RIELAC, Vol.XXXIV 1/2013 p.40-58 Enero - Abril ISSN: 1815-5928

RIELAC
Revista de Ingeniería Electrónica, Automática y Comunicaciones

Gestión automatizada e integrada de controles de seguridad informática

Raydel Montesino Perurena[1], Walter Baluja García[2], Joelsy Porvén Rubier[3]

[1]Universidad de las Ciencias Informáticas (UCI), raydelmp@uci.cu

[2] Instituto Superior Politécnico José Antonio Echeverría (CUJAE),Dr. C. Tec. walter@tesla.cujae.edu.cu

[1]Universidad de las Ciencias Informáticas (UCI), jporven@uci.cu

RESUMEN

En el presente trabajo se propone un modelo para la gestión automatizada e integrada de controles de seguridad informática, basado en sistemas de gestión de información y eventos de seguridad (SIEM), que posibilita aumentar la efectividad de los controles implementados y disminuir la complejidad de la gestión de la seguridad de la información. Se define el concepto de automatización en el contexto de la seguridad informática y se determinan los controles que pueden ser automatizados. Como parte de la investigación se seleccionan un grupo de indicadores que permiten medir de forma automatizada la efectividad de los controles, se propone además una guía para la aplicación del modelo propuesto y se describe una posible implementación del mismo utilizando el sistema SIEM de software libre OSSIM.

Palabras claves: gestión de la seguridad informática, automatización, SIEM, métricas.

ABSTRACT

In this paper we propose a SIEM-based model for the automated and integrated management of information security controls, in order to increase the effectiveness and reduce the complexity of information security management. The concept of automation is defined in this context and automatable controls are identified through this research. The model includes a group of security metrics for the measurement of security controls effectiveness in an automatic way. Furthermore we propose a guide for the implementation of the model and we describe a possible application scenario using OSSIM, a free software SIEM system.

Key words: information security management, automation, SIEM, metrics.

Automated and integrated management of information security controls.

INTRODUCCIÓN

En el mundo de hoy las empresas y organizaciones son completamente dependientes de la tecnología para llevar a cabo sus objetivos. Las informaciones críticas son almacenadas, procesadas y transmitidas en formato digital. En un entorno en que el desarrollo tecnológico ha posibilitado la conexión a Internet desde cualquier lugar y mediante múltiples dispositivos electrónicos, los sistemas informáticos se encuentran constantemente expuestos a múltiples amenazas.

Los diferentes ataques a los activos informáticos pueden provocar la pérdida de la disponibilidad, confidencialidad o integridad de la información; lo cual generalmente implica graves consecuencias para las empresas y en muchas ocasiones se ocasionan daños irreparables. Según datos estadísticos (1), las pérdidas promedio de las instituciones, debido a incidentes de seguridad informática, fueron de 234 mil dólares en el año 2009. Teniendo en cuenta además el crecimiento exponencial de los programas malignos, los cuales aumentan por decenas de miles diariamente (2)(3), las más de 8 mil nuevas vulnerabilidades de sistemas operativos y aplicaciones descubiertas anualmente (4)(5), y la organización cada vez más estructurada de los atacantes informáticos (6); es

evidente la necesidad de garantizar la seguridad informática de las instituciones, mediante un adecuado proceso de gestión de todas las medidas necesarias.

Los controles de seguridad informática a establecer son muchos y muy variados. El estándar ISO/IEC 27001 propone más de 130 controles que están relacionados con aplicaciones, dispositivos tecnológicos, recursos humanos y cuestiones organizativas. La gran cantidad y variedad de controles que es necesario implementar, en un entorno donde la tecnología evoluciona a una gran velocidad, hace que la gestión de la seguridad informática sea un proceso complejo, en el que hay que lograr una adecuada armonía entre tecnología, personas y procedimientos (7).

Una de las vías para lograr que la gestión de la seguridad informática sea un proceso menos complejo y más efectivo, en un entorno de constantes amenazas de seguridad, y teniendo en cuenta la gran cantidad de medidas a implementar; es la automatización de controles de seguridad informática. En las diferentes secciones del presente trabajo se analizan los conceptos de gestión de la seguridad informática y de automatización en este contexto, se valoran las investigaciones previas en esta temática, se estudian los sistemas SIEM y su potencial de automatización, y finalmente se propone un modelo para la gestión automatizada e integrada de controles de seguridad informática; así como una metodología para su aplicación y una posible implementación del mismo utilizando un sistema SIEM basado en software libre.

GESTIÓN DE LA SEGURIDAD INFORMÁTICA

La seguridad informática, o seguridad de la información, es la preservación de la confidencialidad, integridad y disponibilidad de la información. Esto se logra mediante la implantación de un grupo de controles que incluyen políticas, procedimientos, estructuras organizativas y sistemas de hardware y software (8). La seguridad de la información no es un estado que se alcanza en determinado instante de tiempo y permanece invariable, sino que es un proceso continuo que necesita ser gestionado. El proceso de gestión de la seguridad informática se encuentra descrito en el estándar ISO/IEC 27001, el cual constituye una norma certificable a nivel internacional. Esta norma ofrece un modelo para el diseño, implementación, operación, monitorización, revisión y mejora continua de un sistema de gestión de la seguridad de la información (SGSI). Se plantea la utilización del modelo PDCA (*Plan* - planificar, *Do* - hacer, *Check* – verificar, *Act* - actuar) para llevar a cabo estos objetivos, donde es necesario realizar las siguientes acciones en cada fase (8):

- Planificar: establecer las políticas, los objetivos, procesos y procedimientos de seguridad informática pertinentes para gestionar los riesgos y mejorar la seguridad de la información, en concordancia con las políticas y objetivos globales de la organización. En esta etapa se realiza el análisis de riesgos y se seleccionan los controles que garantizarán la seguridad informática.
- Hacer: implementar y operar las políticas, controles, procesos y procedimientos establecidos.
- Verificar: evaluar y medir el desempeño del sistema de seguridad informática contra las políticas y los objetivos de seguridad establecidos, así como revisar la experiencia práctica adquirida, reportando los resultados a la máxima dirección para su revisión.
- Actuar: emprender acciones correctivas y preventivas basadas en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del sistema de seguridad informática.

AUTOMATIZACIÓN DE CONTROLES DE SEGURIDAD INFORMÁTICA

El enfoque de procesos definido de manera global para la gestión de la seguridad informática, también se presenta al nivel de los controles de seguridad informática. De esta forma se puede afirmar que los controles de seguridad informática necesitan ser adecuadamente establecidos, implementados, operados, monitorizados, revisados, mantenidos y mejorados; para mantener un sistema de seguridad informática efectivo a lo largo del tiempo (9). Por tanto, gestionar los controles de seguridad informática implica realizar las siete acciones mencionadas.

¿Qué debería entenderse entonces por gestión automatizada de controles de seguridad informática?

Para poder definir este concepto es necesario referirse a la definición de automatización en general, que implica la operación, actuación o autorregulación independiente, sin intervención humana. La automatización involucra herramientas, máquinas, dispositivos, instalaciones y sistemas para realizar determinadas actividades sin que se produzca intervención humana en el transcurso de las mismas (10).

Atendiendo a los conceptos anteriores, en el presente trabajo se adoptará la siguiente definición:

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 o herramientas de hardware; sin que se produzca intervención humana en la realización de estas acciones.

Para ilustrar el concepto se pudiera tomar como ejemplo el control 10.5.1 de la guía de buenas prácticas ISO/IEC 27002: *respaldo de información*. Este control puede ser automatizado mediante un sistema informático que permita la realización de copias de respaldo de forma programada. Una vez que se define el horario de los respaldos, el tipo de respaldo y la información a respaldar; el proceso transcurre de forma automática, sin intervención humana en el mismo. El propio sistema monitorea la realización de los respaldos y notifica ante la ocurrencia de cualquier problema.

Es necesario señalar que la definición anterior acota el proceso de automatización a la operación, monitorización y revisión de los controles de seguridad informática, debido a que se considera que las acciones de establecimiento, implementación, mantenimiento y mejora de los controles no son completamente automatizables de acuerdo a las prácticas y condiciones tecnológicas actuales.

Evidentemente los controles automatizables son aquellos que están más relacionados con medios técnicos, los cuales pueden ser implementados mediante sistemas informáticos o herramientas de hardware. Los controles relacionados con los recursos humanos o cuestiones organizativas no pueden ser automatizados porque requieren de la intervención de personas en el proceso. Como ejemplos de controles que no son automatizables se pueden mencionar los siguientes:

ISO/IEC 27002 - 5.1.1: *Documento de políticas de seguridad de la información*. Este control implica la elaboración, aprobación, publicación y comunicación a todos los trabajadores, de un documento con las políticas de seguridad informática (9).

