Análisis de la Seguridad en los Sistemas de e-Gobierno mediante el Problema SAT*

Security Analysis of e-Government Systems Using SAT Problem

DOI: http://dx.doi.org/10.17981/ingecuc.12.1.2016.07

Artículo de investigación científica - Fecha de recepción: diciembre 29 de 2014 - Fecha de aceptación: 22 de septiembre de 2015

Mónica Marlene Baquerizo Anastacio
Máster Universitario en Investigación en Informática. Universidad de Guayaquil, Guayaquil (Ecuador).
monica.baquerizoa@ug.edu.ec

César Byron Guevara Maldonado
Máster Universitario en Investigación en Informática. Universidad Complutense de Madrid, Madrid (España).
cesargue@ucm.es

Para citar este artículo / To reference this paper:
M. M. Baquerizo Anastacio y C. B. Guevara Maldonado., "Análisis de la seguridad en los sistemas e-gobierno mediante el problema SAT," *INGE CUC*, vol. 12, no. 1, pp. 73-79, 2016. DOI: http://dx.doi.org/10.17981/ingecuc.12.1.2016.07

Resumen-- La propuesta de esta investigación es evaluar la seguridad en los sistemas de e-gobierno con marcos de seguridad existentes y las bases de la satisfactibilidad booleana. El modelo propuesto consta de dos partes que son: la construcción de cinco marcos de seguridad basados en normas internacionales y la construcción de un modelo de evaluación de seguridad administrativa. Esta propuesta permitirá plantear el problema de la seguridad de forma matemática y conocer si la seguridad propuesta por el administrador de e-gobierno es satisfactoria o no. El modelo ha sido implementado y alimentado con los indicadores de seguridad investigados con el fin de poner a disposición de los administradores una herramienta que facilite el proceso de análisis de los factores que son cruciales para la seguridad de sus sistemas. Con este modelo se pretende ayudar a la toma de decisiones al momento de añadir o remover factores de seguridad que han demostrado óptimos resultados en la etapa de experimentación.

Palabras claves-- E-gobierno; seguridad administrativa; satisfactibilidad booleana; marcos de seguridad; modelo de evaluación de seguridad.

Abstract-- The proposal of this research is to evaluate e-government security systems with current security frameworks and the Boolean satisfiability bases. The proposed model consists of two segments: the construction of five security frameworks based on international standards and the construction of an evaluation model for administrative security. This proposal poses the security breach problem using mathematical models in order to determine whether a security strategy proposed by the e-government administrator is successful or not. The model has been implemented and powered with the safety indicators studied in order to provide administrators a tool that facilitates the process of analyzing the factors that are crucial for their security systems. This model is intended to help the decision-making process when adding or taking out safety factors that have demonstrated optimum results in the experimental stage.

Keywords-- e-Government; Security Management; Boolean Satisfiability; Security Frameworks; Security Evaluation Model.

* Artículo de investigación científica derivado del proyecto de investigación titulado: "Seguridad en E-Gobierno". Financiado por SENESCYT Ecuador. Fecha de inicio: octubre 2012 - Fecha de finalización: febrero 2017.

I. Introducción

Con el avance de la tecnología, los gobiernos innovaron la manera de interactuar creando portales que brindan diferentes tipos de servicios a las instituciones y ciudadanos en general. Esta transformación de relaciones internas y externas del sector público a través de las tecnologías de la información que aumenta la eficiencia, la eficacia de la gestión administrativa y la participación ciudadana se la denomina *gobierno electrónico* [1].

La información que el gobierno tiene en sus repositorios es de diferente índole y proviene de toda la sociedad. Debido a que el gobierno se relaciona con todos en una nación, éste tiene información pública, privada y clasificada de cada uno de ellos.

Sin duda alguna, la evolución e innovación gradual de este tipo de sistemas está dada por muchos factores como la tecnología, la efectividad en los servicios brindados, la satisfacción del usuario, etc. A partir del hecho de que los datos están expuestos en Internet, la vulnerabilidad de éstos crece ya que pueden sufrir ataques cibernéticos. Cualquiera que fuera la tecnología usada, los sistemas de e-gobierno tienen que ser seguros debido a la sensibilidad de los datos que manipulan.

