Revista Cubana de Ciencias Informáticas
Vol. x, No. x, Mes x-y, 2013
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 14-26

Tipo de artículo: Artículo original
Temática: Seguridad informática
Recibido: 12/12/2014 | Aceptado: 29/02/2016

Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática

Methodology for the Implementation of Automated Management of Computer Security Controls

Michel Miranda Cairo[1]*, Osmany Valdés Puga[1], Iván Pérez Mallea[1], Renier Portelles Cobas[1], Raúl Sánchez Zequeira[1]

Universidad de las Ciencias Informáticas. La Habana, Cuba. mcairo@uci.cu, ovaldes@uci.cu, imallea@uci.cu, renierpc@uci.cu, raulsz@uci.cu.

* Autor para correspondencia: mcairo@uci.cu

Resumen

La gestión de la seguridad informática debe ser vista como un proceso bien definido, con la capacidad de mejorar de manera incremental y continua. El elevado número de controles a implementar en un sistema de información dinámico, implica un enorme esfuerzo para el personal encargado de proteger la información. Por ello este trabajo presenta una metodología basada en la integración de varios modelos, normas, herramientas y buenas prácticas para la implementación de la gestión automatizada de controles de seguridad informática, combinando varios métodos orientados a la gestión de riesgos con un enfoque de automatización durante las etapas de operación, monitorización y revisión de un Sistema de Gestión de Seguridad de la Información. Teniendo en cuenta que aproximadamente el 30% de los controles contenidos en el estándar internacional ISO/IEC 27002 son automatizables, la aplicación del resultado de esta investigación presupone lograr que la gestión de la seguridad informática sea un proceso menos complejo y más efectivo, afirmación que es validada a través de un análisis estadístico que demuestra la disminución de la complejidad y el aumento de la eficiencia en cuanto al tiempo y el esfuerzo requerido por el proceso en un factor cercano al 90% para ambos casos.

Palabras clave: automatización, controles, metodología, seguridad informática, sistemas de información.

Revista Cubana de Ciencias Informáticas
Vol. x, No. x, Mes x-y, 2013
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 14-26

Abstract

The information security management should be seen as a well-defined process, with the ability to be incrementally and continuously improved. The high number of controls implemented in a dynamic information system involves a huge effort from the staff responsible for the protection of the information. That is why this paper presents a methodology based on the integration of several models, standards, tools and best practices for implementing automated management of computer security controls, combining several methods focused on risk management with an automation approach during the operation, monitoring and revision of an Information Security Management System. Having in mind that nearly 30% of the controls gathered in the international standard ISO/IEC 27002 can be automatized, the application of this research could lead to archive a less complex and more effective computer security management, and this affirmation is validated by a statistic analysis that shows a reduction of the complexity and an increment in the efficiency based in costs of time and effort required by the process in both cases by a factor near to 90%.

Keywords: *automation, computer security, controls, information systems, methodology*

Introducción

En la actualidad las empresas y organizaciones utilizan para la creación, procesamiento, transmisión y almacenamiento de su información las ventajas de las Tecnologías de la Información y las Comunicaciones. Debido a esto, el número de amenazas se incrementa y obliga a que garantizar la disponibilidad, confidencialidad e integridad de la información signifique un aspecto de primer orden sobre el cual invertir para evitar la pérdida, modificación o robo de los activos informáticos.

Los ataques más importantes se deben principalmente a aspectos como las vulnerabilidades de software, malware, dispositivos móviles, personal interno y hackers, los cuales acaparan alrededor del 69% del total de las incidencias de seguridad atendidas por los especialistas encuestados, según un estudio de *International Information Systems Security Certification Consortium* (ISC^2) (SUBY, 2013). Según el Reporte Norton de Symantec (SYMANTEC, 2014), los ataques a la información llegaron en el año 2013 a la alarmante cifra de 378 millones de víctimas, o sea, más de un millón de personas diarias, ocasionando pérdidas cercanas a los 113 millones de dólares.

Con el objetivo de lograr adecuados niveles de seguridad, se han creado una serie de modelos, estándares, recomendaciones y regulaciones como lo son (ISO/IEC, 2005) y (NIST, 2013), que indican la realización de un número importante de controles, según las referencias investigadas entre 100 y 200 controles. Unido a esto, la

heterogeneidad y velocidad de desarrollo de las tecnologías utilizadas en los sistemas de información, hacen que el proceso de gestión se torne complejo y en ocasiones ineficiente.

