UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

VICERRECTORÍA DE TECNOLOGÍA

DIRECCIÓN DE SEGURIDAD INFORMÁTICA

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

Tesis presentada en opción al grado científico de Doctor en Ciencias Técnicas

Autor: Ing. Raydel Montesino Perurena

Tutores: Dr C. Walter Baluja García

Dr C. José Lavandero García

La Habana

2012

A mi hija……

A mi esposa……

A mis padres……

AGRADECIMIENTOS

Quiero agradecer en primer lugar a mi esposa, por asumir una gran carga en este período, por entender mi ausencia y por alentarme en los momentos necesarios.

A mi preciosa hija, por ser mi inspiración y porque a pesar de su corta edad también supo entender que su papá estaba haciendo un Doctorado.

A mis padres, porque con su ejemplo y educación supieron conducirme por el camino correcto.

A toda mi familia en general, por la preocupación que mostraron en esta etapa.

A mis tutores Walter y Lavandero, que con sus ideas, sabios consejos y críticas constructivas contribuyeron en gran medida a la realización de este trabajo y a mi formación científica.

Al Programa Especial de Formación Científica en Informática (PEFCI), por lo productivo de sus seminarios científicos y por el empuje tan necesario para vencer las diferentes etapas.

A los investigadores del centro SBA-Research de Austria, en especial a Edgar Weippl y Stefan Fenz, por la colaboración en las publicaciones científicas.

A Joelsy, administrador de la red de la UCI y amigo, por su contribución definitiva en la aplicación práctica de la presente investigación.

A mis compañeros de trabajo, en especial a Pablo y Aleida, por asumir y sacar adelante todas las tareas durante mi ausencia.

A mis distintos jefes en esta etapa (Romillo, Miriam y Ortiz), por el apoyo brindado en los momentos necesarios.

A los colegas de la OSRI (Gerardo, Humberto), de Segurmatica (Bidot, Lodos) y del Grupo de Seguridad Tecnológica del MININT (Jesús, Andrés y Josué) por sus acertados criterios y el apoyo brindado.

A la Universidad de las Ciencias Informáticas, donde me he formado como profesional.

A TODOS los que hicieron posible que este sueño se hiciera realidad.

SÍNTESIS

El proceso de gestión de la seguridad informática requiere el establecimiento de gran cantidad de controles, la implementación de variados sistemas de seguridad con mecanismos de gestión independientes, y una elevada capacidad de respuesta ante los diversos ataques y vulnerabilidades existentes; lo que hace que el mismo sea complejo y en muchas ocasiones inefectivo.

En el presente trabajo se desarrolla un modelo para la gestión automatizada e integrada de controles de seguridad informática (GAISI), que contribuye a aumentar la efectividad de los controles y a disminuir la complejidad de la gestión de la seguridad informática. En el modelo se definen diez macro-controles de seguridad informática, los cuales representan una agrupación y síntesis de los controles automatizables identificados en los principales estándares internacionales sobre gestión de la seguridad de la información. Se automatizan las acciones de operación, monitorización y revisión de dichos controles; mientras que la gestión integrada se logra a través de un sistema SIEM, que constituye el componente central del modelo.

Como parte de la investigación se presentan otros aportes prácticos entre los que se encuentran un listado de métricas para medir la efectividad de los controles de seguridad informática, una guía para la aplicación del modelo propuesto, y las especificaciones necesarias para la implementación del modelo utilizando OSSIM y otros sistemas de software libre.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

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.

Entre los ataques que se producen con mayor frecuencia se pueden mencionar los programas malignos, la denegación de servicios, la desfiguración de sitios web, los ataques de ingeniería social, entre otros. En las encuestas anuales realizadas por el prestigioso Computer Security Institute (CSI) [1], los ataques con mayor incidencia han sido históricamente los programas malignos, afectando a más del 60% de las instituciones participantes en la encuesta.

Los diferentes ataques informáticos pueden provocar la pérdida de la disponibilidad, confidencialidad o integridad de la información; lo cual generalmente implica graves consecuencias para las organizaciones y en muchas ocasiones se ocasionan daños irreparables. Según datos estadísticos [2], las pérdidas promedio de las grandes empresas debido a incidentes de seguridad informática son valoradas en 5,9 millones de dólares al año.

Teniendo en cuenta además el crecimiento exponencial de los programas malignos, los cuales aumentan por decenas de miles diariamente [3], [4], las más de ocho mil nuevas vulnerabilidades de sistemas operativos y aplicaciones descubiertas anualmente [5], [6], y la organización cada vez más estructurada de los atacantes informáticos [7]; es evidente la

necesidad de garantizar la seguridad informática de las instituciones, mediante un adecuado proceso de gestión de todas las medidas y controles necesarios.

Actualmente existen varios modelos, estándares, recomendaciones y regulaciones relacionados con la gestión de la seguridad de la información. Entre ellos se destaca el estándar ISO/IEC 27001, el cual posee gran aceptación a nivel internacional y constituye una norma certificable. De manera general todos plantean que el proceso de gestión implica la realización de varias acciones que conforman un ciclo cerrado para la mejora continua del sistema. Como parte de este proceso se recomiendan más de 100 controles[1] de seguridad informática que no son solo de corte técnico, sino que involucran también aspectos organizativos y de recursos humanos.

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 [8].

Por otra parte se presentan también los siguientes retos a la hora de gestionar la seguridad informática [9]:

- *La cantidad y variedad de sistemas a asegurar*: la mayoría de las organizaciones posee una gran cantidad de aplicaciones y sistemas que necesitan ser protegidos, cada uno con sus diferentes mecanismos de soporte y configuraciones de seguridad.
- *La necesidad de responder rápidamente a nuevas amenazas*: las organizaciones necesitan frecuentemente reconfigurar las aplicaciones o instalar parches, para eliminar nuevas vulnerabilidades que son descubiertas constantemente y utilizadas por los atacantes. Cada minuto perdido en la implantación de un parche de seguridad significa la exposición a amenazas concretas y un gran riesgo para las instituciones.

[1] Control: medida, salvaguarda.

- *La falta de interoperabilidad e integración de los sistemas de seguridad*: es necesario utilizar varias herramientas y aplicaciones de seguridad informática que utilizan formatos propietarios y nomenclaturas diferentes; lo cual no permite su interoperabilidad y una gestión integrada de las mismas.

Para ejemplificar un poco lo anteriormente expresado se pudieran brindar algunos datos de la Universidad de las Ciencias Informáticas (UCI). En la misma se encuentran interconectadas en red más de 6000 computadoras y alrededor de 65 servidores, mientras que la Intranet está compuesta por más de 50 aplicaciones y sitios web. Entre los sistemas operativos utilizados se encuentran Microsoft Windows (XP, Vista, 7, Server 2003), NOVA[2], Ubuntu, CentOS y Debian. Por otra parte existe una gran variedad de aplicaciones y sistemas de gestión de bases de datos que soportan los diferentes servicios telemáticos: Apache, IIS, MySQL, Postgre SQL, Squid, Postfix, entre otros. Esto hace que la "superficie de ataque"[3] sea grande y por tanto es necesario dar seguimiento a los parches y vulnerabilidades de una amplia gama de sistemas operativos y aplicaciones.

Sobre los sistemas a utilizar para la implementación de los controles de corte técnico se puede afirmar que generalmente se utilizan más de diez herramientas diferentes con aplicaciones de gestión independientes. Se pudieran mencionar los siguientes: antivirus, cortafuegos, detectores de intrusiones, sistemas criptográficos, sistemas de control de acceso, de monitoreo de la red, de copias de respaldo, de gestión de parches, de detección de vulnerabilidades, de gestión de configuraciones, de gestión de incidentes, entre otros.

Los aspectos mencionados anteriormente, unidos a temas de preparación de los recursos humanos y una deficiente gestión, provocan que en muchas ocasiones el sistema de seguridad informática de las instituciones resulte inefectivo. En Cuba por ejemplo, según

[2] NOVA: Distribución cubana de GNU/Linux desarrollada en la UCI.
[3] Término empleado en el contexto de la seguridad informática para denotar las posibilidades de ataque de un atacante informático.

datos suministrados por la Oficina de Seguridad para las Redes Informáticas (OSRI), el 60,7% de las inspecciones realizadas a los sistemas de seguridad informática de diferentes instituciones cubanas, han obtenido la calificación de “Vulnerable” o “Muy Vulnerable” [10].

Teniendo en cuenta lo planteado anteriormente se identificó el siguiente **problema científico**: el proceso de gestión de la seguridad informática requiere el establecimiento de gran cantidad de controles, la implementación de variados sistemas de seguridad con mecanismos de gestión independientes, y una elevada capacidad de respuesta ante los diversos ataques y vulnerabilidades existentes; lo que hace que el mismo sea complejo y en muchas ocasiones inefectivo.

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 heterogéneo tecnológicamente, de constantes amenazas de seguridad, y teniendo en cuenta la gran cantidad de controles a implementar; es la automatización de controles de seguridad informática [11-13].

Para solucionar el problema planteado se consideró como **objeto de estudio** el proceso de gestión de la seguridad de la información, y como **campo de acción** la automatización e integración en la gestión de controles de seguridad informática.

El **objetivo general** de la presente investigación es desarrollar un modelo para la gestión automatizada e integrada de controles de seguridad informática, que contribuya a aumentar la efectividad de los controles y a disminuir la complejidad de la gestión de la seguridad informática.

Para alcanzar el objetivo general se plantean los siguientes **objetivos específicos**:

1. Analizar los referentes teóricos en que se fundamenta la gestión de la seguridad informática y los sistemas que permiten la automatización e integración en este contexto.
2. Determinar los controles de seguridad informática que son automatizables.

3. Definir métricas e indicadores que permitan evaluar la efectividad de los controles de seguridad informática.
4. Elaborar una guía para la aplicación del modelo propuesto.
5. Validar el modelo propuesto mediante su aplicación en la Universidad de las Ciencias Informáticas (UCI) y la consulta a un panel de expertos.
6. Valorar el posible impacto que tendría la aplicación del modelo en las instituciones cubanas.

Como **hipótesis de investigación** se plantea la siguiente: el desarrollo de 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), posibilitará un incremento de la efectividad de los controles y la disminución de la complejidad de la gestión de la seguridad informática.

Dentro de los **métodos teóricos** de investigación empleados se destacan el método *hipotético-deductivo* en la elaboración de la hipótesis de la investigación y en la propuesta de nuevas líneas de trabajo a partir de los resultados obtenidos. El método *histórico-lógico* y el *dialéctico* son utilizados para el estudio crítico de los trabajos anteriores en esta temática. El método *sistémico* es empleado en la concepción del modelo propuesto.

Los **métodos empíricos** utilizados son el *análisis documental* en la revisión de la literatura especializada, el *experimental* y la *medición* para la validación del modelo. Se emplea además la *encuesta* para la consulta a un panel de expertos y la valoración del posible impacto del modelo en las instituciones cubanas.

La **novedad** de la investigación radica en el desarrollo de un modelo que permitirá la gestión automatizada e integrada de controles de seguridad informática. El modelo se encuentra alineado con los principales estándares, recomendaciones y regulaciones sobre gestión de la seguridad de la información, brindando un enfoque de automatización, integración y síntesis

a las propuestas existentes. Se 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 la detección de eventos de seguridad.

El **aporte teórico** de la investigación lo constituye el modelo para la gestión automatizada e integrada de controles de seguridad informática.

Los **aportes prácticos** del presente trabajo se mencionan a continuación:

- Listado de métricas para medir la efectividad de controles de seguridad informática.
- Guía para la aplicación del modelo propuesto.
- Especificaciones y configuraciones necesarias para la implementación del modelo utilizando el sistema SIEM de software libre OSSIM (Open Source Security Information Management).

Para exponer los resultados de la investigación, este documento de tesis está dividido en introducción, tres capítulos, conclusiones, recomendaciones, referencias bibliográficas y anexos. El contenido de los capítulos se distribuye de la siguiente forma:

- Capítulo 1: contiene un análisis de los principales modelos, estándares, recomendaciones y regulaciones que, tanto a nivel internacional como nacional, están relacionados con la gestión de la seguridad de la información. Se realiza además una valoración de los principales trabajos e investigaciones existentes en el campo de la automatización e integración en la gestión de controles de seguridad informática y se analizan un grupo de sistemas que, desde el punto de vista práctico, pueden ser empleados para lograr este propósito.
- Capítulo 2: contiene el principal aporte de la investigación realizada. En él se desarrolla un modelo para la gestión automatizada e integrada de controles de seguridad informática (GAISI). Como parte del modelo se define el concepto de

gestión automatizada de controles, se identifican los controles automatizables y se proponen un grupo de métricas para medir la efectividad de los mismos.

- Capítulo 3: presenta la propuesta de una guía para la implementación del modelo GAISI con el objetivo de facilitar su adopción y aplicación. La misma contiene un grupo de especificaciones necesarias para la configuración de los sistemas, así como un listado de diferentes aplicaciones, propietarias y libres, que permiten la implementación de los diez macro-controles del modelo. Se procede además a la validación del modelo GAISI mediante su aplicación en la UCI y la consulta a un panel de expertos. Finalmente se realiza un análisis del posible impacto que tendría la aplicación del modelo en las instituciones cubanas.

CAPÍTULO 1

GESTIÓN DE LA SEGURIDAD INFORMÁTICA.

AUTOMATIZACIÓN E INTEGRACIÓN DE CONTROLES.

CAPÍTULO 1. GESTIÓN DE LA SEGURIDAD INFORMÁTICA. AUTOMATIZACIÓN E INTEGRACIÓN DE CONTROLES

En el presente capítulo se presenta una valoración de los principales modelos, estándares, recomendaciones y regulaciones que, tanto a nivel internacional como nacional, están relacionados con la gestión de la seguridad de la información. Se realiza además una valoración de los principales trabajos e investigaciones existentes en el campo de la automatización e integración en la gestión de controles de seguridad informática y se analizan un grupo de sistemas que, desde el punto de vista práctico, pueden ser empleados para lograr este propósito.

1.1. Gestión de la seguridad informática.

La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información [14]. Esto se logra mediante la implantación de un grupo de controles que incluyen políticas, procedimientos, estructuras organizativas y sistemas de hardware y software [15].

Los atributos de la información previamente mencionados poseen las siguientes definiciones [14]:

- *Confidencialidad*: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- *Integridad*: propiedad de salvaguardar la exactitud y el estado completo de la información.

- *Disponibilidad*: propiedad que determina que la información sea accesible y utilizable siempre que sea solicitada por una entidad autorizada.

A pesar de que pueden existir diferentes enfoques con respecto a las definiciones de "seguridad de la información", "seguridad informática" y "seguridad de las tecnologías de la información (TI)", en el presente trabajo se considerarán equivalentes estos términos, tal y como se plantea en la Resolución 127/2007 del Ministerio de la Informática y las Comunicaciones de Cuba (MIC) [16], la cual constituye el ´"Reglamento de seguridad para las tecnologías de la información" en el país.

Aunque comúnmente pudiera asociarse la seguridad informática a un pequeño grupo de medidas técnicas como antivirus y cortafuegos, los controles a establecer son muchos y muy variados [17]. 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, pero 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 estos y sus relaciones, para repensar la seguridad informática más allá de la experiencia tecnológica tradicional [18].

Según Solms [19], la seguridad informática ha transitado en la historia a través de cuatro etapas. La primera etapa se caracterizó por el aspecto técnico, la segunda estuvo relacionada con el enfoque de gestión, donde aspectos como políticas y procesos comenzaron a ser tenidos en cuenta. La tercera etapa devino con la estandarización y comenzaron a aparecer documentos de buenas prácticas y certificaciones. Temas como la cultura de seguridad informática, la evaluación y la monitorización comenzaron a ser importantes. La cuarta etapa ha sido impulsada por las regulaciones, donde la seguridad

informática ha pasado a ser un aspecto clave para los directivos de las organizaciones y por tanto es atendida desde el primer nivel de dirección.

Actualmente existen varios modelos, estándares, recomendaciones y regulaciones relacionados con la gestión de la seguridad informática; los cuales son valorados en la siguiente sección.

1.1.1. Principales estándares y regulaciones sobre seguridad informática

En el contexto de la seguridad informática existen estándares que constituyen normas certificables, marcos de trabajo que representan una recopilación de mejores prácticas y regulaciones que son de obligatorio cumplimiento en determinadas naciones.

1.1.1.1. ISO/IEC 27001 y 27002

La Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) han elaborado un grupo de estándares que constituyen una referencia a nivel mundial en la temática de seguridad de la información. La serie ISO/IEC 27000 está destinada completamente a la seguridad informática, donde los estándares ISO/IEC 27001 y 27002 abordan el tema de manera general, y el resto tratan temas específicos que complementan a los anteriores.

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 establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI) [14]. Se plantea la utilización del modelo PDCA (Plan - planificar, Do - hacer, Check – verificar, Act - actuar), para llevar a cabo estos objetivos (ver Figura 1.1).

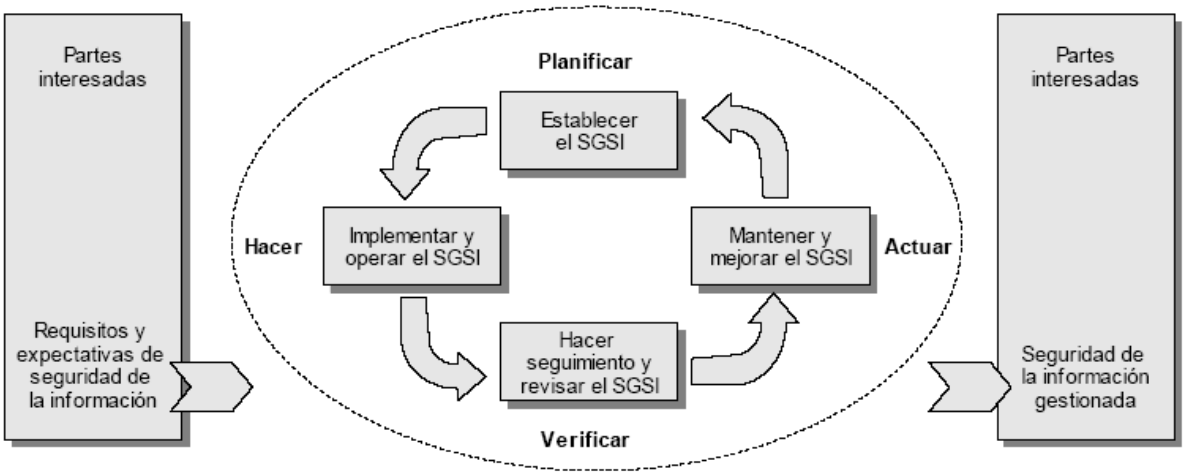


Figura 1.1: Modelo PDCA. Fuente: ISO/IEC 27001 [14]

En las diferentes fases del ciclo PDCA es necesario realizar las siguientes acciones [14]:

- *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*: medir y evaluar el desempeño del sistema de seguridad informática con respecto a 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.

Como se puede apreciar, el estándar propone un enfoque de procesos donde 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. Se proponen varias acciones que forman un ciclo cerrado para la mejora continua del sistema.

La norma certificable ISO/IEC 27001 especifica, en su Anexo A, 133 controles de seguridad divididos en 11 dominios y 39 objetivos de control. Estos controles son explicados detalladamente en la guía de buenas prácticas ISO/IEC 27002 [15], donde pueden apreciarse un grupo de controles técnicos, otros más relacionados con los recursos humanos y un grupo de controles de tipo organizativo. En la Tabla 1.1 se ofrece un listado de los dominios, la cantidad de controles que posee cada uno de ellos y algunos ejemplos.

Tabla 1.1: Dominios y controles de seguridad informática especificados en ISO/IEC 27002

No.	Dominio	Controles	Ejemplos
5	Política de seguridad	2	5.1.1 - Documento de política de seguridad de la información
6	Organización de la seguridad de la información	11	6.1.3 - Asignación de responsabilidades sobre seguridad de la información
7	Gestión de activos	5	7.1.1 - Inventario de activos
8	Seguridad ligada a los recursos humanos	9	8.2.2 - Concientización, educación y formación en seguridad de la información
9	Seguridad física y ambiental	13	9.1.2 - Controles de acceso físico
10	Gestión de comunicaciones y operaciones	32	10.4.1 - Controles contra código maligno
11	Control de acceso	25	11.5.2 - Identificación y autenticación de usuarios
12	Adquisición, desarrollo y mantenimiento de sistemas de información	16	12.6.1 - Control de vulnerabilidades técnicas
13	Gestión de incidentes de seguridad informática	5	13.1.1 - Reporte de eventos de seguridad informática
14	Gestión de la continuidad del negocio	5	14.1.3 - Desarrollo e implementación de planes de continuidad
15	Cumplimiento	10	15.2.1 - Cumplimiento de las políticas y normas de seguridad
	Total	**133**	

1.1.1.2. NIST SP 800-53

La división de seguridad del Instituto Nacional de Estándares y Tecnologías de EEUU (NIST) posee gran prestigio a nivel internacional y desarrolla un grupo de especificaciones técnicas, procedimientos y estándares sobre seguridad de la información. Las publicaciones especiales (SP) en su serie 800 están destinadas completamente a esta temática. En ellas se presentan varías guías y estándares resultantes de un trabajo colaborativo entre la industria, el gobierno y organizaciones académicas.