A causa de que las TIC llegan a ser estratégicas para brindar un servicio eficiente y eficaz, es esencial la administración correcta de las mismas. Enfocarse en la protección de toda la infraestructura computacional, tanto física, lógica y administrativa, es hablar de seguridad informática; sin embargo, en este trabajo sólo analizaremos la seguridad administrativa, la cual trata de suministrar, proporcionar, distribuir y velar por el cumplimiento de normas y políticas de seguridad de todas las TIC en una organización de manera integral, comprometiendo desde los altos mandos hasta el personal operativo.

La seguridad administrativa es fundamental, ya que da a conocer si las organizaciones están alineadas a normas internacionales, si cumplen con requerimientos de seguridad estándares, si se tiene una buena gestión de recursos, entre otros. Es por ese motivo que este trabajo pretende desarrollar un modelo que ayude a los administradores de sistemas de e-gobierno a analizar los factores de seguridad. Para este fin, se examinaron los marcos referenciales que identificaron factores de seguridad administrativa, y el problema de la satisfactibilidad booleana ayudó a plantear esos factores matemáticamente para conocer si la propuesta por el administrador de e-gobierno es satisfacible o no. El modelo fue implementado en el lenguaje de programación Java y la base de datos de Mysql; asimismo, tuvo pruebas experimentales.

El artículo está estructurado de la siguiente manera. En la sección II se presenta la importancia de la seguridad y los marcos de seguridad que hemos considerado en esta investigación. En la sección III se explica el problema de la satisfactibilidad booleana y su objetivo. Posteriormente, se expone nuestra propuesta, que modelará el conocimiento de las ISO (International Standard Organization) y su desarrollo utilizando SAT (Boolean satisfiability problem); y finalmente, en la sección IV se detallan las conclusiones.

II. Importancia de la Seguridad y Marcos Existentes

Estudios han demostrado que los aspectos no técnicos son tan importantes como los técnicos al momento de salvaguardar una organización, y estos aspectos no técnicos están relacionados con la administración de los recursos [2]. Es por este motivo, que la seguridad también tiene que ser administrada. La seguridad informática podría definirse como un conjunto de procedimientos, dispositivos y herramientas que reducen los posibles riesgos a los bienes en una organización [3].

En los sistemas informáticos vamos a encontrar bienes tangibles, como la infraestructura física, servidores, humanos, redes, etc., e intangibles, como la información, servicios que se prestan, aplicaciones desplegadas, conocimiento organizacional, etc. La seguridad informática debe establecer normas que minimicen los riesgos a toda la infraestructura.

La seguridad de éstos es un factor crucial, por lo que se requiere de medidas fuertemente preventivas, tanto tecnológicas como administrativas. Un punto importante de la seguridad es el de la información, la cual tiene que estar fundamentada bajo tres aspectos [4]:

A. Confidencialidad

Un sistema de e-gobierno tiene que ser confiable porque debe garantizar la protección, clasificación y seguridad de la información que alberga en sus servidores, sea ésta clasificada, pública, reservada, datos personales o institucionales. Por esta razón, el acceso a la información sólo la deben realizar los individuos que tengan autorización.

B. Integridad

La integridad se refiere a asegurar que la información que fue generada y guardada en los repositorios sea verdadera, sin ser manipulada o alterada por usuarios o procesos no autorizados.

C. Disponibilidad

La disponibilidad es la condición de la información de encontrarse a disposición de personas, procesos o aplicaciones en el momento que así lo requieran.

Marcos Existentes

Actualmente hay un sin número de marcos referentes a la administración de la seguridad. En esta investigación se consideran cinco categorías: seguridad integral, seguridad Web, computación en la nube, infraestructuras críticas, y gobierno y gestión TI. El motivo por el cual se decidió analizarlas es porque un sistema de gobierno electrónico es tan sensible que es necesario salvaguardar su infraestructura desde varias aristas.

