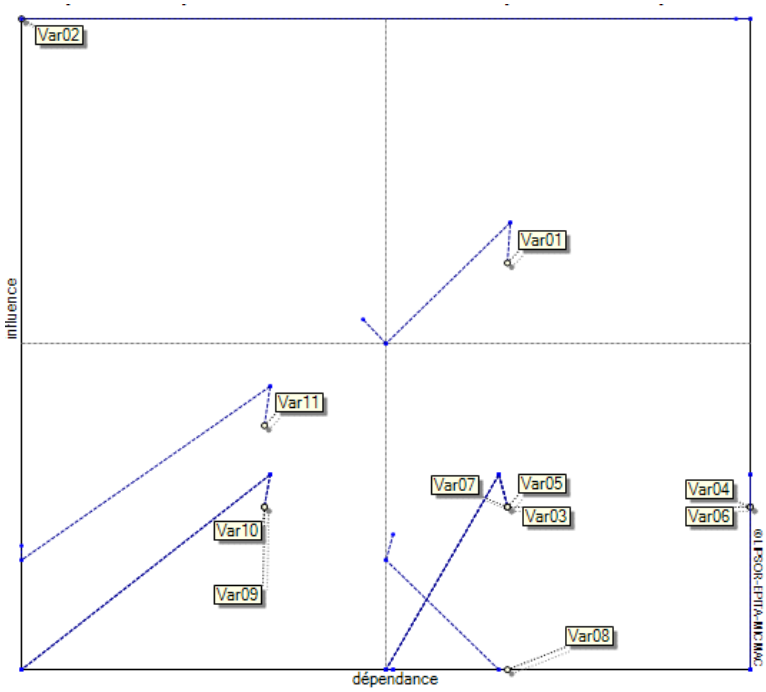

Figura 4. Plano de desplazamientos: directo/indirecto/directo potencial/indirecto potencial
Fuente: Software MicMAc®

Referencias

ARISTA, Anarrosa, et al. Prospectiva: Construcción social del futuro. Santiago de Cali: ILPES, 1997, p. 116

BALLESTEROS, Diana Paola. Análisis estructural prospectivo aplicado al sistema logístico. En: Scientia et Technica. Vol. 14, No. 39 (2008); p. 194.

BRIGHTMAN, J. Buith. "Treading Water. The 2007 Technology, Media & Telecommunications Security Survey", Deloitte, 2007. Citado por: Burgos Salazar, Jorge & Campos, Pedro G. Modelo para seguridad de la información en TIC. p. 234-253. Universidad del Bío-Bío, Chile. Disponible en internet: <http://ceur-ws.org/Vol-488/paper13.pdf>

DE JOUVENEL, Hugues. Sur la démarch eprospective, un brief guide méthodologique. Futuribles. 1993, Citado por ARISTA, Anarrosa, et al. Op, cit., p. 154.

FLÓREZ, María Camila y SERRANO, Ximena Paola. Identificación de líneas estratégicas de investigación para la Universidad Industrial de Santander a partir de herramientas de vigilancia tecnológica y prospectiva área: salud. Trabajo de grado Ingeniería Industrial. Bucaramanga: Universidad Industrial de Santander. Facultad de Ingenierías Fisicomecánicas. Escuela de Estudios Industriales y Empresariales, 2011, p. 86.

GARAVITO, Edwin. Presentación 2. Material académico para la asignatura Técnicas modernas de optimización. Presentación en formato PDF [En línea]. [Consultado el 15 de febrero de 2012] Disponible en: http://gavilan.uis.edu.co/~garavito/index_general.htm

GODET, Michel. La caja de herramientas de la prospectiva estratégica. 4 ed. París: Gerpa con la colaboración de Electricité de France, Mission Prospective, 2000, p.74.

MOJICA, Francisco José. La construcción del futuro. Bogotá: Universidad Externado de Colombia, 2005, p.123.

NIST - National Institute of Standards and Technology.Sitio web: http://www.nist.gov/index.html

O'BRIEN, J. Management Information Systems: A Managerial End User Perspective. 2 ed. Boston: Irwin, 1998.

OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation.Ver Capitulo 3. Estado del Arte

PORTAL DE SOLUCIONES TÉCNICAS Y ORGANIZATIVAS A LOS CONTROLES DE ISO/IEC 27002. Capítulo 6: Organización de la seguridad de la información. [en línea]. [consultado 15 agosto 2012]. Disponible en: <http://iso27002.wiki.zoho.com/6-1-Organizaci%C3%B3n-Interna.html>

PROSPECTIVA. Análisis Estructural, Mic Mac. Matriz de Impactos cruzados – Multiplicación Aplicada a una clasificación, p. 7. [Consultado 2 febrero de 2012] Disponible en: <http://www.ucol.mx/acerca/coordinaciones/cgic/cgic/Ejeinvestigacion/Bibliografia/Micmac_instrucciones.pdf>

SISTESEG. Organización de la Seguridad de la Información. [en línea] [consultado 15 agosto 2012]. Disponible en: <http://www.sisteseg.com/files/Microsoft_Word_-_Organizaci_n_de_la_seguridad_de_la_informaci_n.pdf>