La automatización de controles de seguridad informática, es una de las posibles vías para lograr que la gestión de la seguridad informática sea un proceso menos complejo y más efectivo en un entorno tecnológicamente heterogéneo y de constantes amenazas de seguridad, teniendo en cuenta la gran cantidad de controles a implementar.

El campo de la gestión automatizada de controles de seguridad informática es un tema bien novedoso en la comunidad científica internacional, por lo que resulta difícil encontrar trabajos de gran impacto en la temática. Durante el desarrollo de la investigación se analizaron varios, entre los que se pueden mencionar (CSIS, 2013) y (NIST, 2009), el primero abarca un compendio de 20 controles críticos a implementar en SGSI con una visión de automatización; mientras que el segundo introduce la definición de nomenclaturas y lenguajes estándares que permiten la interoperabilidad de diferentes aplicaciones mediante la adopción de un lenguaje de seguridad común. Otros, como (CORTI, 2006), abordan la implementación de un SGSI desde un punto de vista de proceso, pero enfocando su atención en particularidades regionales y abordando la automatización solamente hasta un nivel de requerimientos de software.

En el ámbito nacional, el estudio más importante en tal sentido es el modelo para la gestión automatizada e integrada de controles de seguridad informática (MONTESINO, 2012), que tiene como principal objetivo contribuir al aumento de la efectividad de los controles y a disminuir la complejidad de la gestión de la seguridad informática. Aunque este modelo provee una guía para su implementación, enfoca la automatización a nivel de la operación, monitorización y revisión del SGSI, sin especificar cómo determinar qué controles deben contemplarse y el orden en que se implementan a partir de las características y necesidades de las organizaciones, así como tampoco incluye métodos para la medición de la efectividad de los mismos.

Existen además metodologías que guían de implementación de un SGSI, como son MAGERIT (MINHAP, 2012) y OCTAVE (DUQUE, 2014) basadas en el análisis de los riesgos a que se exponen los activos informáticos. Aunque muy descriptivas, estas metodologías generan excesiva documentación y los cálculos que deben efectuarse durante la evaluación de los riesgos pueden complicarse de manera innecesaria, lo que se traduce en más tiempo para su aplicación. Además, a pesar de llegar a identificar que controles pudieran ser utilizados en el proceso de implementación de un SGSI, no proponen como estos deben ser implementados, operados, monitoreados y revisados.

El objetivo de este trabajo es proponer una metodología para implementar la gestión automatizada de los controles de seguridad informática a través de la integración de los elementos que aportan los modelos, normas y metodologías mencionados anteriormente.

Materiales y métodos

La seguridad de la información no constituye un activo que se pueda comprar, ni un estado alcanzable mediante la realización de inversiones; sino un proceso gestionado (RUIZ, 2010). Un sistema de información se debe monitorear y evaluar de manera constante, con métricas establecidas que permitan medir con objetividad y tomar las decisiones oportunas respecto a los riesgos que se enfrentan (MEDINA, 2011).

Implementación de un sistema de gestión de la información

Según el estándar internacional ISO/IEC 27001, el proceso de establecer y manejar un SGSI implica la realización de las siguientes actividades:

- **Establecer**: Definir los objetivos y el alcance del SGSI, los objetivos de control y controles a partir del análisis de riesgos realizado y especificar los procedimientos de operación.
- **Implementar**: Implementar los controles establecidos y definir cómo medir la efectividad de los mismos.
- **Operar**: Llevar a cabo las acciones necesarias para la ejecución de los procedimientos establecidos.
- **Monitorizar**: Supervisar el funcionamiento de los controles con el objetivo de detectar errores e identificar incidentes y violaciones.
- **Revisar**: Evaluar la efectividad del SGSI con respecto al cumplimiento de sus objetivos, mediante indicadores previamente establecidos.
- **Mantener y mejorar**: Realizar las acciones correctivas necesarias e implementar las mejoras identificadas en el SGSI.

Gestión automatizada de controles de seguridad informática

La gestión automatizada de un control de seguridad informática implica que la operación, monitorización y revisión del mismo se realizan de forma automática, mediante sistemas informáticos y/o herramientas de hardware existentes sin que se produzca intervención humana en la realización de estas acciones (MONTESINO, 2012).