En el caso del marco de seguridad integral, se necesita administrar la seguridad de la información, tanto en el ámbito administrativo como operacional, y tener medidas de control [5]. Al ser un sistema de e-gobierno Web, es necesario que la aplicación considere parámetros de seguridad necesarios para una plataforma en Internet.

El marco la computación en la nube lo consideramos porque actualmente es la tendencia; la mayoría de los gobiernos están optando por este nuevo modelo que permite el acceso bajo demanda [6]. Un sistema de e-gobierno es tan crucial que debe tratarse dentro de las infraestructuras críticas que tiene un país, guardando protocolos de seguridad que salvaguarden el sistema de e-gobierno.

Finalmente, estimamos la importancia de un gobierno y gestión TI, ya que debería de existir un compromiso, tanto de la parte directiva (gobierno TI) como de la parte operativa (gestión TI). El gobierno TI traza una dirección estratégica a seguir, mientras que la gestión planifica, construye, ejecuta y controla actividades alineadas con la estrategia establecida por el gobierno TI [7]. A continuación se detallan los marcos existentes en cuanto a las aristas propuestas.

Las ISO 27000, 27001, 27002 y SANS buscan salvaguardar la seguridad desde aspectos físicos hasta lógicos. En cuanto a la seguridad de las aplicaciones, tenemos las normas OWASP, ISO 27000, el marco CCN-STIC-812 de España, etc., las cuales contemplan parámetros y guías estratégicas para la seguridad de una aplicación en línea.

Las ISO 38500, 20000, COBIT, Calder Moir e ITIL son marcos y estándares que ayudan a un gobierno y gestión TI [8], [9], [10] y [11]. El marco de gobierno y gestión TI es estratégico debido a que si el estado decidiera implementar un gobierno TI, la organización, planificación y ejecución de proyectos se realizaría de una manera más eficiente beneficiando así a toda una nación.

En cuanto a la computación en la nube, las ISO 27000, CCN-STIC-823 y SANS, entre otras, son guías de seguridad para un sistema de computación en la nube.

Otro marco considerado es el de infraestructuras críticas. Así como se disfruta de los beneficios del avance de las TIC, también debemos considerar que éstas pueden ser utilizadas con fines maliciosos por terroristas. Éstos podrían tener fines personales, económicos, religiosos, o de cualquier otra índole. Debido a los ciberataques, los países empiezan con la identificación, priorización y protección de las infraestructuras críticas [12]. La Comisión Europea define como infraestructura crítica a aquellas instalaciones, redes, servicios, equipos físicos y tecnologías de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos [12]. Como guías para esta sección, se han considerado la Estrategia de Seguridad Nacional y la Ley 8/2011 del gobierno español y la Strategic Plan Fiscal Years 2012-2016 del gobierno de los Estados Unidos.

Los sistemas de e-gobierno, al manipular datos privados de ciudadanos e instituciones de un país, se convierten en una infraestructura crítica, debido a la sensibilidad de estos datos que se albergan en los servidores gubernamentales. Un sistema de gobierno electrónico debe tener la capacidad de estar preparado para adaptarse a cambios inesperados en su plataforma y para recuperarse rápidamente de interrupciones que pudiera tener el servicio ante ataques, accidentes naturales o antrópicos, e incidentes o amenazas virtuales o físicas, y así poder garantizar el servicio a la comunidad [13]. Es por este motivo que es fundamental que la infraestructura lógica y física de los sistemas de gobierno electrónico se considere dentro del plan estratégico de protección de infraestructuras críticas de un país.

III. El Problema de la Satisfactibilidad

El problema de satisfactibilidad booleana (SAT) tiene como objetivo evaluar toda una fórmula constituida por conectores lógicos que puede ser verdadera, dando a sus variables booleanas valores de verdadero o falso [14]. Procedimientos como SAT27 pueden comprobar fórmulas con cientos de miles de variables debido a las innovaciones de los algoritmos básicos, la estructura de datos y el uso de los modernos microprocesadores. El progreso de los *SMT solvers*, ha permitido que se utilicen para demostrar teoremas, análisis de programas en desarrollo, estáticos y en ejecución, y planeación y programación de trabajos en el microprocesador [15] y [16].

