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

Recebido/Submission: 05/02/2019
Aceitação/Acceptance: 08/04/2019

Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información

Mauricio Diéguez[1,2], Carlos Cares[1,3]

mauricio.dieguez@ufrontera.cl,carlos.cares@ceisufro.cl

[1] Departamento de Ciencias de la Computación e Informática, Universidad de La Frontera, 4811230, Temuco, Chile.

[2] Grupo de Ciberseguridad, Centro de Excelencia de Modelación y Computación Científica, Universidad de La Frontera, 4811230, Temuco, Chile.

[3] Centro de Estudios de Ingeniería de Software, Universidad de La Frontera, 4811230, Temuco, Chile.

DOI: 10.17013/risti.32.113–128

Resumen: Proporcionar procesos y herramientas sistemáticos para tomar una decisión sobre inversiones en seguridad en un escenario con restricciones presupuestarias, es de suma importancia para asegurar que dichas decisiones se tomen adecuadamente. Presentamos un enfoque de programación de conjunto de respuestas (ASP) para resolver este problema. Nuestra propuesta se compara con el desarrollo del problema utilizando programación lineal (PL). Ilustramos la fase de modelado y el rendimiento computacional de ambas soluciones. El modelo ASP presenta tiempos de resolución del tipo exponencial a medida que aumenta el número de controles sobre los que debe decidirse. Por otro lado, el modelo basado en PL no presenta variaciones importantes en sus tiempos de resolución de problemas. Sin embargo, el problema es más fácil de modelar en ASP. Luego, esta propuesta tiene ventajas para modelar y resolver problemas específicos en los que se requiere una respuesta rápida con una baja cantidad de controles.

Palabras-clave: Answer set programming; Programación lineal; Optimización; Controles de seguridad de la información; Sistema de gestión de seguridad de la información.

Comparing Two Quantitative Approaches to Select Information Security Controls

Abstract: Provide systematic processes and tools to make a decision about security investments under a scenario of budget constraints, is of paramount importance to assure that such decisions are soundly made. We present a answer set programming (ASP) approach to solve this problem. Our proposal is then compared against a traditional linear programming (LP) operational research technique. We illustrate the modeling phase and computational performance of both solutions. The model based on ASP presents resolution times of the exponential type as the number of controls over which it must be decided increases. On the other hand, the model based on LP does not present important variations in its problem resolution times.

However, the problem is easier to model in ASP. Then, this proposal has advantages for modeling and solving specific problems in which a rapid response is required and which do not require many controls.

Keywords: Answer set programming; linear programming; optimization; information security controls; information security management systems.

1. Introducción

El actual escenario en ciberseguridad, ha obligado a las organizaciones a incorporar un conjunto de buenas prácticas de seguridad en sus sistemas de gestión de la información. Estas prácticas de protección se han extendido por todo el mundo y han llevado a diferentes organizaciones a definir e implementar estándares de seguridad de la información (Tofan, 2011).

Un estándar para la seguridad de la información consiste en un conjunto de reglas que tienen como objetivo regular las operaciones de una empresa, con un énfasis especial en la gestión y el aseguramiento de la información. En términos generales, el cumplimiento de algún estándar de seguridad de la información implica el logro de un conjunto de objetivos, la adquisición de recursos o la implementación de acciones regulares que se definen en el estándar (Pereira & Santos, 2014). Todos estos elementos se conocen como controles de seguridad de la información (ISC por sus siglas en inglés) (Yau, 2014) y pueden agruparse por dimensiones.

El mapa de controles implementados-no implementados se convierte en una herramienta de administración para avanzar en la seguridad de la información. En este contexto, es necesario definir un programa de selección de controles que proponga un camino hacia el logro de la norma y que pueda evaluarse continuamente a través de un programa de auditoría. Sin embargo, la limitación de recursos y la existencia de dependencias entre ellos pueden impedir que algunos de los controles se implementen juntos. Por lo tanto, la progresión hacia un cumplimiento total de un estándar definido, viene a menudo a través de múltiples avances parciales. En este escenario, la selección del subconjunto de controles de seguridad que debe implementarse, debe ser tal que maximice el progreso, minimice los riesgos y optimice los recursos.

El enfoque tradicional para enfrentar esta situación, ha sido la gestión del riesgo mediante el uso de instrumentos cualitativos y juicios de expertos (Cano, 2018). Sin embargo, algunos autores consideran que dichos enfoques cualitativos son subjetivos y están incompletos (A. Otero, Otero, & Qureshi, 2010), que deben ir acompañados de algún tipo de enfoque cuantitativo y objetivo. Se han propuesto varias técnicas con el objetivo de formalizar el proceso de selección del ISC, sin embargo, estas propuestas mantienen un grado de subjetividad (A. R. Otero, 2015).

Una solución cuantitativa para la selección de ISC se considera un problema NP-Hard (Tosatto, Governatori, & Kelsen, 2015). Existen propuestas que apuntan al uso de métodos matemáticos para apoyar la selección del ISC -ver por ejemplo (Breier & Hudec, 2013b; Cuihua & Jiajun, 2009; J. Lv, Zhou, & Wang, 2011; Yang, Shieh, Leu, & Tzeng, 2009) -. Sin embargo, agregar variables y restricciones reales al considerar casos específicos hace que sea más compleja la etapa de modelado, y transforma

esta etapa en una barrera difícil de cruzar para alcanzar una solución cuantitativa al problema.

