Original Research / Articulo original - Tipo 1

Support tool for verifying the compliance of standards and regulations in implementations of strategies for information security

Felipe Reyes López, MSc. / felipe.reyes1@correo.icesi.edu.co

Yaneth Betancurt Domínguez, MSc. / janbetan@gmail.com

Ingrid Lucia Muñoz Periñán, MSc. / ingridmunoz@domuz.co

Andrés Felipe Paz Loboguerrero, MSc. / afpaz@icesi.edu.co

Universidad Icesi. Cali, Colombia.

ABSTRACT Organizations are increasingly concerned about ensuring the security of their information. In addition, government regulations and the market itself are demanding compliance with appropriate levels to remain in operation. This article presents a support tool to the process of gap analysis on the current state of the company and the specifications of the most recognized referents in the Colombian scope in the subject of information security. The tool allows for the evaluation of an organization's level of compliance with regard to the ISO 27001 and ISO 27002 standards in their 2013 versions and Notices 038 and 042 of the financial regulatory authority of Colombia (Superintendencia Financiera de Colombia). The tool conceives a data model that incorporates the results of a comparative analysis between the ISO 27001:2013 and ISO 27002:2013 standards and the Notices 038 and 042, and allows the inclusion of new referents and relates them to the existing ones. Several evaluation scenarios were created to validate the functional completeness and precision of the implemented prototype.

KEYWORDS Information security, ISO 27001, ISO 27002, Notice 038, Notice 042, gap analysis.

Herramienta de soporte para verificar el cumplimiento de estándares y regulaciones en implementaciones de estrategias de seguridad de la información

RESUMEN La preocupación de las organizaciones por asegurar su información crece cada dís. Tanto las regulaciones gubernamentales, como el mercado les exigen cumplir con niveles apropiados en ello, para seguir operando. En este artículo se presenta una herramienta de soporte al proceso de análisis de brecha respecto del estado de la compañía y de las disposiciones de los referentes más reconocidos en el ámbito colombiano en materia de seguridad de la información. La herramienta permite evaluar el nivel de cumplimiento con respecto a los estándares ISO 27001, ISO 27002 en sus versiones 2013 y las Circulares 038 y 042 de la Superintendencia Financiera de Colombia. En la herramienta se concibe un modelo de datos que recoge los resultados de un análisis comparativo entre los estándares y las circulares mencionadas, capaz de soportar la inclusión de nuevos referentes y relacionarlos con los ya incluidos. Para validar la completitud y correctitud del funcionamiento del prototipo implementado se crearon varios escenarios de evaluación.

PALABRAS CLAVE Seguridad de la información; ISO 27001; ISO 27002; Circular 038; Circular 042; análisis de brecha.

Ferramenta de suporte para verificar a conformidade com as normas e regulamentos na implementação de estratégias de segurança da informação

RESUMO As organizações estão preocupando-se cada vez mais, para garantir a segurança de suas informações; os regulamentos governamentais e o mercado estão exigindo-lhes o cumprimento de níveis adequados, para continuar operando. Neste artigo, apresenta-se uma ferramenta de apoio para o processo de análise de lacunas sobre o estado atual da empresa e das disposições das referências mais reconhecidas no âmbito colombiano sobre a segurança da informação. A ferramenta permite avaliar o grau de cumprimento de uma organização com relação às normas ISO 27001, ISO 27002 nas versões 2013 e circulares 038 e 042 da Superintendência Financeira da Colômbia. Na ferramenta é concebido um modelo de dados que recolhe os resultados de uma análise comparativa das normas e circulares mencionadas, capaz de suportar a inclusão de novos padrões e relacioná-los com os já incluídos. Para validar a integralidade e exatidão da operação do protótipo implementado, foram criados vários cenários de avaliação.

PALAVRAS-CHAVE Segurança da informação; ISO 27001; ISO 27002; Circular 038; Circular 042; análise de lacunas.

Received / Recepción: Febrero 1, 2015 - Accepted / Aceptación: Marzo 23, 2015 *doi:10.18046/syt.v13i32.2032*

I. Introduction

In the current globalized world, organizations increasingly rely on information and its related systems, which in turn, are a source of great risk. This situation has increased the importance of performing risk management within organizations. However, organizations have failed to keep pace with the speed and complexity of change, expedited by rapid technological advances and the increasing competition among organizations for an increasingly demanding market (Ernst & Young, 2012). This lack of dynamism of organizations to keep pace with the new requirements and challenges means that these efforts are insufficient, despite ongoing efforts to implement measures for information assurance, and in all kinds of organizations security incidents which have seriously affected both entities and individuals continue to happen.

All these factors cause organizations concern and force them to ensure the security of their information. To perform measurements of the current state of their safety and, from there on, implement measures to ensure that the information is at acceptable risk levels is the next step. This type of analysis is performed by identifying the current state of the organization in terms of the implementation of established controls or requirements in applicable referents, such as the ISO 27000 family or notices issued by control institutions. Once the current state has been recognized, action plans and strategies to help minimize the gap are determined.

The task of conducting these gap analyses is onerous but important; however, it is usually done manually or using expensive tools that are not easily adaptable to different local regulations. Thus, it has been identified that tools are required to analyze the gaps in organizations, not only in regard to the minimal control on international referents applicable to each organization, such as the ISO 27000 standards family, but also with requirements established by different norms and local regulations. In this way, organizations are able to obtain a consolidated report on the existing gaps to implement controls and policies consistent with the needs of the organization.

This article presents a tool to support this gap analysis process regarding the current state of the company and the provisions of the most recognized Colombian referents concerning information security. This tool makes it possible to assess the level of compliance of an organi-

I. Introducción

En el mundo globalizado actual las organizaciones confían cada vez más en la información y sus sistemas relacionados, los que a su vez, son una fuente de mucho riesgo. Esta situación ha incrementado la importancia de realizar gestión de los riesgos dentro de las organizaciones. Sin embargo, las organizaciones no han podido seguirle el paso a la velocidad y la complejidad del cambio, acelerado por el rápido avance tecnológico y la creciente competencia entre las organizaciones por un mercado cada vez más exigente (Ernst & Young, 2012). Esta falta de dinamismo de las organizaciones para seguirle el ritmo de las nuevas exigencias y retos que se plantean ha hecho que, a pesar de los continuos esfuerzos por implementar medidas para el aseguramiento de la información, estos sean insuficientes y se sigan presentando incidentes de seguridad en organizaciones de todo tipo que han afectado gravemente, tanto a las entidades, como a las personas.

Todos estos factores llevan a que las organizaciones se preocupen –y se vean obligadas–, cada vez más, por cuidar la seguridad de su información. Realizar mediciones del estado actual de su seguridad y, a partir de allí, implementar medidas para asegurar la información a niveles de riesgo aceptables, es el procedimiento que se sigue. Este tipo de análisis se realiza mediante la identificación del estado actual de la organización frente a la implementación de controles o requisitos establecidos en referentes aplicables, tales como los estándares de la familia ISO 27000 y las circulares emitidas por entes de control. Una vez ha sido reconocido el estado actual, se determinan planes de acción y estrategias que lleven a minimizar la brecha existente.