Mediante el planteamiento del problema del SAT, podemos conocer si los factores de seguridad sugeridos por el administrador para la plataforma e-gobierno son válidos. De ser así, la propuesta satisface la seguridad, caso contrario, se tendría que revisar los factores que no permiten tener una seguridad adecuada. A continuación, el planteamiento del SAT.

A. Planteamiento del problema SAT

Lógica proposicional y definiciones

La lógica proposicional es una formalización matemática que estudia las proposiciones (Fig. 1), sus valores de verdad y su nivel absoluto de verdad a partir de los operadores lógicos.

Los operadores lógicos son: disyunción (∨), conjunción (∧), negación (¬), entre otros. Para resolver problemas SAT se utilizan los tres operadores lógicos mencionados.

Los valores de verdad pueden ser: verdadero o falso {0,1}, pero nunca una variable puede tomar los dos valores a la vez. Hay diferentes asignaciones que pueden ser definidas sobre el conjunto de variables proposicionales.

Las variables proposicionales (VP) son el conjunto de variables proposicionales X = {X1, X2, X3….. Xn}. Éstas pueden tomar el valor de verdadero y falso, en caso de que esté precedida por el símbolo de negación.

Literal: es una variable proposicional o la negación de la misma.

Cláusula: es una disyunción de literales (∨). Una cláusula puede ser unitaria, es decir, que contiene un solo literal.

Fórmula: está dada por la conjunción de las cláusulas.

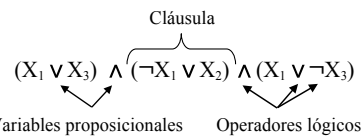

Fig. 1. Fórmula que representa un problema SAT.
Fuente:[17].

Mediante el problema de la satisfactibilidad, podemos analizar factores de seguridad (variables proposicionales) y conocer si estos factores hacen que la seguridad sea satisfacible en el planteamiento propuesto.

IV. Propuesta

Actualmente existen marcos de seguridad, estándares internacionales, marcos referenciales, guías de seguridad, entre otros, que permiten la administración de la seguridad. Cada uno gira en torno a enfoques diferentes pero con un mismo fin: preservar la seguridad integral, física y lógica institucional.

La propuesta aquí planteada consiste en utilizar el problema de la satisfactibilidad booleana para modelar el conocimiento de los estándares internacionales, marcos referenciales, guías de seguridad y conocer si los requerimientos propuestos por los administradores cumplen con requerimientos de seguridad basados en normas internacionales.

La propuesta está dividida en dos partes:

a. La construcción de los marcos de seguridad basados en normas internacionales.
b. La implementación de un modelo basado en indicadores de seguridad mediante el problema de satisfactibilidad booleana.

A. Construcción de los marcos de seguridad

Un marco es un conjunto de buenas prácticas para la gestión en alguna área específica [5]. Basados en este concepto decidimos realizar cinco marcos de seguridad estratégicos (Fig. 2) en las siguientes áreas:

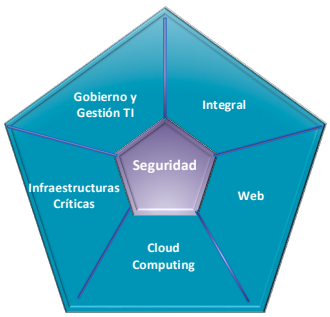

Fig. 2. Marcos que se han analizado.
Fuente:[17].

Basados en la recopilación de estándares, guías, leyes, marcos internacionales, de países líderes en administración de TIC, en este trabajo se generaron marcos de seguridad propios.