En un trabajo anterior, hemos tratado de superar este problema proponiendo un enfoque basado en "Answer Set Programming" (ASP) (Cares & Diéguez, 2017). ASP es un área de investigación basada en la representación del conocimiento, la programación lógica y la satisfacción de restricciones diseñada para hacer frente principalmente a los problemas de NP-Hard (Brewka, Eiter, & Truszczyński, 2011). Hoy en día, hay herramientas que permiten la especificación y solución de estos modelos, tales como Clingo (Gebser et al., 2011).

Otra forma propuesta para resolver la selección de ISC es aplicar un enfoque de Programación Lineal (PL). La programación lineal es un producto de investigación que proviene de la disciplina de Investigación de Operaciones (OR). La programación lineal es parte del cuerpo de conocimientos de OR y también requiere una etapa de modelado. Existen varias herramientas para implementar estos algoritmos. Ilustramos esta solución específica utilizando NEOS Server (NEOS, 2018), una herramienta web para resolver problemas de optimización.

El objetivo de este documento es doble: por un lado, presentamos una versión ampliada del enfoque ASP, que mejora la versión anterior en (Cares & Diéguez, 2017). Por otro lado, para validar esta propuesta, la comparamos con el enfoque de PL, que se ha propuesto como un enfoque cuantitativo para la selección óptima de controles de seguridad (Kawasaki & Hiromatsu, 2014; Sawik, 2013; Yevseyeva, Fernandes, Van Moorsel, Janicke, & Emmerich, 2016). El aporte de este trabajo radica en presentar la aplicación de modelos de optimización y restricciones de operación que no habían sido consideradas en el dominio de la seguridad de la información. Además se proporciona un estudio respecto de la medición del desempeño de ambas técnicas, lo cual no se ha tratado con anterioridad.

El documento está organizado de la siguiente manera: en la sección 2, se presenta una búsqueda bibliográfica basada en un mapeo sistemático de los métodos actuales que tratan la gestión del ISC. En la Sección 3, el problema de la selección de controles se modela utilizando los dos enfoques en revisión, es decir, ASP y PL, e ilustramos cómo se implementa el modelo propuesto en dos plataformas tecnológicas diferentes. En la Sección 4, se realiza una prueba de concepto utilizando datos extraídos de un caso real para comparar el desempeño de ambas propuestas. Finalmente, la Sección 5 presenta las conclusiones del estudio.

2. Gestión de los Controles de Seguridad de la Información

La gestión de la seguridad de la información en una organización se realiza mediante la implementación y operación de un Sistema de Gestión de Seguridad de la Información (SGSI). Estos sistemas están orientados a identificar e implementar controles de seguridad para reducir el riesgo en el manejo de la información (Saint-Germain, 2005).

Actualmente, existen varios estándares de seguridad de la información que guían la implementación, operación, monitoreo, revisión, mantenimiento y mejora de un SGSI

(Tofan, 2011). En particular, uno de los estándares de seguridad más conocidos es ISO/IEC 27001: 2013 (International Organization for Standardization, 2013).

Es importante tener en cuenta que el enfoque de la selección de ISC no es solo la cantidad de controles que se deben implementar para lograr un nivel de seguridad, sino también la idoneidad del conjunto de controles (A. Otero et al., 2010).

Sin embargo, se ha reconocido que los intereses propios del administrador de seguridad pueden influir en el conjunto resultante de controles para implementar (Bachlechner, Maier, Innerhofer-Oberperfler, & Demetz, 2011), lo que hace que el proceso sea subjetivo. Este hecho se explica por la teoría de la agencia (Jensen & Meckling, 1976), que reconoce que un objetivo organizativo, como el objetivo de reducir el riesgo organizativo, no está necesariamente alineado con el objetivo de quien lo administre. Esta teoría señala que los intereses entre una organización (principal) y un administrador (agente) pueden divergir y que es necesario incurrir en lo que se conoce como costos de vinculación para lograr cierta alineación de objetivos y comportamientos. Si bien la Teoría de la Agencia reconoce que el mercado tiende a eliminar estas diferencias, una extensión de esta teoría ilustra cómo las anomalías del mercado pueden retrasar considerablemente el proceso de ajuste. Como ejemplo de lo anterior, es posible pensar en términos de un caso en el que un gerente de seguridad desea mostrar un aumento considerable en el porcentaje de controles implementados, como un indicador de su éxito en la gestión, aunque esto no necesariamente signifique una reducción significativa de los riesgos de seguridad de la información. Estos diferentes objetivos aumentan la complejidad del problema, ya que, bajo numerosas opciones de seguridad, las organizaciones buscarían elegir e implementar el conjunto óptimo de controles que reducen el riesgo y aumentan la rentabilidad, mientras que los administradores buscarían mejorar su propia posición como agentes de la organización.

Además, se debe considerar el caso en el que una organización desea cumplir con más de una norma de seguridad, como las organizaciones públicas, que, además de intentar lograr una norma internacional, debe cumplir con las normas locales regulaciones y políticas gubernamentales (Diéguez, Cares, & Sepúlveda, 2012).

Para identificar los estudios que han abordado el problema, hemos llevado a cabo una búsqueda bibliográfica basada en un protocolo de mapeo sistemático (Petersen, Vakkalanka, & Kuzniarz, 2015). En nuestro caso, el objetivo fue identificar qué métodos o técnicas se han propuesto para la selección de ISC. La pregunta que guió a los hallazgos principales fue: "¿Qué métodos o técnicas se han propuesto para resolver el problema de la selección y programación de un conjunto de controles de un estándar de seguridad de la información que permite la evaluación del riesgo en una organización?"

Para definir la cadena de búsqueda, se definieron los conceptos clave, que fueron: ("Evaluación de seguridad" O "Selección de controles" O "Soluciones de seguridad") Y "Cumplimiento de la seguridad de la información").