La labor de realizar estos análisis de brecha es dispendiosa pero importante, se suele hacer de manera manual o empleando costosas herramientas que no son fácilmente adaptables a las diferentes regulaciones locales, por lo que se ha identificado que se requiere de herramientas que permitan analizar la brecha de las organizaciones, no solo con respecto de los controles mínimos de referentes internacionales aplicables a cada organización, como por ejemplo los estándares de la familia ISO 27000, sino también con requisitos establecidos por diferentes normativas y regulaciones locales. De esta forma se les permite a las organizaciones obtener un reporte consolidado, global, de las brechas existentes, útil para implementar controles y políticas acordes con las necesidades de la organización.

En este artículo se presenta una herramienta de soporte a este proceso de análisis de brecha respecto del estado actual de la compañía y respecto de las disposiciones de los referentes más reconocidos en el ámbito colombiano en materia de seguridad de la información. La herramienta permite evaluar el nivel de cumplimiento de una organización con respecto de los estándares ISO 27001 e ISO 27002, en sus versiones 2013, y de las circulares 038 y 042 de la Superintendencia Financiera de Colombia [SFC]. En la herramienta se concibe un modelo de datos que reco-

ge los resultados de un análisis comparativo entre dichos estándares y las circulares citadas, capaz de soportar la inclusión de nuevos referentes y relacionarlos con los ya incluidos. Para validar la completitud y correctitud del funcionamiento del prototipo implementado se crearon varios escenarios de evaluación.

El resto de este artículo se organiza de la siguiente manera. La sección 2 muestra el contexto global y colombiano en materia de seguridad de la información; en la sección 3 se describen los trabajos relacionados; en la sección 4 se describe el análisis realizado sobre la familia de estándares ISO 27000 y las circulares 038 y 042; la sección 5 presenta los detalles de la herramienta propuesta; la sección 6 ofrece una validación de la completitud y correctitud del funcionamiento del prototipo implementado, a través de varios escenarios de evaluación; y en la sección 7 se exponen las conclusiones del presente trabajo y se referencian algunas tareas para el futuro.

II. Contexto

El objetivo primordial de la seguridad de la información es proteger la información y los activos de las organizaciones, y proveer confidencialidad, integridad y disponibilidad de sus activos de información (Wheeler, 2011). Una estrategia efectiva para mitigar los riesgos en estos activos es la evaluación, el control y el análisis del estado de la seguridad de la información. Muchas organizaciones han visto esto como una prioridad y están optando por este tipo de evaluaciones para mitigar sus riesgos potenciales (Feng & Li, 2011).

El estándar ISO 27001 (ISO/IEC, 2013a) es la norma principal de la familia ISO 27000 y contiene los requisitos del sistema de gestión de seguridad de la información [SGSI]. Es sobre esta norma que se certifican, por auditores externos, los SGSI de las organizaciones. En su Anexo A, este estándar enumera, en forma de resumen, los objetivos de control y los controles que desarrolla el estándar ISO 27002 (ISO/IEC, 2013b), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI. A pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Esta norma es conveniente para varios tipos de uso empresarial: para asegurar el cumplimiento legal; como herramienta para uso de auditores internos y externos en la determinación del grado de cumplimiento con las políticas, directivas y normas adoptadas por una empresa; y en la identificación y clarificación de los procesos existentes en la gestión de la seguridad de la información (Álvarez & García, 2007). El estándar ISO 27002 es una guía de buenas prácticas que describe los objetivos de control y los controles recomendables, en cuanto a seguridad de la información. No es certificable. Contiene 35 objetivos de control y 114 controles, agrupados en 14 dominios.

zation with respect to versions 2013 of the ISO 27001, ISO 27002 standards and Notices 038 and 042 of the Superintendencia Financiera de Colombia. The tool conceives a data model that reflects the results of a comparative analysis between the ISO 27001:2013 and ISO 27002:2013 standards and Notices 038 and 042, and is capable of supporting the inclusion of new standards and relating them with those already included. To validate the completeness and correctness of operation of the implemented prototype, evaluation scenarios were created.

The rest of this article is organized as follows. Section 2 shows the overall Colombian context regarding information security. Section 3 describes related works. In Section 4 the analysis performed concerning the ISO 27000 standards family and Notices 038 and 042 is described. Section 5 presents the details of the proposed tool. Section 6 provides a validation of the completeness and correctness of operation of the prototype implemented through various evaluation stages. And finally, in Section 7 the conclusions of this study are discussed and some future works are referenced.

II. Context

The primary objective of information security is to protect the information and assets of organizations, in addition to providing confidentiality, integrity and availability of their information assets (Wheeler, 2011). An effective strategy to mitigate risks in these information assets is the evaluation, control and analysis of the state of information security. Many organizations have seen this as a priority and are opting for this type of assessment to mitigate potential risks (Feng & Li, 2011).

The ISO 27001 (ISO/IEC, 2013) standard is the main rule of the ISO 27000 family and contains the requirements of the information security management system (ISMS). It is based upon this rule that ISMSs of organizations are certified by external auditors. Its Annex A enumerates in the form of a summary the control objectives and controls that develop the ISO 27002 standard, so that they can be chosen by the organizations in the development of their ISMSs. Although the implementation of all the controls listed in Annex is not mandatory, the organization must firmly argue the inapplicability of any non-implemented controls. This norm is suitable for several different types of business use, such as (Álvarez & García, 2007): ensuring legal compliance;

as a tool for internal and external auditors to determine the compliance of policy, directives and norms adopted by a company; and for identification and clarification of existing processes in the management of information security. The ISO 27002 standard is a good practice guide that describes the control objectives and recommended controls in terms of information security. It is not certifiable. It contains 35 control objectives and 114 controls, grouped into 14 domains.

Notice 038 of the *Superintendencia Financiera de Colombia* (SFC) allows the government entity to track the evolution of the Internal Control System (ICS) of the entities subjected to inspection and surveillance. It starts with the application for certification regarding the structuring and implementation of the fundamental components of the system elements. The ICS constitutes the foundations and essential and basic conditions that guarantee its effectiveness according to the nature of the authorized operations, functions and characteristics, and is applied to each of the aspects listed below; in consequence, entities should include these principles, document them with pertinent supports and keep them available to the SFC. Within special areas of internal control listed in this notice, the Internal Control Norms for the Management of Technology are the area of interest for this work.