Revista Cubana de Ciencias Informáticas
Vol. x, No. x, Mes x-y, 2013
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 14-26

Otro concepto es el asumido por (CSIS, 2013) que expresa que la automatización de estos controles consiste en la automatización de las defensas de manera tal que una organización puedan obtener medidas confiables, escalables y continuas sobre su adherencia a los controles y las métricas relacionadas.

Metodología para la implementación de la gestión automatizada de controles de seguridad informática

Una metodología es una secuencia sistémica de etapas cada una de las cuales incluye acciones o procedimientos dependientes entre sí y que permiten el logro de determinados objetivos (URIZARRI, 2006).

Partiendo de lo planteado, se presenta en este trabajo el desarrollo de una metodología basada en la integración de varios modelos, normas, herramientas y buenas prácticas para la implementación de la gestión automatizada de controles de seguridad informática, combinando varios métodos dirigidos a la gestión de riesgos con un enfoque de automatización durante las etapas de operación, monitorización y revisión de un SGSI.

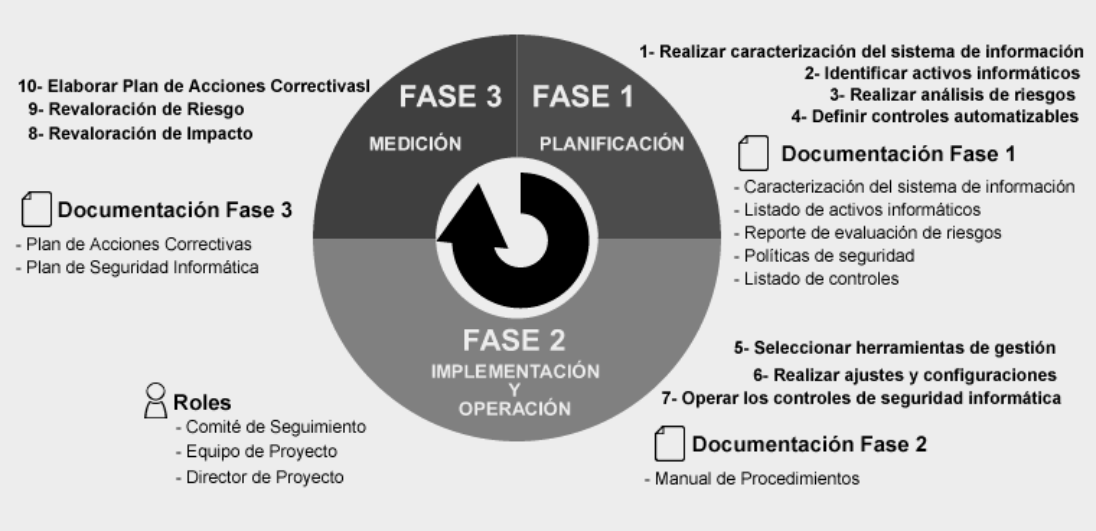

Figura 1. Metodología para la implementación de la gestión automatizada de controles de seguridad informática

La metodología especifica un total de 10 actividades agrupadas en 3 fases que componen un ciclo cerrado (Figura 1), donde cada iteración presupone un nivel de seguridad de la información mayor que el anterior.

Revista Cubana de Ciencias Informáticas
Vol. x, No. x, Mes x-y, 2013
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 14-26

Roles y responsabilidades de la metodología para la implementación de la gestión automatizada de controles de seguridad informática

La implementación de un SGSI deberá ser asumida con una visión de proyecto, donde existan roles y responsabilidades bien definidos que tributen al éxito del proceso. En la presente metodología se propone la selección de los siguientes roles:

- **Comité de seguimiento**: La seguridad informática no es responsabilidad de una persona, sino de todos los involucrados en el sistema de información, es por eso que se debe involucrar a la dirección de la organización como representación activa de todos los actores del sistema. El proceso de implementación de un SGSI requerirá del apoyo de la dirección de la empresa, para posibilitar que el equipo de trabajo a cargo del proceso cuente con los recursos necesarios. En este comité quedará también la responsabilidad de la toma de decisiones críticas y la aprobación de la documentación que se vaya generando.
- **Equipo de proyecto**: Estará formado por personas con conocimientos avanzados en tecnologías y sistemas de información, y personal técnico de la organización afectada con conocimientos generales de gestión de seguridad y de la aplicación de la metodología que se propone. Este grupo estará a cargo de llevar a cabo todas las actividades del proyecto de implementación, así como de elaborar la documentación que se propone.
- **Director de proyecto**: Es la persona responsable de velar por la seguridad informática en la organización. Será quien dirija al equipo de proyecto y sirva de enlace comunicativo entre éste y el comité de seguimiento.