Para las búsquedas utilizamos los principales repositorios bibliográficos digitales de informática y disciplinas relacionadas: IEEE Xplore, Biblioteca Digital ACM, Springer Link y Science Direct. Además, se realizó una búsqueda manual en las actas de las principales conferencias del área.

Los artículos encontrados fueron evaluados por tres revisores para decidir su inclusión o exclusión, de acuerdo a los criterios descritos en la tabla 1. En la tabla 2, se muestra la lista con los artículos encontrados, después de filtrar respecto de los criterios de inclusión y exclusión.

De los 35 artículos seleccionados, cinco se refieren a investigaciones que incluyen modelos de optimización cuantitativos para la selección de ISC (Almeida & Respício, 2018; Kawasaki & Hiromatsu, 2014; Sawik, 2013; Yevseyeva, Basto-Fernandes, Emmerich, & van Moorsel, 2015; Zhang, Chari, & Agrawal, 2018). Estos enfoques proponen un modelo de selección de controles mediante la aplicación de un modelo de optimización de multi-objetivos, en el que relacionan los controles con sus riesgos asociados y su distribución de costos, para obtener una solución óptima. Sin embargo, no consideran la dependencia entre los controles de seguridad. En estas propuestas, la programación lineal se utiliza como la técnica principal de modelado y solución.

En un artículo anterior (Diéguez et al., 2012), propusimos un método de selección de ISC. Nuestro modelo, al igual que los cinco seleccionados, puede considerarse como un problema de optimización multi-objetivos, pero, a diferencia de los anteriores, considera las dependencias entre los controles. Además, el modelo se puede codificar según diferentes enfoques, como Answer Set Programming (ASP) y programación lineal (PL).

Criterios de Inclusión	**Criterios de Exclusión**
1. Artículos que presentan propuestas, modelos teóricos, ejemplos teóricos o casos de estudio, respecto de la selección y/o programación de controles de un estándar de seguridad de la información o que abordan el problema de selección de medidas de seguridad de la información.	1. Artículos que no presentan propuestas, modelos teóricos, ejemplos teóricos o casos de estudio, respecto de la selección y/o programación de controles de un estándar de seguridad de la información o que abordan el problema de selección de medidas de seguridad de la información. 2. Libros y Reportes Técnicos. 3. Documentos de tesis. 4. Trabajos duplicados del mismo estudio en diferentes fuentes. 5. Documentos de discusión o revisiones bibliográficas. 6. Artículos que no son accesibles. 7. Artículos que no están escritos en inglés.

Tabla 1 – Criterios de inclusión y exclusión del protocolo de mapeo sistemático

3. Descripción de las propuestas para la selección de controles de seguridad

En esta sección, presentamos dos enfoques alternativos para resolver el problema de optimización. El primer enfoque consiste en resolver el problema utilizando ASP, mientras que el segundo enfoque resuelve el problema utilizando PL.

Dado que puede haber múltiples combinaciones de controles que cumplan con un presupuesto determinado, se esperaría que los modelos presentados pudieran determinar el conjunto de controles que optimiza el presupuesto de una organización.

3.1. Modelado del problema con el enfoque ASP

ASP es un lenguaje de programación declarativo flexible, que se enfoca en resolver problemas combinatorios difíciles. Como tal, es una herramienta poderosa para la representación y razonamiento del conocimiento (Bonatti, Calimeri, Leone, & Ricca, 2010), y se puede usar para resolver problemas de tipo NP. Por lo tanto, encaja bien con los problemas de optimización y la programación de restricciones (Hooker, 2002), en la cual la función objetivo debe ser maximizada o minimizada, sujeta a algunas restricciones (Gebser et al., 2011).

Referencia	Año	Referencia	Año
(Bistarelli, Fioravanti, & Peretti, 2007)	2007	(Kiesling, Ekelhart, Grill, Straub, & Stummer, 2013)	2013
(Ojamaa, Tyugu, & Kivimaa, 2008)	2008	(Kiesling, Strauss, Ekelhart, Grill, & Stummer, 2013)	2013
(Yang et al., 2009)	2009	(Yang, Shieh, & Tzeng, 2013)	2013
(Gao, Li, & Song, 2009)	2009	(Sawik, 2013)	2013
(Cuihua & Jiajun, 2009)	2009	(Breier & Hudec, 2013b)	2013
(Chen, Li, Hu, & Lian, 2009)	2009	(Breier & Hudec, 2013a)	2013
(Nagata, Amagasa, Kigawa, & Cui, 2009)	2009	(Breier, 2014)	2014
(A. Otero et al., 2010)	2010	(Choo, Mubarak, Mani, & others, 2014)	2014
(J.-J. Lv & Wang, 2010)	2010	(Al-Safwani, Hassan, & Katuk, 2014)	2014
(Angel Otero, Ejnioui, Otero, & Tejay, 2011)	2011	(Kawasaki & Hiromatsu, 2014)	2014
(Yameng, Yulong, Jianfeng, Xining, & Yahui, 2011)	2011	(Meng & Liu, 2015)	2015
(J. Lv et al., 2011)	2011	(Shahpasand, Shajari, Golpaygani, & Ghavamipoor, 2015)	2015
(Rees, Deane, Rakes, & Wade H. Baker, 2011)	2011	(Yevseyeva et al., 2015)	2015
(Angel Otero, Tejay, Otero, & Ruiz-Torres, 2012)	2012	(Sarala, Zayaraz, & Vijayalakshmi, 2015)	2015
(Ejnioui, Otero, Tejay, Otero, & Qureshi, 2012)	2012	(Jiménez-Martín, Vicente, & Mateos, 2015)	2015
(Breier & Hudec, 2012)	2012	(Khajouei, Kazemi, & Moosavirad, 2017)	2017
(Viduto, Maple, Huang, & López-Peréz, 2012)	2012	(Almeida & Respício, 2018)	2018
(Kiesling, Strausss, & Stummer, 2012)	2012	(Zhang et al., 2018)	2018