En particular el estándar NIST SP 800-53 [20] especifica los controles de seguridad a implementar en las agencias federales de los EEUU. El estándar esta asociado a una ley federal establecida en el año 2002 conocida como FISMA (Federal Information Security Management Act), la cual es de obligatorio cumplimiento y establece, a través de los estándares FIPS 199 y 200 (Federal Information Processing Standards), los requerimientos mínimos de seguridad en dependencia del tipo de organización y de la información que se procese. Según la categoría de la institución y el nivel de impacto de la misma se seleccionan los controles descritos en NIST SP 800-53 que deben ser implementados.

A pesar de que el estándar NIST SP 800-53 constituye una regulación solo en EEUU, esta publicación es muy utilizada y referenciada a nivel internacional por el prestigio que normalmente poseen los estándares del NIST. El estándar contiene una recomendación de controles de seguridad informática que pueden servir en general para diferentes organizaciones y toda la documentación pueden ser obtenida sin costo alguno[4]. En este caso se especifican 18 dominios de seguridad y 198 controles, clasificados en técnicos, operacionales y de gestión (ver Tabla 1.2).

[4] Serie NIST SP 800: http://csrc.nist.gov/publications/PubsSPs.html

Tabla 1.2: Dominios y controles de seguridad informática propuestos por NIST SP 800-53

No.	ID	Familia	Controles	Tipo
1	AC	Control de acceso	19	Técnico
2	AT	Formación y concienciación	5	Operacional
3	AC	Auditoría y reportes	14	Técnico
4	CA	Evaluación de la seguridad	6	Gestión
5	CM	Gestión de la configuración	9	Operacional
6	CP	Planificación de contingencias	9	Operacional
7	IA	Identificación y autenticación	8	Técnico
8	IR	Respuesta a incidentes	8	Operacional
9	MA	Mantenimiento	6	Operacional
10	MP	Protección de los medios	6	Operacional
11	PE	Protección física y ambiental	19	Operacional
12	PL	Planificación	5	Gestión
13	PS	Seguridad ligada al personal	8	Operacional
14	RA	Evaluación de riesgos	4	Gestión
15	SA	Adquisición de servicios y sistemas	14	Gestión
16	SC	Protección de los sistemas y las comunicaciones	34	Técnico
17	SI	Integridad de la información y los sistemas	13	Operacional
18	PM	Gestión del programa	11	Gestión
		Total	**198**	

1.1.1.3. ISF-SoGP. Recomendación de buenas prácticas de seguridad.

El Fórum para la Seguridad de la Información (ISF por sus siglas en inglés), compuesto por más de 300 organizaciones, ha desarrollado lo que denominan el Estándar de Buenas Prácticas (SoGP) para la seguridad informática. Esta recomendación aborda el tema de la seguridad de la información desde la perspectiva del negocio, enfocándose en la implementación de los controles necesarios para mitigar los riesgos asociados con los sistemas de información críticos [21].

El estándar está dividido en seis aspectos fundamentales, para los cuales se establecen 36 objetivos y 166 controles. Los aspectos son: gestión de la seguridad informática,

aplicaciones de negocio críticas, instalaciones de sistemas, redes, desarrollo de sistemas y entorno del usuario final.

El SoGP posee gran aceptación entre los miembros del ISF, pero a nivel internacional su aplicación es limitada, debido a que predominan otros estándares con mayor aceptación como ISO/IEC 27001.

1.1.1.4. ISM3. Modelo de madurez para la gestión de la seguridad informática.

El consorcio ISM3, compuesto por varias empresas y organizaciones, ha desarrollado el Modelo de Madurez de Gestión de la Seguridad Informática (ISM3 por sus siglas en inglés). Este modelo pretende extender los principios de calidad establecidos en ISO 9001 a un SGSI. En lugar de estar orientado a controles, se enfoca en los procesos de seguridad informática que pueden ser comunes a todas las organizaciones [22].

Se describen cinco configuraciones básicas para un SGSI, equivalentes a niveles de madurez, lo cual permite a las organizaciones ir escalando los niveles en dependencia de sus necesidades. Se plantean tres categorías de gestión: estratégica, táctica y operacional, para las cuales se definen 45 procesos que deben ser tenidos en cuenta.

En ISM3 los procesos relacionados con la seguridad informática son descritos detalladamente, estableciendo objetivos y métricas que permitan establecer un sistema de calidad. El enfoque práctico y de medición, así como la orientación hacia los objetivos de negocio de la organización, es lo que diferencia este modelo del resto de los estándares relacionados con la seguridad de la información.

A pesar de que ISM3 plantea un enfoque novedoso, su publicación es relativamente reciente y tiene competidores muy fuertes como ISO/IEC 27001, COBIT e ITIL (recomendaciones explicadas en la siguiente sección), por lo que en general todavía no posee un amplio reconocimiento a nivel internacional.

1.1.1.5. Mejores prácticas para la gestión de TI: COBIT, ITIL.

Existen un grupo de recomendaciones y mejores prácticas sobre gestión de las TI, que abordan de alguna manera la temática de la seguridad de la información como parte del proceso, por lo que constituyen también un referente en este sentido. Tales son los casos de COBIT e ITIL.

Los Objetivos de Control para las Tecnologías de la Información (COBIT por sus siglas en inglés), constituyen un conjunto de mejores prácticas desarrollado por la Asociación para la Auditoría y Control de Sistemas (ISACA). COBIT plantea un marco de trabajo para el gobierno de las TI que permite a los ejecutivos alinear las tecnologías de la información con los objetivos del negocio [23].

En su cuarta edición, COBIT plantea 34 procesos de alto nivel que cubren 210 controles clasificados en cuatro macro-procesos: Planificación y Organización, Adquisición e Implementación, Entrega y Soporte, y Supervisión y Evaluación. Es una recomendación que posee una amplia aceptación a nivel internacional.

Por otra parte, la Biblioteca de Infraestructura de Tecnologías de Información (ITIL por sus siglas en inglés) es un conjunto de buenas prácticas para la gestión de servicios de TI, desarrollado por el gobierno británico. ITIL ofrece descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI, contribuyendo de esta manera a una mayor efectividad del negocio [24].

ITIL, en su tercera versión, consta de cinco libros basados en el ciclo de vida del servicio. Se plantean las fases de estrategia, diseño, transición, operación y mejora continua del servicio; especificando 86 tópicos fundamentales a tener en cuenta en la gestión de TI. Esta guía de buenas prácticas también es muy utilizada a nivel internacional.

A pesar de que ITIL y COBIT poseen un amplio reconocimiento, no son dedicados por entero a la seguridad de la información, sino que este tema lo abordan por parte de la gestión de TI. Por tanto, en el contexto de la seguridad informática los referentes más utilizados son otros estándares que se dedican por entero a esta temática.

1.1.1.6. Estándares y regulaciones para sectores específicos: PCI DSS, HIPAA.

Existen otros estándares que son muy utilizados a nivel internacional, pero que abordan la temática de la seguridad de la información para sectores específicos como la salud o el sector comercial. Tales son los casos de HIPAA y PCI DSS respectivamente.

El Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS por sus siglas en inglés) ha sido desarrollado por el Payment Card Industry Security Standards Council (PCI SSC), como una guía que ayude a proteger los datos de tarjetas de débito y crédito durante su procesamiento, almacenamiento y transmisión, con el fin de prevenir los fraudes relacionados con las tarjetas de pago. Las compañías que procesan, guardan o trasmiten datos de tarjetas deben cumplir con el estándar o arriesgan la pérdida de sus permisos para procesar las tarjetas. La versión actual del estándar [25] especifica 12 requisitos mínimos organizados en 6 objetivos de control.

Por otra parte la Regla de Seguridad del HIPAA (Health Insurance Portability and Accountability Act) [26] es también muy conocida en el ámbito de la seguridad informática y constituye una regulación de obligatorio cumplimiento para las instituciones de salud de EEUU, con el objetivo de proteger los datos electrónicos de los pacientes. La norma establece 18 dominios y 42 controles agrupados en tres categorías: administrativos, físicos y técnicos.

Es importante señalar que tanto PCI DSS como HIPAA proponen una menor cantidad de controles de seguridad informática, lo cual está asociado a que tienen un propósito más específico y están orientados a determinados sectores.

1.1.1.7. Estándares y regulaciones de alcance regional.

Existen también otras guías y regulaciones que tienen un carácter regional. En general la mayoría de los países poseen regulaciones relacionadas con la seguridad informática. Algunas recomendaciones son conocidas fuera de sus fronteras porque constituyen guías de buenas prácticas aplicables a diferentes organizaciones. Cabe mencionar aquí al IT Baseline Protection Catalog (IT-Grundschutz) de Alemania [27] y el Manual de Seguridad de la Información (ISM) de Australia [28].

En el caso de Cuba la Resolución 127/2007 del MIC [16] constituye el marco regulatorio nacional en materia de seguridad de la información. Esta resolución posee 100 artículos de los cuales 89 constituyen controles de seguridad informática que deben ser implementados en las instituciones. En la Tabla 1.3 se muestra la cantidad de controles especificados en los diferentes capítulos de la resolución.

Tabla 1.3: Controles de seguridad informática especificados en la Resolución 127/2007 del MIC

Cap.	Sección	Controles
II	Del sistema de seguridad informática	9
III	Clasificación y control de bienes informáticos	4
	Del personal	10
	Seguridad física y ambiental	15
	Seguridad de operaciones	3
	Identificación, autenticación y control de accesos	4
	Seguridad ante programas malignos	4
	Respaldo de información	4
	Seguridad en redes	29
IV	Gestión de incidentes de seguridad	6
VI	De la inspección a la seguridad de las tecnologías de la información	1
	Total	**89**

1.1.1.8. CAG. 20 controles críticos de seguridad

Como puede apreciarse, los estándares y recomendaciones analizados anteriormente especifican una gran cantidad de controles diferentes que deben ser implementados para garantizar la seguridad de la información. Esto resulta realmente complejo para los responsables de la gestión de la seguridad informática, ya que deben garantizar la implementación y el seguimiento de un gran número de controles. En este sentido se hace necesaria una labor de síntesis, donde se identifiquen los controles más críticos de acuerdo al análisis de riesgos, así como las acciones elementales dentro de los mismos para garantizar un nivel básico de seguridad de la información.

De acuerdo a un estudio realizado por un gran número de expertos de seguridad informática, que fue publicado bajo el título Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG) [29], existen veinte controles 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.

Los veinte controles propuestos representan un subconjunto de los controles identificados como prioridad uno (P1) en el estándar NIST SP 800-53. Esta recomendación brinda descripciones detalladas de implementación y plantea además que quince controles pueden ser operados y monitorizados automáticamente, utilizando herramientas de seguridad informática existentes. Esto representa un enfoque completamente diferente al ofrecido por el resto de las recomendaciones existentes. El tema de la automatización será abordado con mayor detenimiento en la sección 1.2.

1.1.1.9. Resumen de estándares, guías y regulaciones de seguridad informática.

En la Tabla 1.4 se ofrece un resumen de los estándares, recomendaciones y regulaciones mencionados previamente. Se ha realizado una clasificación con respecto al alcance,

enfoque y características fundamentales de cada uno, lo cual permitirá realizar una valoración crítica del tema.

Tabla 1.4: Resumen de estándares y regulaciones de seguridad informática

	Clasificación	**Alcance**	**Enfoque**	**Características**	**Procesos**
ISO/IEC 27001	Estándar. Norma certificable.	Internacional General.	Orientado a procesos.	Ciclo PDCA, 4 fases, 7 procesos, 30 acciones.	Establecer, implementar, operar, monitorizar, revisar, mantener, mejorar.
ISO/IEC 27002	Mejores prácticas.	Internacional General.	Orientado a controles.	11 dominios, 39 objetivos, 133 controles.	-
NIST SP 800-53	Regulación.	Regional (EEUU). General.	Orientado a controles.	18 dominios, 198 controles.	-
ISF-SoGP	Mejores prácticas.	Internacional General.	Orientado a controles.	6 dominios, 36 objetivos, 166 controles.	-
ISM3	Modelo.	Internacional General.	Orientado a procesos.	3 categorías, 45 procesos, 5 niveles de madurez.	Gestión estratégica, táctica y operacional.
CoBIT 4.1	Mejores prácticas.	Internacional General.	Orientado a procesos.	4 fases, 8 macro-procesos, 34 procesos, 210 controles.	Planificar y organizar, adquirir e implementar, entrega y soporte, monitorear y evaluar.
ITIL v3	Mejores prácticas.	Internacional General.	Orientado a procesos.	5 fases, 86 tópicos fundamentales.	Estrategia, diseño, transición, operación, mejora continua.
PCI DSS v2	Regulación.	Internacional Sectorial (tarjetas de pago)	Orientado a controles.	6 objetivos de control, 12 requisitos.	-
HIPAA	Regulación.	Regional (EEUU) Sectorial (servicios médicos)	Orientado a controles.	3 categorías, 18 dominios, 42 controles.	-
IT-Grundschutz	Mejores prácticas.	Regional (Alemania). General.	Orientado a controles	5 dominios, 46 objetivos, + 500 controles.	-
ISM	Regulación.	Regional (Australia) General.	Orientado a controles.	5 dominios, 20 objetivos, 91 controles.	-
Res.127/2007 MIC	Regulación.	Regional (Cuba). General.	Orientado a controles.	11 dominios, 89 controles.	-
CAG v3	Mejores prácticas.	Internacional General	Orientado a controles	20 controles	-

Sobre los estándares y regulaciones existentes el autor del presente trabajo realiza las siguientes valoraciones:

- Existen algunos orientados a procesos y otros se enfocan en los controles, aunque de manera general todos coinciden en que la seguridad informática es un proceso continuo que necesita ser gestionado. Los que brindan un enfoque de procesos plantean acciones que conforman un ciclo cerrado para la mejora continua del sistema de seguridad informática. Esto deberá constituir un principio fundamental en cualquier modelo de gestión de la seguridad de la información.
- Se reconoce que la seguridad informática no es solo un problema técnico, sino que involucra también aspectos organizativos y de recursos humanos, concepto que ha sido expresado reiteradamente en otras investigaciones [18], [30-36]. Teniendo en cuenta que el objetivo fundamental del presente trabajo está relacionado con la automatización de controles, será necesario realizar un análisis exhaustivo de los controles de seguridad informática que pueden ser automatizados.
- Los que poseen un carácter general proponen una gran cantidad de controles (más de 90), lo cual resulta complejo para los responsables de la gestión de la seguridad informática. Se hace necesaria una labor de síntesis de controles que permita identificar las prioridades de un sistema de seguridad informática.
- Las guías y estándares que recomiendan una menor cantidad de controles están orientados a propósitos más específicos como HIPAA y PCI DSS. Constituye una excepción en este sentido la recomendación CAG, la cual es de propósito general y plantea solo 20 controles. Sin embargo, esta publicación se enfoca solamente en controles técnicos y quedan fuera de su alcance los temas organizativos y de recursos humanos. Además no se toman en cuenta los controles de seguridad física que también son considerados por el resto de las recomendaciones.

- El estándar ISO/IEC 27001 es el que tiene mayor aceptación a nivel internacional y constituye una norma certificable. En total se han emitido 7940 certificados distribuidos en 86 países[5]. De alguna manera el resto expresa su compatibilidad con este estándar y se establecen correspondencias con sus procesos y controles para reforzar la idea de que están alineados. Las publicaciones [37-39] y [40] son una muestra de lo expresado.

Es válido mencionar que en el mundo académico existen otras publicaciones que plantean modelos relacionados con la seguridad informática [41-45], pero en la práctica no son muy utilizados. Es importante señalar también que los estándares sobre gestión de la seguridad informática son complementados con otros que tratan el tema de la gestión de riesgos. Entre los más conocidos están OCTAVE [46], MAGERIT [47], ISO/IEC 27005 [48] y NIST SP 800-30 [49].

1.1.2. Efectividad de los controles. Métricas de seguridad informática.

La gestión de la seguridad informática implica realizar un grupo de acciones que conforman un ciclo cerrado para la mejora continua del sistema. Aunque la terminología de los procesos propuestos por los diferentes estándares varía, todos plantean una fase de revisión y evaluación como parte de la gestión, de tal manera que pueda determinarse la efectividad del sistema de seguridad informática con respecto a las políticas y los objetivos de seguridad establecidos. Esto se logra mediante la adecuada definición de indicadores y métricas que permitan medir el desempeño del sistema de seguridad informática.

Las métricas son el resultado de la recopilación, análisis y reporte de datos relevantes del sistema de seguridad informática que permiten la toma de decisiones [50]. Es importante señalar que el término más utilizado en el contexto de la seguridad informática es métricas, pero también se emplean otros como indicadores o medidas (measures en inglés) en la

[5] Certificados ISO/IEC 27001: http://www.iso27001certificates.com

literatura especializada. A los efectos de este trabajo los términos mencionados poseen el mismo significado.

Las métricas de seguridad informática no pueden estar relacionadas únicamente con la ocurrencia de incidentes de seguridad. La cantidad de ataques informáticos efectivos no es necesariamente un indicador de cuán seguro es un sistema. Por tanto, no existe una única métrica para caracterizar completamente y cuantificar la seguridad informática. Múltiples indicadores son necesarios y deben ser actualizados regularmente [51].

El tema de las métricas de seguridad informática ha sido tratado frecuentemente en investigaciones académicas y en el sector empresarial en los últimos años, pero todavía se encuentra en desarrollo. La falta de consenso sobre métricas de seguridad informática pudiera estar 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 [52].

Los enfoques tradicionales para obtener métricas de seguridad informática han sido insatisfactorios. En muchas ocasiones no se obtiene la información que realmente se necesita para tomar decisiones y evaluar la efectividad del sistema de seguridad informática. Según Hayden [53], es necesario considerar nuevas métricas, medir mejor y analizar adecuadamente los datos que se obtienen.

La publicación NIST IR 7564 (Directions in Security Metrics Research) demuestra que este es un campo que todavía se encuentra en investigación y desarrollo. La mayoría de lo que se ha escrito sobre métricas de seguridad informática son recomendaciones y guías para la correcta definición de las mismas. Sin embargo, poco se ha reportado sobre métricas que han probado ser útiles en la práctica [54]. En [55] se ofrecen varias razones que argumentan que la medición de la seguridad informática de un sistema es un problema complejo.

Entre las recomendaciones más reconocidas en esta temática se encuentran ISO/IEC 27004 [56] y NIST SP 800-55 [50], que explican cómo llevar a cabo un programa de medición en seguridad informática. Sin embargo, en estos documentos solo se brindan algunos ejemplos de métricas, dejando la completa definición de las mismas a las organizaciones.

1.1.2.1. Tipos de métricas

La madurez de una organización y de su sistema de seguridad informática determinan los tipos de métricas que pueden utilizarse. Esta madurez está determinada por la existencia e institucionalización de procesos y procedimientos en la organización. A medida que un sistema de seguridad informática se desarrolla y evoluciona, las políticas se tornan más detalladas y mejor documentadas, los procesos se vuelven más estandarizados y repetibles; de manera tal que existe una mayor cantidad de datos que pueden ser usados para medir la efectividad del sistema. Las métricas de seguridad informática se clasifican entonces de la siguiente manera [50]:

- *Métricas de implementación*: evalúan la implantación de controles de seguridad informática, de acuerdo a las políticas de seguridad definidas. Responden a la pregunta: ¿qué controles de seguridad informática se encuentran implementados? Este tipo de métricas permite evaluar el cumplimiento de regulaciones y normas establecidas.
- *Métricas de efectividad*: permiten determinar si los controles de seguridad informática implementados realizan la función para la que fueron concebidos. Este tipo de métricas permite determinar si el sistema de seguridad informática diseñado es efectivo o si necesita ser revisado y mejorado.
- *Métricas de impacto en el negocio*: permiten determinar el impacto que la seguridad informática ha tenido en el cumplimiento de la misión de la organización. Este tipo de

métricas ofrece una visión más global, considerando la seguridad informática como un medio para alcanzar los objetivos de la organización y no como un fin en sí misma.

En la Tabla 1.5 se muestra la relación entre los diferentes tipos de métricas de seguridad informática y el grado de madurez de las instituciones. El presente trabajo tiene entre sus objetivos el aumento de la efectividad de los controles de seguridad informática, por tanto las métricas que interesan son las métricas de efectividad.