Notice 042 corresponds to the minimum requirements of safety and quality for performing operations, which must be adopted by entities subject to inspection and monitoring of the SFC. These requirements are grouped into the following categories: general obligations; additional obligations per channel type; rules for software updating; specific obligations for debit and credit cards, and v) analysis of vulnerabilities. From the general obligations, the items of interest to us are 3.1 *Security and Quality* and 3.4 *Information Disclosure*. From the additional obligations per channel type item 4.9 *Internet* is of interest. From the rules about software updating item 5.1 A*dequate control over the software* is of interest, and from the analysis of software vulnerabilities, item 7.1 *Analysis of IT vulnerabilities*.

III. Related works

In the Colombian context, nowadays, the organizations that need assessments for gap analysis and to verify compliance with references such as the ISO 27000 standards family and notices issued by the control institutions, do not have the appropriate tools to facilitate this task

La Circular 038 de la SFC le permite a esta entidad gubernamental realizar el seguimiento a la evolución del Sistema de Control Interno [SCI] de las entidades sometidas a inspección y vigilancia; inicia con la solicitud de certificación respecto de la estructuración y aplicación de los componentes fundamentales de los elementos del sistema. El SCI está constituido por los fundamentos y las condiciones imprescindibles y básicas que garantizan su efectividad, de acuerdo con la naturaleza de las operaciones autorizadas y las funciones y características propias; se aplican para cada uno de los aspectos enumerados a continuación, por lo que las entidades deben incluir estos principios, documentarlos –con los soportes pertinentes– y tenerlos a disposición de la SFC. Dentro de las áreas especiales de control interno enumeradas en esta circular, el apartado referido a las normas de control interno para la gestión de tecnología, es el área de interés para este trabajo.

La Circular 042 corresponde a los requisitos mínimos de seguridad y calidad para la realización de operaciones, los cuales deben ser adoptados por las entidades sometidas a la inspección y vigilancia de la SFC. Estos requisitos se agrupan en las siguientes categorías: obligaciones generales; obligaciones adicionales por tipo de canal; reglas sobre actualización de software; obligaciones específicas para tarjetas débito y crédito; y análisis de vulnerabilidades. Son de interés, para efectos de esta investigación: de las obligaciones generales, los ítems 3.1 –Seguridad y calidad–, y 3.4 –Divulgación de información–; de las obligaciones adicionales por tipo de canal, el ítem 4.9 –Internet–; de las reglas sobre actualización de software, el ítem 5.1 –Adecuado control sobre el software–; y del análisis de vulnerabilidades informáticas, el ítem 7.1 –Análisis de vulnerabilidades informáticas–.

III. Trabajos relacionados

En el contexto colombiano, actualmente las organizaciones que necesitan realizar evaluaciones para obtener análisis de brechas y verificar el cumplimiento de referentes –como los estándares de la familia ISO 27000 y las circulares emitidas por los entes de control– no cuentan con las herramientas idóneas que les faciliten esta tarea, pues éstas no están adaptadas a las características específicas de la normatividad colombiana. Herramientas existentes, como Risk Manager (http://modulo.com/grc-solutions/), ClearRisk (http://www.clearrisk.com), vsRisk (http://www.vigilantsoftware.co.uk/c-33-risk-management-tools.aspx) o G2eTIC (http://g2etic.com/portada.html), entre otras, tienen un enfoque exclusivamente internacional y no permiten la adaptación a la normatividad local específica. Otras herramientas son de uso privativo gubernamental (Check up..., 2013) y no pueden emplearse en organizaciones colombianas.

G2eTIC da un primer paso al proponer una fábrica modular que produce elementos adaptados a cada organización, enfocada hacia el análisis y la evaluación del gobierno y la gestión de TI, bajo el marco de trabajo COBIT 5. La seguridad de la información la abarcan con la familia de estándares ISO 27000. Según sus creadores la herramienta podría ser adaptada a la normatividad colombiana e incluir referentes locales como las circulares de la SFC; sin embar-

go, el proceso de agregar estos referentes es dispendioso y poco práctico, pues está sujeto a la cotización del proveedor y a las herramientas que componen la fábrica, que no son necesariamente adaptables.

Una alternativa a emplear estas herramientas, la cual es ampliamente adoptada, es realizar estos análisis y verificaciones de manera manual por medio de tablas, cruces y relaciones en hojas de cálculo o formatos físicos (Robinson, 2014). Sin embargo, esto tiene el inconveniente de que es un procedimiento dispendioso y propenso a errores.

IV. Análisis de la familia de estándares ISO 27000 y las circulares 038 y 042 de la SFC

El análisis de los estándares ISO 27000 y las circulares 038 y 042 es una actividad que busca identificar concordancias entre los elementos de ambos tipos de referentes que permitan analizar cómo el cumplimiento de ciertos elementos de los estándares ISO 27001 e ISO 27002 puede apoyar el cumplimiento de los requisitos estipulados en las circulares de la SFC. Con el fin de generar recomendaciones para el cumplimiento de estas circulares se creó un mapeo que relaciona sus diferentes elementos, con los elementos de las normas ISO 27000, de forma que estas normas sirvan de guía en la implementación de estrategias para lograr el cumplimiento de dichas circulares.

El mapeo se realizó entre las ISO 27001 y 27002, y el componente tecnológico de las Circulares 038 y 042. Como resultado se cruzaron las quince cláusulas de la norma ISO 27001 y los 114 controles de la norma ISO 27002, contra cinco requisitos de la Circular 038 y cinco de la Circular 042. Se obtuvieron, para todos los requisitos de las dos circulares, cruces con una o ambas normas. La **Figura 1**, corresponde a un fragmento de toda la matriz de mapeo, en el cual se hace referencia al cruce entre el requisito 7.6.2.1, Plan estratégico de tecnología (Circular 038) y el requisito 4.1.1, Conocimiento de la organización y de su contexto (ISO 27001), señalado con una "X". De esta forma se indica la relación entre un elemento de las circulares y un elemento de las normas ISO de la serie 27000.

Así por ejemplo, la cobertura del primer requisito de la circular 038: 7.6.2.1, Plan estratégico de Tecnología, se alcanza con la cobertura de los estándares, procedimientos y directrices que se producen como resultado del cumplimiento de los requisitos de la ISO 27001: 4.1.1, Conocimiento de la organización y de su contexto; 4.2.1, Comprensión de las necesidades y expectativas de las partes interesadas; 4.4.1, Sistema de gestión de seguridad de la información; y de los controles de la ISO 27002: A.5.1.1, Políticas para la seguridad de la información; y A.5.1.2, Revisión de las políticas para la seguridad de la información.

V. Herramienta propuesta

La herramienta propuesta es una aplicación web en la cual se permite el ingreso y despliegue de información al usuario. La interfaz web se comunica con una base de datos que cumple la doble función de almacenar los registros de las evaluaciones realizadas y contener la lógica de funcionamiento de los diferen-

because they are not adapted to the specific characteristics of Colombian legislation. Existing tools such as Risk Manager (http://modulo.com/grc-solutions/) ClearRisk (http://www.clearrisk.com), vsRisk (http://www.vigilantsoftware.co.uk/c-33-risk-management-tools.aspx%7d) or G2eTIC (http://g2etic.com/portada.html) among others have an exclusively international focus and do not allow adaptation to specific local regulations . Other tools are for exclusive government use (Check up..., 2013) and cannot be used in Colombian organizations.