Tabla 2 – Lista de artículos encontrados en Mapeo Sistemático

La figura 1 muestra un extracto de la formulación de este problema utilizando ASP, de acuerdo con la formulación presentada en (Cares & Diéguez, 2017). El modelo, es decir, predicados, reglas y restricciones de este caso se puede descargar desde http://dci.ufro.cl/fileadmin/Software/OptimalSecurityControls-OSCUFRO.zip.

```
#show planned/1.
#show totalCost/1.
#show totalProfit/1.

%controls
control(c6_1; c6_1_1; c6_1_2; c6_1_3; c6_1_3_1; c6_2; c6_2_1; c6_2_2;

%implementation of
%controls implies costs
cost(c6_1,480000).
cost(c6_1_1,800000).
cost(c6_1_2,160000).
cost(c6_1_3,220000).
cost(c6_1_3_1,100000).

%implementation of controls
%implies security profits

profit(c6_1,1).
profit(c6_1_1,1).
profit(c6_1_2,1).
profit(c6_1_3,1).
profit(c6_1_3_1,1).
profit(c6_2,1).
profit(c6_2_1,1).
```

(a) Configuración de Variables

```
%some controls requires
%other controls

require(c6_1,(c6_1_1;c6_1_2;c6_1_3)).
require(c6_1_3,(c6_1_3_1)).
require(c6_2,(c6_2_1;c6_2_2;c6_2_3;c6_2_4;c6_2_5)).

budget(4000000).

%Generate

0 { planned(Y) } 1 :- terminal(Y).
0 { planned(X) } 1 :- totalRequired(X,D), totalIncluded(X,W), D==W.

%Define
totalRequired(X,D):- control(X), D = #count {Z:require(X,Z),control(Z)}.
totalIncluded(X,D):- control(X), D = #count {Z:require(X,Z),planned(Z)}.
totalProfit(Y):- Y = #sum {D,X: planned(X),profit(X,D)}.
totalCost(N) :- N = #sum {D,X: planned(X),cost(X,D)}.
terminal(X):-control(X), not require(X,_).


%Test
:- totalCost(N), budget(T), N>T.

%Optimization
#maximize  { I:totalProfit(I) }.
```

(b) Definición de ecuaciones

Figura 1 – Codificación de Clingo del modelo ASP.

3.2. Modelación del problema con el enfoque PL

La formulación para el problema presentado, considerando las restricciones de presupuesto, las dependencias de control y los beneficios de la implementación, se describe en la ecuación 1. La ecuación 2, es el costo de la restricción de implementación, donde la suma de estos costos no puede exceder el presupuesto disponible para la implementación. La ecuación 3 representa el anidamiento de primer nivel y la ecuación 5 el anidamiento de segundo nivel.

Para formular el problema, utilizamos el Sistema de modelado algebraico general (GAMS) (GAMS, 2018), un sistema de modelado de alto nivel para programación y optimización matemática. Para resolver el problema, utilizamos el portal web NEOS Server (NEOS, 2018), un sitio web gratuito para resolver problemas de optimización. En el Servidor NEOS, el problema se modeló como Programación lineal de enteros mixtos, utilizando la entrada GAMS.

En la Figura 2, se muestra un extracto de la configuración de las variables y la definición de las ecuaciones, en lenguaje GAMS.

$$Max\left(\sum_{i>0,j>0,j\neq k,j\neq l} P_{ij}X_{ij} + \sum_{i>0,j>0,k\in A_{ij}} P_{ijk}X_{ijk} + \sum_{i>0,j>0,k\in A_{ijl},l\in A_{ijk}} P_{ijkl}X_{ijkl}\right) \quad (1)$$

s.t.

$$\left(\sum_{i>0,j>0,j\neq k,j\neq l} C_{ij}X_{ij} + \sum_{i>0,j>0,k\in A_{ij}} C_{ijk}X_{ijk} + \sum_{i>0,j>0,k\in A_{ijl},l\in A_{ijk}} C_{ijkl}X_{ijkl}\right) - B \leq 0 \quad (2)$$

$$X_{ij} - X_{ijk} \leq 0$$
$$i > 0, j > 0, k \in A_{ij}, A_{ij} \neq \emptyset \quad (3)$$

$$X_{ijk} - X_{ijkl} \leq 0$$
$$i > 0, j > 0, k \in A_{ij}, l \in A_{ijk}, A_{ij} \neq \emptyset, A_{ijk} \neq \emptyset \quad (4)$$

Donde,
P: Beneficio de implementar cada control
i: Dimensión desde el estándar de seguridad multidimensional.
j: Identificación del control en la dimensión.
k: Primer nivel de anidamiento para el control j-ésimo
l: Segundo nivel de anidamiento para el control jk-ésimo
B: Presupuesto disponible
Aij: Conjunto de controles anidados de primer nivel
Aijk: Conjunto de anidado de controles de segundo nivel