Fases y actividades de la metodología para la implementación de la gestión automatizada de controles de seguridad informática

Fase 1: Planificación

El objetivo principal de esta fase es conocer los principales objetivos de control a partir del análisis de riesgos a que se exponen los diferentes activos informáticos. Para lograrlo se definen cuatro actividades, las cuales deben generar la información necesaria para dar paso a la fase 2. Ellas son:

- **Realizar caracterización del sistema de información**: Esta actividad comprende parte de la tarea 4.2.1.a definida en el estándar ISO/IEC 27001, haciendo énfasis en la descripción del sistema de información en cuanto a la organización gerencial que presenta, la descripción física del espacio que ocupa y las características del personal con acceso a las tecnologías. Además, en esta actividad se debe establecer el equipo de trabajo que realizará las tareas de implementación del SGSI, asignando, desde este punto, las personas que se desempeñarán en los roles definidos por la metodología. Otro paso importante es identificar

los reglamentos, disposiciones, regulaciones y demás documentos que regulen, desde una instancia superior, la seguridad informática de la organización.

- **Identificar activos informáticos**: Esta actividad se desprende de la tarea 4.2.1.a, definida en el estándar ISO/IEC 27001, y se encarga de la realización del inventario de activos presentes en el sistema de información, realizando; además, el cálculo de valor por activo para la organización mediante un análisis cuantitativo donde a cada atributo o dimensión de la información (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) se le asigna un valor D_i (entre 0 y 10) que representa la importancia de dicho atributo para un activo determinado.
- **Realizar análisis de riesgos**: El análisis de riesgos es la actividad que permitirá determinar cuán comprometido está un activo dependiendo de la probabilidad de ocurrencia de un evento nocivo, ya sea que se trate de la explotación de una vulnerabilidad del sistema de información o de una amenaza, y el impacto de dicho activo en el sistema. El principal objetivo es proveer la información necesaria para tomar las decisiones sobre qué debe protegerse, de qué y cómo. Esta actividad comprende las tareas 4.2.1.c, 4.2.1.d y 4.2.1.e definidas en el estándar ISO/IEC 27001 y se han utilizado técnicas de análisis propuestas en (MINHAP, 2012).
- **Definir controles automatizables**: Respondiendo a las tareas 4.2.1.f, 4.2.1.g, 4.2.1.h, 4.2.1.i y 4.2.1.j definidas en el estándar ISO/IEC 27001, se procederá con el tratamiento de los riesgos identificados, lo cual implica cuatro acciones posibles: reducirlos, aceptarlos, evitarlos o transferirlos. La redacción de las políticas de seguridad es el comienzo de esta actividad, que se dictan con el objetivo de darle tratamiento a los riesgos, y exponen explícitamente las acciones a tomar sobre los mismos; deben estar alineadas con los objetivos de la organización y disposiciones legales o regulaciones regionales dictadas por organismos superiores.

Si se decide trabajar en la reducción de los riesgos, es necesario comenzar a definir los objetivos de control y seleccionar los controles apropiados que puedan calificarse como automatizables (Tabla 1). Además, se deben identificar los controles que puedan ya estar implementados dentro de la organización.

Tabla 1. Dominios de amenazas por macro-control

No.	Macro-control	Dominios
1	Inventario de activos	hardware, software, comunicaciones y recursos físicos
2	Gestión de usuarios	recursos humanos
3	Gestión de trazas	información, datos y servicios
4	Monitoreo de los sistemas	software

5	Protección contra programas malignos	software
6	Detección de vulnerabilidades y gestión de parches	software
7	Configuraciones de seguridad y cumplimiento de políticas	información, datos, servicios, software, hardware, comunicaciones, recursos administrativos, recursos físicos y recursos humanos
8	Respaldo de información	información, datos
9	Seguridad física	recursos físicos
10	Gestión de incidentes	información, datos, servicios, software, hardware, comunicaciones, recursos administrativos, recursos físicos y recursos humanos

Fase 2: Implementación y Operación

Esta fase tendrá como objetivo materializar de la implementación de los controles automatizables de seguridad informática y la descripción de los procedimientos utilizados durante la implementación y para la operación de las herramientas.

