Modelo para la evaluación de desempeño de los controles de un SGSI basado en el estándar ISO/IEC 27001

Juan Pablo Berrío, Yury Montoya Pérez, Gustavo Adolfo Pérez Zapata, Jovani Jiménez Builes

jpberriol@unal.edu.co, ymontoyap@unal.edu.co, gaperezz@unal.edu.co, jajimen1@unal.edu.co

Universidad Nacional de Colombia, Colombia
Carrera 80 #49a223
Medellín - Colombia

Resumen: *El estándar ISO/IEC 27001 se desarrolló con el objetivo de proporcionar los requisitos para los sistemas de gestión de seguridad de la información (SGSI) de una organización. Los SGSI son un enfoque sistemático para el manejo de información confidencial de las organizaciones con el fin de que está permanezca segura. La información es un activo valioso para las organizaciones, y la protección de esta un objetivo prioritario para la operación del negocio. La falta de protección de la información ha provocado la fuga de datos valiosos y esto ha provocado incluso tensiones diplomáticas internacionales. En este artículo, nosotros realizamos una revisión del estándar ISO/IEC 27001 para conocer los controles más aplicables dentro de las organizaciones. Nosotros proponemos un modelo que permite evaluar y posteriormente seleccionar controles de seguridad clave con base en la opinión de expertos usando el método Delphi. Se generó una encuesta que tiene preguntas para evaluar los controles de seguridad, dicha encuesta es sometida a un panel de expertos y bajo un mejoramiento continuo de una base de conocimiento, gestionada a través de una herramienta de software desarrollada para aplicar nuestro modelo.*

Palabras clave: ISO/IEC 27001, SGSI, Seguridad de la Información, activos de información, auditoría.

Abstract: *ISO/IEC 27001 standard is developed in order to provide requirements for the information security management system (ISMS) of any organization. ISMS is a systematic approach to manage confidential information of organizations in order to keep it secure. Information is a valuable asset for organizations and its protection is one the main objectives for business operation. The lack of information protection has contributed to the leakage of valuable data and it has also contributed to some international diplomatic tensions. In this paper we present a review of the ISO/IEC 27001 controls to know which of them are the most applicable for organizations. We propose a model for evaluating and later selecting key secure controls based on expert's opinions using the Delphi method. We made a survey, which includes questions for evaluating the security controls. The survey is evaluated by an expert panel, which allows the continuous improvement of the knowledge base. The survey is managed by a software application developed to implement our model.*

Keywords: ISO / IEC 27001 ISMS Information Security, information assets, audit.

1 Introducción

El estándar ISO/IEC 27001 se desarrolló con el objetivo de proporcionar los requisitos que permiten "establecer, implementar, mantener y continuamente mejorar un sistema de gestión de seguridad de la información". El estándar ISO/IEC 27001 se puede implementar para evaluar la habilidad que tienen las organizaciones para cumplir sus propios requisitos de seguridad de la información. Los requisitos propuestos por esta norma son aplicables a todo tipo de organización. El modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA) es implementado en el estándar ISO/IEC 27001 con el objetivo de estructurar los procesos de los SGSI (sistemas de gestión de seguridad de la información) que utilizan las organizaciones [Deming89].

Los SGSI tienen por objetivo brindar conocimiento acerca del tratamiento adecuado de la información y de todo activo digital que pueda representar un riesgo en las manos equivocadas [Susanto+11]. Los procesos de gestión de riesgos que se implementan en los SGSI ayudan a preservar la confidencialidad, la integridad y disponibilidad de la información [Broderick06]. El estándar ISO/IEC 27001 define un SGSI como "parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información"[ICONTEC06].

Dentro de las organizaciones es clave mantener la información asegurada, sin embargo, muchas compañías no son conscientes de los riesgos que corren al no tener controles de seguridad. Para minimizar esos riesgos, existen los llamados SGSI, los cuales contienen una serie de controles que permitirán verificar con el tiempo el nivel de seguridad de la información. La frecuente ocurrencia de eventos de riesgo operacional genera pérdidas económicas y deterioro de la imagen en diferentes organizaciones, lo cual invita a la evaluación de la efectividad de las actividades de control que se realizan en el manejo de seguridad de la información. El caso Manning, que filtró miles de documentos del ejército de Estados Unidos, o el caso Snowden que divulgó información clasificada de la NSA, son evidencia del reto que supone la implementación adecuada de un SGSI, y la correcta elección de controles para tener un nivel de efectividad que permite mitigar los riesgos más altos o críticos [Cleave13].