4. Comparación de los enfoques en una situación industrial: Prueba de concepto.

Como ya se mencionó, se utilizaron los datos de una auditoría informática realizada en una organización gubernamental chilena. En este caso, la organización debe cumplir con dos regulaciones de seguridad de la información establecidas por el Gobierno de Chile: (i) Decreto Supremo 83 (DS83) (Gobierno de Chile, 2005), una norma de seguridad para oficinas públicas; y (ii) la guía metodológica para la seguridad de la información (GUI) (Gobierno de Chile, 2011), que describe los requisitos técnicos asociados con el diagnóstico, la planificación y la implementación de un sistema de seguridad de la información. Además, la organización decidió evaluar su cumplimiento con la norma internacional ISO 27001, en su versión 2005. A los efectos de la prueba, solo presentaremos la dimensión referente a la seguridad de las instalaciones, ya que fue el principal foco de evaluación después del terremoto del año 2010 en Chile.

```
$OFFSYMXREF
$OFFSYMLIST

option limrow=0;
option limcol=0;
option solprint=on;
option sysout=off;

option LP=CPLEX;
option MIP=CPLEX;
option NLP=CONOPT;
option MINLP=DICOPT;
option OPTCR=0;

$TITLE   Ejercicio de Prueba

VARIABLES

F, ppto ;

POSITIVE VARIABLES

ppto ;

BINARY VARIABLES

X1, X2, X3, X4, X5, X6, X7, X8, X9, X10 ;
```

(a) Configuración de Variables

```
EQUATIONS

funcObj, R1, R2, R3, R4, R5, R6, R7, R8, R9, R10 ;

funcObj.. F =E= 3*X1 + 5*X2 + 3*X3 + 2*X4 + 2*X5 +
5*X6 + 6*X7 + 2*X8 + 5*X9 + 1*X10 ;

R1.. 120*X1 + 202*X2 + 150*X3 + 120*X4 + 202*X5 +
171*X6 + 230*X7 + 100*X8 + 100*X9 + 140*X10 - ppto =L= 0;

R2.. ppto =L= 900    ;
R3.. X5 - X1 =L= 0;
R4.. X5 - X2 =L= 0;
R5.. X8 - X3 =L= 0;
R6.. X9 - X4 =L= 0;
R7.. X9 - X5 =L= 0;
R8.. X9 - X6 =L= 0;
R9.. X10 - X7 =L= 0;
R10.. X10 - X8 =L= 0;


MODEL    optTotal  /ALL /   ;

SOLVE optTotal using MIP maximizing F ;
```

(b) Definición de ecuaciones

Figura 2 – Configuración del modelo en lenguaje GAMS

La tabla 3 muestra un resumen de los beneficios y costos (en miles de pesos chilenos) asociados con la implementación de cada control.

Para esta prueba de concepto, ambos modelos se ejecutaron en tres escenarios, en los que el número de controles se incrementó en una magnitud de diez en diez con un máximo de 31 controles; en el primer caso se evaluaron un total de 11 controles, en el segundo caso se evaluaron un total de 22 controles y en el tercer caso se evaluaron 31 controles.

Los beneficios asociados con cada control se establecieron considerando el estándar al que pertenecen. Se otorgó una puntuación más alta a los controles que cumplían con las reglas específicas del gobierno de Chile y aquellos que cumplían con más de una norma. Los costos de implementación de cada control se estimaron según las condiciones operativas de la organización. El presupuesto considerado para el ejemplo es $ 4.000.000 (en pesos chilenos).

La tabla 4, muestra un resumen de los resultados óptimos obtenidos con ambos modelos, destacando los costos, beneficios, controles propuestos y tiempos de procesamiento.

Como se observa, en los tres casos, los resultados, desde el punto de vista de los beneficios logrados por la implementación del conjunto de controles propuestos, son iguales, es decir, ambos modelos maximizan el beneficio.

Para el caso de 22 controles, hay una diferencia con respecto al conjunto de controles que se seleccionaron y, por lo tanto, los costos asociados con el conjunto mencionado anteriormente. Sin embargo, el beneficio es el mismo para ambos modelos.

Control	Beneficio	Costo	Dependencia	Control	Beneficio	Costo	Dependencia
C1	1	480	-	C7	1	480	-
C1-1	1	800	C1	C7-1	1	120	C7
C1-2	1	160	C1	C7-2	1	50	C7
C1-3	1	220	C1	C7-3	1	50	C7
C1-3-1	1	100	C1-3	C7-4	1	50	C7
C2	1	800	-	C7-5	1	50	C7
C2-1	1	80	C2	C8	1	200	-
C2-2	1	160	C2	C9	1	1.480	-
C2-3	1	920	C2	C9-1	1	80	C9
C2-4	1	120	C2	C9-2	1	80	C9
C2-5	1	160	C2	C9-3	1	80	C9
C3	2	290	-	C9-4	1	1.080	C9
C3-1	3	50	C3	C9-4-1	1	80	C9-4
C4	1	120	-	C9-4-2	1	800	C9-4
C5	1	320	-	C9-4-3	1	120	C9-4
C6	1	600	-				

Tabla 3 – Costos y beneficios de implementar cada control.