Tabla 1.5: Métricas de seguridad informática en función de la madurez de la organización [50]

	Métricas de seguridad informática		
	Implementación	**Efectividad**	**Impacto**
Procesos	Definidos y documentados	Bien establecidos	En fase de auto-regeneración
Procedimientos de operación	En fase de estabilización	Institucionalizados	En fase de auto-ajuste
Disponibilidad de los datos	Pueden ser obtenidos	Disponibles	En repositorios estandarizados
Dificultad de obtención de datos	Media	Baja	Integrados a los procesos del negocio
Automatización de la recolección de datos	Media	Alta	Completa

Como puede apreciarse, las instituciones deberán tener cierto grado de madurez en su sistema de seguridad informática para poder obtener los datos necesarios que permitirán el cálculo de estos indicadores, lo cual deberá realizarse con un alto nivel de automatización.

1.1.2.2. Fuentes de datos para las métricas

Para calcular los indicadores de seguridad informática que se definan, es necesario obtener los datos que permitan realizar los análisis correspondientes. Los datos para las métricas de seguridad informática pueden provenir de una gran variedad de fuentes, entre las que cabe mencionar las siguientes [56]:

- Resultados de análisis de riesgos.
- Cuestionarios y entrevistas al personal.
- Reportes de auditorias internas y externas.
- Trazas de seguridad de los sistemas y aplicaciones.
- Reportes de incidentes de seguridad.
- Resultados de pruebas de seguridad, como por ejemplo pruebas de penetración y escaneo de vulnerabilidades
- Documentos de políticas y procedimientos de la organización.
- Resultados de cursos y entrenamientos de seguridad informática.

1.1.2.3. Elementos a tener en cuenta para la definición de buenas métricas

Los indicadores de seguridad informática deben reunir un grupo de características para que sean útiles. A pesar de que la terminología varía en diferentes documentos [52], [53], [57], [58], en sentido general las buenas métricas de seguridad informática deben poseer las siguientes características [59]:

- Deben comunicar y medir aspectos que son relevantes en el contexto específico para las que fueron concebidas; y deben ser significativas, tanto en su contexto como en su presentación, para las personas encargadas de interpretarlas.
- La frecuencia de medición y su proyección en el tiempo debe estar acorde con la frecuencia de cambios de los controles que son objetos de medición. Debe ser posible realizar un seguimiento de los indicadores a través del tiempo.
- Deben ser objetivas y cuantificables, lo cual implica que deben ser obtenidas de datos y valores numéricos confiables, no de evaluaciones cualitativas que pudieran tener un alto grado de subjetividad. Las métricas deben expresarse en unidades de medida bien definidas.

- El proceso de medición tiene que ser repetible de forma consistente por diferentes evaluadores bajo circunstancias similares, por lo que este proceso debe ser definido con un alto grado de formalidad.

Hayden [53] plantea la utilidad del método Objetivo-Pregunta-Métrica (GQM, por sus siglas en inglés) para definir buenas métricas de seguridad informática. En primer lugar es necesario tener claramente definidos los objetivos a lograr con cada uno de los controles, posteriormente se formulan preguntas más específicas permiten evaluar el cumplimiento de los objetivos, y finalmente se definen las métricas que responden a las preguntas formuladas. Este método asegura que las métricas estén perfectamente alineadas con los objetivos del sistema de seguridad informática.

1.1.2.4. Ejemplos de métricas de seguridad informática

En los trabajos previamente referenciados se ofrecen algunos ejemplos concretos de buenas métricas de seguridad informática, aunque hay que señalar que estas solo abarcan un número reducido de controles. Desde el punto de vista práctico, el Centro para la Seguridad de Internet (CIS, por sus siglas en inglés) ha tratado de estandarizar un grupo de métricas mediante el consenso de un equipo de 150 expertos. El resultado ha sido un documento que plantea la definición de 28 métricas de seguridad informática [60]. En la Tabla 1.6 se mencionan algunas de las métricas propuestas.

A pesar de que las métricas del CIS poseen gran aceptación a nivel internacional, los indicadores propuestos abarcan solo algunos controles de seguridad informática entre los que se encuentran la gestión de incidentes, de vulnerabilidades y parches, de configuraciones y la seguridad de aplicaciones; quedando fuera un grupo importante de controles necesarios en un sistema de seguridad informática.

Tabla 1.6: Ejemplos de métricas de seguridad informática [60]

Control	Pregunta	Métricas
Gestión de incidentes	¿Cuán efectiva es la detección, identificación, respuesta y recuperación de incidentes de seguridad?	Cantidad de incidentes
		Tiempo medio de detección de incidentes
		Tiempo medio para la solución de incidentes
Gestión de parches	¿Cuán actualizados se mantienen los sistemas informáticos?	Cobertura del sistema de gestión de parches
		Tiempo medio para la aplicación de parches
Gestión de vulnerabilidades	¿Cuán efectiva es la detección e identificación de vulnerabilidades conocidas?	Cobertura del escaneo de vulnerabilidades
		Porciento de sistemas con vulnerabilidades críticas
		Tiempo medio para la mitigación de vulnerabilidades

Entre las métricas más utilizadas a nivel internacional se encuentran también ALE (expectativa de pérdida anual) y ROSI (retorno de inversión en seguridad). Sin embargo, ambas han recibido fuertes críticas por el alto nivel de subjetividad e incertidumbre involucradas en sus cálculos [52], [53]. Además, constituyen métricas de impacto en el negocio según la clasificación especificada en la sección 1.1.2.1, por lo que no son de interés del presente trabajo.

De manera general se puede decir que existen algunos ejemplos de métricas de seguridad informática, pero no existe consenso sobre las mismas y estas no abarcan el amplio espectro de controles propuestos por los principales estándares. Por tanto, será necesario definir y seleccionar las métricas que permitan medir la efectividad de los controles de seguridad informática, lo cual está directamente relacionado con la validación de la hipótesis de la presente investigación.

1.2. Automatización en el contexto de la seguridad informática

La automatización en general 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 [61].

El término automatización ha tenido variaciones con el transcurso del tiempo, donde en un principio se utilizó el término mecanización y más recientemente se emplea el término autonómico, especialmente en el área de la computación y las tecnologías de la información. De esta manera, el término automático se utiliza para denotar acciones repetitivas y el término autonómico se emplea para referirse a un sistema que se auto-gestiona completamente sin intervención externa [62].

1.2.1. Gestión autonómica

IBM fue la primera compañía en utilizar el término computación autonómica (AC), en el sentido de desarrollar una nueva generación de sistemas de computación inteligentes [63]. Los conceptos de AC implican que los administradores de los sistemas no tienen que lidiar con la gestión a bajo nivel, para que puedan concentrarse en los procesos de gestión a alto nivel. Se comienza a utilizar entonces el término gestión autonómica y se plantea que esta puede desarrollarse con diferentes grados de autonomía. Los investigadores de IBM han identificado cinco categorías que describen distintos niveles de gestión autonómica, los cuales han sido ampliamente aceptados por la comunidad científica [64]:

1. *Nivel básico*: el operador necesita configurar y monitorear de forma manual cada elemento del sistema, durante todo el ciclo de vida del mismo, que va desde la instalación hasta la desinstalación.

2. *Nivel de gestión*: el operador se auxilia de tecnologías y sistemas de gestión para monitorear múltiples sistemas simultáneamente, utilizando consolas de gestión con interfaces hombre-máquina apropiadas.
3. *Nivel proactivo*: sistema con capacidades predictivas que permite analizar la información adquirida, identificar y predecir problemas; proponiendo soluciones adecuadas al operador del sistema para su posterior implementación.
4. *Nivel adaptativo*: en este nivel el sistema es capaz de reaccionar automáticamente sin intervención humana en muchas situaciones. Una vez que se especifican las acciones a realizar ante diferentes situaciones, el sistema puede realizarlas y tomar decisiones a bajo nivel.
5. *Nivel autonómico*: este es el máximo nivel donde la interacción entre las personas y los sistemas se basan solamente en la definición de objetivos de alto nivel. Los operadores solo definen las políticas del negocio por la que se regirán los sistemas y estos interpretan esos objetivos actuando consecuentemente con estos.

El proceso de auto-gestión planteado en las definiciones de gestión autonómica puede dividirse en cuatro categorías: auto-configuración, auto-corrección, auto-optimización y auto-protección. Estos conceptos son la base del marco de trabajo *IBM Tivoli Management* [65]. Cada elemento es gestionado utilizando un lazo de control, que posibilita el monitoreo del estado de los elementos y la toma de decisiones sobre cómo gestionarlos, basado en las políticas definidas por el administrador del sistema [66].

Los conceptos de computación autonómica han encontrado un campo de aplicación importante en la gestión de redes, donde se ha planteado el estudio de nuevas arquitecturas y protocolos que permitan el desarrollo de redes que puedan gestionarse con cierto nivel de autonomía, siendo capaces de adaptarse eficientemente a nuevas situaciones sin que sea necesaria la intervención humana de forma directa [62]. Algunas investigaciones que

abordan esta temática son [67-71]. Sin embargo, en el campo de la seguridad informática existen relativamente pocas investigaciones relacionadas con la automatización.

1.2.2. Trabajos previos sobre automatización en seguridad informática

La mayoría de los estudios académicos sobre la automatización de la seguridad informática aborda 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 [72-77], en la detección de vulnerabilidades [78-82], en el chequeo del cumplimiento de regulaciones [83], [84] y en la gestión de configuraciones [85-91].

Desde el punto de vista de los procesos en [92] se realiza una investigación dirigida al desarrollo de un sistema para automatizar y facilitar la adopción de un sistema de gestión de seguridad informática, acorde a un proceso de certificación ISO/IEC 27001. Existen varios sistemas desarrollados con este propósito como Callio Secura 17799[6], ISMS Tool Box[7] y CRAMM Information Security Toolkit[8], donde se va guiando a los responsables del proceso de gestión de la seguridad de la información a través del ciclo PDCA. Para esto se utilizan herramientas que facilitan el análisis de riesgos, la formulación de políticas, la selección de controles y la generación de toda la documentación asociada al sistema de seguridad informática. En estos casos el objetivo fundamental es básicamente la identificación de riesgos y la generación de los documentos necesarios para la certificación, lo cual no llega a abarcar la automatización de los controles de seguridad informática.

Por otra parte en [93] se aborda la automatización del proceso de revisión mediante el desarrollo de un sistema para la medición y visualización automatizada de métricas de

[6] http://www.acinfotec.com/callio.php
[7] http://isms-toolbox.com/
[8] http://www.cramm.com/

seguridad informática, pero básicamente se utilizan métricas relacionadas con vulnerabilidades, las cuales son obtenidas a través de escaneos automáticos.

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. Los trabajos que resultan un poco más abarcadores en este sentido son el Protocolo de Automatización de Contenido de Seguridad (SCAP, por sus siglas en inglés), desarrollado por el NIST; y la recomendación CAG mencionada en la sección 1.1.1.8.

1.2.2.1. SCAP. Protocolo de automatización de contenido de seguridad

Los trabajos del NIST con respecto a la automatización de la seguridad informática han estado relacionados con la definición de nomenclaturas y lenguajes estándares que permitan la interoperabilidad de diferentes aplicaciones, y la adopción de un lenguaje de seguridad común. Esto se ha materializado mediante el estándar NIST SP 800-126 [94], el cual define el protocolo SCAP. Otras publicaciones relacionadas con este protocolo son [95-97].

SCAP tiene dos grandes componentes. En primer lugar es un protocolo: posee varias especificaciones abiertas que estandarizan el formato y la nomenclatura mediante las cuales las aplicaciones informáticas brindan información relacionada con la seguridad informática. Estas especificaciones son conocidas como los “componentes SCAP”. En segundo lugar SCAP incluye datos de referencia estandarizados, relacionados con vulnerabilidades y configuraciones de seguridad, a los cuales se les denomina “contenidos SCAP”. En la Tabla 1.7 se mencionan todos los componentes de la versión 1.2 de SCAP.

En la práctica las organizaciones deberían emplear listas de chequeo de configuraciones de seguridad expresadas en SCAP para mejorar y monitorear la seguridad de los sistemas [99]. Los contenidos SCAP están disponibles en múltiples fuentes. Por ejemplo, en la Base de

Datos Nacional de Vulnerabilidades[9] (NVD, por sus siglas en inglés) se mantiene un diccionario actualizado de CPE y CVE. Igualmente este sitio posee un repositorio de listas de chequeo de configuraciones de seguridad para una gran variedad de sistemas operativos y aplicaciones.

Tabla 1.7: Componentes de SCAP [98]

Componente SCAP	Descripción
Enumeraciones (diccionarios)	
Common Platform Enumeration (CPE)	Nomenclatura y diccionario para hardware, sistemas operativos y aplicaciones
Common Configuration Enumeration (CCE)	Nomenclatura y diccionario de configuraciones de seguridad de los sistemas
Common Vulnerabilities and Exposures (CVE)	Nomenclatura y diccionario de vulnerabilidades de seguridad de los sistemas
Sistemas de puntuaciones	
Common Vulnerability Scoring System (CVSS)	Especificación para aplicar criterios de medida a la severidad relativa de las vulnerabilidades de los sistemas
Common Configuration Scoring System (CCSS)	Especificación para aplicar criterios de medida relativos a la configuración de los sistemas
Lenguajes	
Extensible Configuration Checklist Description Format (XCCDF)	Lenguaje para la especificación de listas de chequeo de configuraciones de seguridad y para el reporte de los resultados obtenidos en las verificaciones
Open Vulnerability and Assessment Language (OVAL)	Lenguaje para la especificación de procedimientos de pruebas de seguridad de bajo nivel empleados por las listas de chequeo
Open Checklist Interactive Language (OCIL)	Lenguaje para representar chequeos que recolectan información de personas y almacenes de datos
Formatos de reporte	
Asset Identification (AI)	Formato para identificar unívocamente a los activos mediante identificadores conocidos
Asset Reporting Format (ARF)	Formato para el intercambio de información y generación de reportes sobre los activos

[9] "National Checklist Program Repository." http://web.nvd.nist.gov/view/ncp/repository

Un ejemplo real de la utilización de SCAP es una guía emitida por el gobierno de Estados Unidos, denominada Federal Desktop Core Configuration (FDCC)[10], 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)[11]. 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.

El NIST, por su parte, ha establecido un programa de validación de SCAP para asegurar que las aplicaciones que implementan SCAP han sido debidamente probadas de acuerdo a los requerimientos del estándar [100]. En el Anexo 1 se muestra un listado de algunos de los productos que han alcanzado las certificaciones del NIST, donde se aprecia que empresas líderes en software de seguridad como Symantec, McAfee y otros, han ido adoptando el estándar SCAP. Algunas aplicaciones de libre utilización que incorporan componentes de SCAP son eSCAPe[12], Ovaldi[13] y OpenSCAP[14].

Como puede apreciarse, SCAP fue creado para proveer una forma estandarizada de gestionar la seguridad de los sistemas informáticos, sin embargo su alcance es todavía

[10] "Federal Desktop Core Configuration (FDCC)." http://nvd.nist.gov/fdcc/index.cfm
[11] "CIS Benchmarks.", http://benchmarks.cisecurity.org/en-us/?route=downloads.benchmarks
[12] eSCAPe: Enhanced SCAP Editor, http://www.g2-inc.com/escape/
[13] Ovaldi: The OVAL Interpreter, http://sourceforge.net/projects/ovaldi/
[14] The OpenSCAP Project, http://www.open-scap.org/page/Main_Page

limitado. Analizando la propia definición de los componentes de SCAP puede apreciarse que este posee aplicación solamente en los controles relacionados con la detección de vulnerabilidades (CVE, CVSS), el chequeo de las configuraciones de seguridad y del cumplimiento de regulaciones (XCCDF, OVAL, CCE, CCSS), así como el inventario de activos (CPE, AI, ARF). En [101] se mencionan los principales retos que todavía tiene por delante SCAP y las principales líneas de investigación a desarrollar en el futuro en lo que respecta a este protocolo.

1.2.2.2. CAG. Automatización de controles críticos.

En la sección 1.1.1.8 se realizó una valoración de la recomendación CAG desde el punto de vista de la gestión de seguridad informática. Además de los aportes relacionados con la identificación de los controles críticos, esta publicación posee un marcado enfoque de automatización con relación la operación y monitorización de los controles. Se plantea que quince de los controles propuestos pueden ser automatizados. Uno de los principios fundamentales en los que se basa esta recomendación es el siguiente [29]:

- Los controles deben ser automatizados siempre que sea posible, y deben ser medidos continuamente o periódicamente utilizando técnicas automatizadas de medición donde sea viable.

Siguiendo este principio es que se describe la implementación de los controles críticos, especificando las pruebas que pueden realizarse para medir la efectividad de los mismos. Esto representa un enfoque completamente diferente al que tienen el resto de las recomendaciones y estándares, los cuales en la mayoría de los casos no ofrecen detalles de implementación, mientras que la automatización es tratada de manera muy puntual en los mismos. A juicio del autor del presente trabajo, CAG contiene el análisis más completo sobre

la automatización de controles de seguridad informática comparado con el resto de los trabajos consultados en esta temática.

Sin embargo, la automatización de los quince controles es vista de manera independiente, sin tener una visión integradora del proceso de gestión de la seguridad informática. Esto puede apreciarse en la propuesta que se realiza sobre los posibles sistemas y aplicaciones que implementan los controles[15], donde se mencionan 28 herramientas de diferentes desarrolladores, todas con sistemas de administración y gestión independientes. Si se analiza detalladamente esta propuesta, se puede apreciar que en la mejor de las combinaciones es necesario utilizar diez sistemas diferentes para la implementación de los controles automatizables.

Por otra parte, tal y como se señaló anteriormente, CAG no toma en cuenta los controles de seguridad física, los cuales son imprescindibles en un sistema de seguridad informática y admiten un alto grado de automatización. Además, el autor de esta tesis considera que las métricas propuestas para la evaluación de la efectividad de los controles no pueden ser obtenidas de forma automatizada, porque implican la realización de determinadas pruebas para medir el tiempo de reacción de los controles.

1.2.3. Sistemas que permiten la automatización de controles de seguridad informática

Desde el punto de vista práctico existen varios sistemas, aplicaciones y herramientas que permiten la automatización de un grupo determinado de controles de seguridad informática. En este sentido cabe mencionar los siguientes:

- *Sistemas de inventario de activos*: son herramientas que permiten realizar de forma automatizada el inventario de todos los equipos conectados a la red de datos. Se

[15] http://www.sans.org/critical-security-controls/user-tools.php

registran tanto sus características de hardware como los sistemas operativos y aplicaciones instaladas en los diferentes dispositivos (ej. *OCS Inventory NG*[16])

- *Sistemas de gestión de parches*: son aplicaciones que permiten distribuir de forma automatizada los parches y actualizaciones de sistemas operativos y aplicaciones, para sellar vulnerabilidades presentes en las mismas (ej. *Microsoft Windows Server Update Services*[17]).
- *Sistemas de detección de vulnerabilidades*: permiten escanear de forma programada todos los dispositivos conectados a la red para detectar la presencia de vulnerabilidades en los sistemas operativos y las aplicaciones. Las vulnerabilidades son clasificadas de acuerdo a su nivel de importancia y el sistema propone la solución para eliminar cada una de ellas (ej. *OpenVAS*[18]).
- *Sistemas de implementación de políticas*: permiten automatizar la implementación de políticas de seguridad en las computadoras conectadas a la red. Estas políticas son definidas en un servidor central y las configuraciones son aplicadas a los equipos cuando estos se autentican en el mismo (ej. *Microsoft Active Directory*[19]).
- *Sistemas de gestión de configuraciones*: permiten automatizar el proceso de configuración de servidores y estaciones de trabajo. Las configuraciones son definidas centralmente y estas son aplicadas a los diferentes equipos de forma automática. Periódicamente se chequean y rectifican las configuraciones definidas para asegurar que ningún equipo se desvíe de los parámetros establecidos (ej. *Puppet*[20]).