En este artículo, proponemos el diseño, estructura e implementación de una herramienta que surge del modelo, que permite identificar los controles clave, a partir del relacionamiento de variables cualitativas definidas y valoradas por expertos en temas de auditoría

del estándar ISO/IEC 27001. Se realizó el estudio de un caso real, en la compañía de financiamiento Coltefinanciera S.A, se implementó un SGSI basado en el estándar ISO/IEC 27001, los diferentes objetivos de control fueron seleccionados con ayuda del modelo seleccionado, con una base de conocimiento de 15 expertos, el tiempo de implementación fue de seis meses. La evaluación de cumplimiento del sistema fue realizada por la compañía Bureau Veritas.

Este artículo está organizado de la siguiente manera. En la sección 2, presentamos el marco teórico, el cual incluye una descripción del estándar ISO 27001 para la gestión de la seguridad de la información y de los SGSI. En la sección 3, presentamos una revisión de la literatura. En la sección 4, presentamos modelo de evaluación. En la sección 5, presentamos la aplicación para evaluar el desempeño de los controles de un SGSI. En la sección 6, presentamos los resultados y, finalmente, en la sección 5, presentamos las conclusiones y trabajo futuro.

2 Teoría del dominio

2.1 ISO/IEC 27001 – Gestión de la seguridad de la información

El estándar ISO/IEC 27001 está orientado únicamente a la seguridad de la información y se desarrolló con el objetivo de proporcionar los requisitos que permiten "establecer, implementar, mantener y continuamente mejorar un sistema de gestión de seguridad de la información". En este estándar se especifican los requisitos y controles para planificar, hacer, verificar y actuar en un SGSI, basado en el modelo de Deming, el cual se puede observar en la Figura 1.

Figura 1: Modelo de Deming

El modelo de Deming aplicado a los SGSI se puede observar en la Figura 2. "La adopción del modelo PHVA refleja los principios establecidos en las directrices OCDE (Organización para la Cooperación y el Desarrollo Económico) que controlan la seguridad de sistemas y redes de información". En la primera fase de este ciclo, la cual es *planificar*, se deben entregar resultados alineados con las políticas y objetivos de una organización, para ello se deben establecer políticas, objetivos, procesos y procedimientos de seguridad.. En la segunda fase, *hacer*, se deben implementar y operar todos los controles que se hayan propuesto en el SGSI al igual que las políticas y los procesos. En la tercera fase, *verificar*, se debe realizar un reporte de los resultados con base en la evaluación y medida del desempeño del proceso del SGSI de acuerdo con las políticas y objetivos de seguridad planteados. En la cuarta y última fase del modelo PHVA, la cual es *actuar*, se deben "emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI", para lograr una mejora continua del SGSI [Deming89].

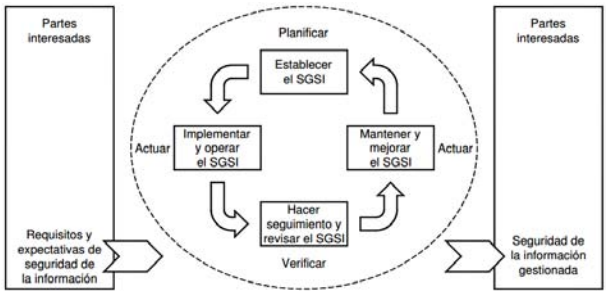

Figura 2: Modelo PHVA aplicado a los procesos de los SGSI

2.2 SGSI – Sistema de gestión de la información

El estándar ISO/IEC 27001 define siete fases para la implementación de un SGSI bajo sus controles, los cuales se pueden observar en la Figura 2.

Figura 3: Fases para la implementación de un SGSI ("Normas ISO," www.bsigroup.com)

EL estándar ISO/IEC 27001 establece un nivel de gobierno TI, pues es necesaria la administración, comprensión y el uso de las TI como un facilitador para alcanzar los objetivos del negocio de manera eficaz, para lograr esto se requiere conocer los riesgos actuales, emergentes, y el impacto posible, ya que la norma debe evitar los peores riesgos relacionados con TI (Susanto,

Almunawar, & Tuan, 2012)(Neubauer, Ekelhart, & Fenz, 2008). La implementación de los SGSI en las organizaciones está basada en "las necesidades, objetivos, procesos, tamaño, estructura y requerimientos de seguridad únicos" [Shojaie14]. Los SGSI son una parte importante de las organizaciones, ya que estos proveen un conjunto de políticas procedimientos, directrices, recursos y actividades que deben ser gestionadas [Shojaie14].