ISO/IEC 27002 - 8.2.2: *Concientización, educación y formación en seguridad de la información*. Este control implica que los trabajadores de la organización deben recibir una formación adecuada en temas relacionados con la seguridad informática y actualizaciones regulares en políticas y procedimientos organizacionales, relevantes para su función laboral (9).

Controles de seguridad informática que pueden ser automatizados

La seguridad informática como concepto ha venido evolucionando a lo largo del tiempo. Inicialmente fue una disciplina dominada por la élite de los profesionales especializados en el tema, dejando generalmente fuera al individuo e incluso a la organización. Desde comienzos del presente siglo se propone una visión más abarcadora de la seguridad de la información, que vincula de manera formal elementos como la tecnología, el individuo y la organización, enfatizando en el estudio de éstos y sus relaciones, para repensar la seguridad informática más allá de la experiencia tecnológica tradicional (11).

A partir de los diferentes enfoques existentes con respecto al papel de la tecnología y los seres humanos en la preservación de la seguridad de la información, es muy importante determinar entonces hasta dónde es posible automatizar los controles de seguridad informática. En (12) se realiza un análisis sobre los límites de la automatización en la configuración de políticas y la toma de decisiones de los usuarios finales. En esa investigación los autores afirman que aunque la automatización pudiera conllevar a la obtención de un sistema más seguro, existen límites en este sentido, basados en factores sociales y humanos. Sin embargo, en ese trabajo solo se consideran los controles de seguridad relacionados con los usuarios finales, y no se analizan el resto de los controles de seguridad informática.

De acuerdo a un estudio realizado por un gran número de expertos de seguridad que fue publicado bajo el título "*Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines*" (CAG) (13), existen 20 controles técnicos que son críticos e indispensables en un sistema de seguridad informática. La selección de los controles está basada en los ataques informáticos que se producen con mayor frecuencia actualmente. Un aspecto importante de ese estudio es que se propone un número relativamente pequeño de controles, permitiendo que los responsables de la gestión de la seguridad informática se concentren en los controles más críticos. Se plantea además que 15 de esos controles pueden ser operados y monitoreados automáticamente, utilizando varias herramientas de seguridad existentes.

Sin embargo, a pesar de que esa publicación ofrece una visión general de controles automatizables, solo se toman en consideración los controles críticos, ignorando controles que no se consideran críticos y otros controles de seguridad física que también admiten determinado nivel de automatización. Otro aspecto a señalar es que la automatización de los 15 controles es vista de manera independiente, sin tener en cuenta una visión integradora del proceso de gestión de la seguridad informática. Esto puede apreciarse en la propuesta que se realiza en el sitio web del instituto SANS (14), sobre los posibles sistemas y aplicaciones que implementan los controles propuestos, donde se mencionan 28 herramientas de diferentes desarrolladores, todas con sistemas de administración y gestión independientes. En la mejor de las combinaciones es necesario utilizar 10 sistemas diferentes para la implementación de los 15 controles automatizables.

Un análisis más integrador fue realizado por uno de los autores del presente trabajo en (15), donde se valoran todos los controles de seguridad informática especificados en los estándares ISO/IEC 27002 (9) y NIST SP 800-53 (16), llegando a la conclusión de

que el 30% de los controles pueden ser automatizados. En la Figura 1 se muestran los resultados del análisis para el estándar NIST SP 800-53, especificando el porciento de controles automatizables en cada dominio de seguridad.

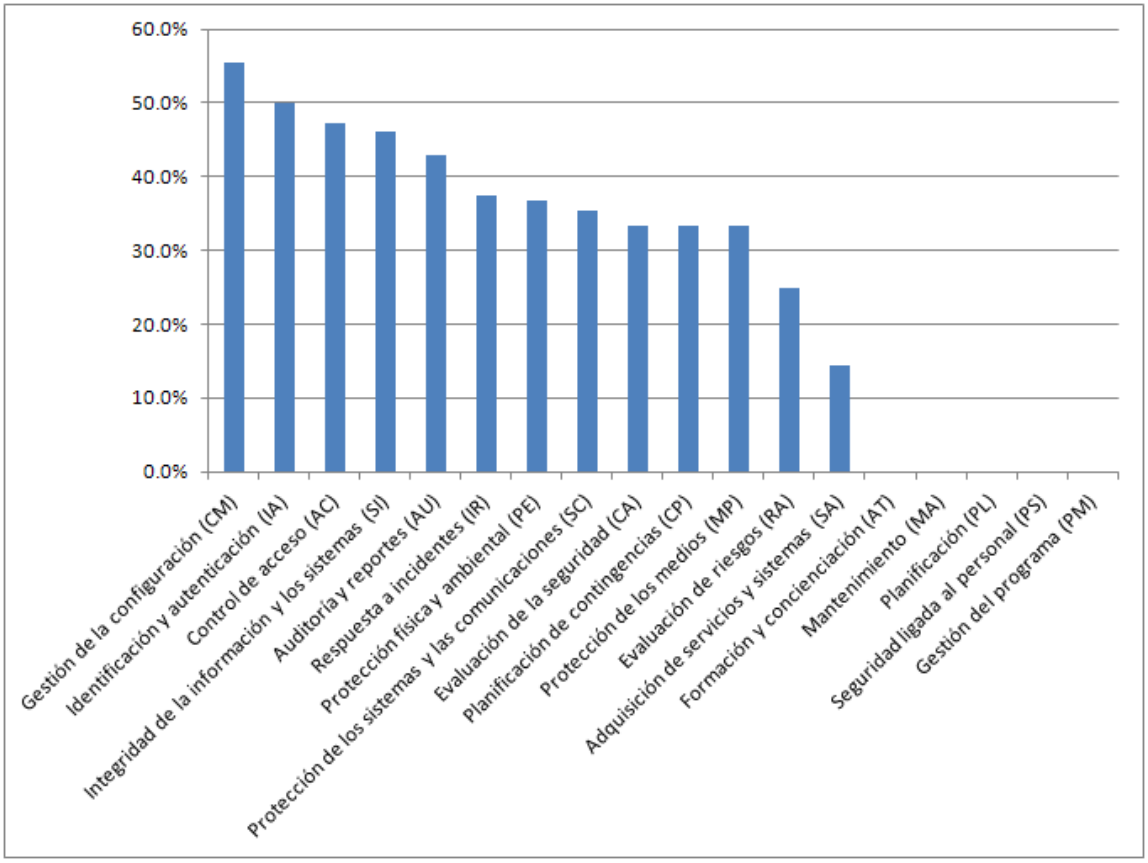

Figura 1: Porciento de controles automatizables en cada dominio de NIST SP 800-53

Trabajos previos relacionados con la automatización de la seguridad informática

En el campo de la seguridad informática existen pocas investigaciones que abordan la temática de la automatización. La mayoría de los estudios académicos enfoca el tema desde una perspectiva puntual, refiriéndose a la automatización de controles específicos de seguridad informática. De esta manera se aprecian trabajos dirigidos a la automatización en la implementación de políticas de seguridad informática (17)(18)(19), en la gestión de vulnerabilidades (20)(21)(22), en el chequeo del cumplimiento de regulaciones (23) y en la gestión de configuraciones (24).

En el campo de la gestión de redes en general, se aprecia un gran avance en la temática de la automatización, donde incluso se utiliza el término "gestión autonómica" para describir el proceso de auto-gestión en los dispositivos, protocolos y servicios de red; de forma tal que el sistema pueda recuperarse automáticamente ante fallas y adaptarse a nuevas situaciones (25).

Sin embargo, en el campo de la gestión de la seguridad informática pocas investigaciones y estudios abordan la temática de la automatización con una visión integral, analizando el amplio espectro de controles de seguridad recomendados por estándares internacionales. El trabajo que resulta un poco más abarcador en este sentido es SCAP (*Protocolo de Automatización de Contenido de Seguridad*, por sus siglas en inglés) (26), desarrollado por el Instituto Nacional de Estándares y Tecnologías de Estados Unidos (NIST). SCAP fue creado para proveer una forma estandarizada de gestionar la seguridad de los sistemas informáticos, sin embargo su alcance es todavía limitado. Analizando la propia definición de los componentes de SCAP puede concluirse que este posee aplicación solamente en los controles relacionados con la verificación automática de parches y vulnerabilidades, el chequeo de las configuraciones de seguridad y el inventario de activos informáticos.

Un ejemplo real de la utilización de SCAP es una guía emitida por el gobierno de Estados Unidos, denominada *Federal Desktop Core Configuration (FDCC)* (27), con el objetivo de definir una configuración de seguridad homogénea para todas las

computadoras con sistemas operativos Microsoft Windows XP y Vista, empleadas en las organizaciones federales norteamericanas. Estas guías están escritas en XCCDF y OVAL, utilizando dentro de ellas enumeraciones CPE y CCE.