[16] http://www.ocsinventory-ng.org/en/
[17] http://www.microsoft.com/windowsserversystem/updateservices/default.mspx
[18] http://www.openvas.org/
[19] http://www.microsoft.com/spain/windowsserver2008/roles/apps_ad.mspx
[20] http://puppetlabs.com/puppet/puppet-open-source/

- *Sistemas de gestión de trazas*: permiten la recolección y almacenamiento de trazas de seguridad de forma centralizada. Las trazas de múltiples dispositivos, sistemas operativos y aplicaciones son enviadas a un servidor central de forma automatizada para su conservación y análisis (ej. *Rsyslog*[21])
- *Sistemas de detección de intrusiones*: son dispositivos o aplicaciones que permiten detectar en tiempo real los ataques que se producen a través de la red. Se emiten alertas automáticamente ante la detección de los ataques y es posible también, en dependencia de la configuración, bloquear las direcciones IP desde donde provienen los mismos (ej. *Snort*[22])
- *Sistemas de monitoreo de disponibilidad*: son sistemas que permiten detectar y notificar la falta de disponibilidad de dispositivos, aplicaciones y servicios; con el objetivo de alertar sobre las interrupciones de los sistemas y que estos estén disponibles la mayor parte del tiempo (ej. *NAGIOS*[23])

Como puede apreciarse existen varios sistemas que automatizan controles de seguridad informática. Sin embargo, la mayoría de ellos funcionan de manera independiente y tienen aplicaciones de gestión diferentes. Teniendo en cuenta la gran cantidad de controles a implementar, es necesario encontrar una solución que sea capaz de integrar los diferentes sistemas existentes para lograr una gestión integrada de los controles y disminuir la complejidad de este proceso [102].

Cabe mencionar el caso de empresas líderes en el mundo de la seguridad informática que ofrecen una gran variedad de aplicaciones con la posibilidad de integrar algunas de ellas. Tal es el caso de Symantec y McAfee, los cuales ofrecen una amplia gama de productos con posibilidades de integración, pero en estos casos los sistemas son propietarios y caros.

[21] http://sourceforge.net/projects/rsyslog/
[22] http://www.snort.org/
[23] http://www.nagios.org/

Además, a pesar de que incluyen un mayor número de controles en sus sistemas, no se llega a abarcar el amplio espectro de controles automatizables.

1.3. Integración de sistemas de seguridad informática

La integración de aplicaciones es tratada en informática mediante el término EAI (Enterprise Application Integration), el cual está relacionado con las tecnologías que permiten el intercambio de información entre diferentes aplicaciones y procesos empresariales [103]. Se plantea que este es un aspecto clave para la competitividad y eficiencia de las empresas [103-105].

La integración de aplicaciones puede ser vista desde diferentes dimensiones que incluyen el alcance (dentro de la empresa o entre empresas), los niveles (hardware, plataformas, sintáctico, semántico) o las capas de integración (comunicación, datos, negocio, presentación) [106]. Múltiples técnicas pueden ser utilizadas para la implementación de los componentes y conceptos asociados a la integración de aplicaciones empresariales. EAI involucra sistemas middleware como MOM (message-oriented middleware), estándares de representación de datos como XML (extensible markup language) y el uso de servicios web como parte de arquitecturas orientadas a servicios (SOA, por sus siglas en inglés) [107-110].

El desarrollo de sistemas para la integración de aplicaciones empresariales comenzó desde mediados de los 90, inicialmente con los conceptos de middleware y posteriormente con las arquitecturas orientadas a servicios [111-113]. Los productos y empresas líderes en esta temática son analizados en [114]. En esa publicación de la consultora Gartner se ofrece una valoración de los sistemas que permiten la integración de aplicaciones empresariales en sentido general. En el contexto de la seguridad informática destacan los sistemas SIEM (Security Information and Event Management), los cuales posibilitan la integración específicamente de aplicaciones de seguridad informática.

1.3.1. Sistemas de gestión de información y eventos de seguridad (SIEM)

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 [115]:

- *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 el monitoreo 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 el monitoreo 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 [116]. La arquitectura funcional de un sistema SIEM se muestra en la Figura 1.2.

Las trazas de los diferentes sistemas, aplicaciones, herramientas y dispositivos pueden ser recolectadas mediante los siguientes métodos [115]:

- Recepción de una cadena de datos en formato *syslog*[24] 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.

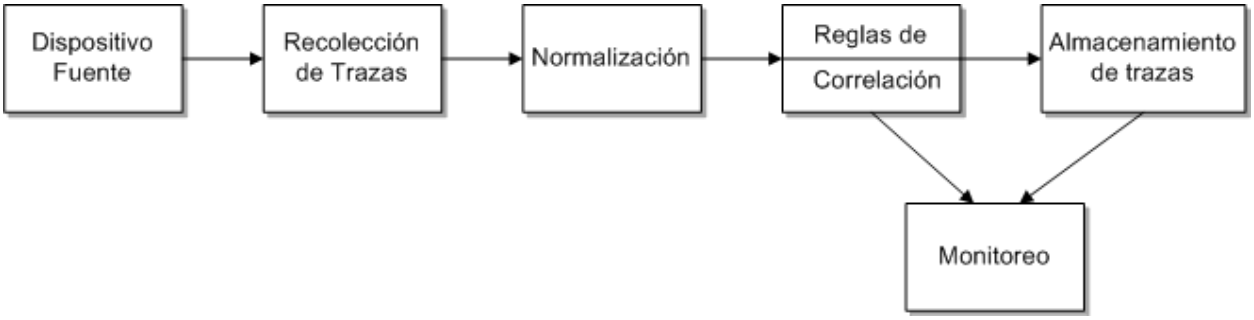


Figura 1.2: Arquitectura funcional de un sistema SIEM. Fuente: Miller et al. [116]

Una vez que las trazas de los diferentes sistemas son obtenidas por alguno 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

[24] *Syslog* es un estándar de facto para el envío de trazas. Por *syslog* se conoce tanto al protocolo como a la aplicación o biblioteca que envía los mensajes de registro.

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. Para llevar a cabo esta función el sistema SIEM posee un grupo de reglas de correlación predefinidas y permite la definición de nuevas reglas. Se pueden definir tres tipos de correlación [117]:

- *Correlación lógica*: tiene en cuenta la ocurrencia de eventos del mismo tipo en diferentes instantes de tiempo para identificar con mayor fiabilidad los ataques. Un ejemplo de este tipo de correlación lo constituye el análisis de varios eventos de autenticación fallida contra un sistema operativo o aplicación, lo cual pudiera constituir un ataque de fuerza bruta.
- *Correlación cruzada*: implica el análisis de eventos de seguridad de diferentes sistemas, dispositivos y aplicaciones, para eliminar alertas que pueden constituir falsos positivos. Un ejemplo de esto lo constituye la correlación de información entre un IDS y un escáner de vulnerabilidades, donde se emitirían alarmas de mayor impacto ante la detección de ataques (reportados por el IDS) que van dirigidos contra sistemas que son vulnerables (reportados por el escáner de vulnerabilidades).
- *Correlación de activos*: implica el análisis de eventos de seguridad en el contexto de la organización, donde se tiene en cuenta la importancia de los activos informáticos a la hora de emitir alertas sobre los ataques detectados. Este tipo de correlación implica que se le debe definir al sistema SIEM la importancia de los activos de la organización, para que pueda contextualizar los ataques recibidos.

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 [116].

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.

1.3.1.1. Principales sistemas SIEM existentes

El mercado de los sistemas SIEM se considera maduro y muy competitivo. Se encuentra en una fase de adopción amplia donde múltiples desarrolladores de SIEM ofrecen las funciones básicas de gestión de trazas, monitoreo de eventos y cumplimiento de regulaciones. Se aprecia además una tendencia a expandir el alcance de los sistemas SIEM para incluir capacidades adicionales en áreas adyacentes de la seguridad informática, como por ejemplo la evaluación de vulnerabilidades, el chequeo de configuraciones y el monitoreo de integridad de ficheros [118]. En la Figura 1.3 se muestran los principales productos SIEM, de acuerdo a un estudio de la consultora Gartner, los cuales son ubicados en diferentes cuadrantes según las características que poseen, sus capacidades y los ingresos de las compañías que los desarrollan. En esa publicación se detallan las fortalezas y debilidades de cada uno de los sistemas SIEM analizados.

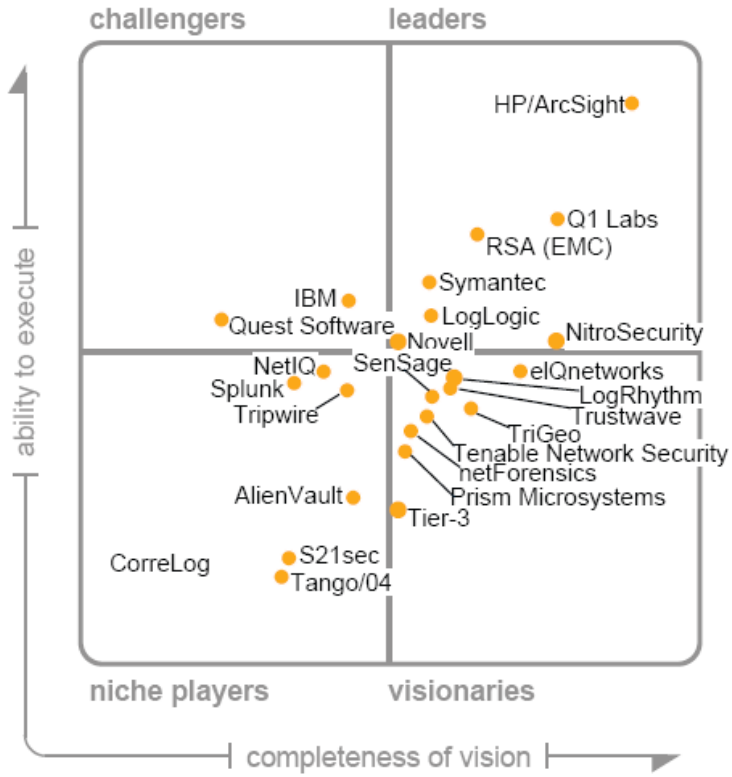


Figura 1.3: Cuadrante mágico para los sistemas SIEM. Fuente: Gartner [118]

Cabe destacar que en el cuadrante de los líderes están ubicadas las empresas que proveen productos SIEM completamente funcionales de acuerdo a los requerimientos del mercado, con una gran visión en el desarrollo de sus sistemas, y que exhiben grandes ingresos anuales, con un crecimiento sostenido por la venta de estos sistemas [118].

Es importante señalar también que todos los productos SIEM que aparecen en la Figura 1.3 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[25].

[25] La Licencia Pública General de GNU (GPL por sus siglas en inglés) es una licencia creada por la Free Software Foundation que está orientada principalmente a proteger la libre distribución, modificación y uso del software.

1.3.1.2. Potencial de integración y automatización de los sistemas SIEM

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 algún software para la gestión de trazas [1]. Por otra parte, la encuesta del instituto SANS sobre gestión de trazas muestra que las tres principales razones para recolectar trazas y utilizar sistemas SIEM son: 1) detectar incidentes, 2) analizar lo que ha sucedido mediante análisis forense, y 3) cumplir con las regulaciones establecidas [119].

En otros trabajos consultados [115], [120], [121] se ofrece una visión un poco más amplia del uso que puede hacerse de los sistemas SIEM, donde se incluyen capacidades adicionales como el monitoreo de la actividad de los usuarios, la protección contra programas malignos y la respuesta a incidentes. Sin embargo, el autor del presente trabajo considera que 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 controles.

A continuación se describen un grupo de características de los sistemas SIEM que, a juicio del autor del presente trabajo, son fundamentales para la gestión automatizada e integrada de controles de seguridad informática.

- *Gestión centralizada de información de seguridad*: los sistemas SIEM permiten concentrar un único lugar todos los eventos y trazas de seguridad generados por las diferentes herramientas, aplicaciones y dispositivos; permitiendo tener una visión integral del estado de la seguridad informática.
- *Correlación automatizada de eventos*: los sistemas SIEM realizan de forma automática la correlación de información de diferentes herramientas de seguridad, lo

cual elimina gran cantidad de falsos positivos y permite a los especialistas de seguridad informática concentrarse en las alarmas significativas. Esto ahorra gran cantidad de tiempo en el análisis de información y añade de forma automática cierta inteligencia a la gestión de eventos de seguridad.

- *Integración de diferentes herramientas de seguridad*: los sistemas SIEM permiten integrar prácticamente cualquier sistema, aplicación, dispositivo o herramienta de seguridad existente. Mediante la definición de conectores es posible interpretar la información proveniente de todos los sistemas, convirtiendo al sistema SIEM en un concentrador universal.
- *Espectro de controles incluidos*: los sistemas SIEM han ido evolucionando e incluyendo más funcionalidades dentro de la propia solución. Varios desarrolladores de sistemas SIEM han comenzado a comercializar sus productos como plataformas con mayor alcance que incluyen otros controles de seguridad. En la Tabla 1.8 se ofrece un resumen de las capacidades de los sistemas SIEM líderes en el mercado, donde puede apreciarse que van más allá de la detección de incidentes y la gestión de trazas.
- *Generación automática de reportes*: al tener toda la información de seguridad concentrada en el sistema SIEM, es posible generar reportes de forma automatizada, con información significativa para la gestión de la seguridad. Estos reportes pueden ser actualizados en tiempo real, permitiendo un adecuado monitoreo y revisión de la efectividad del sistema de seguridad informática implementado.

Tabla 1.8: Controles de seguridad informática incluidos en sistemas SIEM

Sistemas SIEM	Controles de seguridad informática					
	Inventario de activos	**Monitoreo de usuarios**	**Gestión de trazas**	**Monitoreo de eventos**	**Chequeo de cumplimiento**	**Gestión de incidentes**
HP/ArcSight – *ESM*		X	X	X	X	X
Q1 Labs – *Qradar*	X		X	X	X	X
RSA (EMC) – *enVision*			X	X	X	X
Symantec – *SSIM*			X	X	X	X
LogLogic – *SEM*			X	X	X	X
NitroSecurity - *NitroView ESM*			X	X	X	X
Novell – *Sentinel*		X	X	X	X	X

Es importante señalar que la simple instalación de un sistema SIEM no garantiza por sí sola la integración de los sistemas y la automatización de controles. Para que este tipo de sistema sea efectivo es necesario realizar un proceso profundo de ajuste y personalización donde se defina de forma adecuada el contexto de la organización. Esto se logra mediante la utilización de reglas de correlación, la valoración correcta de los activos de la organización y un adecuado filtraje de eventos de seguridad [120], [121]. Aunque la utilización de los sistemas SIEM no es el único factor para disminuir la complejidad y aumentar la efectividad de los controles de seguridad informática, ha quedado evidenciado que estos cuentan con virtudes que le permiten ser utilizados en la concepción de una gestión integrada con elevados niveles de automatización.

1.4. Conclusiones parciales

Actualmente existen varios modelos, estándares, recomendaciones y regulaciones relacionados con la gestión de la seguridad de la información. De manera general todos plantean varias acciones que conforman un ciclo cerrado para la mejora continua del sistema. Como parte de este proceso se recomiendan más de 100 controles que no son solo de corte técnico, sino que involucran también aspectos organizativos y de recursos humanos. En este sentido es necesario realizar una labor de síntesis de controles y un análisis exhaustivo de los controles de seguridad informática que pueden ser automatizados.

La efectividad de los controles de seguridad informática se mide mediante métricas que permitan evaluar el cumplimiento de los objetivos de seguridad establecidos. Este es un campo que todavía se encuentra en investigación y desarrollo. Existen algunos ejemplos de métricas pero no hay consenso sobre las mismas y estas no abarcan el amplio espectro de controles propuestos por los principales estándares. Por tanto, será necesario definir y seleccionar las métricas que permitan medir la efectividad de los controles de seguridad informática.

La mayoría de las investigaciones sobre automatización en el contexto de la seguridad de la información aborda el tema desde una perspectiva puntual, refiriéndose a la automatización de controles específicos de seguridad informática. Los trabajos que son un poco más abarcadores son SCAP y CAG. Sin embargo, el alcance los mismos todavía es limitado y la automatización de los controles es vista de manera independiente mediante sistemas con aplicaciones de gestión diferentes. Es necesaria una solución que permita la gestión no solo automatizada, sino también integrada de los controles de seguridad informática. En este sentido el autor del presente trabajo se inclina por la utilización de los sistemas SIEM, los cuales poseen un gran potencial para lograr este objetivo.

CAPÍTULO 2

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

CAPÍTULO 2. MODELO PARA LA GESTIÓN AUTOMATIZADA E INTEGRADA DE CONTROLES DE SEGURIDAD INFORMÁTICA

Con el objetivo de aumentar la efectividad de los controles y disminuir la complejidad de la gestión de la seguridad informática, en el presente capítulo se desarrolla un modelo para la gestión automatizada e integrada de controles de seguridad informática. Como parte del modelo se define el concepto de gestión automatizada de controles, se identifican los controles automatizables y se proponen un grupo de métricas para medir la efectividad de los mismos.

2.1. Gestión automatizada de controles de seguridad informática.

Para poder desarrollar un modelo de gestión basado en la integración y la automatización de controles, se impone primeramente trabajar con una definición clara de lo que significa la gestión automatizada de controles de seguridad informática. Resulta entonces necesario tomar como referencia los conceptos de gestión de la seguridad de la información y de automatización especificados en las secciones 1.1.1.1 y 1.2.1 del presente trabajo.

El enfoque de procesos definido de manera global para un SGSI también se presenta al nivel de los controles de seguridad informática. En el presente trabajo se asumirá el modelo de gestión propuesto en el estándar ISO/IEC 27001. De esta forma se puede afirmar que los controles necesitan ser adecuadamente establecidos, implementados, operados, monitorizados, revisados, mantenidos y mejorados; para garantizar el cumplimiento de los objetivos del sistema de seguridad informática. Por tanto, gestionar los controles de seguridad informática implica realizar las siete acciones mencionadas.

A partir de las definiciones globales de estas acciones para un SGSI, en el presente trabajo se definen las mismas al nivel de los controles de seguridad informática como sigue:

- *Establecer*: definir los objetivos y el alcance del control de acuerdo al análisis de riesgos realizado, especificar los procedimientos de operación y seleccionar los medios técnicos y humanos encargados de su implementación.
- *Implementar*: instalar los sistemas informáticos y/o herramientas de hardware, así como establecer los aspectos organizativos necesarios para la implantación del control.
- *Operar*: llevar a cabo las acciones necesarias para la ejecución de los procedimientos establecidos.
- *Monitorizar*: supervisar el correcto funcionamiento del control emitiendo alertas ante fallos de operación.
- *Revisar*: evaluar la efectividad del control con respecto al cumplimiento de sus objetivos, mediante indicadores previamente establecidos.
- *Mantener y mejorar*: realizar las modificaciones necesarias al control para el mantenimiento y la mejora continua del mismo, a partir de los resultados de la revisión y las experiencias adquiridas.

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 y/o herramientas de hardware existentes; 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 monitoriza la realización de los respaldos y notifica ante la ocurrencia de cualquier problema. La revisión del mismo puede realizarse mediante la comprobación automatizada de la existencia e integridad de los respaldos para los sistemas operativos y aplicaciones que lo requieran.

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. Por tanto, la automatización se enmarca en las fases *Hacer* y *Verificar* del ciclo PDCA, descrito en la sección 1.1.1.1, para la gestión de la seguridad de la información. Con respecto a las categorías que describen los distintos niveles de gestión autonómica (sección 1.2.1), el concepto propuesto correspondería a la categoría dos: nivel de gestión.

2.2. Controles de seguridad informática automatizables

Teniendo en cuenta la definición de automatización adoptada en la sección anterior, es posible determinar los controles de seguridad informática que pueden ser automatizados. Evidentemente los controles automatizables son aquellos que están más relacionados con medios técnicos, los cuales pueden ser implementados mediante sistemas informáticos y/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 [15].
- 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 [15].

Como ya fue comentado en el capítulo anterior, existe un estudio sobre veinte controles críticos de seguridad informática que plantea que quince de esos controles pueden ser automatizados; pero se ignoran un grupo de controles de seguridad física. En [122] 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 relacionados con los usuarios finales, y no se analizan el resto de los controles de seguridad informática.

Un análisis más integrador, donde se tienen en cuenta todos los controles de seguridad informática propuestos por las principales guías y estándares internacionales, fue realizado por el autor del presente trabajo en [123]. Los resultados de esa investigación constituyen un aporte en el área de la automatización de controles de seguridad informática y se exponen a continuación.

Para determinar los controles de seguridad informática automatizables, se realizó un análisis de todos los controles especificados en los estándares ISO/IEC 27002 y NIST SP 800-53, aplicando la definición de automatización de la sección 2.1. En la Tabla 2.1 se muestran los resultados del análisis para el estándar ISO/IEC 27002, especificando la cantidad de controles automatizables en cada dominio y poniendo un ejemplo en cada caso. El listado completo de los controles automatizables se muestra en el Anexo 2.