La implementación de los controles automatizados consiste en la instalación, configuración y personalización de aplicaciones que automaticen de manera parcial o completa los controles de seguridad informática definidos, y la complementación de las mismas a través de pequeños desarrollos en caso de ser necesario.

Esta fase propone la realización de tres actividades descritas a continuación:

- **Seleccionar herramientas de gestión**: Esta actividad responde a las tareas recogidas en el acápite 4.2.2 del estándar ISO/IEC 27001. Los objetivos a alcanzar son identificar, seleccionar e instalar las herramientas necesarias para la implantación de los controles definidos en la primera fase de esta metodología.
- **Realizar ajustes y configuraciones**: Luego de seleccionar e instalar los sistemas se procederá a la realización de ajustes y la configuración de los mismos. De ser necesario, se harán los pequeños desarrollos que tributen a este fin. Esta actividad debe generar un *manual de procedimientos* en el cual deben quedar claramente explicadas las acciones realizadas durante todo el proceso de instalación, configuración y desarrollo para cada herramienta de seguridad informática utilizada.
- **Operar los controles de seguridad informática**: Durante la operación de los controles de seguridad informática se deberán identificar y aplicar las métricas que posibilitarán la obtención de la información de los indicadores definidos por el modelo a partir de los datos existentes en el sistema. Esta información

referente a los indicadores deberá ser informada de manera periódica y oportuna a la dirección de la organización y a los especialistas que se encuentran a cargo de gestionar el SGSI.

Fase 3: Medición

Los controles implantados actúan disminuyendo la probabilidad o frecuencia de incidentes asociados a una amenaza y/o sobre el impacto que tiene la misma sobre un activo, reduciendo el daño o la degradación que sufre el mismo (CORTI, 2006).

La última fase de la metodología que se propone, consiste en comprobar la eficacia de los controles automatizados, medir la disminución de la degradación sufrida por los activos informáticos identificados en la organización y recalcular los valores de impacto y riesgo a que estos permanecen expuestos luego de la implementación de los controles. El objetivo principal es realizar el plan de acciones correctivas en caso de ser necesario, en correspondencia con las tareas recogidas en la sección 4.2.4 referente a la mantención y el mejoramiento del SGSI del estándar ISO/IEC 27001.

Las actividades definidas para esta fase consisten en:

- **Revaloración de impacto**: Dado un cierto conjunto de controles desplegados y una medida de la madurez de sus procesos de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que se ha modificado el impacto desde un valor potencial a un valor residual (MINHAP, 2012).
- **Revaloración de riesgo**: El riesgo residual es el nivel de riesgo en que queda el SGSI tras la implementación de los controles, y depende del impacto residual y la probabilidad de ocurrencia de las amenazas luego de haber implementado los controles automatizados.
- **Elaborar plan de acciones correctivas**: Los análisis de impacto y riesgo residuales contribuyen a entender la situación en que se encuentra la organización luego de haber aplicado los controles definidos. Según sus valores es posible identificar cuáles deben ser las acciones convenientes y dónde realizarlas para seguir trabajando en su disminución.

Resultados y discusión

La metodología fue aplicada en el sistema de información de la Facultad 4 de la Universidad de Ciencias Informáticas. Con el objetivo de probar su validez se realizó un experimento haciendo uso del método de post prueba con un grupo de control (GRAU, 1999), para lo que se determinaron diez controles automatizables a implementar en los SGSI de las facultades 4 y 5, tomando esta última facultad como grupo de control. Los valores de tiempo medio

Revista Cubana de Ciencias Informáticas
Vol. x, No. x, Mes x-y, 2013
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 14-26

de ejecución (TME) y tiempo medio de ejecución automatizado (TME-A) son valores que indican en horas (h) el tiempo que toma como promedio la ejecución de un control determinado. En aras de garantizar estricta homogeneidad entre ambos grupos el experimento se realizó en 120 computadoras ubicadas en los laboratorios docentes, 60 por cada facultad. Los trabajos se realizaron por un equipo conformado por 6 especialistas de los respectivos Departamentos de Tecnología de ambas facultades y se fijó como tiempo para el experimento un total de 24 horas hábiles, es decir tres días de trabajo.