Otro ejemplo ilustrativo de la aplicación práctica que tiene en estos momentos SCAP es la publicación de más de 40 listas de chequeo de configuraciones de seguridad por parte del Centro para la Seguridad de Internet (CIS) (28). En este sitio se pueden encontrar guías escritas en XCCDF para evaluar la seguridad de las aplicaciones y los sistemas operativos más utilizados, entre los que se encuentran servidores Web (Apache, IIS), sistemas de gestión de bases de datos (MSSQL, MySQL), equipos de redes (Cisco, Checkpoint), entre otros.

Pero como ocurre en todo proceso de estandarización, la adopción de SCAP es lenta y requiere de su incorporación por los diferentes desarrolladores de sistemas. Teniendo en cuenta su alcance limitado y lentitud de adopción es necesario encontrar otra alternativa para lograr el propósito de la automatización e integración en la gestión de controles de seguridad informática.

SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

En esta sección se valorarán los sistemas de gestión de información y eventos de seguridad (SIEM) con el objetivo de analizar sus posibilidades de automatización de algunos controles y de integración de diferentes herramientas de seguridad.

Los sistemas SIEM son utilizados para analizar eventos de seguridad informática en tiempo real y para recolectar y almacenar trazas de seguridad, permitiendo el análisis forense de incidentes y el cumplimiento de lo establecido en las regulaciones existentes. Estos sistemas poseen dos funciones principales (29):

- Gestión de información de seguridad (SIM): esta función esta relacionada con la gestión de trazas y el reporte del cumplimiento de regulaciones. Mediante esta funcionalidad se garantiza la recolección, reportes y análisis de trazas de seguridad. Las fuentes de los datos recolectados pueden ser aplicaciones, sistemas operativos, herramientas de seguridad y dispositivos de la red.
- Gestión de eventos de seguridad (SEM): esta función está relacionada con la monitorización de eventos en tiempo real y la gestión de incidentes de seguridad informática. Mediante esta funcionalidad se procesan en tiempo real las trazas recolectadas de las diferentes herramientas de seguridad, dispositivos de red, aplicaciones y sistemas operativos; con el objetivo de garantizar la monitorización de los sistemas, la correlación de eventos de seguridad y la respuesta a incidentes.

Los sistemas SIEM actúan como un repositorio central para las trazas generadas por las diferentes herramientas y permiten seleccionar, a través de reglas lógicas, los eventos de seguridad informática que interesan (30). Las trazas de los diferentes sistemas, aplicaciones, herramientas y dispositivos pueden ser recolectadas mediante los siguientes métodos (29):

- Recepción de una cadena de datos en formato *syslog* proveniente de la fuente de datos.
- Aplicaciones agentes instaladas directamente en los dispositivos a monitorear.
- Invocación de la interfaz de línea de comandos de los sistemas monitoreados.
- Interfaces de programación de aplicaciones (API) provistas por los desarrolladores de los sistemas monitoreados.

Una vez que las trazas de los diferentes sistemas son obtenidas por cualquiera de los métodos anteriores, estas deben ser normalizadas para ser almacenadas en un formato único dentro del sistema SIEM. Esta función se realiza mediante conectores o *plugins* que proveen los desarrolladores de sistemas SIEM, para interpretar y normalizar los datos contenidos en las trazas de las diferentes herramientas monitoreadas. Generalmente los sistemas SIEM traen incluidos varios conectores que permiten interpretar los datos de diferentes aplicaciones, sistemas operativos, dispositivos de red y herramientas de seguridad; y además brindan la posibilidad de definir nuevos conectores que no vienen incluidos por defecto en la solución.

La información de seguridad normalizada es entonces correlacionada para establecer relaciones entre eventos generados en diferentes instantes de tiempo y por distintos dispositivos. Esto permite la reducción de falsos positivos generados por sistemas como los IDS, y la generación de alarmas significativas que tienen en cuenta el contexto de la organización, analizando en todo momento la importancia de los activos que están siendo víctimas de un ataque informático.

Otra de las funciones elementales de todos los sistemas SIEM es el almacenamiento y preservación de las trazas de seguridad. Esto se realiza con el propósito de esclarecer los incidentes de seguridad, realizar búsquedas de información en diferentes momentos y cumplir con lo establecido en las regulaciones existentes. Generalmente los sistemas SIEM almacenan los eventos más recientes en una base de datos y pasado determinado tiempo, configurable en la aplicación, las trazas son movidas a ficheros donde permanecen por el tiempo establecido (30).

Finalmente los sistemas SIEM poseen un módulo de reportes que provee información útil a los especialistas de seguridad informática y directivos de la organización. Son reportados en tiempo real los eventos y alarmas significativos que están teniendo

lugar, analizando estos datos en el contexto de la organización y evaluando el estado de la seguridad a partir de los ataques identificados. Los sistemas SIEM permiten personalizar los reportes y generar los mismos a partir de los datos coleccionados de las diferentes herramientas de seguridad.

De acuerdo a un estudio de la consultora Gartner (31), el mercado de los sistemas SIEM se considera maduro y muy competitivo, encontrándose en una fase de adopción amplia donde múltiples desarrolladores de SIEM ofrecen las funciones básicas de gestión de trazas, monitorización de eventos y cumplimiento de regulaciones. En dicho estudio se analizan los principales productos SIEM, los cuales son ubicados en diferentes cuadrantes según las características que poseen, sus capacidades y los ingresos de las compañías que los desarrollan. Es importante señalar que prácticamente todos los productos SIEM son sistemas propietarios. El único que está basado en una solución de software libre es AlienVault, el cual es la versión propietaria del sistema OSSIM (*Open Source Security Information Management*), desarrollado bajo licencia GPL.

A pesar de la evolución de los sistemas SIEM, la conocida encuesta anual del Instituto de Seguridad de Computadoras (CSI) no considera los sistemas SIEM entre las tecnologías de seguridad a implementar por las organizaciones, y solo el 46.2% de los que responden la encuesta utiliza software para la gestión de trazas (32). Por otra parte, la encuesta del instituto SANS sobre gestión de logs muestra que las tres principales razones para recolectar trazas y utilizar sistemas SIEM son: detectar incidentes, analizar lo que ha sucedido mediante análisis forense, y cumplir con las regulaciones establecidas (33).

En otros trabajos consultados se ofrece una visión un poco más amplia del uso que puede hacerse de los sistemas SIEM, donde se incluyen capacidades adicionales como el seguimiento de la actividad de los usuarios, la protección contra programas malignos y la respuesta a incidentes (34) (31). Sin embargo, la utilización de los sistemas SIEM en la práctica está por debajo de las posibilidades que esta tecnología permite, especialmente para la gestión integrada de herramientas de seguridad informática y la automatización de un grupo de tareas. En la siguiente sección se propone realizar un uso de los sistemas SIEM mucho más abarcador del que normalmente tienen este tipo de sistemas.

MODELO PARA LA GESTIÓN AUTOMATIZADA E INTEGRADA DE CONTROLES DE SEGURIDAD INFORMÁTICA

Con el objetivo de lograr una gestión automatizada e integrada de controles de seguridad informática, en el presente trabajo se propone el desarrollo de un modelo basado en los siguientes principios:

1. Automatización: se deben tener en cuenta todos los controles de seguridad informática automatizables.
2. Integración: la gestión de los controles de seguridad informática debe realizarse desde un sistema centralizado que permita la monitorización y la revisión de los mismos.
3. Síntesis: debe realizarse un adecuado proceso de agrupación y síntesis de los controles automatizables para gestionar un número relativamente pequeño de controles.
4. Medición objetiva: se debe medir la efectividad de los controles mediante indicadores objetivos obtenidos de forma automática a partir de los datos suministrados por las diferentes herramientas de seguridad informática.
5. Mejora continua: la gestión de los controles debe verse como un proceso dinámico que consta de varias acciones, las cuales conforman un ciclo cerrado para la mejora continua de los controles de seguridad informática.
6. Generalidad: el modelo debe ser aplicable en una gran variedad de organizaciones.

Teniendo en cuenta los principios mencionados, el concepto de automatización definido previamente, los controles de seguridad informática identificados como automatizables y el potencial de automatización de los sistemas SIEM; se propone el modelo mostrado en la Figura 2 para la gestión automatizada e integrada de controles de seguridad informática (GAISI).

El modelo propuesto posee las siguientes características generales:

- Se definen 10 macro-controles de seguridad informática que deberán ser automatizados para la protección de las tecnologías de la información de la organización.
- La automatización es aplicada a las acciones de operación, monitorización y revisión de los 10 macro-controles de seguridad informática.