Tabla 2.1: Controles de seguridad informática automatizables en ISO/IEC 27002

No.	Dominio	Controles	Controles automatizables	Porciento	Ejemplos
5	Política de seguridad	2	0	0.0 %	-
6	Organización de la seguridad de la información	11	0	0.0 %	-
7	Gestión de activos	5	1	20.0 %	Inventario de activos
8	Seguridad ligada a los recursos humanos	9	1	11.1 %	Remoción de derechos de acceso
9	Seguridad física y ambiental	13	2	15.4%	Controles de acceso físico
10	Gestión de comunicaciones y operaciones	32	15	46.9%	Respaldo de información
11	Control de acceso	25	13	52.0 %	Identificación y autenticación de los usuarios
12	Adquisición, desarrollo y mantenimiento de sistemas de información	16	4	25.0 %	Control de vulnerabilidades técnicas
13	Gestión de incidentes de seguridad informática	5	1	20.0 %	Reporte de eventos de seguridad informática
14	Gestión de la continuidad del negocio	5	1	20.0 %	Desarrollo e implementación de planes de continuidad
15	Cumplimiento	10	1	10.0 %	Verificación del cumplimiento técnico
	Total	**133**	**39**	**29.3 %**	

Como puede apreciarse, el análisis muestra que el 29,3% de los controles propuestos en ISO/IEC 27002 son automatizables. Al analizar la cantidad de controles que pueden ser automatizados por cada dominio, puede observarse que aquellos que tienen un fuerte componente de controles organizativos y de recursos humanos, poseen, como es de esperar, menos controles automatizables que los dominios donde predominan los controles técnicos.

Al realizar un análisis similar para el estándar NIST SP 800-53, se aprecia que el 31,3% de los controles de seguridad informática pueden ser automatizados. En la Figura 2.1 se muestra el porciento de controles automatizables para cada dominio y en el Anexo 3 se ofrece el listado completo de los controles automatizables en este caso.

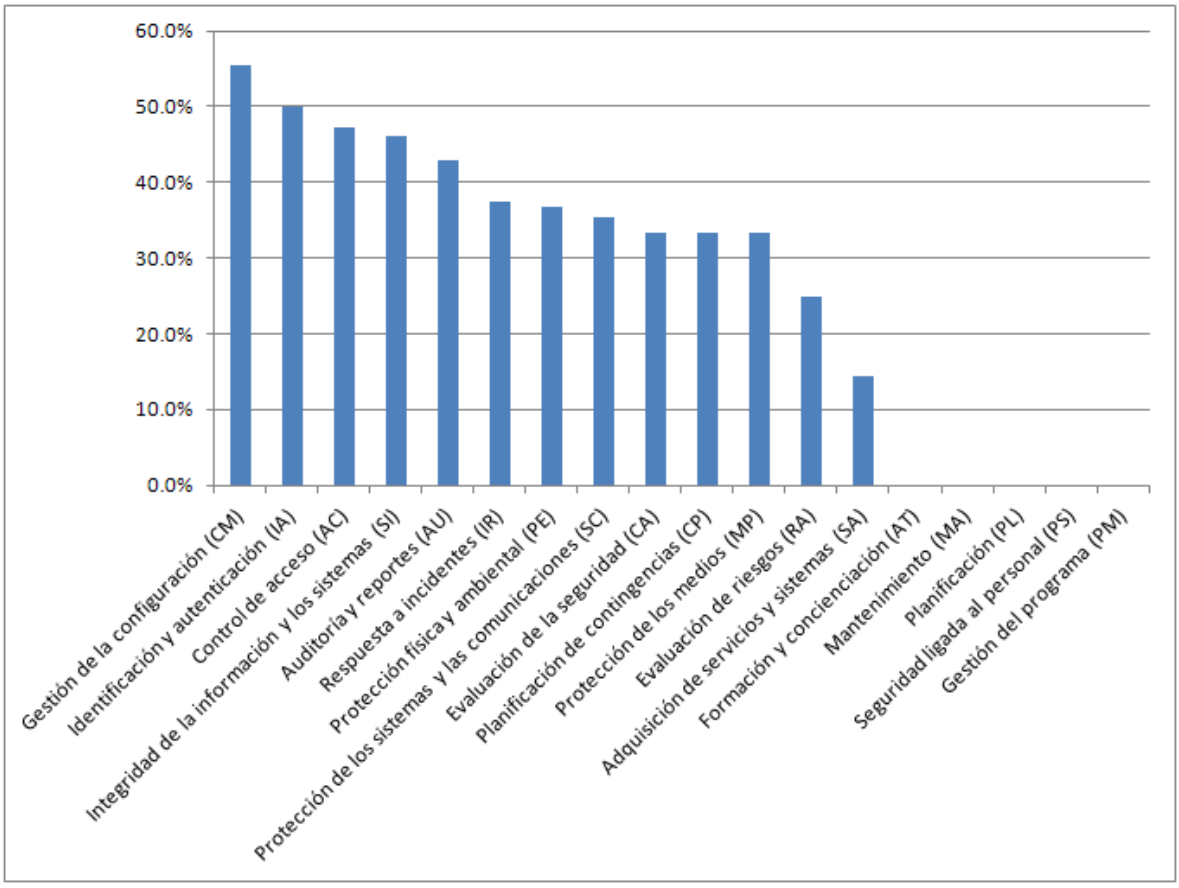


Figura 2.1: Porciento de controles automatizables en cada dominio de NIST SP 800-53

Del análisis realizado se puede concluir que aproximadamente el 30% de los controles de seguridad informática definidos en los principales estándares internacionales son automatizables.

2.3. Modelo para la gestión automatizada e integrada de controles de seguridad informática (GAISI)

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

1. *Máxima 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 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 evaluar y 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 a una gran variedad de organizaciones.

2.3.1. Esquema y características generales del modelo

Teniendo en cuenta los principios anteriores, el concepto de automatización definido previamente, los controles automatizables identificados, y considerando el potencial de automatización e integración que poseen los sistemas SIEM; en el presente trabajo se

propone un modelo para la **g**estión **a**utomatizada e **i**ntegrada de controles de **s**eguridad **i**nformática (GAISI), que constituye el principal aporte de la investigación realizada. La representación gráfica del modelo se muestra en la Figura 2.2.

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. Estos macro-controles representan una agrupación y síntesis de los controles automatizables identificados en los estándares ISO/IEC 27002 y NIST SP 800-53. Mediante la Tabla 2.2 se establece una correspondencia con los estándares mencionados.
- 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, 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 herramientas, pero su monitorización se realiza de forma centralizada en el sistema SIEM. Este recibe la información mediante las trazas generadas por los diferentes sistemas, para lo cual es necesario definir **conectores** que permitan interpretar los diferentes formatos de trazas existentes.
- La revisión de los controles se realiza mediante un grupo de **métricas** de seguridad informática, definidas también como parte del modelo, que son calculadas y reportadas de forma automatizada.

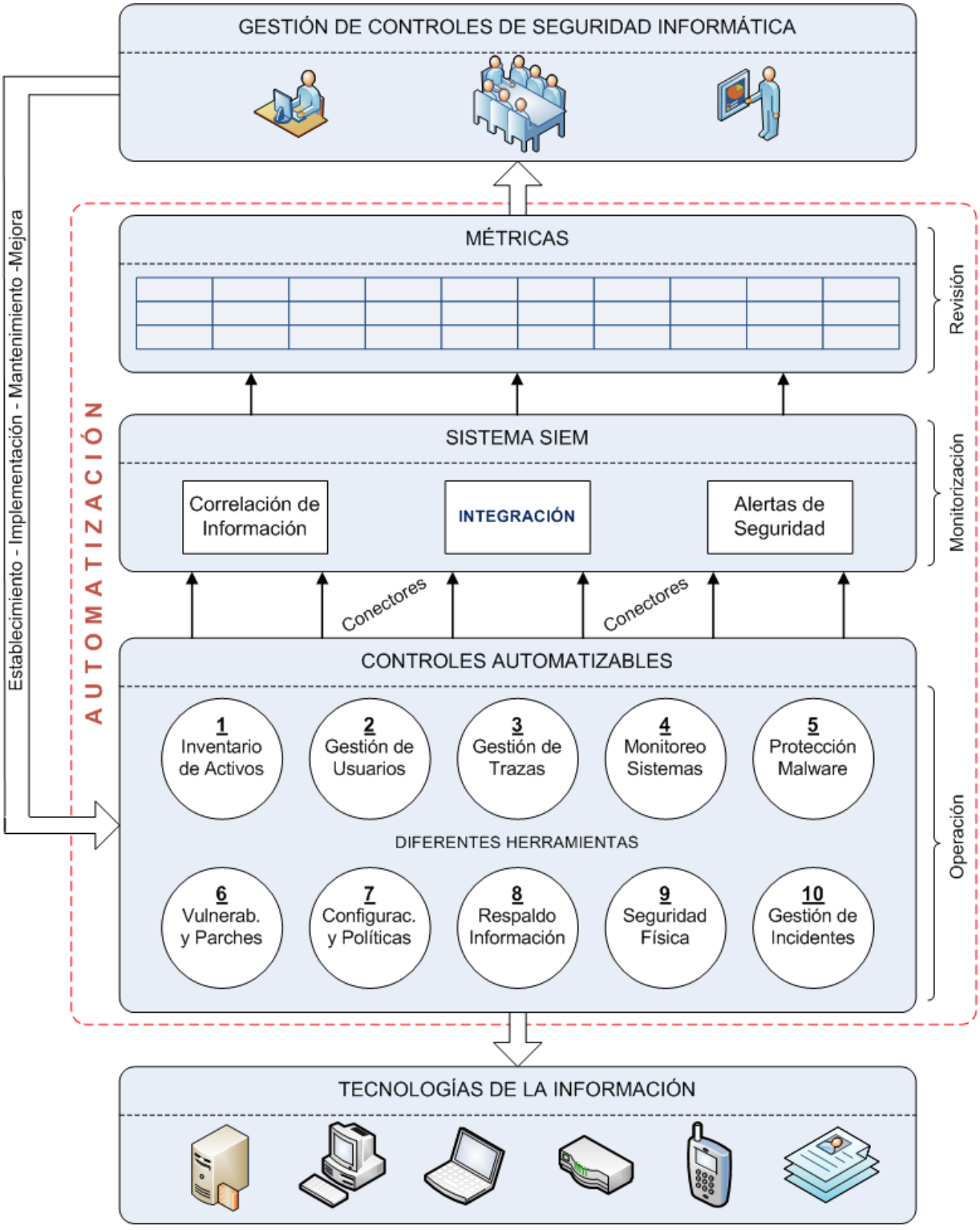


Figura 2.2: Modelo para la gestión automatizada e integrada de controles de seguridad informática (GAISI)

Tabla 2.2: Agrupación de los controles automatizables en 10 macro-controles

No.	Macro-control	Correspondencia entre los controles			
		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 incidentes	13.1.1	IR-4, IR-5, IR-6	18	86,89

En la clasificación presentada en la Tabla 2.2 se incluyó además la correspondencia con los veinte controles críticos definidos en [29] y con los controles especificados en los artículos de la Resolución 127/2007 del MIC. En estos casos están representados el 80% de los controles de CAG y el 37% de los controles de la Resolución 127.

El modelo propuesto constituye una extensión de un marco de trabajo propuesto por el autor del presente trabajo en [124] , a partir de la incorporación de la actividad de revisión de los macro-controles mediante un grupo de métricas definidas como parte del modelo GAISI.

2.3.2. Automatización de los controles y su interacción con el sistema SIEM

A continuación se ofrece una explicación detallada de los componentes del modelo propuesto, mediante la descripción de los 10 macro-controles automatizables y su interacción con el sistema SIEM. Es importante señalar que aunque los controles de seguridad informática están descritos en diferentes estándares y que los 10 macro-controles definidos en el modelo poseen una correspondencia con dichos controles reflejada en la Tabla 2.2, el enfoque de automatización y la síntesis de los mismos, así como su interrelación con el sistema SIEM, constituyen aportes de la presente investigación.

1. *Inventario de activos*: se debe tener un inventario de todos los activos de la institución, tanto de hardware como de software, el cual deberá ser continuamente actualizado y mantenido.

Para implementar este control debe emplearse un sistema que permita realizar de forma automatizada un descubrimiento de todos los equipos conectados a la red de datos de la organización, identificando los sistemas operativos y aplicaciones que estos poseen. Se deberán instalar “agentes” en todas las computadoras, servidores y dispositivos; que ofrezcan información detallada sobre las características de hardware y software que poseen todos los equipos. El sistema de inventario deberá identificar los sistemas operativos y aplicaciones instaladas en los diferentes equipos, así como las versiones y parches aplicados.

Deberán emplearse otras herramientas, como analizadores de tráfico y escáneres de red, para identificar los sistemas que se encuentran conectados a la red de datos, y así complementar la información del sistema de inventario.

El inventario de hardware y software debe encontrarse actualizado en tiempo real, identificando cualquier desviación fuera de lo establecido. El sistema deberá emitir alertas si se añade o sustrae cualquier dispositivo de la red, si se modifican las características de hardware de los equipos, o si se instala o desinstala cualquier aplicación en las computadoras.

1.1. El sistema SIEM permite diferenciar los activos de la organización de acuerdo a su nivel de importancia, lo cual posibilita contextualizar las alertas recibidas por las diferentes herramientas, permitiendo ejecutar acciones diferenciadas para activos con diferente valor. La integración de otros sistemas de monitoreo de red en el sistema SIEM permite complementar la información del sistema de inventario con la ofrecida por los escáneres de red y las herramientas de monitoreo de tráfico, para detectar la presencia de equipos no autorizados.

2. *Gestión de usuarios*: se deberá emplear un sistema de gestión de identidades y accesos (IAM, por sus siglas en inglés) para la gestión de las cuentas de los usuarios de las tecnologías de la información. Esto implica el establecimiento, activación, modificación y eliminación de cuentas de usuarios.

Deben emplearse mecanismos automatizados para la revisión de todas las cuentas establecidas y deshabilitar aquellas que no pueden ser asociadas con áreas o procesos de la organización. Se debe establecer un procedimiento automático para revocar los permisos y deshabilitar las cuentas, de forma inmediata, al personal que cause baja de la institución.

Se deberá monitorear regularmente el uso de todas las cuentas de usuarios de la organización, deshabilitando automáticamente aquellas que no han tenido actividad en un

período de tiempo determinado (ej. 30 días) y notificando inmediatamente al directivo responsable del área a la que pertenece el usuario. Los sistemas informáticos deberán terminar las sesiones de usuarios pasado un determinado tiempo de inactividad, forzando a una nueva autenticación en el sistema.

Las instituciones deberán definir el horario de trabajo de los usuarios, de forma tal que se notifique automáticamente ante el uso de cuentas fuera del horario establecido a los administradores del sistema y los jefes de las diferentes áreas de la organización.

2.1. El sistema SIEM permite realizar un seguimiento a la actividad de los usuarios de las tecnologías de la información en la institución. Mediante la correlación de información y la integración del sistema de gestión de identidades es posible asociar las trazas de las diferentes aplicaciones, que generalmente registran las direcciones IP, a las cuentas de usuarios de la institución. Se deberá monitorear especialmente la actividad de cuentas de usuarios que causaron baja de la institución, emitiendo alertas y creando un nuevo ticket en el sistema de gestión de incidentes cuando esto ocurra.

3. *Gestión de trazas*: las aplicaciones, sistemas operativos y diferentes dispositivos deberán generar trazas de seguridad donde se registre la actividad de los usuarios, errores, conexiones de red y otros eventos de seguridad en general; las cuales deberán ser almacenadas automáticamente en un sistema centralizado de gestión de trazas. Las trazas deberán ser almacenas, como mínimo, por el tiempo establecido en las regulaciones existentes, con el objetivo de aclarar cualquier incidente de seguridad en ese período de tiempo.

3.1. El sistema SIEM permite la implementación completa de este control, porque precisamente está diseñado para recibir las trazas de seguridad de una gran cantidad de aplicaciones, con la posibilidad de definir conectores para aquellos

sistemas y dispositivos que no vienen incluidos por defecto en la solución. Los sistemas de gestión de eventos e información de seguridad permiten realizar búsquedas “inteligentes” en las trazas porque consolidan la información de diferentes herramientas y poseen una interfaz gráfica que facilita esta tarea; permitiendo filtrar por fecha, direcciones IP y palabras clave, entre otros atributos. El sistema SIEM almacena las trazas más recientes en una base de datos para agilizar la búsqueda de información.

4. *Monitoreo de los sistemas*: la organización deberá realizar un monitoreo constante de los sistemas para detectar ataques informáticos, problemas en las aplicaciones que afecten la disponibilidad de las mismas, y modificaciones de información en los diferentes sistemas.

Para implementar este control deberán instalarse sistemas de detección de intrusiones (IDS), sistemas de chequeo de la disponibilidad de aplicaciones, así como herramientas que permitan realizar chequeos de integridad a los sistemas y archivos importantes de la organización. Todos estos sistemas deberán emitir notificaciones automáticas ante la detección de problemas, alertando en tiempo real a los administradores de los sistemas sobre los eventos de seguridad que están ocurriendo.

Es posible emplear sistemas que reaccionen de forma activa ante la detección de eventos, tomando acciones correctivas y no solo notificando ante la detección de los mismos. En este sentido pudieran utilizarse sistemas de prevención de intrusiones (IPS) que automáticamente bloqueen las direcciones IP desde donde se producen los ataques, así como otros mecanismos que reinicien automáticamente los sistemas no disponibles y que restituyan la información modificada.

La autenticación en los diferentes sistemas y servidores críticos de la institución, utilizando cuentas con privilegios de administración, deberá ser adecuadamente monitoreada y

notificada a los especialistas de seguridad informática y administradores de los sistemas; con el objetivo de llevar un control estricto de este tipo de acciones. De la misma forma se deberá notificar sobre intentos fallidos de autenticación a estos sistemas, debido a que pueden ser indicios de posibles ataques sobre los mismos.

4.1. El sistema SIEM posibilita el análisis en tiempo real de todos los eventos de seguridad de las aplicaciones integradas al mismo, generando automáticamente alertas y abriendo tickets en el sistema de gestión de incidentes ante determinados tipos de eventos de seguridad. La correlación de la información de los diferentes sistemas permite reducir los falsos positivos y realizar un análisis contextualizado de lo que está sucediendo. Es posible correlacionar las alertas del IDS con la información del escáner de vulnerabilidades y el sistema de inventario de activos, para eliminar aquellas que se refieren a ataques sobre vulnerabilidades, sistemas operativos y aplicaciones inexistentes; generando alarmas de mayor impacto cuando se producen ataques sobre sistemas críticos de la organización.

5. *Protección contra programas malignos*: se deberán emplear mecanismos de protección contra programas malignos en los puntos de entrada y salida de información, estaciones de trabajo y servidores; para detectar y erradicar código malicioso.

Para la implementación adecuada de este control es necesario utilizar sistemas antivirus concebidos para entornos empresariales, que permitan una gestión centralizada mediante un kit de administración. Esto permitirá la configuración y el monitoreo automático de los programas antivirus instalados en los servidores y estaciones de trabajo, teniendo el reporte actualizado de la actualización de las bases de virus de los sistemas y los programas malignos detectados. El software utilizado deberá tener las funcionalidades de antivirus, anti-spyware, anti-SPAM y detección de intrusos de host (HIDS, por sus siglas en inglés), para que provea una protección integral ante estos tipos de ataques.

La organización deberá gestionar centralizadamente los mecanismos de protección empleados, identificando continuamente aquellos sistemas que no tienen las firmas de virus actualizadas y actuando rápidamente sobre ellos.

5.1. Los ficheros de reportes, trazas y eventos de los sistemas de protección contra programas malignos deben ser enviados al sistema SIEM para su correlación con otros eventos de seguridad, y la apertura de tickets en el sistema de gestión de incidentes en caso de epidemias generalizadas. Mediante el análisis del tráfico de la red realizado por otras herramientas integradas al sistema SIEM, es posible descubrir de forma automática la presencia de gusanos y otros programas malignos no detectados por los sistemas antivirus, debido a que pueden generar tráfico anómalo en la red de datos de la institución.

6. *Detección de vulnerabilidades y gestión de parches*: se deben realizar escaneos periódicos en busca de vulnerabilidades en los sistemas, así como emplear un sistema automatizado de gestión de parches para todos los sistemas operativos y aplicaciones de la institución.

Se deberán utilizar herramientas de escaneo de vulnerabilidades que permitan automatizar la detección periódica de vulnerabilidades en los sistemas y la comparación automática de los resultados de los escaneos a lo largo del tiempo, para verificar que las vulnerabilidades fueron mitigadas adecuadamente. Las herramientas de escaneo de vulnerabilidades deberán integrarse con los sistemas de gestión de incidentes, para reportar automáticamente las vulnerabilidades detectadas y garantizar de esta manera que el problema está registrado y deberá ser solucionado.

El sistema de gestión de parches a emplear deberá distribuir automáticamente las actualizaciones a los diferentes sistemas operativos y aplicaciones, llevando un registro centralizado del estado de los sistemas y priorizando las actualizaciones críticas de

seguridad que pondrían en peligro la seguridad informática de la organización. En el caso de los sistemas críticos deberán probarse las actualizaciones de las aplicaciones en un entorno de pruebas, antes de distribuirlas, para garantizar el correcto funcionamiento de los diferentes sistemas informáticos después de la instalación de los parches.