G2eTIC takes a first step by proposing a modular factory that produces elements adapted to each organization and focused on the analysis and evaluation of the government and IT management under the COBIT 5 framework. Information security is covered with the ISO 27000 standards family. According to its creators, the tool could be adapted to Colombian legislation and include local referents such as the notices issued by the Superintendencia Financiera. However, the process of adding these references is quite onerous and impractical, as it is subject to the quotation of the provider and the tools that comprise the factory are not necessarily adaptable.

An alternative to using these tools, which is broadly adopted, is to perform these analyses and verifications manually by using tables, data crossings and relations in spreadsheets or physical formats (Robinson, 2014). However, this has the inconvenience that it is an onerous process and prone to errors.

IV. Analysis of the ISO 27000 standards family and Notices 038 and 042 of the Superintendencia Financiera de Colombia

The analysis of the ISO 27000 standards and Notices 038 and 042 is an activity that seeks to identify matches between elements of both types of referents that allow analysis of how the compliance of certain elements of ISO 27001 and ISO 27002 can support the fulfillment of requirements established by SFC notices. In order to generate recommendations for compliance of these notices, a mapping was created, which relates the different elements of these notices with elements of the ISO 27000 standards in such a way that these rules can serve as a guide in the implementation of strategies to achieve the compliance of these notices.

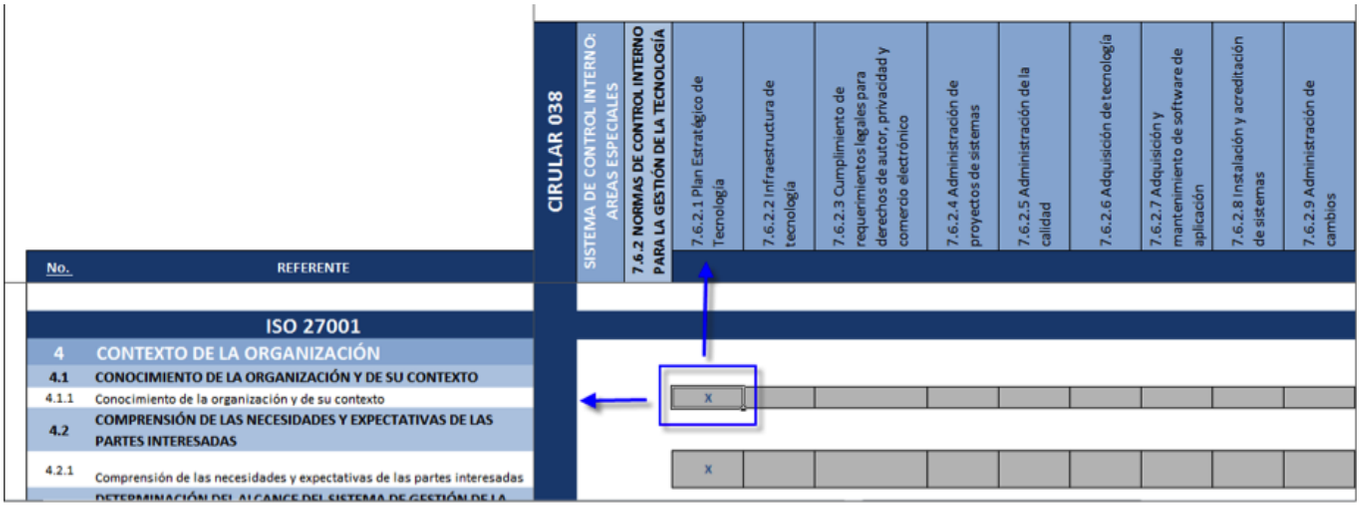

Figure 1. Fragment of the mapping matrix between the referents ISO 27001, 27002 and Notices 038 and 042 / Figura 1. Fragmento de la matriz de mapeo entre los referentes ISO 27001, ISO 27002 y las Circular 038 y 042

The mapping was performed between ISO 27001, ISO 27002 and technological components of Notices 038 and 042. As a result, 15 clauses of ISO 27001 and 114 controls from the ISO 27002 standard were crossed against five requirements of Notice 038 and five of Notice 042. Crosses were obtained for all requirements of the two notices with one or both standards. **Figure 1** shows a fragment of the entire mapping matrix. In this fragment there is a reference to the cross between requirement *7.6.2.1 Technology Strategic Plan* (Notice 038) and requirement 4.1.1 *Knowledge of the organization and its context* (ISO 27001), marked with an "X". This is how the relation between an element of the notices and an element of the ISO standard of the 27000 series is indicated.

Thus, for example, for the first requirement of Notice 038 "*7.6.2.1 Technology Strategic Plan*", it is recommended to achieve its coverage of the standards, procedures, and guidelines that are produced as a result of the compliance with the requirements of ISO 27001 "4.1.1 *Knowledge of the organization and its context", "4.2.1 Understanding needs and expectations of interested parties", "4.4.1 Information security management system"* and of the controls of ISO 27002 "*A.5.1.1 Policies for information security"* and "*A.5.1.2 Revision of policies for information security"*.

V. Proposed tool

The proposed tool is a web application that allows the login and deployment of information to the user. The web interface communicates with a database that has two functions: Storing records of performed assessments referentes configurados en la herramienta. Esta lógica está basada en el mapeo realizado entre las normas ISO 27001, ISO 27002 y las circulares 038 y 042, descrito en la sección anterior.

5.1 Modelo de datos

El modelo de datos de la herramienta presenta una solución al problema planteado: apoyar en el análisis de brechas, cruzar y verificar el cumplimiento de los referentes que se han incluido en la herramienta.

El nivel de información de los referentes se estructuró de forma abstracta para acomodar, no solo a los cuatro referentes en los que se enfoca este trabajo, sino también a otros que pueden ser adicionados. La estructura de la información es la siguiente:

Nivel 1 = Referente (e.g., ISO 27001, ISO 27002, Circular 038, Circular 042)

Nivel 2 = Cláusula (e.g., Dominio para ISO 27002)

Nivel 3 = Sub-cláusula (e.g., Objetivo para ISO 27002)

Nivel 4 = Requisitos (e.g., Control para ISO 27002)

Nivel 5 = Guía de Implementación

La **Figura 2** presenta la estructura general del modelo implementado. En él se observan nueve entidades que corresponden a los objetos implementados en la herramienta propuesta.

5.2 Implementación de la herramienta

La herramienta es capaz de apoyar las evaluaciones de diferentes referentes de seguridad de la información por medio de la automatización de la evaluación, a través de tres casos de uso principales:

- crear una evaluación;
- editar una evaluación; y
- resultados.