Los marcos generados se han dividido en secciones (Fig. 3). En el caso de marco de gobierno y gestión TI hay tres grandes aristas: marco administrativo, operacional y medidas de protección. Para cada una de ellas, se recopilaron diferentes indicadores relevantes de los estándares y marcos existentes como: ISO 27000, 27001, 27002, Guía de seguridad (CCN-STIC-804), SANS, e-Government: Strategy Framework Policy and Guidelines. A continuación se presenta un diagrama con sus secciones principales:

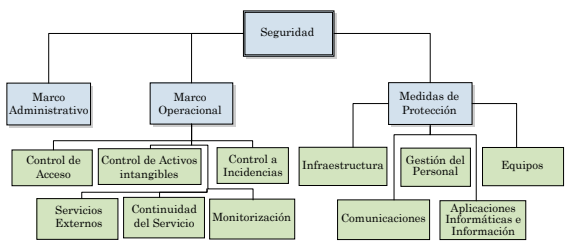

Fig. 3. Diagrama del marco de seguridad integral.
Fuente: [17].

Al ser el sistema de e-gobierno una aplicación web, es necesario construir este marco de seguridad. Para su construcción nos basamos en la Guía de seguridad de las TIC (CCN-STIC-812), ISO 27000,

27001, SANS y guías OWASP. A continuación, en la Fig. 4 se muestran las secciones principales de este marco:

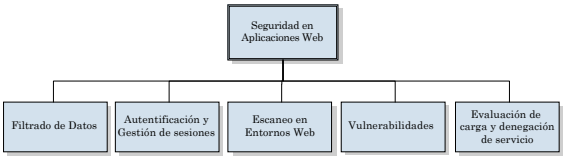

Fig. 4. Diagrama del marco de seguridad para aplicaciones Web.
Fuente: [17].

Si un gobierno decide tener una plataforma en la nube, es imperante cumplir con ciertos elementos de seguridad. Es por este motivo que también construimos un marco con base en las ISO 27001, 27002, Guía/Norma de seguridad de las TIC (CCN-STIC-823) y SANS. Las secciones de este marco se muestran en la Fig. 5:

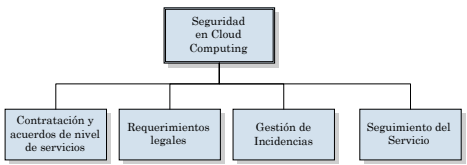

Fig. 5. Diagrama del marco de seguridad para la computación en la nube.
Fuente:[17].

Los sistemas de e-gobierno tienen información delicada, por ese motivo se clasifica como una infraestructura crítica y se consideró importante realizar un marco en esta categoría (Fig. 6). Este marco fue construido con base en la Estrategia de Seguridad Nacional, la Ley 8/2011 del 28 de abril del Gobierno de España y la Department of Homeland Security Strategic Plan Fiscal Years 2012-2016 del Gobierno de Estados Unidos.

Fig. 6. Diagrama del marco de seguridad para infraestructuras críticas.
Fuente:[17].

Todas estas tecnologías deben tener un responsable que lidere la administración de los recursos informáticos a nivel nacional. Es por esto que también se consideró realizar un marco para la administración de las TIC (Fig. 7). Este marco tiene dos partes, el Gobierno TI y la Gestión TI. El gobierno TI se establece a nivel de directiva, mientras que el de gestión se da en los medios mandos hasta el operacional. Este marco se basó en la ISO 38500 para Gobierno TI, ISO 20000 para Gestión TI y los marcos COBIT 5 y Calder Moir para el marco en general.

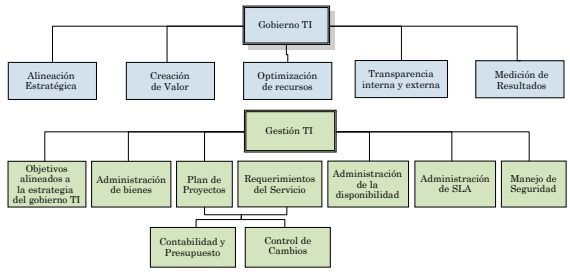

Fig. 7. Diagrama del marco de gobierno y gestión TI.
Fuente: [17].

B. Implementación de un modelo de seguridad mediante el problema de satisfactibilidad booleana.

En la construcción de cada marco de seguridad se recolectaron los indicadores y se agruparon por secciones según su afinidad. Cada sección tiene indicadores que se tienen que cumplir para asegurar la seguridad en esa sección. Hay que considerar que un indicador puede estar relacionado con otro indicador de una sección diferente.