Modelo ASP	Modelo PL
Universo de Controles: 11 Tiempo de ejecución: 0,109 seg. Número de controles seleccionados: 11 Costo: 4.000 (Miles de pesos) Beneficio: 11	Universo de Controles: 11 Tiempo de ejecución: 0,006 seg. Número de controles seleccionados: 11 Costo: 4.000 (Miles de pesos) Beneficio: 11
C1; C1-1; C1-2; C1-3; C1-3-1; C2; C2-1; C2-2; C2-3; C2-4; C2-5.	C1; C1-1; C1-2; C1-3; C1-3-1; C2; C2-1; C2-2; C2-3; C2-4; C2-5.
Universo de Controles: 22 Tiempo de ejecución: 12,016 seg. Número de controles seleccionados: 19 Costo: 3.980 (Miles de pesos) Beneficio: 22	Universo de Controles: 22 Tiempo de ejecución: 0,01 seg. Número de controles seleccionados: 19 Costo: 3.980 (Miles de pesos) Beneficio: 22
C1; C1-1; C1-2; C1-3; C1-3-1; C2; C2-1; C2-2; C2-4; C2-5; C3; C3-1; C4; C5; C7; C7-1; C7-2; C7-3; C7-4; C7-5.	C1; C1-1; C1-2; C1-3; C1-3-1; C2; C2-1; C2-2; C2-4; C2-5; C3; C3-1; C4; C5; C6; C7-1; C7-2; C7-3; C7-4; C7-5.
Universo de Controles: 31 Tiempo de ejecución: 9.744,287 seg. Número de controles seleccionados: 24 Costo: 3.820 (Miles de pesos) Beneficio: 27	Universo de Controles: 31 Tiempo de ejecución: 0,019 seg. Número de controles seleccionados: 24 Costo: 3.820 (Miles de pesos) Beneficio: 27
C1-2; C1-3; C1-3-1; C2-1; C2-2; C2-4; C2-5; C3; C3-1; C4; C5; C6; C7; C7-1; C7-2; C7-3; C7-4; C7-5; C8; C9-1; C9-2; C9-3; C9-4-1; C9-4-3.	C1-2; C1-3; C1-3-1; C2-1; C2-2; C2-4; C2-5; C3; C3-1; C4; C5; C6; C7; C7-1; C7-2; C7-3; C7-4; C7-5; C8; C9-1; C9-2; C9-3; C9-4-1; C9-4-3.

Tabla 4 – Resultados de la ejecución de los modelos.

A partir de esta prueba de concepto, se observa que ambos modelos pueden maximizar el beneficio de acuerdo con las restricciones presupuestarias y las dependencias entre controles.

La gran diferencia se da en la velocidad de ejecución de ambos modelos. Si bien el modelo PL presenta tiempos de procesamiento muy bajos e incrementos pequeños a medida que se consideran más controles, el modelo ASP, aunque comienza con un tiempo de configuración muy bajo, aumenta su tiempo de ejecución de manera exponencial con respecto al número de controles. Esto implica que el modelo ASP se vuelve poco práctico al evaluar un gran número de controles, a pesar de su facilidad de modelado.

5. Conclusiones

Un enfoque contemporáneo para administrar la seguridad de la información en las organizaciones, es cumplir con los estándares basados en procesos, que se basan en la implementación de un conjunto de buenas prácticas denominados controles de seguridad. La primera etapa requiere una evaluación de la seguridad de la información que produzca, como resultado relevante, un conjunto de controles ya implementados y otro conjunto de controles a implementar. Tomar una decisión acerca de la próxima implementación de ISC no es una respuesta trivial, ya que implica diferentes escenarios de riesgo alternativos, restricciones presupuestarias y objetivos comerciales, lo que genera un problema de optimización combinatoria del tipo np-hard.

Para obtener una visión de las actuales soluciones, hemos llevado a cabo una búsqueda bibliográfica basada en un protocolo de revisión de mapeo sistemático, el cual ha dado como resultado 35 artículos que abordan el problema de selección de ISC. De este conjunto, solo 5 abordaron el problema desde una perspectiva cuantitativa bajo un conjunto limitado de restricciones.

Para agregar nuevas restricciones, hemos presentado dos enfoques cuantitativos: uno basado en Answer Set Programming y otro basado en la Programación lineal. Hemos utilizado un ejemplo con tres tipos de restricciones: dependencias temporales entre controles, un presupuesto limitado y diferentes beneficios de seguridad de la información dados por los diferentes controles a implementar. La solución ASP resulta simple e ilustrativa. En primer lugar, hemos demostrado que una solución cuantitativa no es difícil de modelar; en segundo lugar, se puede extender fácilmente para admitir controles adicionales (hechos) y restricciones. Sin embargo, el rendimiento de ASP fue lento, con un rendimiento aceptable hasta un espacio de búsqueda de 30 controles en máquinas secuenciales y 40 en máquinas paralelas. Por lo tanto, este tipo de solución es muy adecuado para realizar diagnósticos limitados con respecto al estándar, por ejemplo, sobre algún dominio específico, donde se desea obtener resultados rápidamente a un bajo costo de modelado.

Por otro lado, el enfoque PL resulta en una etapa de modelado más compleja, sin embargo, su rendimiento fue completamente satisfactorio. En las diferentes soluciones, incluso considerando la cantidad total de controles involucrados, el tiempo de procesamiento, incluido el tiempo de proceso web, no alcanzó 30 segundos.

Por lo tanto, hemos propuesto dos enfoques cuantitativos basados en la tecnología existente y abierta para abordar el problema de seleccionar ISC. Uno de ellos, basado en ASP, resulta adecuado para unos pocos controles que facilitan la etapa de modelado debido al alto nivel de abstracciones de su lenguaje de programación. El segundo, basado en PL, presenta un excelente rendimiento, aunque su formulación algebraica resulta un poco más complejo de especificar que ASP.

En términos de trabajo futuro, experimentaremos sobre el desempeño de enfoques más complejos, principalmente en soluciones no lineales e incluyendo el riesgo como variables estocásticas. Mantendremos el enfoque en la dualidad de la evaluación que requiere mucho tiempo considerando tanto el tiempo de modelado como el tiempo de cálculo, ya que ambos factores forman parte del esfuerzo total necesario para resolver el problema presentado.

Agradecimientos

Trabajo financiado por la Universidad de La Frontera, Proyecto DI19-0116.

Referencias

Al-Safwani, N., Hassan, S., & Katuk, N. (2014). A multiple attribute decision making for improving information security control assessment. International Journal of Computer Applications, 89(3).