3 Revisión de literatura

Peciña et al. [Peciña11] proponen una metodología para el análisis de riesgos de los procesos de activos físicos y activos de información, es una metodología dirigida a organismos de administración y a organismos empresariales principalmente. La metodología se basa en el estándar ISO/IEC 27001 y ISO/IEC 31000. Resulta confusa la propuesta de los autores, ya que se refieren a ésta como una *metodología*, como un *método* y también como un *modelo*. La metodología propuesta contiene indicadores y criterios que se pueden implementar para evaluar y comparar tanto los riesgos físicos como los riesgos de información. Ristov et al. [Ristov12] proponen una extensión del estándar ISO/IEC 27001:2005 y también un nuevo control de virtualización dirigido a los sistemas en la nube. Los autores también proponen una métrica. Los autores consideran que tener el certificado del estándar ISO/IEC 27001 no es suficiente para sistemas de seguridad de la información, especialmente para la computación en la nube.

Shojaie et al. [Shojaie14] realizan una comparación entre el estándar ISO/IEC 27001:2005 e ISO/IEC 27001:2013. Los autores clasifican los controles de estos estándares en 5 categorías: data, hardware, software, people y network. Estas categorías permiten de manera más fácil que pequeñas y medianas empresas implementen los controles necesarios y relevantes basándose en sus propios requerimientos. Hajdarevic et al. [Hajdarevic13] proponen una metodología basada en el paradigma de GQM (Goal, Question, Metric) para determinar los pasos necesarios para la detección y solución de diferentes violaciones de los controles de seguridad de la información. Esta metodología divide los posibles eventos detectables y luego los resuelve si es posible.

4 Modelo de evaluación

El estándar ISO/IEC 27001 proporciona orientación sobre la elaboración y uso de medidas para evaluar la eficacia de un SGSI, siendo estas aplicadas a la medición de controles o grupos de controles, sin embargo, no describen ni especifican cómo medir u evaluar la efectividad de los controles, ya que sólo se limitan a exigir su evaluación y cumplimiento [Pierce05].

En el nivel de auditorías a los SGSI, se ha observado según la literatura que en un mayor porcentaje los procedimientos se apoyan y fundamentan principalmente en el conocimiento, experiencia y percepción de los expertos auditores, quienes, además, agregan y usan controles no formalizados en el estándar y continuamente están realizando cambios en la metodología de auditoría.

El modelo que proponemos en este trabajo pretende recopilar una base de información generada por una cantidad x de expertos. Dicha cantidad crecerá continuamente con el aporte de un nuevo experto, el objetivo es identificar y evaluar con un criterio más conservador los controles del estándar ISO/IEC 27001 existentes y su efectividad, como se puede observar en la Figura 4.

El objetivo del modelo que proponemos es identificar y evaluar con un criterio más conservador los controles del estándar ISO/IEC 27001 existentes y su efectividad, mediante la recopilación una base de información generada por una cantidad x de expertos. Dicha cantidad crecerá continuamente con el aporte de un nuevo experto y generará una valoración con base en la experiencia y análisis razonable de un conjunto y no de un individuo.

Previo a la aplicación del modelo, ya debieron ser identificadas las causas y riesgos que se quieren mitigar.

En la primera fase, se realiza una encuesta con criterios que permitirán la evaluación de un control, los criterios de esta encuesta son inicialmente recopilados con base en el conocimiento de los expertos. Una vez consolidada una versión preliminar de la encuesta, se inicia la fase de consolidación mediante el método Delphi [Herlmer+63], los expertos asignarán a cada criterio una valoración por medio de una escala de Likert, de acuerdo con dos criterios los cuales son:

- La importancia del criterio.
- La pertinencia del criterio en el bloque de contenido.

Así mismo, al concluir una ronda de valoración de criterios, al aporte de cada experto se le asigna un peso respecto a la valoración que realizan los demás expertos, esto con el fin de tener en cuenta aspectos como: años de experiencia, certificaciones en el conjunto de ISO/IEC27000, entre otros.