- El sistema SIEM es el componente central del modelo, permitiendo la integración de diferentes herramientas de seguridad informática, el seguimiento centralizado de los controles, la correlación de información y la generación de reportes de seguridad de forma automatizada.
- Los controles de seguridad informática son implementados y operados por diferentes sistemas, pero su monitorización se realiza de forma centralizada en el sistema SIEM.
- La revisión de los controles se realiza mediante un grupo de indicadores de seguridad informática, definidos también como parte del modelo, que son calculados y reportados de forma automatizada.
- El sistema SIEM recibe la información de los controles de seguridad informática mediante las trazas de los diferentes sistemas que implementan los mismos, para lo cual es necesario definir conectores que permitan interpretar los diferentes formatos de trazas existentes.

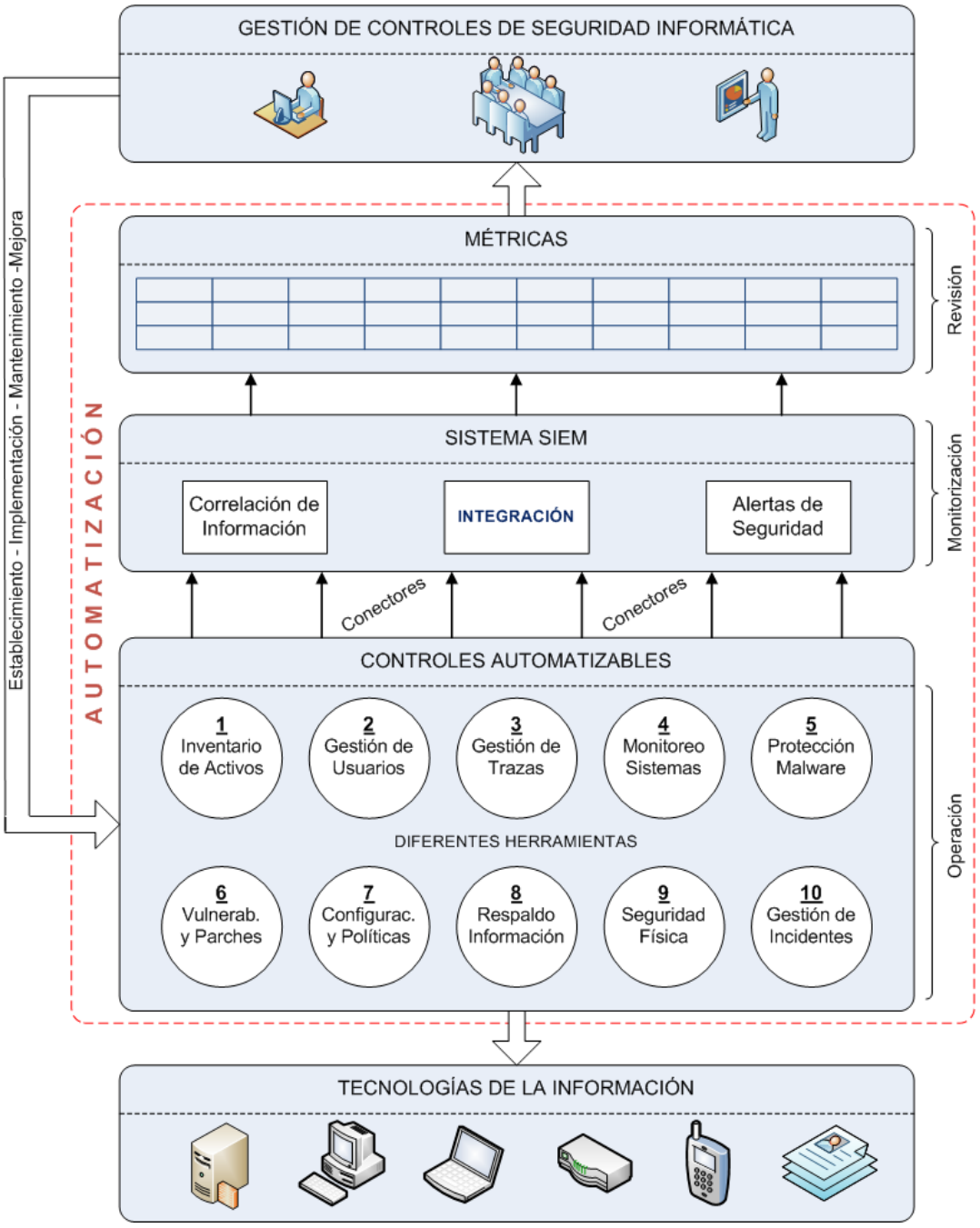

Figura 2: Modelo para la gestión automatizada e integrada de controles de seguridad informática

El modelo propuesto constituye una extensión de un marco de trabajo propuesto por los autores en (35), a partir de la incorporación de la actividad de revisión de los controles mediante un grupo de métricas seleccionadas y definidas en el presente trabajo. A continuación se mencionan los objetivos a lograr mediante la automatización de cada uno de los 10 macro-controles. Una descripción más detallada de los macro-controles y su interacción con el sistema SIEM puede encontrarse en el artículo referenciado previamente.

1. Inventario de activos: mantener un inventario actualizado de todos los activos informáticos de la institución, tanto de hardware como de software, identificando cualquier desviación fuera de lo establecido.

2. Gestión de usuarios: garantizar la correcta activación, modificación y eliminación de cuentas de usuarios de las tecnologías de la información.
3. Gestión de trazas: almacenar y conservar por el tiempo establecido, en una localización centralizada, las trazas de las aplicaciones, sistemas operativos y diferentes dispositivos; donde se registre la actividad de los usuarios, errores, conexiones de red y otros eventos de seguridad en general.
4. Monitoreo de los sistemas: realizar un monitoreo constante de los sistemas para detectar ataques informáticos, falta de disponibilidad de las aplicaciones, y modificaciones a la información.
5. Protección contra programas malignos: emplear mecanismos de protección contra programas malignos que se encuentren constantemente actualizados, para detectar y erradicar código malicioso.
6. Detección de vulnerabilidades y gestión de parches: detectar y mitigar las vulnerabilidades presentes en los sistemas, así como garantizar la aplicación de los parches necesarios para todos los sistemas operativos y aplicaciones de la institución.
7. Configuraciones de seguridad y cumplimiento de políticas: garantizar que los sistemas operativos, aplicaciones y demás dispositivos posean configuraciones seguras, acorde a las políticas definidas por la institución, las regulaciones establecidas y referentes internacionales.
8. Respaldo de información: realizar frecuentemente copias de respaldo de la información y los sistemas, que posibiliten la recuperación ante la ocurrencia de algún incidente.
9. Seguridad física: proteger adecuadamente los locales y las tecnologías mediante sistemas de control de acceso físico, respaldo eléctrico, control de humedad y clima, protección contra incendios y sistemas de alarmas contra intrusos.
10. Gestión de incidentes: establecer un sistema de gestión de incidentes de seguridad informática que incluya la detección, análisis, contención, solución y recuperación de los incidentes.

Los 10 macro-controles representan una agrupación y síntesis de los controles automatizables identificados en los estándares internacionales. La agrupación se realiza a partir de los controles que abordan aspectos similares y la síntesis sobre la base de los aspectos esenciales de los controles automatizables. Mediante la Tabla 1 se establece una relación entre los 10 macro-controles del modelo GAISI y los controles de ISO/IEC 27002, NIST SP 800-53, CAG y la Resolución 127/2007 del Ministerio de la Informática y las Comunicaciones de Cuba, que constituye el Reglamento de Seguridad para las Tecnologías de la Información en el país.