Almeida, L., & Respício, A. (2018). Decision support for selecting information security controls. Journal of Decision Systems, 0125(May), 1–8. https://doi.org/10.1080/12460125.2018.1468177

Bachlechner, D., Maier, R., Innerhofer-Oberperfler, F., & Demetz, L. (2011). Understanding the management of information security controls in practice. In Proceedings of the 9th Australian Information Security Management Conference. Perth Western Australia: Edith Cowan University.

Bistarelli, S., Fioravanti, F., & Peretti, P. (2007). Using CP-nets as a guide for countermeasure selection. In Proceedings of the 2007 ACM symposium on Applied computing. https://doi.org/10.1145/1244002.1244073

Bonatti, P., Calimeri, F., Leone, N., & Ricca, F. (2010). Answer set programming. In A 25-year perspective on logic programming (pp. 159–182). Berlin: Springer.

Breier, J. (2014). Security Evaluation Model based on the Score of Security Mechanisms. Information Sciences and Technologies Bulletin of the ACM, 6(1), 19–27.

Breier, J., & Hudec, L. (2012). New approach in information system security evaluation. In IEEE First AESS European Conference on Satellite Telecommunications (ESTEL) (pp. 1–6). IEEE. https://doi.org/10.1109/estel.2012.6400145

Breier, J., & Hudec, L. (2013a). On Identifying Proper Security Mechanisms. Information and Communicatiaon Technology, 285–294.

Breier, J., & Hudec, L. (2013b). On Selecting Critical Security Controls. In International Conference on Availability, Reliability and Security (pp. 582–588).

Brewka, G., Eiter, T., & Truszczyński, M. (2011). Answer set programming at a glance. Communications of the ACM, 54(12), 92–103.

Cano, J. J. M. (2018). Repensando los fundamentos de la gestión de riesgos. Una propuesta conceptual desde la incertidumbre y la complejidad. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (E15), 76–87.

Cares, C., & Diéguez, M. (2017). An Answer Set Solution for Information Security Management. In proceedings of the Eighth International Conference on Computational Logics, Algebras, Programming, Tools, and Benchmarking (pp. 11–15).

Chen, L., Li, L., Hu, Y., & Lian, K. (2009). Information Security Solution Decision-Making Based on Entropy Weight and Gray Situation Decision. In 2009 Fifth International Conference on Information Assurance and Security (Vol. 2, pp. 7–10). IEEE. https://doi.org/10.1109/IAS.2009.9

Choo, K. K., Mubarak, S.,...& Mani, D. (2014). Selection of information security controls based on AHP and GRA. Pacific Asia Conference on Information Systems.

Cuihua, X., & Jiajun, L. (2009). An Information System Security Evaluation Model Based on AHP and GRAP. International Conference on Web Information Systems and Mining, 493–496.

Diéguez, M., Cares, C., & Sepúlveda, S. (2012). On Optimizing the Path to Information Security Compliance. In 8th International Conference on the Quality of Information and Communications Technology (QUATIC'12) (pp. 182–185).

Ejnioui, A., Otero, A., Tejay, G., Otero, C., & Qureshi, A. (2012). A Multi-attribute Evaluation of Information Security Controls in Organizations Using Grey Systems Theory. In Proceedings of the International Conference on Security and Management (p. 1).

GAMS. (2018). General Algebraic Modeling System. Retrieved from: https://www.gams.com/

Gao, C., Li, Z., & Song, H. (2009). Security Evaluation Method Based on Host Resource Availability. In Multimedia and Ubiquitous Engineering, 2009. MUE'09. Third International Conference on (pp. 499–504).

Gebser, M., Kaufmann, B., Kaminski, R., Ostrowski, M., Schaub, T., & Schneider, M. (2011). Potassco: The Potsdam answer set solving collection. Ai Communications, 24(2), 107–124.

Gobierno de Chile. (2005). Decreto 83: Norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.

Gobierno de Chile, G. U. I. (2011). Programa de mejoramiento de la gestión sistema de seguridad de la información: Versión 2011.

Hooker, J. N. (2002). Logic, optimization, and constraint programming. INFORMS Journal on Computing, 14(4), 295–321.

International Organization for Standardization. (2013). ISO 27001:2013 - Information security management. Retrieved from https://www.iso.org/standard/54534.html

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360.

Jiménez-Martín, A., Vicente, E., & Mateos, A. (2015). Selección de salvaguardas en gestión del riesgo en sistemas de la información: un enfoque borroso. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (15), 83–100. https://doi.org/10.17013/risti.15.83-100

Kawasaki, R., & Hiromatsu, T. (2014). Proposal of a model supporting decision-making on information security risk treatment. International Journal of Computer, Electrical, Automation, Control and Information Engineering, 8(4), 583–589.

Khajouei, H., Kazemi, M., & Moosavirad, S. H. (2017). Ranking information security controls by using fuzzy analytic hierarchy process. Information Systems and E-Business Management, 15(1), 1–19. https://doi.org/10.1007/s10257-016-0306-y

Kiesling, E., Ekelhart, A., Grill, B., Straub, C., & Stummer, C. (2013). Simulation-based optimization of IT security controls: Initial experiences with meta-heuristic solution procedures. In Proceedings of 14th EUME Workshop.

Kiesling, E., Strauss, C., Ekelhart, A., Grill, B., & Stummer, C. (2013). Simulation-based optimization of information security controls: An adversary-centric approach. In Proceedings of Winter Simulations Conference (WSC).