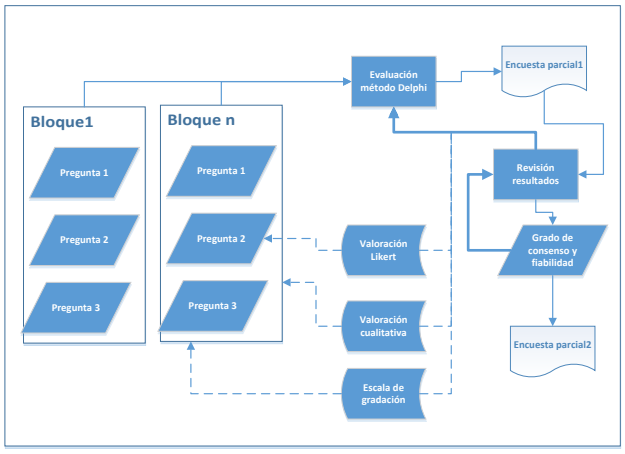

Figura 4: Modelo de evaluación Delphi

Una vez obtenida la encuesta con la valoración de los criterios con una mediana y desviación estándar baja de +/- 1, es decir se tiene un elevado consenso para los criterios que se deben tener en cuenta para medir un control, entonces procedemos a medir los controles por medio del segundo modelo de evaluación que se puede ver en la Figura 5, en el cual se usa un estadístico de fiabilidad Alfa de Cronbach [Cronbach51], el cual nos

permite estimar la precisión con la que un conjunto de criterios mide la conducta de un objeto a evaluar, la calificación el Alfa se mide de acuerdo con la Tabla 1.

Tabla 1: Valoración Alfa de Cronbach.

Alfa	Evaluación
<0,70	No se acepta
>0,70 y <0,86	Aceptable
>=0,86	Notable de aceptación

$$\alpha = \frac{K}{K-1}\left[1-\frac{\sum S_i^2}{S_T^2}\right]$$

Donde:
K: El número de ítems
Si2: Sumatoria de Varianzas de los Ítems
St2: Varianza de la suma de los Ítems
α: Coeficiente de Alfa de Cronbach

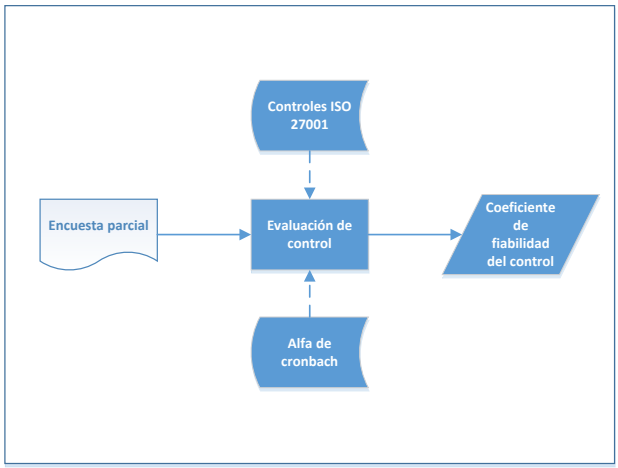

Figura 5: Modelo evaluación de controles

5 APP SGSI

Como herramienta de evaluación del modelo, hemos diseñado y desarrollado una aplicación de software en el framework Laravel, la cual nos permite administrar los usuarios y perfiles de acuerdo con el rol que desempeñarán en el proceso, bien sea como un experto que aportará a la base de conocimiento o un auditor, implementador que quiere evaluar la efectividad de sus controles ya implementados lo que desea implementar en el SGSI. A continuación, presentamos algunas vistas del proceso en la herramienta desarrollada.

En la Figura 6, podemos observar la evaluación que se le da a un experto que se registra en el sistema, de acuerdo con las variables de ponderación.

Figura 6: Evaluación de experto para determinar su score

En la Figura 7, podemos ver la presentación de los controles que fueron registrados del estándar ISO/IEC 27001 y que serán objeto de estudio.

Figura 7: Registro y visualización de los controles a medir

Podemos observar en la Figura 8, las preguntas que serán sometidas a ser parte de la encuesta para la auditoría, las cuales serán calificadas posteriormente en la Figura 9.

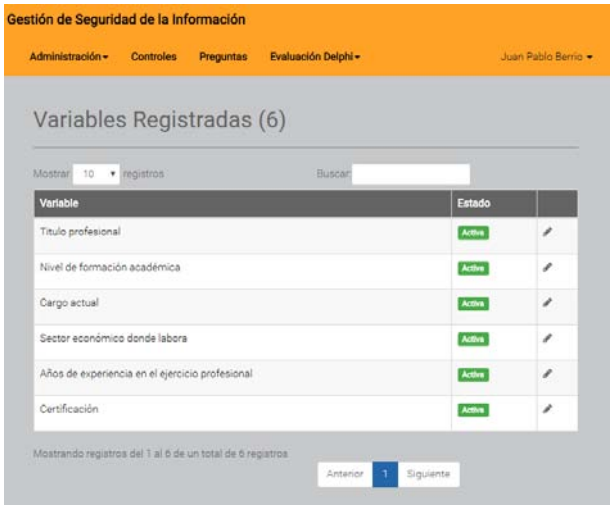

Figura 8: Registro de preguntas para la encuesta

Figura 9: Calificación de las preguntas asociadas a un control por parte de los expertos