Tabla 1: Relación entre los 10 macro-controles del modelo GAISI y los controles de diferentes estándares y regulaciones

No.	Macro-control	Controles relacionados			
		ISO/IEC 27001	NIST SP 800-53	CAG	Res 127
1	Inventario de activos	7.1.1, 10.1.2, 11.4.3	AC-18, CM-8, SA-7	1, 2, 14	14, 36, 41, 43, 64
2	Gestión de usuarios	8.3.3, 11.2.2, 11.2.3, 11.3.2, 11.4.2, 11.4.6, 11.5.1, 11.5.2, 11.5.3, 11.5.5, 11.5.6, 12.3.2	AC-2, AC-7, AC-9, AC-10, AC-11, AC-17, AU-14, IA-2, IA-3, IA-5, IA-7, SC-17, SC-12, SC-23	8, 9, 11	23, 45, 46, 47
3	Gestión de trazas	10.10.1, 10.10.3, 10.10.4, 10.10.5, 10.10.6	AU-6, AU-7, AU-8, AU-11, AU-12, PE-8	6	58
4	Monitoreo de los sistemas	10.3.1, 10.6.1, 10.7.1, 10.7.4, 10.8.4, 10.9.3, 10.10.2, 10.10.4, 11.4.6, 11.4.7, 12.4.3, 12.5.3	AC-8, AC-21, AU-6, AU-14, CA-7, CM-3, CM-5, IR-5, MP-2, PE-6, SA-10, SC-5, SC-7, SC-14, SI-4, SI-5, SI-7, SI-13	6, 8, 13, 15	21, 57, 66, 70, 74, 79, 81
5	Protección contra programas malignos	10.4.1, 10.8.4	SI-3, SI-8	12	50
6	Detección de vulnerabilidades y gestión de parches	11.4.4, 12.6.1	RA-5, SC-14, SI-2	7, 10	43, 44, 67
7	Configuraciones de seguridad y cumplimiento de políticas	10.1.2, 10.6.1, 11.4.4, 11.4.6, 11.4.7, 15.2.2	CA-2, CM-2, CM-3, CM-6, SA-10, SC-7, SC-14	3, 4	57, 58, 60, 96
8	Respaldo de información	10.5.1, 14.1.3	CP-6, CP-7, CP-9	19	53, 56
9	Seguridad física	9.1.2, 9.2.2	PE-3, PE-11, PE-12, PE-13, PE-14	-	23, 30, 32, 36
10	Gestión de incidents	13.1.1	IR-4, IR-5, IR-6	18	86,89

Métricas de seguridad informática

De acuerdo a la definición de automatización de controles de seguridad informática presentada en este trabajo, es posible automatizar también la revisión de los controles de seguridad informática. Para lograr este propósito es necesario definir un grupo de indicadores y métricas que permitan evaluar continuamente la efectividad de los controles.

El tema de las métricas de seguridad informática ha sido bastante tratado en la literatura del presente siglo, pero todavía se encuentra en investigación. La falta de consenso sobre métricas de seguridad informática está relacionada con el hecho de que esta temática impacta directamente en el prestigio de las empresas e instituciones, las cuales prefieren no ofrecer datos públicos sobre los incidentes de seguridad informática (36). A pesar de que no existe un consenso sobre las métricas a utilizar, sí existen varias guías y estándares, como el ISO/IEC 27004 (37) y el NIST SP 800-55 (38), que explican cómo llevar a cabo un programa de medición en seguridad informática. Desde el punto de vista práctico, el Centro para la Seguridad de Internet (CIS) ha tratado de establecer un grupo de métricas de seguridad mediante el consenso de un equipo de 150 expertos (39). Otros trabajos que abordan el tema de las métricas de seguridad informática son (40)(41)(36) y (42).

En el presente trabajo se seleccionan algunas métricas propuestas por los autores referenciados y se proponen otras, las cuales en su conjunto pueden ser obtenidas de forma automatizada. En el sistema SIEM se deberán mostrar reportes, actualizados en tiempo real, con las métricas de seguridad informática que se definen en la Tabla 2. El hecho de que el sistema SIEM centralice la información de las diferentes herramientas de seguridad, posibilita el cálculo automático de todos los indicadores propuestos.

Tabla 2: Métricas de seguridad informática para medir la efectividad de los 10 macro- controles del modelo

No.	Macro-control	ID	Indicador	Origen de los datos
1	Inventario de activos	1.1	Cantidad de equipos desconocidos conectados a la red	Sistema de inventario de activos Sistema de escaneo de red
		1.2	Porciento de equipos con software no autorizado	Sistema de inventario de activos Política de software autorizado
2	Gestión de usuarios	2.1	Cantidad de cuentas de usuario que no pueden ser asociadas con algún proceso o área de la institución	Directorio LDAP Base de datos de recursos humanos
		2.2	Cantidad de cuentas de usuario que permanecen activas sin ser usadas por más de 30 días.	Directorio LDAP
3	Gestión de trazas	3.1	Porciento de sistemas que almacenan trazas de seguridad en un servidor centralizado (36)	Sistema de almacenamiento de trazas Sistema de inventario de activos
		3.2	Tiempo de conservación de las trazas	Sistema de almacenamiento de trazas
4	Monitoreo de los sistemas	4.1	Cantidad de intentos de ataques (por hora) a la DMZ	Sistema de detección de intrusos de red
		4.2	Porciento del tiempo en que los sistemas críticos se encuentran disponibles (36)	Sistema de monitoreo de disponibilidad Resultados del análisis de riesgos
5	Protección contra programas malignos	5.1	Porciento de equipos con el antivirus autorizado instalado	Sistema de inventario de activos Kit de administración del sistema antivirus
		5.2	Porciento de equipos con el antivirus desactualizado	Kit de administración del sistema antivirus
6	Detección de vulnerabilidades y gestión de parches	6.1	Cantidad de vulnerabilidades críticas detectadas (38)	Sistema de escaneo de vulnerabilidades
		6.2	Porciento de equipos con vulnerabilidades críticas (39)	Sistema de escaneo de vulnerabilidades
		6.3	Tiempo medio de mitigación de vulnerabilidades (39)	Sistema de escaneo de vulnerabilidades
		6.4	Porciento de equipos con parches de seguridad críticos pendientes de instalación(38)	Sistema de gestión de parches
		6.5	Tiempo medio de aplicación de los parches de seguridad (desde su publicación hasta la instalación) (39)	Sistema de gestión de parches
7	Configuraciones de seguridad y cumplimiento de políticas	7.1	Porciento de equipos acorde con la imagen y configuraciones de seguridad definidas (39)(36)	Sistema de inventario de activos Sistema de chequeo de configuraciones
		7.2	Puntuación (*benchmark*) de seguridad promedio de acuerdo a patrones internacionales (36)	Sistema de chequeo de configuraciones
8	Respaldo de información	8.1	Porciento de sistemas críticos respaldados	Sistema de copias de respaldo Resultados del análisis de riesgos
		8.2	Última fecha en la que todos los respaldos se realizaron de forma exitosa	Sistema de copias de respaldo
9	Seguridad física	9.1	Temperatura promedio de operación de los sistemas	Sistema de monitoreo
		9.2	Cantidad de fallos de corriente (por semana)	Sistema de gestión de la UPS
10	Gestión de incidentes	10.1	Cantidad de incidentes de seguridad informática (por semana) (39)(37)(38)	Sistema de gestión de incidentes
		10.2	Tiempo medio de detección de incidentes (desde que ocurrió hasta su registro en el sistema) (39)	Sistema de gestión de incidentes
		10.3	Tiempo medio de solución de incidentes (a partir de que son reportados) (39)	Sistema de gestión de incidentes

Las métricas especificadas permitirán revisar la efectividad de los de los 10 macro-controles de seguridad informática propuestos en el modelo. Estas deberán ser analizadas por los especialistas de seguridad informática para que sean tomadas las acciones de corrección necesarias. Las diferentes organizaciones deberán establecer criterios de medida para cada métrica en dependencia de los objetivos de seguridad, lo cual permitirá evaluar continuamente el estado de los controles establecidos. Es importante señalar que en la Tabla 2 solo se definen métricas que pueden ser calculadas de forma automatizada a través del modelo propuesto. Seguramente será posible definir otros indicadores de efectividad donde el cálculo de los mismos no sea posible realizarlo de forma automatizada. La lista propuesta no es exhaustiva, puede enriquecerse con más indicadores que las diferentes instituciones consideren necesario incorporar. No obstante, el listado de los indicadores definidos en este trabajo pudiera constituir una referencia para la medición de la efectividad de los controles de seguridad informática incluidos en el modelo GAISI.

Consideraciones generales sobre el modelo

En el modelo propuesto se ofrece una visión integral de la automatización de controles de seguridad informática, considerando todos los posibles controles automatizables y definiendo las acciones a realizar de forma automática en cada uno de los casos. El modelo propone además una utilización de los sistemas SIEM que va más allá del uso que normalmente tienen este tipo de sistemas, destinados comúnmente a la gestión de trazas y detección de eventos de seguridad. Esto presupone que se debe realizar un proceso profundo de personalización y adaptación del sistema SIEM utilizado, para aplicar el modelo propuesto, mediante la definición de conectores, políticas, reglas de correlación y reportes de seguridad informática.

Es importante señalar que mediante la aplicación del modelo se automatiza la operación, monitorización y revisión de un grupo de controles de seguridad informática, representado con línea de puntos rojos en la Figura 2; lo cual representa una parte del proceso de gestión de seguridad informática en todo su conjunto. No debe interpretarse que el modelo resuelve todos los problemas de forma automática. Para una adecuada gestión de la seguridad de la información es necesario implementar el resto de los controles propuestos por guías y estándares internacionales, que no son contemplados en este modelo. Además el modelo solo aborda una parte del ciclo PDCA, específicamente las fases de **hacer** y **verificar**, por lo que será necesario completar el ciclo de gestión incluso para los controles automatizados.