Kiesling, E., Strausss, C., & Stummer, C. (2012). A Multi-objective Decision Support Framework for Simulation-Based Security Control Selection. In Seventh International Conference on Availability, Reliability and Security, 454–462. https://doi.org/10.1109/ares.2012.70

Lv, J.-J., & Wang, Y.-Z. (2010). A ranking method for information security risk management based on ahp and promethee. In Management and Service Science (MASS), 2010 International Conference on (pp. 1–4).

Lv, J., Zhou, Y., & Wang, Y. (2011). A Multi-criteria Evaluation Method of Information Security Controls. In Fourth International Joint Conference on Computational Sciences and Optimization, 190–194.

Meng, M., & Liu, E. (2015). The Application Research of Information Security Risk Assessment Model Based on AHP Method. Journal of Advances in Information Technology, 6(4).

Nagata, K., Amagasa, M., Kigawa, Y., & Cui, D. (2009). Method to Select Effective Risk Mitigation Controls Using Fuzzy Outranking. In 2009 Ninth International Conference on Intelligent Systems Design and Applications. https://doi.org/10.1109/isda.2009.186

NEOS. (2018). NEOS Server web portal. Retrieved from https://neos-server.org/neos/

Ojamaa, A., Tyugu, E., & Kivimaa, J. (2008). Pareto-optimal situaton analysis for selection of security measures. In MILCOM 2008 - 2008 IEEE Military Communications Conference. IEEE. https://doi.org/10.1109/milcom.2008.4753520

Otero, A., Ejnioui, A., Otero, C., & Tejay, G. (2011). Evaluation of information security controls in organizations by grey relational analysis. International Journal of Dependable and Trustworthy Information Systems, 2(3), 36–54.

Otero, A., Otero, C., & Qureshi, A. (2010). A Multi-Criteria Evaluation of Information Security Controls Using Boolean Features. International Journal of Network Security & Its Applications, 2(4), 1–11. https://doi.org/10.5121/ijnsa.2010.2401

Otero, A. R. (2015). An information security control assessment methodology for organizations' financial information. International Journal of Accounting Information Systems, 18, 26–45. https://doi.org/https://doi.org/10.1016/j.accinf.2015.06.001

Otero, A., Tejay, G., Otero, D., & Ruiz-Torres, A. (2012). A fuzzy logic-based information security control assessment for organizations. In Open Systems (ICOS), 2012 IEEE Conference (pp. 1–6).

Pereira, T., & Santos, H. (2014). Challenges in Information Security Protection. In Proceedings 13th European Conference on Cyber Warfare and Security (pp. 160–166).

Petersen, K., Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. Information and Software Technology, 64, 1–18. https://doi.org/10.1016/j.infsof.2015.03.007

Rees, L. P., Deane, J. K., Rakes, T. R., & Wade, H. (2011). Decision support for Cybersecurity risk planning. Decision Support Systems, 51(3), 493–505. https://doi.org/10.1016/j.dss.2011.02.013

Saint-Germain, R. (2005). Information Security Management Best Practice Based on ISO/IEC 17799. The Information Management Journal, (July/August), 60–66.

Sarala, R., Zayaraz, G., & Vijayalakshmi, V. (2015). Optimal Selection of Security Countermeasures for Effective Information Security. In Proceedings of the International Conference on Soft Computing Systems (pp. 345–353). Springer. https://doi.org/10.1007/978-81-322-2674-1_33

Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. Decision Support Systems, 55(1), 156–164. https://doi.org/10.1016/j.dss.2013.01.001

Shahpasand, M., Shajari, M., Golpaygani, S. A. H., & Ghavamipoor, H. (2015). A comprehensive security control selection model for inter-dependent organizational assets structure. Information and Computer Security, 23(2), 218–242. https://doi.org/10.1108/ics-12-2013-0090

Tofan, D. (2011). Information Security Standards. Journal of Mobile, Embedded and Distributed Systems, 3(3), 128–135.

Tosatto, S. C., Governatori, G., & Kelsen, P. (2015). Business process regulatory compliance is hard. IEEE Transactions on Services Computing, 8(6), 958–970. https://doi.org/10.1109/TSC.2014.2341236

Viduto, V., Maple, C., Huang, W., & López-Peréz, D. (2012). A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. Decision Support Systems, 53(3), 599–610. https://doi.org/10.1016/j.dss.2012.04.001

Yameng, C., Yulong, S., Jianfeng, M., Xining, C., & Yahui, L. (2011). AHP-GRAP Based Security Evaluation Method for MILS System within CC Framework. In Seventh International Conference on Computational Intelligence and Security.

Yang, Y., Shieh, H., Leu, J., & Tzeng, G. (2009). A VIKOR-based multiple criteria decision method for improving information security risk. International Journal of Information Technology & Decision Making, 8(2), 267–287.

Yang, Y., Shieh, H., & Tzeng, G. (2013). A VIKOR technique based on DEMATEL and ANP for information security risk control assessment. Information Sciences, 232, 482–500.

Yau, H. (2014). Information Security Controls. Advances in Robotics & Automation, 3(2), e118. https://doi.org/doi:10.4172/2168-9695.1000e118

Yevseyeva, I., Basto-Fernandes, V., Emmerich, M., & Van Moorsel, A. (2015). Selecting optimal subset of security controls. Procedia Computer Science, 64, 1035–1042. https://doi.org/10.1016/j.procs.2015.08.625

Yevseyeva, I., Fernandes, V. B., Van Moorsel, A., Janicke, H., & Emmerich, M. (2016). Two-stage Security Controls Selection. Procedia Computer Science, 100, 971–978. https://doi.org/10.1016/j.procs.2016.09.261

Zhang, H., Chari, K., & Agrawal, M. (2018). Decision support for the optimal allocation of security controls. Decision Support Systems, 115, 92-104. https://doi.org/10.1016/j.dss.2018.10.001