6.1. El sistema SIEM permite la integración del sistema de detección de vulnerabilidades y el sistema de gestión de incidentes, abriendo automáticamente nuevos tickets ante las vulnerabilidades detectadas. La información del escáner de vulnerabilidades puede ser correlacionada con los eventos de seguridad que están ocurriendo en tiempo real, con el objetivo de contextualizar las amenazas y tomar acciones inmediatas ante ataques que se producen contra los sistemas vulnerables e importantes para la organización.

7. *Configuraciones de seguridad y cumplimiento de políticas*: se deberán emplear sistemas de gestión de configuraciones que permitan establecer, de forma automática, configuraciones de seguridad homogéneas en los servidores y estaciones de trabajo. Los sistemas deberán ser chequeados periódicamente para revisar si la configuración de los mismos está acorde con las políticas de seguridad y las regulaciones establecidas.

Se deberán emplear listas de chequeo de configuraciones de seguridad reconocidas a nivel internacional, como las de la Base de Datos Nacional de Vulnerabilidades (NVD) y las del Centro para la Seguridad de Internet (CIS), para la revisión de la configuración segura de los diferentes sistemas operativos y aplicaciones. Este proceso de revisión deberá realizarse mediante aplicaciones que realicen el chequeo de forma automática y generen un reporte con las deficiencias encontradas. Deben seleccionarse herramientas que interpreten listas de chequeo expresadas en SCAP, con el objetivo de utilizar listas estandarizadas y reconocidas por la comunidad internacional. Estas listas pueden ser modificadas y adaptadas a las

condiciones particulares de la institución, estableciendo una línea base de configuraciones de seguridad para los sistemas informáticos.

Será necesario traducir las políticas de seguridad de la organización y las indicaciones de las regulaciones establecidas, en los casos que sea posible, a configuraciones de seguridad de sistemas y aplicaciones expresadas a bajo nivel; con el objetivo de poder evaluar el cumplimiento técnico de las políticas y regulaciones. Esto implica que en las listas de chequeo de configuraciones de seguridad debe haber una referencia a las políticas y regulaciones que se cumplen con las configuraciones implementadas.

7.1. Los sistemas SIEM generalmente poseen un módulo de chequeo del cumplimiento de regulaciones y estándares internacionales, como el ISO/IEC 27001, que revisa precisamente el cumplimiento de esas políticas a partir de un análisis de la información contenida en todos los eventos de seguridad y las trazas de las diferentes aplicaciones que el sistema SIEM colecciona. Mediante la definición de políticas y reglas de correlación en el sistema SIEM, este pudiera emitir alertas ante el incumplimiento de lo que está establecido.

8. *Respaldo de información*: se deben realizar diariamente, o con la frecuencia que se determine, copias de respaldo de la información y los sistemas, que garanticen la recuperación de los mismos ante la ocurrencia de algún incidente.

Los sistemas deben ser respaldados mediante la utilización de herramientas que permitan la definición de un cronograma de salvas y la realización de las mismas de forma completamente automatizada. El monitoreo del proceso y la notificación de problemas en el mismo debe realizarse también automáticamente. Se deberá emplear una herramienta que permita el monitoreo centralizado de todo el proceso del salvas.

8.1. El sistema SIEM podrá realizar el monitoreo centralizado del proceso de respaldo y correlacionar la información con el sistema de inventario de activos, emitiendo

alertas ante sistemas que no tengan respaldos, haciendo especial énfasis en aquellos que son críticos para la organización.

9. *Seguridad física*: los locales donde se encuentran las tecnologías de la información, especialmente los que alojan los sistemas críticos de la organización, deberán estar adecuadamente protegidos mediante sistemas de control de acceso físico, respaldo eléctrico, control de humedad y clima, protección de incendios y sistemas de alarmas contra intrusos. Todos estos sistemas deberán funcionar de forma automatizada garantizando la protección física de los activos. Los sistemas de control de acceso físico pudieran estar integrados con los sistemas lógicos de control de acceso a las tecnologías de la información de la organización, con lo que se lograría un máximo de automatización en este sentido.
    9.1. Si los sistemas de protección física son monitoreados por software y atendidos desde una sala de control, como debiera ocurrir, entonces la información de los mismos pudiera ser recolectada por el sistema SIEM de la misma forma que sucede con el resto de los controles. Al correlacionar la información con el sistema de inventario de activos, se emitirían alertas de mayor impacto ante cualquier incidente de seguridad física que involucre a los sistemas críticos de la organización. El sistema SIEM incorporaría automáticamente los incidentes de seguridad física al sistema de gestión de incidentes.
10. *Gestión de incidentes*: la organización debe establecer un sistema de gestión de incidentes de seguridad informática que incluya la detección, análisis, contención, solución y recuperación de los incidentes. Se deberán utilizar sistemas que implementen de forma automática el proceso de seguimiento de incidentes.

Deberá implementarse un sistema de gestión de incidentes on-line que permita a los usuarios reportar incidentes detectados, y que tenga implementada toda la lógica del

proceso de gestión, de forma tal que los incidentes sean asignados a los especialistas adecuados en dependencia de la naturaleza de los incidentes y las habilidades de los especialistas de seguridad. El sistema deberá emitir automáticamente reportes con el estado de los incidentes de seguridad informática.

10.1. Los sistemas SIEM generalmente tienen integrado un sistema de gestión de incidentes como parte de la solución. El sistema genera tickets automáticamente ante la ocurrencia de alarmas y otros eventos que se definan, como por ejemplo la detección de vulnerabilidades en los sistemas. El monitoreo centralizado de las diferentes herramientas de seguridad permite que el sistema de gestión de incidentes se retroalimente de la información suministrada por las mismas y que posea, en tiempo real, el estado de los incidentes de seguridad informática que ocurren en la institución.

2.3.3. Métricas de seguridad informática

La revisión de los 10 macro-controles de seguridad informática deberá realizarse mediante un grupo de métricas de efectividad que serán calculadas y visualizadas de forma automatizada.

Los controles automatizables identificados en este trabajo, para los cuales será necesario definir y seleccionar los indicadores de efectividad, son controles implementados por diferentes herramientas, de modo que los datos para el cálculo de las métricas de seguridad serán obtenidos de los diferentes sistemas y aplicaciones que implementan dichos controles. El hecho de que el sistema SIEM centralice la información de las diferentes herramientas de seguridad, facilita la obtención de los datos y posibilita el cálculo automático de los indicadores. Normalmente el módulo de reportes del sistema SIEM es configurable por lo

que deberá ser posible visualizar los indicadores calculados en la propia interfaz de este sistema.

La automatización del proceso de medición garantiza que este sea objetivo y repetible en el tiempo, sin depender de evaluadores que puedan influir con criterios subjetivos en los resultados de la medición.

Como parte del modelo GAISI se proponen 24 métricas de seguridad informática, las cuales se listan en la Tabla 2.3. Los indicadores se encuentran enumerados y agrupados por cada uno de los 10 macro-controles del modelo. Para la definición de las métricas se utilizó el método GQM comentado en la sección 1.1.2.3 y en la selección de las mismas se tuvieron en cuenta los indicadores propuestos por otros autores (se indican las referencias en estos casos). En el Anexo 4 se ofrece una descripción detallada de las métricas, incluyendo los objetivos, las preguntas a las que responden, las fuentes de datos, las fórmulas para su cálculo y la frecuencia de medición.

Es importante señalar que solo se definen métricas que pueden ser calculadas de forma automatizada a través del modelo propuesto. Es posible definir otros indicadores de efectividad para los controles de seguridad informática, donde el cálculo de los mismos no puede realizarse de forma automatizada (ver sección 3.2.2.2). La lista propuesta no es exhaustiva, puede enriquecerse con más indicadores que las diferentes instituciones consideren necesario incorporar. No obstante, el listado de las métricas definidas en este trabajo pudiera constituir una referencia para la medición de la efectividad de los controles de seguridad informática incluidos en el modelo GAISI.

Las organizaciones deberán establecer criterios de medida para cada uno de los indicadores de acuerdo a los objetivos trazados en el sistema de seguridad informática, los cuales permitirán evaluar la efectividad de los controles implementados.

Tabla 2.3: Métricas de seguridad informática propuestas en el modelo GAISI

Macro-control	Métricas
1. Inventario de activos	1.1. Cantidad de equipos desconocidos conectados a la red
	1.2. Porciento de equipos con software no autorizado
2. Gestión de usuarios	2.1. Cantidad de cuentas de usuarios que no pueden ser asociadas con algún proceso o área de la institución
	2.2. Cantidad de cuentas de usuarios que permanecen activas sin ser usadas por más de 30 días.
3. Gestión de trazas	3.1. Porciento de sistemas que almacenan trazas de seguridad en una localización centralizada [52]
	3.2. Tiempo de conservación de las trazas
4. Monitorización de los sistemas	4.1. Cantidad de intentos de ataques (por hora) a la DMZ[26]
	4.2. Porciento del tiempo en que los sistemas críticos[27] se encuentran disponibles [52]
5. Protección contra programas malignos	5.1. Porciento de equipos con el antivirus autorizado instalado
	5.2. Porciento de equipos con el antivirus desactualizado [53]
6. Detección de vulnerabilidades y gestión de parches	6.1. Cantidad de vulnerabilidades críticas detectadas [50]
	6.2. Porciento de equipos con vulnerabilidades críticas [60]
	6.3. Tiempo medio de mitigación de vulnerabilidades [60]
	6.4. Porciento de equipos con parches de seguridad críticos pendientes de instalación[50]
	6.5. Tiempo medio de aplicación de los parches de seguridad (desde su publicación hasta la instalación) [60]
7. Configuraciones de seguridad y cumplimiento de políticas	7.1. Porciento de equipos acorde con la imagen y configuraciones de seguridad definidas [60][52]
	7.2. Puntuación (benchmark) de seguridad promedio (de acuerdo a patrones internacionales) [52]
8. Respaldo de información	8.1. Porciento de sistemas críticos respaldados
	8.2. Última fecha en la que todos los respaldos se realizaron de forma exitosa
9. Seguridad física	9.1. Temperatura promedio de operación de los sistemas
	9.2. Cantidad de fallos de corriente eléctrica (por semana)
10. Gestión de incidentes	10.1. Cantidad de incidentes de seguridad informática (por semana) [60][56][50]
	10.2. Tiempo medio de detección de incidentes (desde que ocurrió hasta su registro en el sistema) [60]
	10.3. Tiempo medio de solución de incidentes [60]

[26] La zona desmilitarizada (DMZ) es la subred donde se encuentran los servidores que son accesibles desde una red externa a la organización (generalmente Internet).

[27] Los sistemas críticos son los sistemas más importantes de la organización, identificados en el análisis de riesgos, cuya afectación tendría consecuencias graves para el funcionamiento de la institución.

2.3.4. Consideraciones generales sobre el modelo GAISI

El modelo desarrollado ofrece una visión integral de la automatización de controles de seguridad informática, considerando todos los 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 a utilizar 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, enmarcado con la línea de puntos rojos en la Figura 2.2; lo cual representa una parte importante del proceso de gestión de la seguridad informática en todo su conjunto. No obstante, no debe interpretarse que el modelo resuelve todos los problemas de forma automatizada. Para una adecuada gestión de la seguridad de la información es necesario implementar el resto de los controles propuestos por los estándares y regulaciones existentes, que no son contemplados en este modelo.

Además, el modelo GAISI aborda la automatización de 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. Los indicadores calculados automáticamente deberán ser adecuadamente revisados por los especialistas de seguridad informática para tomar acciones correctivas sobre los controles de seguridad implementados.

El modelo GAISI se encuentra alineado con los principales estándares, recomendaciones y regulaciones existentes, tanto a nivel internacional como nacional, sobre gestión de la seguridad de la información. En este sentido no constituye una nueva propuesta de controles y procesos de gestión, sino que brinda un enfoque de automatización, integración y síntesis a las propuestas existentes, para disminuir la complejidad de la gestión y aumentar la efectividad de los controles de seguridad informática.

2.4. Conclusiones parciales

Después de haber valorado los controles propuestos por los principales estándares internacionales, se puede concluir que alrededor del 30% de los controles de seguridad informática son automatizables. Para la gestión automatizada e integrada de los controles de seguridad informática se propone el modelo GAISI, que constituye el principal aporte de la investigación realizada. El modelo propuesto posee las siguientes características generales:

- Se definen 10 macro-controles de seguridad informática los cuales representan una agrupación y síntesis de los controles automatizables identificados.
- La automatización es aplicada a las acciones de operación, monitorización y revisión de los controles.
- El sistema SIEM es el componente central del modelo, permitiendo la gestión integrada de los controles de seguridad informática
- La revisión de los controles se realiza mediante un grupo de métricas de seguridad informática, definidas también como parte del modelo, que son calculadas y reportadas de forma automatizada.

El modelo desarrollado ofrece una visión integral de la automatización de controles de seguridad informática, considerando todos los controles automatizables y definiendo las acciones a realizar de forma automática en cada uno de los casos. Se propone 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.

El modelo GAISI se encuentra alineado con los principales estándares, recomendaciones y regulaciones sobre gestión de la seguridad de la información. En este sentido no constituye una nueva propuesta de controles y procesos de gestión, sino que brinda un enfoque de automatización, integración y síntesis a las propuestas existentes; con el objetivo de disminuir la complejidad de la gestión y aumentar la efectividad de los controles de seguridad informática.

CAPÍTULO 3

APLICACIÓN Y VALIDACIÓN DEL MODELO GAISI.

CAPÍTULO 3. APLICACIÓN Y VALIDACIÓN DEL MODELO GAISI

En el presente capítulo se brinda una guía para la implementación del modelo GAISI con el objetivo de facilitar su adopción y aplicación. La misma contiene un grupo de especificaciones necesarias para la configuración de los sistemas, así como un listado de diferentes aplicaciones, propietarias y libres, que permiten la implementación de los diez macro-controles del modelo. Se procede además a la validación del modelo GAISI mediante su aplicación en la Universidad de las Ciencias Informáticas (UCI) y la consulta a un panel de expertos. Finalmente se realiza un análisis del posible impacto que tendría la aplicación del modelo en las instituciones cubanas.

3.1. Guía para la implementación del modelo GAISI

La implementación del modelo GAISI se realiza mediante la instalación, configuración y personalización de aplicaciones de seguridad informática existentes, así como la complementación de las mismas a través de pequeños desarrollos que posibilitan su adaptación al modelo propuesto. Para esto es necesario que se cumplan las siguientes premisas:

- Los diferentes sistemas de seguridad informática a emplear para la implementación de los diez macro-controles del modelo, deberán estar diseñados para entornos empresariales, lo que implica que tengan un sistema de administración centralizado. Esto presupone que el sistema SIEM solo debe interactuar con los sistemas instalados en los servidores centrales, en lugar de obtener la información de todas y cada una de las estaciones de trabajo. Por ejemplo, en el caso del macro-control número cinco (protección

contra programas malignos), debe existir un kit de administración que gestione el antivirus instalado en todos los servidores y estaciones de trabajo.

- Los diferentes sistemas de seguridad informática deberán posibilitar la interacción con el sistema SIEM mediante alguno de los siguientes mecanismos:
  - Envío de sus trazas mediante el protocolo *syslog*.
  - Conexión a sus bases de datos donde se almacenan las trazas.
  - Invocación de su interfaz de línea de comandos.
  - Interfaces de programación de aplicaciones (API) provistas por los desarrolladores de los diferentes sistemas.
  - Obtención de información mediante el protocolo SNMP[28].
- El sistema SIEM deberá permitir la definición de nuevos conectores para la integración de los diferentes sistemas, así como la personalización de su módulo de reportes para la visualización de las métricas de seguridad informática definidas en el modelo.

Para la implementación del modelo GAISI se propone la guía de seis pasos que se muestra en la Figura 3.1. A continuación se ofrece una explicación de las acciones a realizar en cada uno de los pasos de la guía propuesta.

1. *Elección e instalación del sistema SIEM*: primeramente se deberá elegir e instalar, con una configuración básica, el sistema de gestión de eventos e información de seguridad, que constituye el componente central del modelo.

La elección del sistema SIEM no depende del modelo GAISI, debido a que es posible aplicar el modelo con cualquier sistema SIEM que realice las funciones básicas. La elección del sistema SIEM dependerá de un análisis de sus funcionalidades, de su facilidad de

[28] El Protocolo Simple de Administración de Red (SNMP, siglas en inglés de Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

administración, de temas de soporte y presupuesto. En dependencia de las características del sistema SIEM elegido será necesario tomar otras decisiones de implementación asociadas al resto de los sistemas.

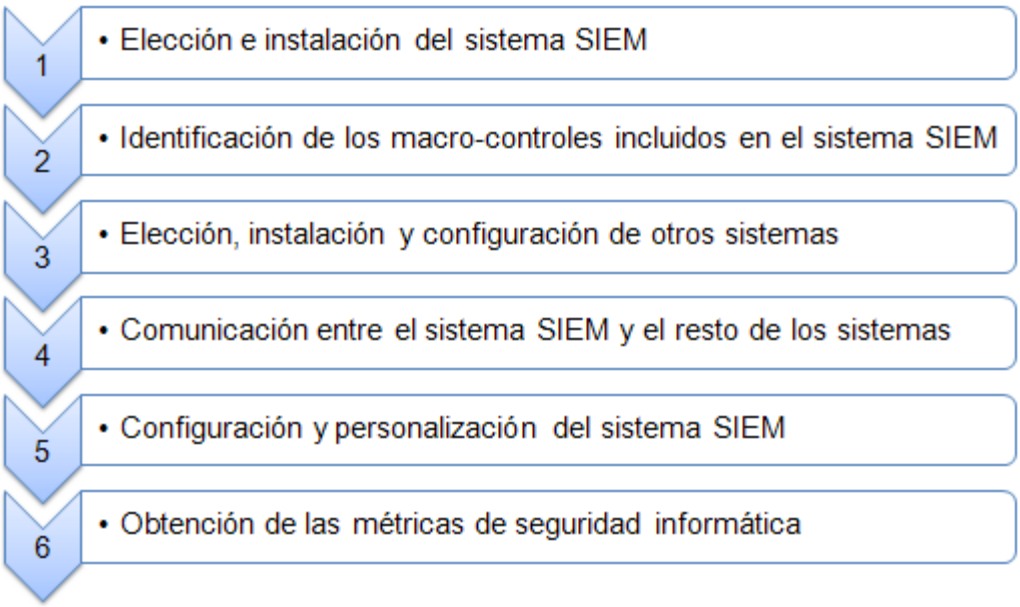


Figura 3.1: Guía para la implementación del modelo GAISI

En la Tabla 3.1 se mencionan los sistemas SIEM líderes en el mercado de acuerdo a un estudio realizado por la consultora Gartner [118]. En dicho estudio se detallan las fortalezas y debilidades de cada uno, lo cual pudiera constituir la base del criterio para la selección. Se incluye el sistema *AlienVault* 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 3.1 se muestran los macro-controles del modelo que son parcialmente[29] (P) o completamente (C) implementados por los principales sistemas SIEM existentes. Como puede apreciarse, los controles 3 (gestión de trazas) y 10 (gestión de incidentes) se encuentran completamente implementados en todos los sistemas SIEM; mientras que los controles 4 (monitoreo de los sistemas) y 7 (configuraciones de seguridad y cumplimiento de políticas) están parcialmente implementados, en mayor o menor medida, en todas las soluciones.

Tabla 3.1: Macro-controles incluidos en diferentes sistemas SIEM

Sistemas SIEM	**Macro-controles**									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
HP/ArcSight - *ESM*		P	C	P			P			C
Q1 Labs - *QRadar*	P		C	P			P			C
RSA (EMC) - *enVision*			C	P			P			C
Symantec - *SSIM*			C	P		P	P			C
LogLogic - *SEM*			C	P			P			C
NitroSecurity - *NitroView ESM*			C	C			P			C
Novell - *Sentinel*		P	C	P			P			C
AlienVault - *Unified SIEM*	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 macro-controles del modelo.

[29] Que el control sea parcialmente implementado por el sistema SIEM significa que este implementa parte del mismo o que facilita grandemente su integración.

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. Adicionalmente pudiera ser necesaria la realización de pequeños desarrollos, generalmente algunos scripts, que complementen los sistemas existentes y los adapten al modelo GAISI.

En la Tabla 3.2 se mencionan, a modo de referencia, algunos sistemas que pudieran utilizarse para implementar cada uno de los macro-controles del modelo, especificando en cada caso sistemas libres y propietarios.