6 Resultados

Con el desarrollo continuo de la herramienta, hemos realizado pruebas durante 3 meses reuniendo expertos en las áreas de auditorías en el estándar ISO/IEC 27001, de los cuales se obtuvieron los siguientes datos:

Fueron 11 expertos registrados en total los cuales se discriminan de la siguiente manera según las variables de calificación:

Tabla 2: Experiencia de expertos

Cantidad de expertos	Años de experiencia
3	De 1 a 3 años
6	De 4 a 5 años
2	De 10 a 15 años

Tabla 3: Certificados de expertos

Cantidad de expertos	Certificación ISO/IEC 27001
9	Auditor Interno
3	Auditor Líder

Tabla 2: Áreas de formación de expertos

Cantidad de expertos	Área de formación académica
6	Título profesional en el área de sistemas
2	Título profesional en el área de administración
3	Título profesional en el área de procesos e industria

Dentro de la organización mencionada, Coltefinanciera, realizamos las pruebas con los controles del SGSI que previamente habían implementado en la compañía, de 47 controles que habían implementados y que se agregaron a la aplicación, 31 controles obtuvieron una notable aceptación con el estadístico del Alfa de Cronbach, 10 controles aceptables y 6 controles no aceptados. Desde la gerencia de riesgo se tomó la decisión de reevaluar el riesgo que se quiere mitigar con los controles no aceptados para establecer nuevos controles y someterlos de nuevo a medición.

Durante el tiempo de entrega de este paper estaba en proceso de evaluación de la efectividad de los controles el SGSI que se quiere implementar en una pequeña empresa de confecciones reconocida en la ciudad, con una cantidad de 24 empleados, de los cuales 16 tienen relación directa con los activos de información de la compañía.

7 Conclusiones y trabajos futuros

El modelo propuesto ha permitido reunir el concepto de varios expertos para tratar de disminuir la valoración subjetiva de la que es vulnerable la implementación de un SGSI y su auditoría.

Con este modelo y con ayuda de la herramienta de software es posible identificar los controles más claves para una pronta implementación de un SGSI, ya que la valoración por el Alfa de Cronbach puede entregar una escala numérica que de ser usada en su orden de calificación, ayuda a indicar cuales controles tienen más efectividad.

Una de las ventajas de tener un sistema apoyando el modelo consiste en que la base de conocimiento puede crecer hasta un número indeterminado. Si logramos mantener la calidad de los datos con una buena evaluación por parte de los expertos, podremos estar ofreciendo una gran herramienta a los implementadores y auditores del estándar, ya que la experiencia que recogemos, sirve como apoyo para el aprendizaje continuo.

Referencias bibliográficas

[Deming89] Deming, E. Calidad, productividad y competitividad. Ediciones Díaz de Santos, 1989, 412ps.

[Susanto+11] Susanto, H. Almunawar, M. Tuan, Y. Information Security Management System Standards : A Comparative Study of the Big Five, 2011.

[Broderick06] Broderick, J. Security standards and security regulations. Information Security Technical Report, 06.

[ICONTEC06] Norma Técnica Colombiana NTC, ISO 27001. 2006.

[Cleave13] Cleave, M. Myth, Paradox & The Obligations of Leadership. Center for Security Policy, 2013

[Herlmer+63] Helmer, O. Dalkey, N. Rescher, N. An Experimental Application of the DELPHI Method to the Use of Experts, Project RAND, 1963.

[Pierce05] Pierce, B. Sweeney, B. Management control in audit firms - Partners perspectives. Management Accounting Research 16, 2005.

[Cronbach51] Cronbach, L. Coefficient alpha and the internal structure of tests. Psychometrika, 1951.

[Peciña11] Peciña, k. Bilbao, A. Bilbao, Enrique. Physical and logical security risk analysis model, 2011, 7 ps.

[Ristov12] Ristov, S. Gusev, M. Kotoska, M. A new methodology for security evaluation in cloud computing, 2012, 6 ps.

[Shojaie14] Shojaie, B. Federrath, H. Saberi, I. Evaluating the effectiveness of ISO 27001:2013 based on annex A, 2014, 6 ps.

[Hajdarevic13] Hajdarevic, K. Allen, P. A new method for the identification of proactive information security management system metrics, 2013, 6 ps.