La herramienta se implementó como una aplicación web para permitir el ingreso y despliegue de información desde cualquier dispositivo. La interfaz web se comunica con una base de datos que representa el modelo presentado en la subsección anterior,

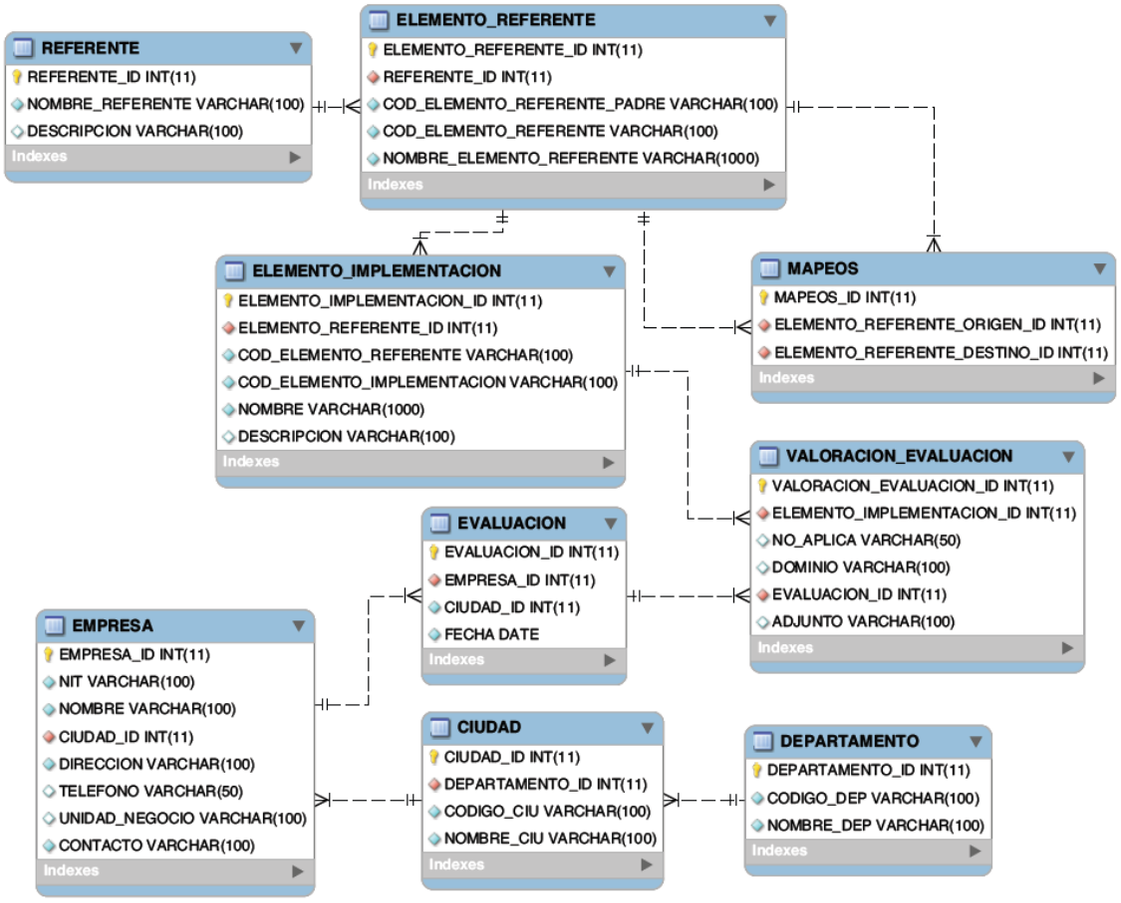

Figure 2. Data model / Figura 2. Modelo de Datos

el cual cumple la doble función de almacenar los registros de las evaluaciones realizadas y contener la lógica de funcionamiento de los diferentes referentes configurados en la herramienta.

La herramienta se encuentra disponible para ser accedida desde Internet a través de la URL http://www.information-securitytool.com

Interfaz web

La interfaz web se genera por medio de código PHP que se ejecuta a nivel de servidor. A su vez este código contiene las instrucciones para realizar las consultas pertinentes a la base de datos, con el fin de ingresar información y retornar resultados de las evaluaciones.

La interfaz se diseñó bajo una óptica minimalista, para lograr que el usuario pueda observar una página fácil de usar y, por tanto, que la curva de aprendizaje del uso de la herramienta sea corta. La interfaz consta de múltiples formularios en los cuales el usuario ingresa los datos de la organización por evaluar y puede escoger los referentes a evaluar y seleccionar su cumplimiento. Por último, cuenta con formularios en los cuales se despliegan los resultados de dicha evaluación, en forma gráfica o textual.

Base de datos

El núcleo de la herramienta es una base de datos MySQL, estructurada en tablas previamente definidas en el modelo de datos descrito en la subsección anterior, alimentadas con los datos de los referentes y el mapeo realizado. Esta base de datos contiene la inte-

ments and containing the operating logic of the various referents set in the tool. This logic is based on the mapping performed between the ISO 27001, ISO 27002 standards and Notices 038 and 042 described in the previous section.

5.1 Data model

The data model of the tool presents a solution to the problem raised of supporting gap analysis, data crossing and verifying compliance with the referents included in the tool.

The information level of the referents was structured in an abstract manner to accommodate not only the four referents on which this work is focused but also others that can be added. The information structure is as follows:

Level 1 = Referent (e.g. ISO 27001, ISO 27002, Notice 038, Notice 042);

Level 2 = Clause (e.g. Domain for ISO 27002);

Level 3 = Sub-clause (e.g. Objective for ISO 27002);

Level 4 = Requirements (e.g. Control for ISO 27002); and

Level 5 = Implementation guide.

Figure 2 presents the general structure of the model implemented. In it, nine entities that correspond to the implemented objects in the proposed tool can be seen.

5.2. Implementation of the tool

The tool is able to support the assessments of different information security referents by the automation of the assessment, through three cases of main use:

- create an assessment;
- edit an assessment; and
- results

The tool was implemented as a web application to allow entry and deployment of information from any device. The web interface communicates with a database that represents the model presented in the subsection above, which has the functions of storing records of performed assessments and containing the operating logic of the various referents set in the tool.

The tool can be accessed from the internet at the following URL http://www.informationsecuritytool.com

Web interface

The web interface is generated by PHP code that is executed at server level. In turn, this code contains the instructions to perform queries pertinent to the database with the object of entering information and returning the results of assessments.

The interface was designed from a minimalist perspective, to ensure that the user can observe an easy-to-use page, so the learning curve for using the tool is short. This consists of multiple forms in which the user enters data on the organization to be assessed, and can select the compliance with such referents. Finally, it has forms where the results of the assessment are displayed in either graphical or textual form.

Database

The core of the tool is a MySQL database structured in tables

ligencia de la herramienta para realizar la respectiva evaluación y proponer las recomendaciones pertinentes en cada caso evaluado.