Producto de la construcción de los marcos de seguridad, tenemos un sin número de indicadores, que básicamente constituyen el conocimiento extraído de las diferentes normas. Todos estos indicadores se almacenaron en una base de datos y se analizaron para la construcción de las cláusulas. Por ejemplo, en el marco de seguridad integral tenemos entre los indicadores:

1. Existencia de una Dirección general.
2. Tener procedimientos, normas, protocolos de seguridad.

De estos requerimientos que son indispensables para el marco de seguridad se puede inferir la siguiente cláusula:

Si existe una Dirección general entonces todos los procedimientos, normas y protocolos de seguridad deben de estar aprobados y firmados por el Comité o Dirección general.

El indicador de "existencia de una Dirección general" es la variable 1 y el indicador "todos los procedimientos, normas, protocolos de seguridad deben estar aprobados y firmados por el Comité o Dirección general" es la variable número 2. En lenguaje natural podemos crear la cláusula1 $\rightarrow$ 2, pero el problema de satisfactibilidad necesita una fórmula en lenguaje proposicional. En lógica proposicional básica sabemos que $p \rightarrow q = -p \vee q$, por consecuencia la fórmula $1 \rightarrow 2$ es equivalente a $-1 \vee 2$ (Fig. 8).

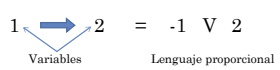

Fig. 8. Lenguaje proposicional.
Fuente: [17].

Una variable de una sección puede estar relacionada con cualquier otra de secciones diferentes, por ejemplo:

Si todos los procedimientos, normas y protocolos de seguridad están aprobados y firmados por el Comité o Dirección general entonces la normativa de seguridad debió ser revisada por el departamento de asesoría legal (Fig. 9).

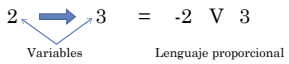

Fig. 9. Lenguaje proposicional.
Fuente:[17].

La variable 2 está en una sección diferente de la variable 3. Una cláusula puede estar formada por una o muchas variables. De esta forma se empiezan a formar cláusulas con cada indicador que está en cada marco de seguridad. Todo este conocimiento se almacena en una base de datos y se proporciona a cada indicador un identificador único. Todo este conocimiento fue expresado en lógica proposicional y almacenado en una base de datos.

Plataforma tecnológica

Con los indicadores de seguridad recolectados a lo largo de esta investigación y con la ayuda de los beneficios de SAT, se realizó un sistema que evalúe la propuesta de seguridad del administrador de sistemas de e-gobierno para conocer si ésta es viable, es decir, si la seguridad es satisfacible según el conocimiento modelado basado en estándares internacionales.

El sistema se implementó en lenguaje Java y se ha usado la librería *Sat4j: SAT tooltit in Java*, que implementa *solvers* para la solución de problemas SAT [16].

La implementación de este sistema tiene como fin conocer qué variables de seguridad impactan según la elección de los administradores, ya sea que ellos elijan las variables porque así está implementado en la institución, o que quizás se quieran implementar tan sólo ciertos aspectos y el administrador no sabe cuál elegir.

Ejecución de la aplicación

Para ejemplificar se puede suponer que un administrador quiere implementar soluciones de seguridad según las limitaciones del presupuesto asignado. Elige las variables que él considere pertinente y manda a analizar al sistema. En caso de que los indicadores den como resultado una respuesta satisfacible, él podrá observar las variables que impactan en su decisión, y en caso de que no sea así dará como resultado que, según los indicadores elegidos, no satisfacen la fórmula. El fin es ayudar al administrador a conocer qué variables influyen en su decisión y hacen que el sistema sea satisfacible.

En el sistema se presentan las cinco opciones de marcos referenciales de seguridad investigados: seguridad, computación en la nube, gobierno y gestión TI, aplicaciones Web e infraestructuras críticas. Entonces, el usuario tiene que elegir qué tipo de evaluación va a realizar (Fig. 10).