APLICACIÓN DEL MODELO PROPUESTO

Para la implementación del modelo propuesto se propone la guía de seis pasos que se explica a continuación:

1. Elección e instalación del sistema SIEM: el primer paso es elegir e instalar, con una configuración básica, el sistema de gestión de eventos e información de seguridad, el cual constituye el componente central del modelo. En dependencia de las características del sistema SIEM elegido será necesario tomar otras decisiones en la implementación. En la Tabla 3 se mencionan los sistemas SIEM líderes en el mercado y en el estudio realizado por la consultora Gartner (31) se detallan las fortalezas y debilidades de cada uno. Se incluye el sistema AlienVault, a pesar de no estar en el cuadrante líder, por ser el único basado en un proyecto de software libre, lo cual puede ser un elemento importante para seleccionar el sistema.
2. Identificación de los macro-controles incluidos en el sistema SIEM: será necesario identificar posteriormente los macro-controles del modelo que están de alguna manera incluidos en el sistema SIEM elegido. En la Tabla 3 se muestran los macro-controles del modelo que son parcialmente (P) o completamente (C) implementados por los principales sistemas SIEM existentes. Como puede apreciarse, los controles 3 y 10 se encuentran completamente implementados en todos los sistemas SIEM; mientras que los controles 4 y 7 están parcialmente implementados, en mayor o menor medida, en todas las soluciones.

Tabla 3: Macro-controles incluidos en diferentes sistemas SIEM

Sistemas SIEM	Macro-controles									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
HP/ArcSight – *ESM* (43)		P	C	P			P			C
Q1 Labs – *Qradar* (44)	P		C	P			P			C
RSA (EMC) – *envision* (45)			C	P			P			C
Symantec – *SSIM* (46)			C	P		P	P			C
LogLogic – *SEM* (47)			C	P			P			C
NitroSecurity - *NitroView ESM* (48)			C	C			P			C
Novell – *Sentinel* (49)		P	C	P			P			C
AlienVault – *Unified SIEM* (50)	C		C	C		P	P			C

3. Elección, instalación y configuración de otros sistemas: después de seleccionado el sistema SIEM y de haber identificado los macro-controles que incluye, es necesario seleccionar, instalar y configurar los otros sistemas que implementan el resto de los controles propuestos en el modelo. Los sistemas a elegir deberán tener un módulo de administración centralizado, diseñado para entornos empresariales. Se configurarán las diferentes herramientas para que la operación de los controles de seguridad se realice de forma automatizada, tal y como se define en el modelo, para cada uno de los 10 macro-controles.
4. Comunicación entre el sistema SIEM y el resto de los sistemas: la monitorización y la supervisión de los controles de seguridad deberán realizarse centralizadamente desde el sistema SIEM. Por tanto es necesario garantizar que la información suministrada por todas las herramientas de seguridad llegue al sistema SIEM, lo cual puede lograrse por cualquiera de los métodos expuestos en la sección que describe el funcionamiento de este tipo de sistemas. Posteriormente deberán definirse los conectores necesarios para interpretar y normalizar los datos contenidos en las trazas de las diferentes herramientas monitoreadas. Los sistemas SIEM traen incluidos varios conectores por defecto que permiten interpretar los datos de diferentes sistemas, y además brindan la posibilidad de definir nuevos conectores que no vienen incluidos en la solución.
5. Configuración y personalización del sistema SIEM: el sistema SIEM deberá ser adecuadamente configurado para ajustarlo a las características de la organización y al modelo propuesto. Esto implica la realización de las siguientes acciones:
    a. *Definición del contexto de la organización*: será necesario definir en el sistema SIEM la importancia de los diferentes activos de la organización, fundamentalmente de los sistemas críticos, para que el propio sistema SIEM sea capaz de diferenciar los niveles de prioridad de los eventos de seguridad informática detectados, en dependencia de los activos involucrados en esos eventos.
    b. *Implementación de los controles 3 y 10 del modelo*: se deberán configurar los detalles necesarios para la correcta implementación de la gestión de trazas y la gestión de incidentes, tal y como se definen en el modelo propuesto.
    c. *Configuración de reglas de correlación*: las reglas de correlación definidas en el sistema SIEM deberán ser ajustadas al contexto de la organización, para lograr que el sistema reaccione de forma adecuada ante los diferentes eventos de seguridad. Igualmente será necesario definir nuevas reglas de correlación para ajustar el sistema SIEM al modelo propuesto, de manera tal que se ejecuten un grupo de acciones de forma automatizada que solo pueden realizarse a partir de la monitorización centralizada y la correlación de la información de dos o más sistemas.
6. Obtención de los indicadores de seguridad informática: para la revisión de la efectividad de los 10 macro-controles de seguridad informática será necesario obtener de forma automatizada los indicadores propuestos en el modelo. Estos indicadores deberán ser actualizados en tiempo real, mostrados en el sistema SIEM y reportados frecuentemente, mediante correo electrónico, a los especialistas de seguridad informática y directivos de la organización que se determinen. Los sistemas SIEM traen incluido un módulo de reportes que es personalizable, por lo que habrá que realizar los ajustes necesarios para que se muestren los indicadores definidos en el modelo, y se eliminen las gráficas y datos que no resultan de interés.

Es importante señalar que la implementación del modelo debe comenzar primero a una pequeña escala para después ir aumentando la cobertura de los controles automatizados a todos los activos informáticos de la organización. Se recomienda comenzar por los servidores centrales, en especial por aquellos que garantizan los servicios críticos de la institución, y después continuar el despliegue en el resto de las áreas.

En la Figura 3 se muestra un esquema con una posible implementación práctica del modelo utilizando el sistema SIEM de software libre OSSIM. En el esquema se detallan además las diferentes aplicaciones que implementarían los 10 macro-controles del modelo, especificando el número del control en cada caso. Se encuentran representados con el mismo color del sistema SIEM aquellas aplicaciones para las que OSSIM trae conectores incluidos por defecto, y en un color diferente se representan los sistemas para los que habría que desarrollar nuevos conectores.

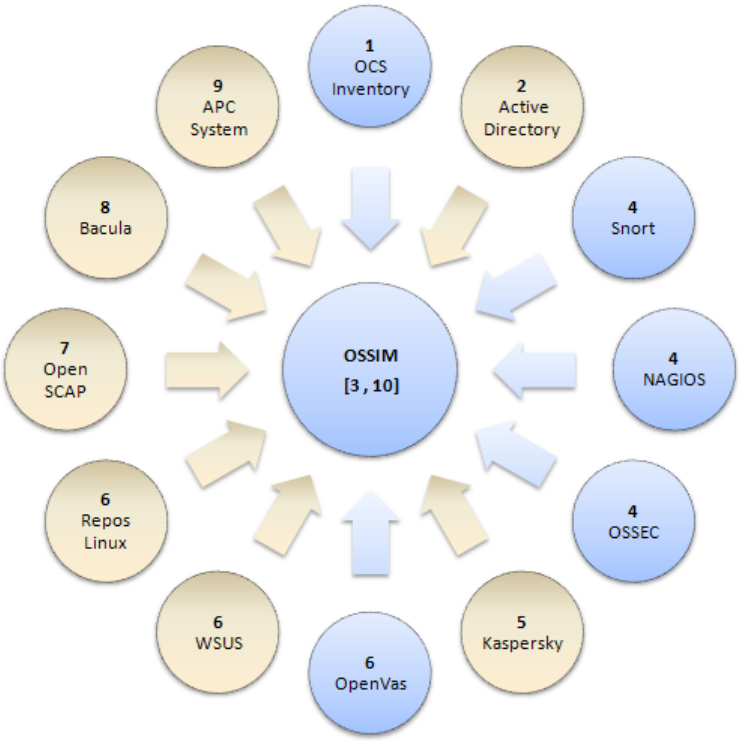

Figura 3: Aplicación del modelo mediante OSSIM y otros sistemas.

Posible impacto de la aplicación del modelo GAISI en instituciones cubanas

Con el objetivo de evaluar el impacto que tendría la aplicación del modelo propuesto en las instituciones cubanas, se aplicó un cuestionario a 20 instituciones pertenecientes a los Ministerios de Informática y Comunicaciones (MIC) y Educación Superior (MES). El 60% de los encuestados lo constituyeron directivos del área informática, el 25% especialistas de seguridad informática y el 15% administradores de redes. En la Figura 4 se muestran los valores promedio obtenidos para el nivel de automatización de cada uno de los 10 macro-controles especificados en el modelo GAISI.