Formularios

Diversos formularios permiten diferentes funcionalidades, entre las cuales se mencionan:

- ingresar los datos básicos de la empresa a evaluar;
- seleccionar el referente a evaluar;
- seleccionar el ítem que será evaluado;
- realizar la evaluación de la cláusula o domino que se está evaluando;
- generar recomendaciones; y
- generar gráficas.

El formulario de evaluación es el eje principal del proceso de evaluación ya que en él se relacionan el referente, la cláusula o dominio, el requisito o control y la guía –o guías– de implementación. Cada requisito o control puede ser calificado como "Aplica" o "No aplica"; si el requisito o control aplica, cada guía debe ser calificada como "Cumple" o "No cumple"; si la guía cumple, se permite adjuntar un archivo correspondiente a la evidencia de cumplimiento respectiva. La **Figura 3** presenta el formulario de evaluación para el dominio 5, Política de Seguridad de la Información. En él se ha evaluado que se cumple totalmente el primer control y parcialmente el segundo.

La información visualizada en resultados corresponde al conjunto de cláusulas o controles que fueron calificados como "Cumple". El formulario de datos cargados permite el descargue de los archivos que fueron adjuntados durante el proceso de la evaluación y que son la evidencia de su cumplimiento. La **Figura 4** presenta el conjunto de guías de Implementación que se calificaron como "Cumple".

El formulario Recomendaciones presenta el conjunto de guías que deben ser aplicadas para logra un cumplimiento del 100% para la cláusula o dominio evaluado. Es este conjunto de información el que permite a los auditores proponer estra-

Figure 3. Assessment form for the ISO 27002 referent – Domain 5, Policies of information security / Figura 3. Formulario de Evaluación para el referente ISO 27002 – Dominio 5 Política de Seguridad de la Información

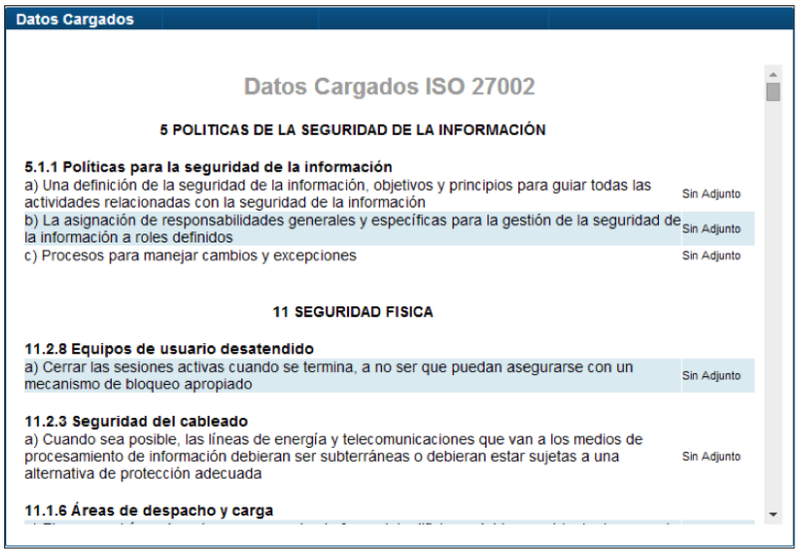

Figure 4. Form of uploaded data / Figura 4. Formulario de datos cargados

tegias que permitan que la organización alcance el nivel de cumplimiento que debe tener de acuerdo al referente. La **Figura 5** presenta el listado de recomendaciones para la evaluación presentada en la **Figura 3**.

Gráficas

Las gráficas permiten visualizar, de forma general y específica, los resultados de la evaluación realizada, a través de las gráficas de telaraña y *pie* respectivamente. La **Figura 6**, presenta la gráfica de telaraña correspondiente a la evaluación de los catorce dominios de la ISO 27002.

En la gráfica de Torta se visualizan, una a una, las cláusulas o dominios evaluados, con su correspondiente avance de implementación, el cual tiene en cuenta el cumplimiento total y el cumplimiento Parcial. La **Figura 7**, muestra el *pie* correspondiente a la evaluación del dominio 5, Política de seguridad de la información.

VI. Validación

Se crearon 23 escenarios que plantean situaciones que se podrían presentar en una organización y los resultados que se esperaría que recomendara la herramienta, con el fin de permitir validar la funcionalidad de la herramienta creada.

6.1 Escenarios de uso del sistema

La cantidad de escenarios obtenidos por referente que se emplearon para validar la completitud y correctitud de la herramienta fue:

- ISO 27001: siete escenarios;
- ISO 27002: catorce escenarios;
- Circular 038: un escenario; y
- Circular 042: un escenario.

En total 23 escenarios que cubren el 100% de la información de los cuatro referentes evaluados. Los escenarios de las circulares 038 y 042 generan recomendaciones basadas en las normas ISO 27001 y 27002.

previously defined in the data model described in the previous subsection and supplied with the data on the referents and the mapping performed. This database contains the intelligence of the tool to perform the respective assessment and raise pertinent recommendations in each case assessed.

Forms

Many forms permit different functionalities, among them:

- entry of basic data on the company to assess;
- option for selecting the referent to assess;
- option for selecting the item to be assessed;
- set of options that permit assessment of the clause or domain that is being assessed;

production of recommendations; and

production of graphs.

The assessment form is the main axis of the assessment process because in it the referent, the clause or domain, the requirement or control, and the implementation guide(s) are related. Each requirement or control can be rated as "Apply" or "Does not apply". If the requirement or control applies, each guide must be rated as "Comply" or "Does not comply". If the guide complies, it is allowed to attach a file corresponding to the evidence of why it complies with the guide. **Figure 3** visualizes the assessment form for domain 5 "Policies of Information Security". In it has been assessed that all of the first control complies and the second one partially complies.

The information visualized in the results corresponds to the set of clauses or controls that were rated as *COMPLY*. The form of uploaded data allows downloading of files attached during the assessment process that are evidence of compliance. **Figure 4** presents the set of Implementation Guides that were rated as *COMPLY*.

The Recommendations form presents the set of guides that must be applied to comply with 100% of the clause or domain assessed. This set of information allows auditors to raise strategies to enable the company to reach the level of compliance that it must have according to

the referent. **Figure 5** presents the list of Recommendations for the assessment shown in **Figure 3.**

Graphs

The graphs permit the visualization, in a general and specific manner, of the results of the assessment performed, using a spider's web graph and pie chart respectively. **Figure 6** presents the spider's web graph that corresponds to the assessment of the 14 domains of ISO 27002.