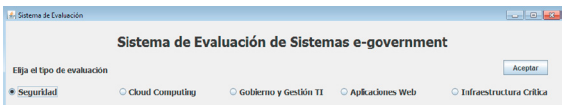

Fig. 10. Elección del marco a evaluar.
Fuente: [17].

Una vez que se ha elegido el marco a evaluar aparecen las secciones pertenecientes a ese marco para que el administrador elija las secciones que considere importantes, como se muestra en la Fig. 11:

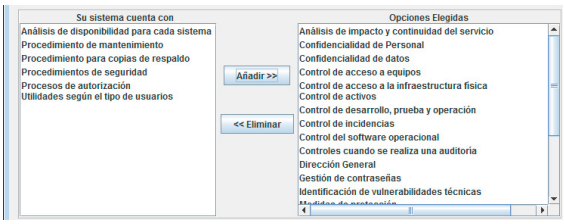

Fig. 11. Secciones del marco elegido.
Fuente: [17].

Una vez que el usuario ha elegido las secciones que propone para su sistema de e-gobierno, lo manda a evaluar. Las acciones que lleva a cabo la aplicación internamente son: primero, con todas las variables, generar una fórmula que son los indicadores recolectados, y segundo, mediante el SAT, conocer si la seguridad es satisfacible con la propuesta del administrador.

La fórmula es generada de la siguiente manera: cada sección escogida por el administrador tiene muchos indicadores. Éstos son obtenidos de la base de datos y debido a que el administrador los escogió, son positivos. A éstos se los va guardando en un archivo de texto en formato CNF (Fig. 12).

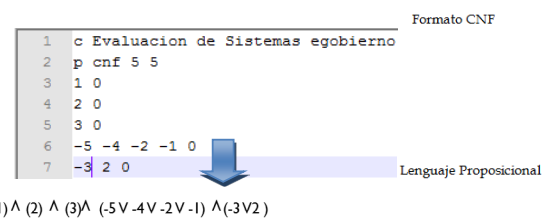

Fig. 12. Formato de archivo CNF y su equivalente en lenguaje proposicional.
Fuente: [17].

Los indicadores que escogió el administrador suelen estar relacionadas con otros indicadores de otras secciones. El sistema busca estas relaciones, que básicamente son el conocimiento basado en las

normas internacionales. Proposicionalmente, son las cláusulas que se construyeron en la primera parte y son añadidas al archivo CNF. Las cláusulas que son importantes y que no las escogió el administrador, están con signo negativo. El formato CNF nos dice que cada cláusula tiene que terminar en 0.

Una vez que ya está el archivo listo, se crea un objeto de tipo *solver* en lenguaje Java, mandando a resolver nuestra fórmula con un *solver* de la librería SAT4j.

ISolversolver = SolverFactory.newDefault();

El *solver* va a buscar si según la fórmula dada el problema tiene solución, es decir, que a las variables proposicionales se les van a dar valores de verdad (cero o uno), y evaluar la fórmula para conocer si la conjunción de todas las cláusulas es igual a 1. Si la fórmula tiene solución, el *solver* nos entrega un arreglo con las variables y su valor, positivas o negativas. Las variables positivas son aquellas que aportan fundamentalmente al modelo propuesto por el administrador. A continuación, en la Fig. 13 se observa una salida por pantalla indicando que el problema ha sido satisfacible y las variables que hacen posible que la fórmula sea verdadera.

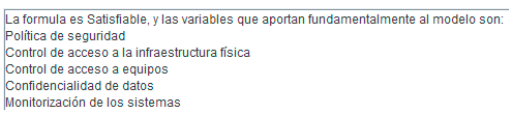

Fig. 13. Resultado de la ejecución del sistema.
Fuente: [17].

Por el contrario, si el *solver* nos da como resultado *insatisfacible*, es porque el planteamiento de seguridad propuesto por el administrador no es viable.

V. Conclusiones

En este artículo se propuso un modelo para evaluar la seguridad en sistemas de e-gobierno basada en normas, guías y estándares internacionales mediante el problema de la satisfactibilidad booleana.