Tabla 3.2: Ejemplos de diferentes sistemas que implementan los 10 macro-controles

No.	**Macro-control**	**Sistemas para su implementación**	
		Sistemas libres	*Sistemas propietarios*
1	Inventario de activos	OCS Inventory	nCircle IP360
2	Gestión de usuarios	FreeIPA	MS Active Directory
3	Gestión de trazas	Rsyslog, NXLOG, OSSIM	Splunk, HP/ArcSight ESM
4	Monitoreo de los sistemas	Snort, Nagios, OSSEC	Cisco IPS 4500, WhatsUp Gold, Tripwire file integrity manager
5	Protección contra programas malignos	ClamAV	Kaspersky Total Space Security
6	Detección de vulnerabilidades y gestión de parches	OpenVas, Repositorios de Linux	Nessus, WSUS
7	Configuraciones de seguridad y cumplimiento de políticas	Puppet, OpenSCAP	nCircle CCM, McAfee ePO
8	Respaldo de información	Bacula	Symantec Veritas Netbackup
9	Seguridad física	-	APC Insfrastruxure, Honeywell: sistemas de control de acceso, contra incendios y contra intrusos.
10	Gestión de incidentes	OTRS, OSSIM	HP/ArcSight ESM

4. *Comunicación entre el sistema SIEM y el resto de los sistemas*: la monitorización y revisión de los controles de seguridad informática 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 los métodos descritos al inicio de la presente sección.

Posteriormente deberán definirse los conectores necesarios para interpretar y normalizar los datos contenidos en las trazas de las diferentes herramientas de seguridad informática. Los sistemas SIEM traen incluidos varios conectores por defecto que permiten interpretar los datos de diferentes sistemas, y además deben brindar 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 GAISI. 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, especificando 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. 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 y a las políticas de seguridad informática definidas en la institución.

c. Personalización de reportes: los reportes emitidos por el sistema SIEM deberán adecuarse al sistema de seguridad informática de la organización, de manera que los datos ofrecidos tengan un significado aporten información útil.

6. *Obtención de las métricas de seguridad informática*: para la revisión de los diez macro-controles de seguridad informática, será necesario obtener, de forma automatizada, los indicadores de efectividad propuestos en el modelo GAISI. Estos indicadores deberán ser actualizados automáticamente con la frecuencia requerida, mostrados en el sistema SIEM y reportados periódicamente, mediante correo electrónico, a los especialistas de seguridad informática y directivos de la organización que se determinen.

Los sistemas SIEM normalmente 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. Por otra parte, para el cálculo de los indicadores será necesario desarrollar una aplicación que consulte los datos y muestre las métricas en el panel de reportes del sistema SIEM. El hecho de que el sistema SIEM centralice la información de las diferentes herramientas de seguridad, facilita la obtención de los datos para el cálculo automático de los indicadores. En el Anexo 4 se detallan las fórmulas, orígenes de datos y frecuencia de medición para todos los indicadores.

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, para después continuar el despliegue en el resto de las áreas.

3.2. Validación del modelo GAISI

La validación de un modelo de gestión de la seguridad informática es un tema complejo. En [125] se realiza una valoración de los métodos de validación empleados en 90 investigaciones efectuadas en este campo en los últimos veinte años. En ese trabajo el autor afirma que no existen formas de experimentación bien establecidas, predominando los casos de estudio que representan momentos específicos en el tiempo. Normalmente no se reportan experimentos de larga duración que contengan una gran recopilación de datos y mediciones repetidas. Se plantea que esto puede estar relacionado a la posibilidad limitada de compartir datos representativos de la seguridad informática de una institución. Por otra parte, tal y como quedó evidenciado en la sección 1.1.2 del presente trabajo, no existe un consenso sobre las métricas de seguridad informática, por lo que la existencia de juegos de datos y la comparación de resultados experimentales es difícil en este campo.

Para la validación del modelo GAISI se procedió a su aplicación parcial en la Universidad de las Ciencias Informáticas (UCI), donde se realiza una comparación de las métricas de seguridad informática antes y después de la aplicación del modelo. Se realizó además una consulta a un panel de expertos para que emitieran sus criterios con relación a un grupo de aspectos del modelo propuesto.

3.2.1. Aplicación parcial en la UCI. Indicadores de efectividad obtenidos.

La aplicación del modelo GAISI en la Universidad de las Ciencias Informáticas se realizó siguiendo los pasos de la guía propuesta en la sección 3.1 del presente trabajo. El modelo fue aplicado primeramente, tal y como recomienda la guía, a una pequeña escala, comenzando el despliegue en el Nodo Central de comunicaciones, donde se encuentran los servidores centrales de la universidad. Posteriormente será extendido al resto de las áreas de la UCI.

Las acciones realizadas y decisiones tomadas en cada uno de los pasos de la guía fueron las siguientes:

1. *Elección e instalación del sistema SIEM*: se seleccionó el sistema OSSIM por ser el único sistema SIEM de software libre, a tono con la política de migración a software libre de la UCI y el país. El sistema fue instalado de forma distribuida en tres servidores: un servidor central con todas las funcionalidades de gestión y dos agentes (uno con el IDS y otro para la recolección de trazas).
2. *Identificación de los macro-controles incluidos en el sistema SIEM*: OSSIM, además de sus características propias como sistema SIEM, integra en su solución un grupo importante de herramientas libres entre las que se encuentran: *OCS Inventory*, *Snort*, *NAGIOS*, *OSSEC*, *OpenVas*, entre otras. Esto implica que OSSIM posibilita la implementación de los macro-controles {1, 3, 4, 10} completamente y {6, 7} parcialmente.
3. *Elección, instalación y configuración de otros sistemas*: para la implementación y operación del resto de los macro-controles del modelo GAISI se seleccionaron los siguientes sistemas:
    - Gestión de usuarios (control 2): *Microsoft Active Directory*.
    - Protección contra programas malignos (control 5): *Kaspersky Antivirus*.
    - Gestión de parches (control 6): *Microsoft Windows Server Update Services* (WSUS), *Repositorios de Linux* (CentOS, Debian).
    - Chequeo de configuraciones de seguridad (control 7): *Puppet* y *OpenSCAP*.
    - Respaldo de información (control 8): *Bacula*.
    - Seguridad física (control 9): a continuación se mencionan los diferentes sistemas que se utilizan en los controles que componen este macro-control.

Es importante señalar que el único de todos ellos que posee un sistema de gestión centralizado por software es el sistema de respaldo eléctrico.

- Sistema de control de acceso físico: lector de tarjetas magnéticas.
- Sistema de detección de incendios: NOTIFIER AFP-200.
- Sistema de detección de intrusos: ADEMCO.
- Sistemas de respaldo eléctrico: UPS APC Symmetra.

Fue necesario además programar un conjunto de scripts que complementaran las funcionalidades de las diferentes herramientas, para llevar a cabo la operación automatizada de los macro-controles de la manera en que se describen los mismos en el modelo GAISI. En el Anexo 5 se muestran algunos fragmentos de código del script desarrollado para la sincronización del *MS Active Directory* con las bases de datos de recursos humanos.

4. *Comunicación entre el sistema SIEM y el resto de los sistemas*: fue necesario desarrollar conectores para todas las herramientas escogidas en el paso anterior porque no venían incluidos dentro del sistema OSSIM.

Para las diferentes herramientas de seguridad que almacenan sus trazas en el contenedor del sistema operativo, *syslog* fue el mecanismo empleado para hacer llegar la información a OSSIM. En los servidores con sistema operativo Linux se utiliza *Rsyslog* y en aquellos con sistema operativo Windows se emplea la herramienta NXLOG. En el resto de los casos fue posible obtener las trazas de las diferentes aplicaciones, a partir de la conexión a las tablas de sus bases de datos donde se almacenan estos registros.

Para la normalización de las trazas y su inclusión en la base de datos del sistema SIEM, se utilizaron los ficheros de configuración que brinda OSSIM con este propósito, donde a través de expresiones regulares se identifican los diferentes campos contenidos en las trazas. En el Anexo 6 se detallan los conectores desarrollados para los casos de *WSUS* y *Bacula*.

5. *Configuración y personalización del sistema SIEM*: en este paso se utilizaron los resultados del análisis de riesgos del plan de seguridad informática, para identificar los sistemas y servidores críticos de la universidad.

A partir de este análisis se definieron los activos dentro de OSSIM, estableciendo la importancia de cada uno mediante la asignación de valores que van desde cero hasta cinco (valor asignado a los activos más importantes). Se habilitaron además todas las reglas de correlación de OSSIM que aplicaban al contexto de la UCI y se personalizaron los reportes que brinda el mismo para que aportaran datos significativos de los incidentes de seguridad informática.

6. *Obtención de las métricas de seguridad informática*: para la obtención de los indicadores fue necesario desarrollar una aplicación que extrae los datos de la base de datos de OSSIM y calcula las métricas definidas en el modelo GAISI. Se modificó además el panel ejecutivo del sistema OSSIM para incluir una nueva sección que visualizara los indicadores calculados.

La vista de la ventana ejecutiva de OSSIM brinda la posibilidad de mostrar dinámicamente paneles que permiten alojar contenido web. Los indicadores se muestran a través de un script que recupera la información almacenada en la base de datos. Otra aplicación contiene todas las funciones que actualizan periódicamente la base de datos con los valores de los indicadores. Ambas aplicaciones se apoyan en las librerías de OSSIM para utilizar parámetros de conexión y otras funciones.

En la Figura 3.2 se muestran las diferentes aplicaciones y mecanismos empleados para la aplicación del modelo GAISI en el Nodo Central de la UCI. Las herramientas que aparecen con un fondo blanco, en la parte del esquema que representa los controles automatizables, son las que vienen integradas por defecto en el sistema OSSIM; mientras que para aquellas señaladas en otro color fue necesario desarrollar conectores que permitieran su integración

al sistema SIEM. En el Anexo 7 se muestran algunas capturas de pantalla del sistema OSSIM, donde puede apreciarse más concretamente la implementación de los diferentes componentes del modelo GAISI.

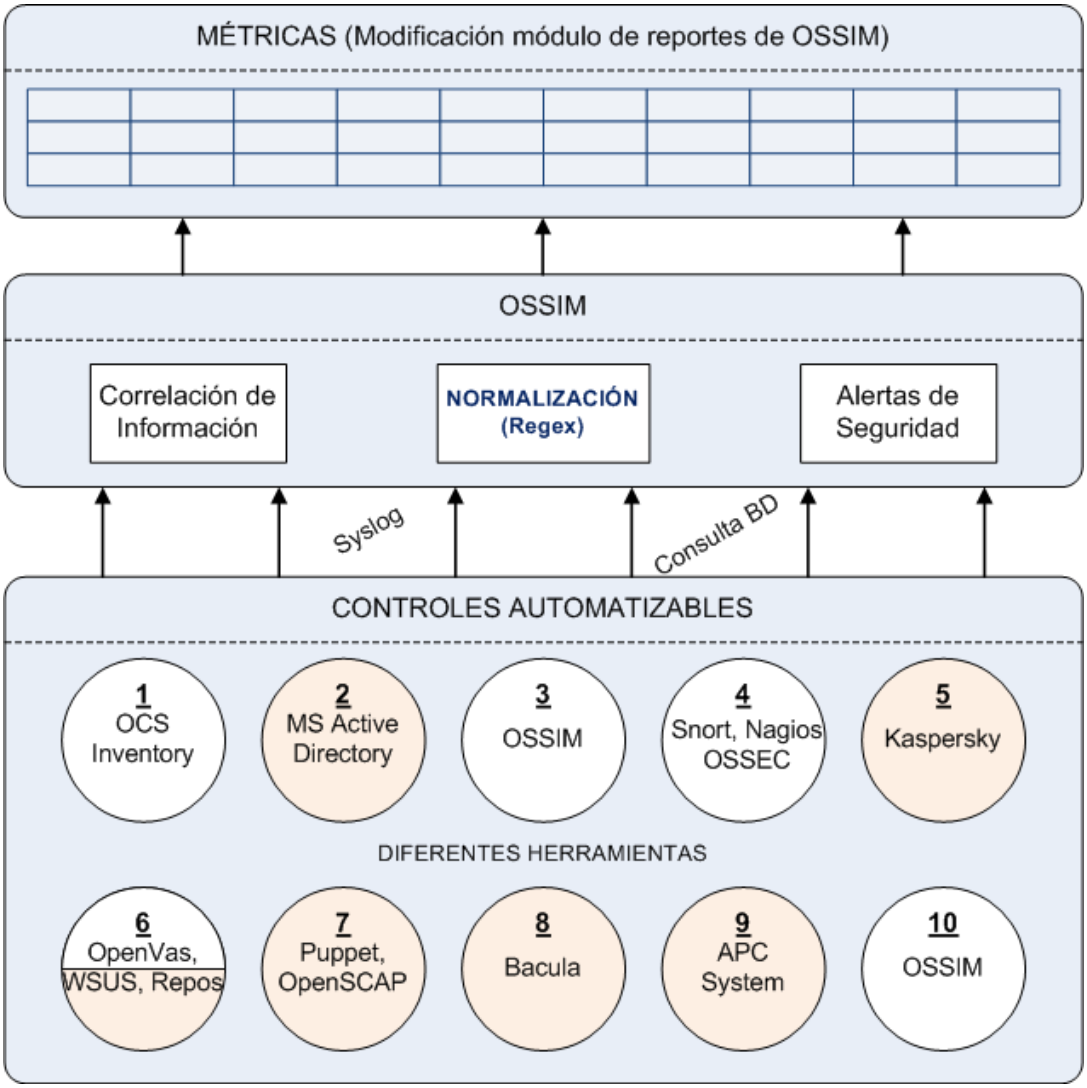


Figura 3.2: Sistemas empleados para la implementación del modelo GAISI en la UCI

3.2.1.1. Métricas de seguridad informática obtenidas

En la Tabla 3.3 se muestran los valores de las métricas de seguridad informática obtenidas antes y después de la aplicación del modelo GAISI en el Nodo Central de la UCI. Fue posible obtener los valores de 14 indicadores de los 24 que se proponen en el modelo GAISI.

Todavía se encuentran en desarrollo los instrumentos de medición que permitirán obtener los restantes indicadores. No obstante, las 14 métricas utilizadas son representativas de ocho de los diez macro-controles del modelo, viéndose reflejados en estos resultados la gran mayoría de los mismos.

Tabla 3.3: Métricas obtenidas antes y después de la aplicación del modelo GAISI

No.	Métricas	Antes (9-Dic-2011)	Después (12-Oct-2012)
1.1	Cantidad de equipos desconocidos conectados a la red	4	0
2.1	Cantidad de cuentas de usuarios que no pueden ser asociadas con algún proceso o área de la institución	369*	7**
2.2	Cantidad de cuentas de usuarios que permanecen activas sin ser usadas por más de 30 días.	899*	12**
3.1	Porciento de sistemas que almacenan trazas de seguridad en una localización centralizada	53,5%	100%
3.2	Tiempo de conservación de las trazas	1 año	1 año
4.2	Porciento del tiempo en que los sistemas críticos se encuentran disponibles	98,3%	99,8%
5.1	Porciento de equipos con el antivirus autorizado instalado	81,8%	100%
5.2	Porciento de equipos con el antivirus desactualizado	18,2%	0
6.1	Cantidad de vulnerabilidades críticas detectadas	16	3
6.4	Porciento de equipos con parches de seguridad críticos pendientes de instalación	20,4%	5,3%
6.5	Tiempo medio de aplicación de los parches de seguridad	57 días	8 días
7.1	Porciento de equipos acorde con la imagen y configuraciones de seguridad definidas	67,0%	100%
8.1	Porciento de sistemas críticos respaldados	73,7%	100%
8.2	Desactualización máxima de las copias de respaldo	1 semana	24 horas
* De un total de 11 586 cuentas de usuarios ** De un total de 11 218 cuentas de usuarios			

Como puede apreciarse, existe una mejoría considerable en todos los indicadores, por lo que puede afirmarse que la aplicación del modelo GAISI ha contribuido a aumentar la efectividad de los controles de seguridad informática.

Es importante señalar que no fue posible obtener los valores de algunos indicadores antes de la aplicación del modelo porque algunos controles no se encontraban implementados. Tales son los casos de las siguientes métricas:

1.2.- Porciento de equipos con software no autorizado: no existía la política de software autorizado en los servidores.

4.1.- Cantidad de intentos de ataques (por hora) a la DMZ: no había un sistema de detección de intrusos (IDS) instalado.

10.1, 10.2, 10.3.- Indicadores relacionados con la gestión de incidentes: no se utilizaba ningún sistema de gestión de incidentes.

Nuevamente es necesario recalcar que aunque el modelo GAISI propone la automatización de un grupo de controles, no todo se resuelve de forma automática. La labor de los administradores de la red y de los especialistas de seguridad informática es clave e influye en los resultados alcanzados. Si las alarmas del sistema SIEM no son atendidas y las métricas no son revisadas con la periodicidad requerida, entonces no se cierra el ciclo de gestión y por tanto no se avanza en la mejora continua del sistema de seguridad informática.

Sobre la complejidad de la gestión de la seguridad de la información es necesario analizar los siguientes factores:

- *Cantidad de sistemas a administrar*: con la aplicación del modelo GAISI, una vez que está todo configurado, solo es necesario concentrarse en un sistema (el sistema SIEM).
- *Cantidad de controles a operar, monitorizar y revisar de forma manual*: se automatizan completamente las acciones operación, monitorización y revisión para los 10 macro-controles, lo que supone un ahorro de tiempo considerable para los especialistas de seguridad informática y administradores de la red.

- *Cantidad de controles a implementar y dar seguimiento*: la síntesis que realiza el modelo GAISI al agrupar los controles automatizables en 10 macro-controles, permite que los encargados de la gestión de la seguridad informática se concentren en un número relativamente pequeño de controles, facilitando el seguimiento de los mismos.

3.2.2. Consulta a un panel de expertos

Para complementar la validación práctica del modelo GAISI, se realizó una encuesta a un grupo de expertos en la temática que aborda la presente investigación con los siguientes objetivos:

- Evaluar el cumplimiento de los principios sobre los que fue desarrollado el modelo.
- Valorar los diferentes componentes del modelo propuesto.
- Validar los resultados esperados con la aplicación del modelo.

En cada pregunta del cuestionario se definió una escala de valores adecuada para garantizar la exactitud del criterio de los expertos. El modelo matemático de Torgerson [126] fue el empleado para el análisis de las respuestas de los cuestionarios, permitiendo no sólo asignar un valor de escala a cada atributo, sino determinar límites entre las categorías de evaluación.

3.2.2.1. Selección de los expertos.

Debe destacarse que en Cuba, la población de expertos en el tema de esta tesis es muy reducida, encontrándose fundamentalmente en la Oficina de Seguridad para las Redes Informáticas (OSRI), el Ministerio del Interior (MININT) y la empresa Segurmática. Esto obligó a incluir a un grupo de especialistas extranjeros de alto nivel en la temática abordada.

Para la selección de los expertos se confeccionó un listado con 17 posibles candidatos y se procedió a la selección de los expertos mediante la determinación del coeficiente de competencia de cada candidato, según el método descrito en el Anexo 8 [127].

Adicionalmente se tuvieron en cuenta aspectos como: eventos y publicaciones, años de experiencia, categoría científica, experiencia práctica, responsabilidades administrativas o científicas asociadas al tema, entre otros.

De los 17 posibles candidatos, solo 11 respondieron el cuestionario, obteniéndose en todos los casos un coeficiente de competencia alto, por lo que el grupo que validó la propuesta quedó conformado por 11 expertos. En la Tabla 3.4 se muestra un resumen de la composición del panel de expertos que participaron en la consulta.

Tabla 3.4: Composición del grupo de expertos

Composición	Cantidad
Doctores	4
Máster	3
Más de 20 años de experiencia	4
Entre 15 y 20 años de experiencia	5
Entre 10 y 15 años de experiencia	2
Sector académico	4
Sector gubernamental o empresarial	7
Extranjeros	5

3.2.2.2. Criterios de los expertos

Una vez seleccionados los expertos se les envió un resumen de la investigación realizada y se procedió a la aplicación del cuestionario que se muestra en el Anexo 9. En la Tabla 3.5 se muestran los resultados del procesamiento estadístico de las respuestas sobre las cualidades del modelo propuesto. Como puede apreciarse, en todos los casos el resultado obtenido es 4 (cumple en buena medida).

Tabla 3.5: Evaluación del cumplimiento de los principios del modelo

Criterio	Evaluación
Automatización	4
Integración	4
Síntesis	4
Medición objetiva	4
Mejora continua	4
Generalidad	4

Sobre los criterios emitidos por los expertos con respecto a los macro-controles propuestos en el modelo GAISI, los resultados se muestran en la Tabla 3.6. En todos los casos se obtienen resultados de 4 (mayormente de acuerdo) y 5 (completamente de acuerdo). En el Anexo 10 se pueden consultar las tablas completas con los detalles de la aplicación del modelo de Torgerson para el procesamiento de las respuestas del cuestionario aplicado a los expertos.