The pie chart visualizes one by one the clauses or domains assessed with the corresponding progress with implementation, which takes into account the total rather than partial compliance. **Figure 7** shows the pie chart that corresponds to the assessment of Domain 5 Policies of Information Security,

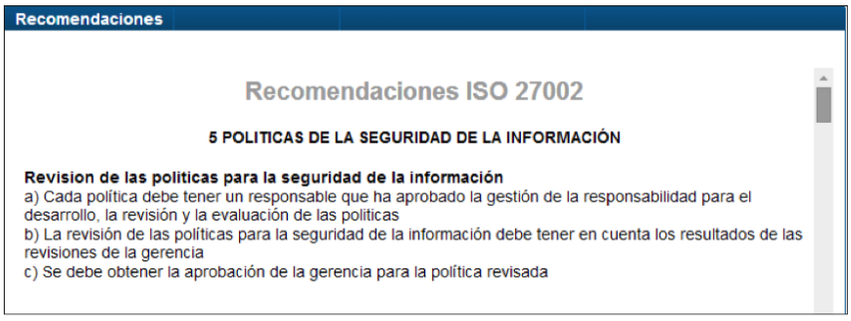

Figure 5. Recommendations form for the ISO 27002 referent – Domain 5, Policies of information security / Figura 5. Formulario Recomendaciones para el referente ISO 27002 – dominio 5, Política de seguridad de la información

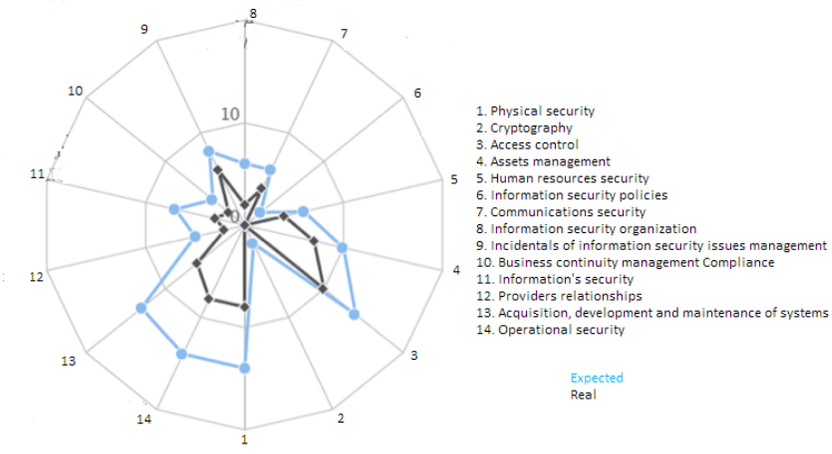

Figure 6. Compliance by domain / Figura 6. Evaluación de los dominios de la ISO 27002

VI. Validation

Twenty-three scenarios were created. These scenarios present situations that could happen in an organization and the results that are expected to be recommended by the tool, with the objective of validating the functionality of the created tool.

6.1. Usage scenarios of the system

The number of scenarios obtained from each referent and used to validate the completeness and correctness of the tool were:

- ISO 27001: seven scenarios;
- ISO 27002: fourteen scenarios;
- Notice 038: one scenario; and
- Notice 042: one scenario.

This brings an overall total of 23 scenarios, thus covering 100% of the information of the four assessed referents. The scenarios from Notices 038 and 042 generate recommendations based on the ISO 27001 and 27002 standards.

To create the scenarios proposed as a methodology for testing the implemented tool, a common base

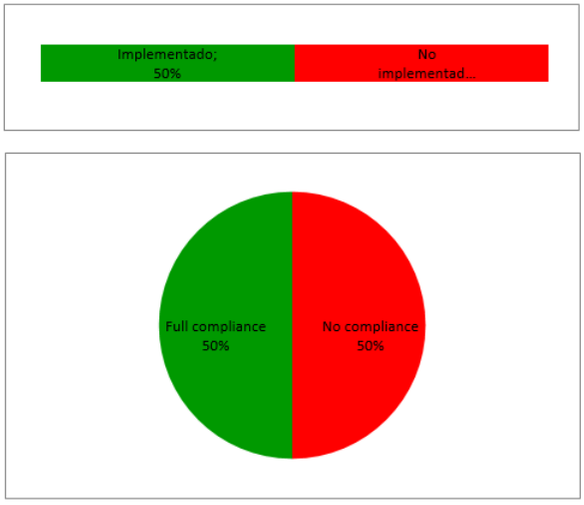

Figure 7. Level of compliance / Figura 7. Cumplimiento de controles

Para crear los escenarios propuestos como metodología para la prueba de la herramienta implementada, se diseñó una estructura base común para todos los referentes. Esta estructura se presenta en la **Figura 8**. En la parte izquierda de la figura se puede visualizar la "Historia de usuario" creada para contextualizar los datos del escenario. En la parte derecha se obser-

HISTORIA DE USUARIO
Actualmente en la compañía se tiene una política de seguridad de la iinformación debidamente documentada donde se expresa el compromiso de las directivas con la misma, la definicion de seguridad de la informacion y su alcance, además cuenta con una asignación precisa de los roles y responsabilidades para la gestión de la seguridad de la información (SI), sin embargo esta política no está sujeta a ningun tipo de revisón periodica y se ha mantenido igual desde la creación de la misma, sin adaptarla a los nuevos cambios que han surgido en la organización, de igual forma la política no es socializada con el personal que labora en la compañía ni con los demás interesados.

NOMBRE ESCENARIO	Referente:	ISO 27002	Dominio:	5		
DOMINIO	5. Políticas de seguridad de la información					
OBJETIVO(S) DE CONTROL	5.1 Orientación de la dirección para la gestion de la seguridad de la información					
CONTROL(ES)	5.1.1. Políticas para la seguridad de la información 5.1.2. Revision de las políticas para la seguridad de la información					
ESTADO CUMPLIDO	Código Control			1	0	N/A
	5.1.1			x		
	5.1.2				x	
ESTADO CUMPLIMIENTO (%)	(1/2)*(100%)=50%					
CUMPLIMIENTO PARCIAL (%)	(0/2)*(100%)=0%					
NO CUMPLIMIENTO (%)	(1/2)*(100%)=50%					
CUMPLIDO O PARCIALMENTE IMPLEMENTADO	* 5.1.1 a) b) c)					
AVANCE DE IMPLEMENTACION (%)	Total: 50%+0%=50%					
RECOMENDACIÓN	* 5.1.2 a) b) c)					

Figure 8. Scenario for the Domain 5 of ISO 27002, Policies of information security / Figura 8. Escenario para el Dominio 5, Política de la seguridad de la información de ISO 27002

van los campos del escenario con sus correspondientes datos; un listado de controles con su evaluación, cumplido (1) o no cumplido (0); el cálculo del estado de cumplimiento, del cumplimiento parcial y el no cumplimiento del dominio; el avance de implementación; y las recomendaciones que debería arrojar la herramienta, como respuesta, al ingresar los datos de este escenario.