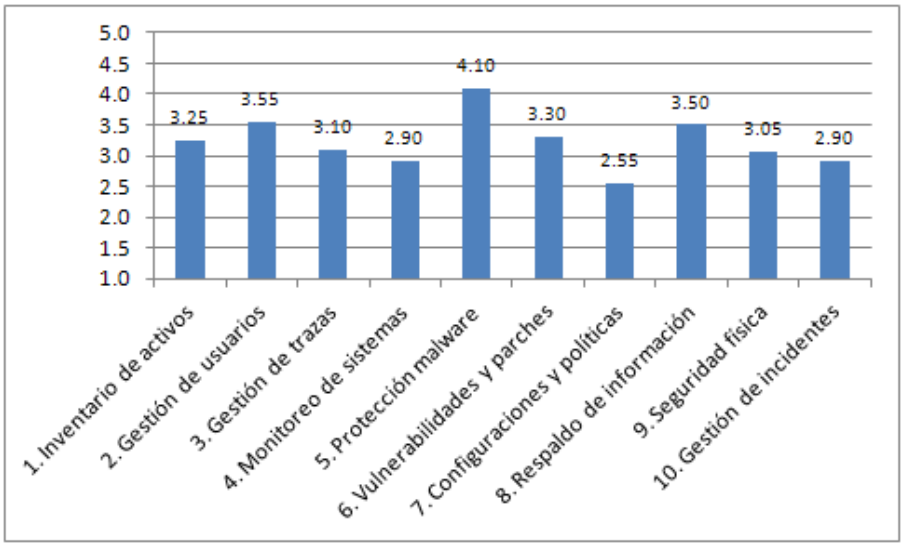

Figura 4: Nivel de automatización de los macro-controles en las instituciones cubanas

Los resultados de la encuesta arrojaron que el nivel de automatización promedio en la operación de los macro-controles es 3,22, en una escala de uno a cinco, donde el mínimo significa que el control no está implementado y el máximo valor implica que el control se encuentra completamente automatizado. Como se puede apreciar, el control con mayor nivel de automatización es el cinco (protección contra programas malignos), mientras que el menos automatizado lo constituye el control siete (configuraciones de seguridad y cumplimiento de políticas).

Por otra parte solo el 30% de las instituciones utilizan algún sistema SIEM, y el empleo que se hace de los mismos es limitado; mientras que solo un 65% tienen establecido algún sistema de indicadores para la seguridad informática, en la mayoría de los casos con una frecuencia de actualización semestral. Este es un período muy largo para el dinamismo que presenta el proceso de gestión de la seguridad informática, donde un día perdido puede significar la exposición a múltiples amenazas y vulnerabilidades.

Los valores obtenidos demuestran que la aplicación del modelo tendría un impacto considerable en las instituciones cubanas, donde se alcanzaría la máxima automatización en la operación de los macro-controles, y además se automatizarían los procesos de monitorización y revisión de los mismos, lo cual se traduciría en una mayor efectividad de los controles de seguridad informática.

CONCLUSIONES

La gestión de la seguridad informática es un proceso complejo que implica el establecimiento de un gran número de controles en un entorno dinámico de múltiples amenazas. Para reducir la complejidad y aumentar la efectividad de la gestión de la seguridad de la información es posible automatizar determinadas acciones y controles. La automatización de controles de seguridad informática implica que la operación, monitorización y la revisión de los mismos se realice de forma automática por herramientas de hardware y software, sin intervención humana en esas acciones.

En el presente trabajo se propone un modelo para la gestión automatizada e integrada de controles de seguridad informática, donde se definen 10 macro-controles que deberán ser automatizados para la protección de las tecnologías de la información de la organización. Estos macro-controles representan una agrupación y síntesis de los controles automatizables identificados en estándares internacionales. Los controles son implementados y operados por diferentes sistemas, pero su monitorización se realiza de forma centralizada en un sistema de gestión de información y eventos de seguridad (SIEM), que constituye el componente central del modelo y posibilita la integración de las diferentes herramientas de seguridad informática. La revisión de los controles se realiza mediante un grupo de indicadores, definidos también como parte del modelo, que deberán ser calculados y reportados de forma automatizada.

En el modelo propuesto se ofrece una visión integradora de la automatización de controles de seguridad informática, considerando todos los posibles controles automatizables y definiendo las acciones a realizar de forma automática en cada uno de los casos. El modelo propone además una utilización de los sistemas SIEM que va más allá del uso que normalmente tienen este tipo de sistemas, destinados comúnmente a la gestión de trazas y detección de eventos de seguridad. Esto implica que se debe realizar un

proceso profundo de personalización y adaptación del sistema SIEM utilizado para aplicar el modelo propuesto, mediante la definición de conectores, políticas, reglas de correlación y reportes de seguridad informática.

Finalmente se propone una guía para la aplicación del modelo propuesto y se describe una posible implementación del mismo utilizando el sistema SIEM de software libre OSSIM.

Basado en los resultados de la presente investigación, los responsables de la gestión de la seguridad informática en las instituciones podrán aumentar la efectividad de los controles y disminuir la complejidad del proceso de gestión mediante la aplicación del modelo propuesto. El trabajo pudiera resultar útil también para los desarrolladores de sistemas SIEM en el sentido de aumentar las funcionalidades de estos sistemas y aumentar su potencial de automatización.

REFERENCIAS

1. RICHARDSON, Robert. *14th Annual Computer Crime and Security Survey* [online]. Computer Security Institute (CSI), 2009. [Accessed 10 April 2010]. Available from: http://gocsi.com/survey.

2. SOPHOS. *Sophos security threat report* [online]. 2011. [Accessed 17 February 2012]. Available from: http://www.sophos.com/en-us/security-news-trends/security-trends/security-threat-report-2011.aspx.

3. KASPERSKY LAB. Kaspersky Security Bulletin. Statistics 2011. In: [online]. [Accessed 17 April 2012]. Available from: http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011.

4. S21SEC. *Informe de vulnerabilidades 2011* [online]. S21sec, 2012. [Accessed 18 April 2012]. Available from: http://www.s21sec.com/descargas/Informe%20Vulnerabilidades%202011.pdf.

5. SECUNIA. *Secunia yearly report 2011* [online]. Secunia, 2012. [Accessed 18 April 2012]. Available from: http://secunia.com/?action=fetch&filename=Secunia_Yearly_Report_2011.pdf.

6. DHANJANI, Nitesh. *Hacking: The next generation*. Sebastopol (CA): O'Reilly, 2009. ISBN 9780596154578.

7. WERLINGER, Rodrigo, HAWKEY, Kirstie and BEZNOSOV, Konstantin. An integrated view of human, organizational, and technological challenges of IT security management. In: *Information Management & Computer Security*. 2009, Vol. 17, no. 1, pp. 4-19.

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

9. ISO/IEC. *ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management*. 2005. : International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

10. NOF, Shimon Y. *Springer Handbook of Automation*. : Springer, 2009. ISBN 978-3-540-78830-0.

11. CANO, Jaimy. *Un concepto extendido de la mente segura: pensamiento sistémico en seguridad informática* [online]. 2005. : Criptored. [Accessed 8 October 2008]. Available from: http://www.criptored.upm.es/guiateoria/gt_m142x.htm.

12. EDWARDS, W. Keith, POOLE, Erika Shehan and STOLL, Jennifer. Security automation considered harmful? In: *Proceedings of the 2007 Workshop on New Security Paradigms - NSPW '07*. New Hampshire, 2008. pp. 33.

13. SANS. *Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines* [online]. August 2011. Available from: http://www.sans.org/critical-security-controls/cag3.pdf.

14. SANS - Tools for the implementation of the Twenty Critical Controls. In: [online]. Available from: http://www.sans.org/critical-security-controls/user-tools.php.

15. MONTESINO, Raydel and FENZ, Stefan. Information Security Automation: How Far Can We Go? In: *Sixth International Conference on Availability, Reliability and Security* . Vienna, Austria, August 2011. pp. 280-285.

16. NIST. *NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations* [online]. August 2009. : National Institute of Standards and Technology. [Accessed 2 July 2010]. Available from: http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf.

17. HAMDI, Hedi, BOUHOULA, Adel and MOSBAH, Mohamed. A Software Architecture for Automatic Security Policy Enforcement in Distributed Systems. In: *The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)*. Valencia, Spain, 2007. pp. 187-192.

18. HASSAN, Ahmad A. and BAHGAT, Waleed M. A framework for translating a high level security policy into low level security mechanisms. In: *2009 IEEE/ACS International Conference on Computer Systems and Applications*. Rabat, Morocco, 2009. pp. 504-511.