Para la realización del cálculo de la complejidad del proceso se tuvo en cuenta como indicadores la cantidad de controles (CC), la cantidad de equipos sobres los cuales se trabajó (CE), el tiempo medio de ejecución del control (TME) y los especialistas que realizaron los controles (E). Básicamente, se entiende como complejidad de un control al esfuerzo necesario realizado por el equipo en ejecutar un control sobre una cantidad determinada de computadoras.

Definiendo la complejidad de un control como:

$$complejidad\ del\ control = \frac{TME \times CE}{E}$$

el cálculo de la complejidad del proceso es:

$$complejidad\ del\ proceso = \frac{\sum_{i=1}^{CC} complejidad\ del\ control_i}{CC}$$

La eficiencia de un control se definió como la razón entre el tiempo total disponible para la ejecución y el tiempo requerido real para la ejecución de un control sobre un número determinado de computadoras. En este caso los indicadores utilizados fueron la cantidad de controles (CC), la cantidad de equipos sobres los cuales se trabajó (CE), el tiempo medio de ejecución del control (TME) y el tiempo establecido para la realización del experimento (T), quedando los valores de eficiencia de un control y eficiencia del proceso como:

$$eficiencia\ del\ control = \frac{T}{TME \times CE}$$

y

$$eficiencia\ del\ proceso = \frac{\sum_{i=1}^{CC} eficiencia\ del\ control_i}{CC}$$

Los resultados obtenidos se encuentran expuestos en la Tabla 2 que se muestra a continuación.

Revista Cubana de Ciencias Informáticas
Vol. x, No. x, Mes x-y, 2013
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 14-26

Tabla 2. Resultados del cálculo de la complejidad y la eficiencia del proceso de gestión de la seguridad informática en los grupos G_1 y G_2

No.	**Control**	**TME G_1**	**TME G_2**	**Co. G_1**	**Co. G_2**	**Ef. G_1**	**Ef. G_2**
1	Inventario de dispositivos	0,33h	0,02h	6,6	0,02	0,51	8,33
2	Inventario de programas	0,17h	0,02h	3,4	0,02	0,98	8,33
3	Configuraciones seguras para hardware y software	0,42h	0,17h	8,4	3,4	0,4	0,98
4	Evaluación continua y remediación de vulnerabilidades	0,25h	0,02h	5	0,02	0,67	8,33
5	Defensas de malware	0,17h	0,01h	3,4	0,01	0,98	16,67
6	Seguridad de software de aplicación	0,05h	0,01h	1	0,01	3,33	16,67
7	Capacidad de recuperación de datos	0,08h	0,01h	1,6	0,01	2,08	16,67
8	Prevención de pérdida de datos	0,08h	0,01h	1,6	0,01	2,08	16,67
9	Respuesta y manejo de incidentes	0,5h	0,01h	10	0,01	0,33	16,67
10	Limitación y control de los puertos de red, protocolos y servicios	0,08h	0,01h	1,6	0,01	2,08	16,67
Total Proceso		**21,3h**	**0,19h**	**4,26**	**0,35**	**1,34**	**12,6**

Las observaciones realizadas durante el desarrollo del experimento confirman la disminución de la complejidad y el aumento de la eficiencia tras la implementación de la gestión automatizada de controles de seguridad informática, en ambos casos en un factor cercano al 90%.

Aunque se incluyen elementos importantes de las metodologías MAGERIT (MINHAP, 2012) y OCTAVE (DUQUE, 2014), la metodología propuesta está pensada para guiar el proceso de implementación de controles de seguridad informática en la UCI, por lo que se encuentra alineada con las disposiciones y regulaciones a las que se somete este centro. Los conceptos incluidos, fundamentalmente los relacionados con el análisis de riesgos, son los que se utilizan en las diferentes áreas de la UCI.