Se construyeron cinco marcos de evaluación de seguridad: seguridad integral, computación en la nube, infraestructuras críticas, aplicaciones Web, y gobierno y gestión TI. Los marcos de evaluación son integrales y están divididos por secciones para fácil comprensión. Los marcos son producto de la investigación de estándares de países líderes en TIC, ISOS y marcos referenciales actuales punteros en el mercado.

Con base en los marcos construidos, se implementó un modelo de evaluación de seguridad utilizando SAT. Así, a partir de los indicadores propuestos por el administrador, se construye una proposición de seguridad utilizando SAT que permite conocer si es válida la propuesta. Al utilizar esta aplicación, los administradores tienen conocimiento de qué indicadores aportan a la seguridad de sus sistemas.

La aplicación ayuda a la toma de decisiones de implementación de normas administrativas de seguridad. Permite plantear problemas de planificación cuyas soluciones pueden aplicarse a problemas concretos basados en factores influyentes como presupuesto, tiempo y recursos, entre otros.

Referencias

[1] C. H. Baum, A. Di Maio y F. Caldwell, "What is e-Government? Gartner's definitions." Research Note (TU-11-6474), 2000.

[2] G. Dhillon y G. Torkzadeh, "Value-focuse dassessment of information system security in organizations," Inf. Syst. J., vol. 16, no. 3, pp. 293–314, Jul. 2006. DOI: 10.1111/j.1365-2575.2006.00219.x

[3] A. García Cervigon Hurtado y M. P. Alegre Ramos, *Seguridad Informática.*, 1st ed. España: Paraninfo, 2011.

[4] W. Al-Ahmad y R. Al-Kaabi, "An extended security framework for e-government," in 2008 IEEE International Conference on Intelligence and Security Informatics, 2008, pp. 294–295. DOI: 10.1109/ISI.2008.4565091

[5] International Organization for Standardization, "ISO 27000." [En línea]. Disponible en: http://www.27000.org/.

[6] P. Mell y T. Grance, *The NIST Definition of Cloud Computing*. Estados Unidos: National Institute of Standards and Technology, 2011.

[7] S. Paquette, P. T. Jaeger y S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," Gov. Inf. Q., vol. 27, no. 3, pp. 245–253, Jul. 2010. DOI: 10.1016/j.giq.2010.01.002.

[8] International Organization for Standardization, "ISO 38500." [En línea]. Disponible en: http://www.38500.org/

[9] International Organization for Standardization, "ISO/IEC 20000," 2011. [En línea]. Disponible en: http://www.iso.org/iso/catalogue_detail?csnumber=51986.

[10] "IT Governance - Governance, Risk Management and Compliance for Information Technology." [En línea]. Disponible en: http://www.itgovernance.co.uk/.

[11] "Best Practice in IT Service Management, Project Management & Cyber." [En línea]. Disponible en: https://www.axelos.com/.

[12] Unión Europea, "Council Directive 2008/114/EC," Off. J. Eur. Union, pp. 75–82, 2008.

[13] "Homeland Security." [En línea]. Disponible en: http://www.dhs.gov/.

[14] H. Mangassarian, A. Veneris y F. N. Najm, "Maximum Circuit Activity Estimation Using Pseudo-Boolean Satisfiability," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. 31, no. 2, pp. 271–284, Feb. 2012. DOI: 10.1109/TCAD.2011.2169259

[15] L. De Moura y N. Bjørner, "Satisfiability module theories," *Commun. ACM*, vol. 54, no. 9, p. 69, Sep. 2011. DOI: 10.1145/1995376.1995394

[16] "The Boolean Satisfaction and Optimization Library in Java." [En línea]. Disponible en: http://www.sat4j.org/.

[17] M. M. Baquerizo Anastacio, "Modelo de Seguridad para Sistemas e-gobierno mediante satisfactibilidad booleana," [Tesis de maestría], Dept. Arq. Comp. And Autom., Univ. Complutense de Madrid, Madrid, España, 2014.