19. OUDA, A., LUTFIYYA, H. and BAUER, M. Automatic Policy Mapping to Management System Configurations. In: *2010 IEEE International Symposium on Policies for Distributed Systems and Networks* . Fairfax, VA, USA, 2010. pp. 87-94.

20. TIAN, H.T., HUANG, L.S., ZHOU, Z. and LUO, Y.L. Arm up administrators: automated vulnerability management. In: *7th International Symposium on Parallel Architectures, Algorithms and Networks, 2004. Proceedings.* Hong Kong, China, 2004. pp. 587-593.

21. SHAHRIAR, Hossain and ZULKERNINE, Mohammad. Automatic Testing of Program Security Vulnerabilities. In: *2009 33rd Annual IEEE International Computer Software and Applications Conference*. Seattle, Washington, USA, 2009. pp. 550-555.

22. AL-AYED, A., FURNELL, S.M., ZHAO, D. and DOWLAND, P.S. An automated framework for managing security vulnerabilities. In: *Information Management & Computer Security*. 2005, Vol. 13, no. 2, pp. 156-166.

23. KOSCHORRECK, Gerhard. Automated Audit of Compliance and Security Controls. In: *2011 Sixth International Conference on IT Security Incident Management and IT Forensics*. Stuttgart, Germany, May 2011. pp. 137-148.

24. LOPES, Miguel, COSTA, Antonio and DIAS, Bruno. Automated network services configuration management. In: *2009 IFIP/IEEE International Symposium on Integrated Network Management-Workshops* . New York, NY, USA, June 2009. pp. 140-143.

25. AGOULMINE, Nazim. *Autonomic network management principles: from concepts to applications*. London: Academic, 2010.

26. QUINN, Stephen, WALTERMIRE, David, JOHNSON, Christopher, SCARFONE, Karen and BANGHART, John. *NIST SP 800-126: The Technical Specification for the Security Content Automation Protocol (SCAP)* [online]. 2009. : National Institute of Standards and Technology. Available from: http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf.

27. Federal Desktop Core Configuration (FDCC). In: [online]. [Accessed 2 May 2011]. Available from: http://nvd.nist.gov/fdcc/index.cfm.

28. Center for Internet Security (CIS). In: [online]. [Accessed 2 May 2011]. Available from: http://cisecurity.org.

29. NICOLETT, Mark and KAVANAGH, Kelly M. *Critical Capabilities for Security Information and Event Management Technology* [online]. May 2011. : Gartner. [Accessed 18 August 2011]. Available from: http://www.arcsight.com/library/download/Gartner-SIEM-Critical-Capabilities-for-SIEM-2011/.

30. MILLER, David R., HARRIS, Shon, HARPER, Allen A., VANDYKE, Stephen and BLASK, Chris. *Security Information and Event Management (SIEM) Implementation*. : McGraw-Hill, 2011.

31. NICOLETT, Mark and KAVANAGH, Kelly M. *Magic Quadrant for Security Information and Event Management* [online]. May 2011. : Gartner. [Accessed 17 August 2011]. Available from: http://www.arcsight.com/collateral/whitepapers/Gartner_Magic_Quadrant_2011.pdf.

32. RICHARDSON, Robert. *CSI 15th Annual Computer Crime and Security Survey* [online]. Computer Security Institute (CSI), 2011. [Accessed 22 December 2011]. Available from: http://gocsi.com/survey.

33. SHENK, Jerry. *SANS Sixth Annual Log Management Survey Report* [online]. SANS, 2010. [Accessed 5 May 2011]. Available from: http://www.sans.org/reading_room/analysts_program/logmgtsurvey-2010.pdf.

34. CHUVAKIN, Anton. *SIEM: Moving Beyond Compliance* [online]. 2010. : RSA. [Accessed 14 September 2011]. Available from: http://www.rsa.com/content_library.aspx.

35. MONTESINO, Raydel, FENZ, Stefan and BAJULA, Walter. SIEM-based framework for security controls automation. In: *Information Management & Computer Security*. July 2012, Vol. 20, no. 4.

36. JAQUITH, Andrew. *Security metrics: replacing fear, uncertainty, and doubt*. Addison-Wesley, 2007.

37. ISO/IEC. *ISO/IEC 27004: Information technology - Security techniques - Information security management systems – Measurements*. 2009. : International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

38. CHEW, Elisabeth, SWANSON, Marianne, STINE, Kevin, BARTOL, Nadya, BROWN, Anthony and ROBINSON, Will. *NIST SP 800-55: Performance measurement guide for information security* [online]. 2008. : National Institute of Standards and Technology. [Accessed 11 February 2012]. Available from: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

39. CIS. *CIS Security Metrics* [online]. 2010. : Center for Internet Security. [Accessed 26 April 2011]. Available from: http://benchmarks.cisecurity.org/en-us/?route=downloads.metrics.

40. BARABANOV, Rostyslav. 11-007: *Information security metrics: state of the art*. Swedish Civil Contingencies Agency (MSB), 2011.

41. HAYDEN, Lance. *IT security metrics a practical framework for measuring security & protecting data*. McGraw Hill, 2010.

42. SAVOLA, Reijo. Towards a security metrics taxonomy for the information and communication technology industry. In: *Proceedings of the International Conference on Software Engineering Advances*. , 2007.

43. ArcSight ESM. [online]. [Accessed 17 April 2012]. Available from: http://www.arcsight.com/products/products-esm/.

44. Q1 Labs - QRadar SIEM. [online]. [Accessed 17 April 2012]. Available from: http://q1labs.com/products/qradar-siem.aspx.

45. RSA-EMC enVision. [online]. [Accessed 17 April 2012]. Available from: http://www.emc.com/security/rsa-envision.htm.

46. Symantec Security Information Manager. [online]. [Accessed 17 April 2012]. Available from: http://www.symantec.com/security-information-manager.

47. LogLogic Security Event Management. [online]. [Accessed 17 April 2012]. Available from: http://www.loglogic.com/products/security-event-management/.

48. McAfee Enterprise Security Manager. [online]. [Accessed 17 April 2012]. Available from: http://www.mcafee.com/us/products/enterprise-security-manager.aspx.

49. Novell Sentinel. [online]. [Accessed 17 April 2012]. Available from: http://www.novell.com/products/sentinel/index.html.

50. OSSIM - Open Source Security Information Management. [online]. [Accessed 17 April 2011]. Available from: http://www.ossim.net.

AUTORES

Raydel Montesino Perurena: Universidad de las Ciencias Informáticas (UCI), La Habana, Cuba, email: raydelmp@uci.cu.

Graduado de Ingeniero en Telecomunicaciones y Electrónica en el año 2003 en el Instituto Superior Politécnico José Antonio Echeverría (ISPJAE). Actualmente es profesor e investigador de la Universidad de las Ciencias Informáticas (UCI), donde ha ocupado el cargo de Director de Seguridad Informática en los últimos siete años (2005 - 2012). Sus intereses de investigación están relacionados con la gestión de la seguridad informática, específicamente en lo referente a estándares, métricas, automatización de controles y sistemas de gestión de información y eventos de seguridad (SIEM).

Walter Baluja García: Instituto Superior Politécnico José Antonio Echeverría (ISPJAE), La Habana, Cuba, email: walter@tesla.cujae.edu.cu.

Graduado de Ingeniero en Telecomunicaciones y Electrónica en el IPSJAE en el año 1997. Máster en Telemática (2000) y Doctor en Ciencias Técnicas (2006) por la misma universidad. Profesor Auxiliar del departamento de Telecomunicaciones y Telemática del ISPJAE. Vicerrector del ISPJAE. Desde 1995 labora en la gestión de redes, en particular en redes de datos. A partir de 1998 se dedica a la Seguridad de redes y sistemas. Su actividad docente y de I+D se desarrolla, fundamentalmente, en la arquitectura y gestión de redes, especialmente en la gestión de seguridad. Sus trabajos actuales se ubican en la seguridad de protocolos y redes inalámbricas, y las normas y sistemas de gestión de seguridad en las redes de telecomunicaciones modernas.

Joelsy Porven Rubier: Universidad de las Ciencias Informáticas (UCI), La Habana, Cuba, email: jporven@uci.cu.

Graduado de Ingeniero en Automática en el año 2003 en el Instituto Superior Politécnico José Antonio Echeverría (ISPJAE). Actualmente es profesor e investigador de la Universidad de las Ciencias Informáticas (UCI), donde se ha desempeñado como Especialista General en el área de los servicios telemáticos (2010 - 2012). Sus intereses de investigación están relacionados con la gestión de servicios telemáticos y la seguridad informática, específicamente en lo relacionado con la gestión de logs (LM), automatización y configuración de herramientas y los sistemas de gestión de eventos de seguridad (SIEM) así como los sistemas de clave pública (PKI).