Entre las principales diferencias se puede mencionar la no inclusión del concepto de Riesgo Acumulado, que es consecuencia directa de las relaciones de dependencia que pueden existir entre diferentes activos. Se opta en la metodología propuesta por no definirlo ya que unos de los objetivos perseguidos es precisamente disminuir la complejidad. Este valor se puede obtener de forma implícita al determinar correctamente si una amenaza afecta directa o indirectamente a un activo y evaluar en la "Relación de activos informáticos y amenazas" los valores probabilidad de ocurrencia de la amenaza y degradación del activo.

Otro aporte importante es la metodología para la implementación de la gestión automatizada de controles de seguridad informática incluye, a diferencia de MAGERIT y OCTAVE, una fase completa dedicada a la implementación de controles. En dicha fase son propuestas una serie de actividades que contienen los mecanismos necesarios para la selección, configuración y operación de las herramientas que permiten la automatización de los controles que cumplen con la condición de ser automatizables.

Conclusiones

La metodología para implementar la gestión automatizada de controles de seguridad informática, es la combinación de varios métodos enfocados a la gestión de riesgos con un enfoque de automatización durante las etapas de operación, monitorización y revisión de un SGSI. Las tareas definidas en la fase de planificación, donde se incluye el análisis de riesgo como componente central, están destinadas a definir los objetivos de control para la determinación de controles automatizables. Otra consideración importante consiste en el carácter iterativo e incremental de la metodología, con el que el SGSI crece a medida que se culmina un ciclo tras haber implementado un nuevo control automatizado.

Teniendo en cuenta que aproximadamente el 30% de los controles contenidos en el estándar internacional ISO/IEC 27002 son automatizables, la aplicación del resultado de esta investigación será una excelente vía para lograr que la gestión de la seguridad informática sea un proceso menos complejo y más efectivo, puesto que libera a los especialistas a cargo de poco menos de un tercio del trabajo a realizar.

Los indicadores establecidos para el cálculo de la complejidad y la eficiencia del proceso de gestión de la seguridad informática que fueron utilizados para realizar el análisis estadístico finalmente confirman la disminución de la complejidad y el aumento de la eficiencia tras la implementación de controles automatizados de seguridad informática.

Referencias

CORTI, M. E.. Análisis y Automatización de la Implantación de SGSI en Empresas Uruguayas. Tesis Doctoral, Instituto de Computación - Facultad de Ingeniería - Universidad de la República, Montevideo, Uruguay, 2006.

CSIS. Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines v4.1. Center for Strategic and International Studies (CSIS). 2013.

DUQUE OCHOA, B. Metodologías de Gestión de Riesgos. Universidad de Caldas – Facultad de Ingeniería, Colombia. 2014. 24 p.

GRAU ABALO, R. et al. Metodología de la Investigación 2da Edición. Ibagué -Tolima, Colombia, 2004. 105 p.

ISO/IEC. ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). 2005.

ISO/IEC. ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management. 2005.

MEDINA LÓPEZ, F. Seguridad Informática - 1. Introducción a la Seguridad Informática [En línea]. Universidad Nacional Autónoma de México. 2011 [citado el 8 de mayo de 2015] 110 p. Disponible en: http://franciscomedina.net/seguridad/2012-1-Seguridad_Informatica_Tema1.pdf

MINHAP. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España, Ministerio de Hacienda y Administraciones Públicas, 2012. 127 p.

MONTESINO PERURENA, R. Modelo para la Gestión Automatizada e Integrada de Controles de Seguridad Informática. Tesis Doctoral, Universidad de las Ciencias Informáticas, La Habana, 2012.

NIST. NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology. 2013.

NIST. NIST SP 800-126: The Technical Specification for the Security Content Automation Protocol (SCAP). National Institute of Standards and Technology. 2009.

RUIZ LARROCHA, E. MISITILEON (Metodología que Integra Seguridad en ITIL Evolucionada y Orientada a la Normalización). Tesis Doctoral, Universidad Nacional de Educación a Distancia, Madrid, España, 2010.

SUBY, M. et al. The 2013 (ISC)2 Global Information Security Workforce Study. Frost & Sullivan, California, Estados Unidos, 2015. 46 p.

SYMANTEC. REPORTE NORTON 2013. [en línea]. SYMANTEC. 2014 [citado el 15 de enero de 2015] Disponible en: http://www.symantec.com/la/reportenorton

URIZARRI, L. Metodología de la investigación científica. Universidad de Ciencias Pedagógicas de Granma, Manzanillo. 2006.