Conclusiones y trabajo futuro

En este artículo se ha presentado una herramienta para evaluar el estado de una organización con respecto a la seguridad de la información, tomando como referentes los estándares ISO 27001, ISO 27002 y el componente tecnológico de las circulares 038 y 042. La herramienta emite recomendaciones con base en el análisis de los referentes mencionados.

Para el desarrollo de dicha herramienta se realizó un análisis de concordancia entre los elementos de las circulares y los elementos de las normas ISO, el cual fue consignado en la matriz de mapeo que constituye una pieza de conocimiento que ilustra la relación entre las normas internacionales y la legislación local, y puede ser tomada como ejemplo para realizar análisis y mapeos similares de otros referentes. De igual manera, el modelo de datos desarrollado para la herramienta permite la inclusión de nuevos referentes, de modo que la herramienta puede ser enriquecida, expandida en su funcionalidad y adaptada a los requerimientos específicos de la situación en donde se vaya a utilizar.

Como trabajo futuro se propone: la inclusión de un mayor número de referentes, con el fin de tener evaluaciones más completas; el desarrollo de una interfaz para la inclusión de estos nuevos referentes a la herramienta; y la mejora de la interfaz gráfica, con nuevas tecnologías como AJAX y HTML5, para mejorar su aspecto estético y agregar funcionalidades dinámicas en la visualización. S&T

structure for all the referents was created. This structure is presented in **Figure 8.** On the left of the figure can be seen the User History, created to contextualize the data of the scenario. On the right can be seen the fields of the scenario with their corresponding data, a list of controls for their rating as complied (1) or not complied (0), the calculation of the compliance state, partial compliance and no compliance of the domain, the progress of the implementation and the recommendations that the tool should return as the answer when entering the data of these scenarios.

Conclusions and future work

This article has presented a tool to assess the state of an organization in regard to information security, taking as referents the ISO 27001, ISO 27002 standards and the technological component of Notices 038 and 042. The tool returned recommendations based on the analysis of the referents mentioned.

For the development of the mentioned tool, a concordance analysis between the elements of the notices and the ISO standards was performed. This analysis stored in the mapping matrix constitutes a piece of knowledge that illustrates the relation between the international standards and the local legislation and can be used as an example to perform analyses and similar mappings of other referents. Likewise, the data model developed for the tool allows the inclusion of new referents, so the tool can be enriched, expanded in its functionality and adapted to the specific requirements for the situation in which it is going to be used.

As future work, it is proposed to include more referents to have more complete assessments, to develop an interface for the inclusion of these new referents in the tool, and to improve the graphical interface with new technologies like AJAX and HTML5 to improve its appearance and add dynamic functionalities in the visualization. S&T

References / Referencias

Álvarez, F.M. & García, P.A. (2007). *Implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001, para la intranet de la Corporación Metropolitana de Salud* [thesis]. Escuela Politécnica Nacional: Quito, Ecuador.

Check-up digital (2013). Retrieved from http://www.naa.gov.au/records-management/check-up/

Ernst & Young [EY]. (2012). *Internal audit* [online]. Retrieved from http://www.ey.com/GL/en/Services/Advisory/EY-internal-audit

Feng, N., & Li, M. (2011). An information systems security risk assessment model under uncertain environment. *Applied Soft Computing*, *11*(7), 4332–4340. doi:10.1016/j.asoc.2010.06.005

International Organization for Standardization / *International Electrotechnical Commission* [ISO/IEC]. (2013a). *ISO/IEC 27001:2013: Information technology -- Security techniques -- Information security management systems -- Requirements*. Geneva, Switzerland: ISO.

International Organization for Standardization / *International Electrotechnical Commission* [ISO/IEC]. (2013b). *ISO/IEC 27002:2013: Information technology -- Security techniques -- Code of practice for information security controls.* Geneva, Switzerland: ISO.

Robinson, M. (2014). *Risk assessment toolkit* [online]. Retrieved from http://www.cio.ca.gov/OIS/Government/risk/toolkit.asp

Superintendencia Financiera de Colombia [SFC]. (2009). *Circular externa 038* [memo].

Superintendencia Financiera de Colombia [SFC]. (2012). *Circular externa 042* [memo].

Wheeler, E. (2011). *Security risk management: Building an information security risk management program from the Ground Up*. The Netherlands: Elsevier. doi:10.1016/B978-1-59749-615-5.00022-0

CURRICULUM VITAE

Felipe Reyes López Electronics Engineer (Universidad del Valle, Cali-Colombia) and Master in Information and Telecommunications Management (Universidad Icesi, Cali). He works as Professional Services Engineer at Schneider Electric. / Ingeniero Electrónico de la Universidad del Valle (Cali-Colombia) con Maestría en Gerencia Informática y Telecomunicaciones de la Universidad Icesi (Cali). Trabaja como Professional Services Engineer en Schneider Electric.

Yaneth Betancurt Domínguez Systems Engineer (Universidad del Valle, Cali-Colombia) and Master in Information and Telecommunications Management (Universidad Icesi, Cali). She works as a process, functional requirements and SQA analyst at Expert LA Information. / Ingeniera de Sistemas de la Universidad del Valle (Cali-Colombia) con Maestría en Gerencia Informática y Telecomunicaciones de la Universidad Icesi (Cali). Trabaja como Analista de procesos, requerimientos funcionales y SQA en Expert LA Information.

Ingrid Lucia Muñoz Periñán Electronic Engineer (Universidad del Valle, Cali-Colombia), Specialist in Organizational Informatics Management and Master in Information and Telecommunications Management (Universidad Icesi, Cali-Colombia); Project Management Professional (PMP) and ISO 27001 Lead Auditor, COBIT Foundation Certified. She is the current manager of Domuz Consultoría S.A.S. and a private consultant in Information Security, Project Management and IT Governance. Currently she coordinates the diploma course in Project Management at Universidad Icesi. / Ingeniera Electrónica de la Universidad del Valle (Cali-Colombia), Especialista en Gerencia Informática Organizacional de la Universidad Icesi (Cali-Colombia) y Máster en Gerencia Informática y Telecomunicaciones de la Universidad Icesi. Gerente de Domuz Consultoría S.A.S., Consultora en Seguridad de la información, gerencia y gobierno de TI. Coordinadora Académica del Diplomado en Gerencia de Proyectos en la Universidad Icesi; Project Management Professional (PMP); y Auditor Líder ISO 27001, COBIT Foundation Certified.

Andrés Felipe Paz Loboguerrero Systems Engineer (Universidad Icesi, Cali-Colombia); Master in Informatics and Telecommunications (Universidad Icesi); professor (Information and Communications Technologies Department) and researcher (Informatics and Telecommunications research group) at Universidad Icesi. / Ingeniero de Sistemas y Máster en Informática y Telecomunicaciones de la Universidad Icesi (Cali-Colombia). Profesor hora cátedra del Departamento de Tecnologías de la Información y las Comunicaciones y miembro del grupo de Investigación en Informática y Telecomunicaciones [i2t] en la Universidad Icesi.