Tabla 3.6: Criterio de los expertos sobre los macro-controles automatizables

No.	Macro-control	Conformidad
1	Inventario de activos	4
2	Gestión de usuarios	5
3	Gestión de trazas	5
4	Monitoreo de los sistemas	5
5	Protección contra programas malignos	5
6	Detección de vulnerabilidades y gestión de parches	5
7	Configuraciones de seguridad y cumplimiento de políticas	5
8	Respaldo de información	4
9	Seguridad física	4
10	Gestión de incidentes	5

Es importante señalar que sobre las acciones a automatizar en la gestión de la seguridad informática, algunos expertos consideran que es posible automatizar parcialmente algunos aspectos en el proceso de planificación. En todos los casos los comentarios son válidos, pero en el modelo propuesto se contempla la completa automatización de las acciones de operación, monitorización y revisión. El autor del presente trabajo considera que no es posible lograr una automatización completa del resto de las acciones. No obstante, sí es válido recomendar la utilización de herramientas que faciliten el análisis de riesgos como las mencionadas en la sección 1.2.2. En este sentido será necesario continuar investigando a partir de los modelos de gestión autonómica mencionados en la sección 1.2.1 del presente trabajo, para evaluar la posibilidad de aplicar niveles más avanzados a la gestión de la seguridad informática.

Con respecto a los indicadores propuestos en el modelo GAISI, los resultados se muestran en el gráfico de la Figura 3.3. Como puede apreciarse, la mayoría de las métricas obtuvo el 100% de los votos, siendo la votación más baja para los indicadores 3.1 y 3.2 con el 70% de los votos; por lo que puede concluirse que para todas las métricas de seguridad informática se obtuvo el consenso de los expertos.

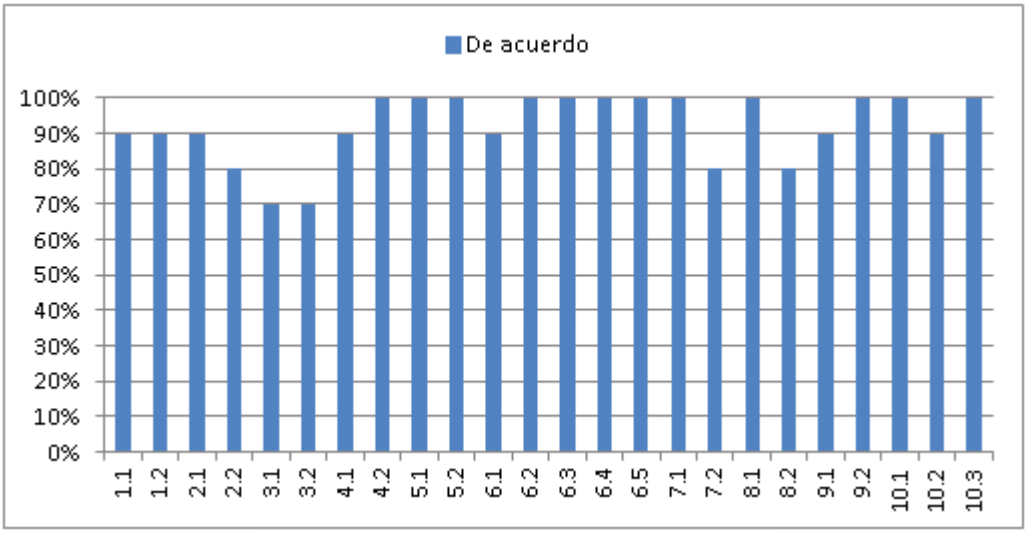


Figura 3.3: Criterios de los expertos sobre las métricas propuestas en el modelo GAISI

Es importante señalar que algunos expertos recomendaron la inclusión de otros indicadores. En algunos casos se recomendaron indicadores de impacto en el negocio según la clasificación mencionada en la sección **Error! Reference source not found.**. Este tipo de indicadores rebasa el alcance de la presente investigación, la cual propone indicadores de efectividad orientados a los responsables de la gestión de la seguridad informática. En otros casos se sugirieron indicadores cuya medición no es posible realizarla de forma automatizada, por lo que tampoco deben considerarse en el modelo. No obstante, es válido mencionar aquí algunos indicadores que en determinado momento se valoraron para su inclusión en el modelo GAISI, los cuales permiten medir el tiempo de reacción de los controles, pero su medición implica la realización de varias pruebas con presencia de evaluadores, no siendo posible su obtención periódica de forma automatizada. Tales son los casos siguientes:

- Tiempo que demora la detección de un nuevo dispositivo conectado a la red [29].
- Tiempo que demora la detección de cambios de configuración en las estaciones de trabajo y servidores [29].
- Tiempo que demora la búsqueda de información en las trazas (ej.: búsqueda de toda la actividad informática de un usuario en un día).
- Tiempo necesario para la recuperación de los sistemas a partir de las copias de respaldo.

A continuación se mencionan algunos de los indicadores propuestos por los expertos, que sí pudieran valorarse para su inclusión en el modelo:

- Cantidad de cuentas bloqueadas por múltiples accesos incorrectos (control 2)
- Cantidad de programas malignos detectados por unidad de tiempo (control 5)
- Cantidad de vulnerabilidades asociadas a sitios web (control 6)
- Cantidad de errores en el sistema de respaldo (control 8)

- Tiempo promedio de conservación de los respaldos (control 8)
- Cantidad de accesos físicos a las áreas con sistemas críticos de la organización (control 9)

Los indicadores sugeridos demuestran, tal y como se explicó en la sección **Error! Reference source not found.**, que la lista de métricas propuesta como parte del modelo GAISI no es exhaustiva. Esta solo constituye una referencia que puede enriquecerse con más indicadores que las diferentes instituciones consideren necesario incorporar.

Sobre los resultados esperados con la aplicación del modelo GAISI, los criterios de los expertos se muestran en el gráfico de la Figura 3.4. Como puede apreciarse, existe consenso sobre los resultados que tendría la aplicación del modelo: un aumento en la efectividad de los controles y la disminución de la complejidad de la gestión de la seguridad informática.

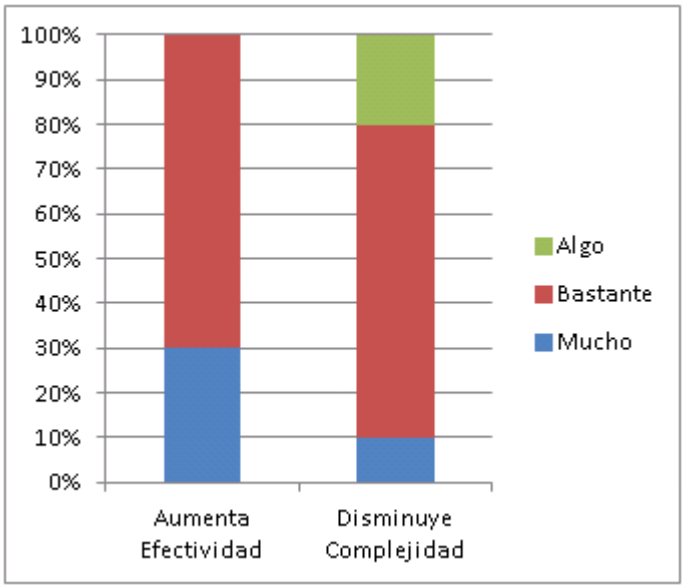


Figura 3.4: Criterios de los expertos sobre la aplicación del modelo GAISI

3.3. Posible impacto de la aplicación del modelo en las instituciones cubanas.

Con el objetivo de valorar el posible impacto que tendría la aplicación del modelo GAISI en las instituciones cubanas, durante el mes de junio de 2012 se aplicó una encuesta a directivos y especialistas de veinte instituciones pertenecientes al Ministerio de Educación Superior (MES) y al Ministerio de la Informática y las Comunicaciones (MIC). El cuestionario aplicado se muestra en el Anexo 11. Participaron en la encuesta las universidades y empresas más representativas de ambos ministerios. La composición de los encuestados fue la siguiente: el 60% directivos del área informática, el 25% especialistas de seguridad informática y el 15% administradores de redes.

Con relación a los factores que contribuyen a aumentar la efectividad de los controles y a disminuir la complejidad de la gestión de la seguridad informática, los resultados se muestran en la Figura 3.5. Se estableció una escala que va desde uno (nada) hasta cinco (mucho). De manera general se reconoce el efecto positivo que tendría la automatización y la gestión integrada de los controles, a la vez que se reconoce la importancia de otros factores que también son claves en la gestión de la seguridad de la información.

En la Figura 3.6 se muestra un gráfico que representa el nivel de automatización que poseen actualmente los 10 macro-controles del modelo GAISI en las instituciones encuestadas, según el criterio de los encuestados. Los valores representan el promedio obtenido por cada macro-control con respecto a una escala que va desde uno hasta cinco, donde el valor más bajo indica que el control no está implementado y el valor más alto significa que la operación del control está completamente automatizada (ver Anexo 1 del cuestionario aplicado).

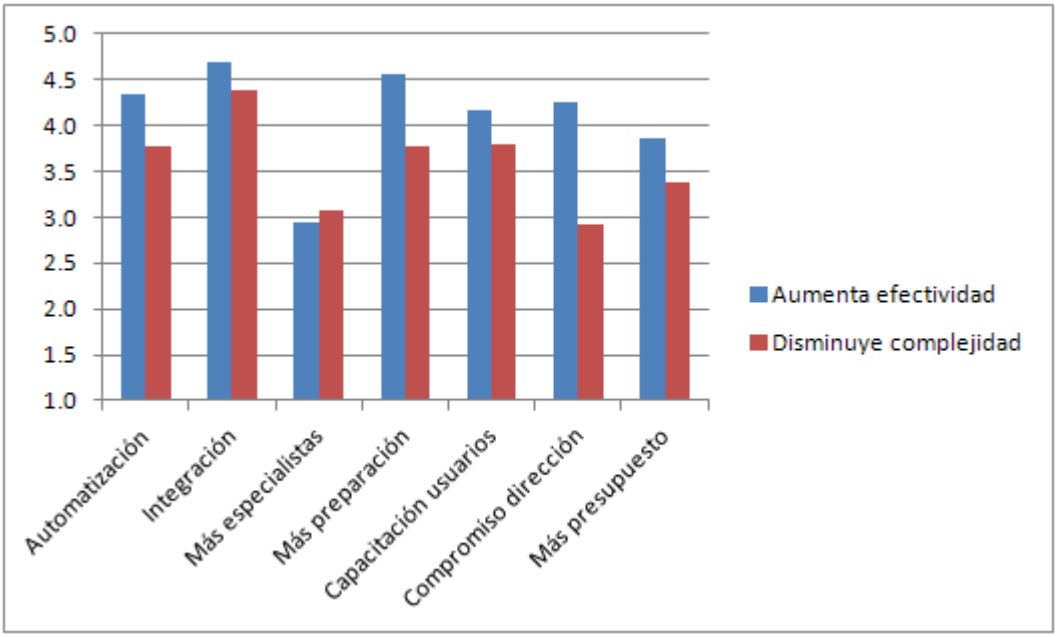


Figura 3.5: Factores que contribuyen a aumentar la efectividad y disminuir la complejidad en la gestión de la seguridad informática.

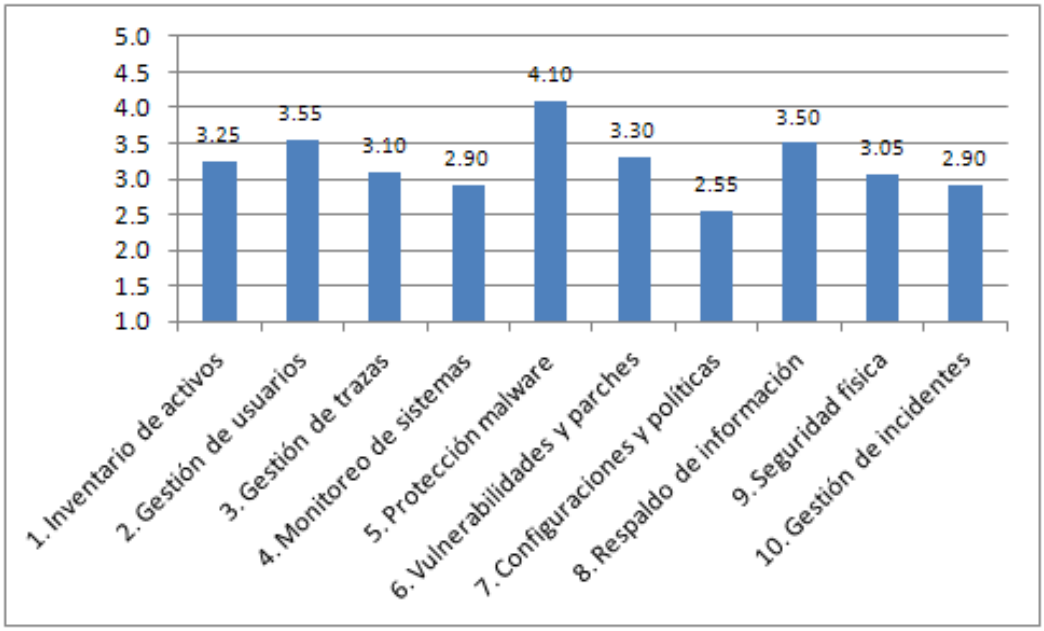


Figura 3.6: Nivel de automatización actual de los macro-controles en las instituciones cubanas

En el gráfico anterior se puede observar que el macro-control con mayor nivel de automatización es el cinco (protección contra programas malignos) y el de más baja

automatización es el siete (configuraciones de seguridad y cumplimiento de políticas), constatándose que en sentido general falta mucho por hacer en materia de automatización.

Por otra parte solo el 30% de las instituciones manifestó utilizar algún sistema SIEM, y en los casos que lo utilizan su objetivo es básicamente el monitoreo de los sistemas. Con respecto al empleo de algún sistema de indicadores para evaluar la efectividad de los controles de seguridad informática, el 65% de los encuestados respondió afirmativamente, mientras que en el 54% de los casos la frecuencia de actualización de los mismos es 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.

Con la aplicación del modelo GAISI 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.

3.4. Conclusiones parciales

La implementación del modelo GAISI se realiza mediante la instalación, configuración y personalización de aplicaciones de seguridad informática existentes, así como la complementación de las mismas a través de pequeños desarrollos que posibilitan su adaptación al modelo propuesto. Para la aplicación del modelo se ofrece una guía de seis pasos que contiene un grupo de especificaciones necesarias para la configuración de los sistemas, incluyendo un listado de diferentes aplicaciones que permiten la implementación de los diez macro-controles del modelo.

El modelo GAISI ha sido aplicado en el Nodo Central de la UCI, para lo cual se han utilizado fundamentalmente sistemas de software libre, a tono con la política del país sobre la

migración a este tipo de plataformas. En el presente trabajo se ofrecen las configuraciones necesarias para la implementación del modelo mediante OSSIM y otros sistemas. Las métricas de seguridad informática obtenidas después de la aplicación del modelo, reflejan claramente un aumento en la efectividad de los controles de seguridad informática.

Con respecto a la complejidad del proceso de gestión de la seguridad informática, se puede afirmar que con la aplicación del modelo es posible realizar la gestión integrada de los controles, convirtiéndose el sistema SIEM en el centro de atención de los especialistas que ya no tendrían que monitorizar más de diez sistemas diferentes. Por otra parte se concentra la atención en un número relativamente pequeño de macro-controles y se automatiza completamente la operación, monitorización y revisión de los mismos; descargando estas tareas de los especialistas que de otra manera tendrían que realizarlas de forma manual.

Como parte del proceso de validación se realizó una consulta a un panel de expertos que emitieron criterios favorables sobre el modelo. Los expertos avalaron los principios sobre los que fue desarrollado el modelo GAISI, los macro-controles contenidos en el mismo y las métricas de seguridad informática propuestas. Finalmente hubo consenso en que la aplicación del modelo posibilitaría un aumento en la efectividad de los controles y una disminución de la complejidad en la gestión de la seguridad informática.

Mediante una encuesta aplicada a veinte instituciones del MES y el MIC, se pudo comprobar que el nivel de automatización que estas poseen con respecto a la operación de los macro-controles es relativamente bajo. Esto implica que la aplicación del modelo GAISI en las instituciones cubanas tendría un impacto considerable, aumentando la efectividad de los sistemas de seguridad informática de las mismas.

CONCLUSIONES

El proceso de gestión de la seguridad informática requiere el establecimiento de gran cantidad de controles, la implementación de variados sistemas de seguridad con mecanismos de gestión independientes, y una elevada capacidad de respuesta ante los diversos ataques y vulnerabilidades existentes; lo que hace que el mismo sea complejo y en muchas ocasiones inefectivo.

El presente trabajo soluciona el problema científico mencionado mediante el desarrollo de un modelo para la gestión automatizada e integrada de controles de seguridad informática (GAISI), que constituye el principal aporte de la investigación realizada. En el modelo se definen diez macro-controles de seguridad informática, los cuales representan una agrupación y síntesis de los controles automatizables identificados en los principales estándares internacionales sobre gestión de la seguridad de la información. Se automatizan las acciones de operación, monitorización y revisión de dichos controles; mientras que la gestión integrada se logra a través de un sistema SIEM, que constituye el componente central del modelo.

En el trabajo se presentan otros aportes prácticos entre los que se encuentran un listado de métricas para medir la efectividad de los controles de seguridad informática, una guía para la aplicación del modelo propuesto, y las especificaciones necesarias para la implementación del modelo utilizando OSSIM y otros sistemas de software libre.

El modelo GAISI ha sido aplicado en el Nodo Central de la UCI. Las métricas de seguridad informática obtenidas después de la aplicación del modelo, reflejan claramente un aumento en la efectividad de los controles de seguridad informática. Como parte del proceso de validación se realizó una consulta a un panel de expertos que emitieron criterios favorables sobre el modelo. Los expertos avalaron los principios sobre los que fue desarrollado el

modelo GAISI, los macro-controles contenidos en el mismo y las métricas de seguridad informática propuestas. Finalmente hubo consenso en que la aplicación del modelo posibilitaría un aumento en la efectividad de los controles y una disminución de la complejidad en la gestión de la seguridad informática.

Mediante una encuesta aplicada a varias instituciones cubanas, se pudo comprobar que el nivel de automatización actual de los macro-controles es relativamente bajo y prácticamente no se utilizan sistemas SIEM. Esto implica que la aplicación del modelo GAISI tendría un impacto considerable, aumentando la efectividad de los sistemas de seguridad informática de dichas instituciones.

El modelo GAISI se encuentra alineado con los principales estándares, recomendaciones y regulaciones sobre gestión de la seguridad de la información. En este sentido no constituye una nueva propuesta de controles y procesos de gestión, sino que brinda un enfoque de automatización, integración y síntesis a las propuestas existentes; con el objetivo de disminuir la complejidad de la gestión y aumentar la efectividad de los controles de seguridad informática.

RECOMENDACIONES

A partir de la investigación realizada se proponen las siguientes recomendaciones:

- Trabajar en la estandarización de un listado de métricas que permitan medir de manera objetiva la efectividad de los sistemas de seguridad informática de las diferentes organizaciones.
- Analizar las posibilidades de aplicación de las investigaciones sobre computación autonómica al contexto de la seguridad informática, donde quizás se pueda abrir una nueva línea de investigación denominada “gestión autonómica de la seguridad”.

REFERENCIAS BIBLIOGRÁFICAS

[1] R. Richardson, *CSI 15th Annual Computer Crime and Security Survey*. Computer Security Institute (CSI), 2011.

[2] *Second Annual Cost of Cyber Crime Study*. Ponemon Institute, 2011.

[3] Sophos, "Sophos security threat report," 2011. [Online]. Available: http://www.sophos.com/en-us/security-news-trends/security-trends/security-threat-report-2011.aspx. [Accessed: 17-Feb-2012].

[4] Kaspersky Lab, "Kaspersky Security Bulletin. Statistics 2011." [Online]. Available: http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011. [Accessed: 17-Apr-2012].

[5] S21sec, "Informe de vulnerabilidades 2011," 2012. [Online]. Available: http://www.s21sec.com/descargas/Informe%20Vulnerabilidades%202011.pdf. [Accessed: 18-Apr-2012].

[6] Secunia, "Secunia yearly report 2011," 2012. [Online]. Available: http://secunia.com/?action=fetch&filename=Secunia_Yearly_Report_2011.pdf. [Accessed: 18-Apr-2012].

[7] N. Dhanjani, *Hacking: The next generation*. Sebastopol (CA): O'Reilly, 2009.

[8] R. Werlinger, K. Hawkey, and K. Beznosov, "An integrated view of human, organizational, and technological challenges of IT security management," *Information Management & Computer Security*, vol. 17, no. 1, pp. 4-19, 2009.

[9] S. Quinn, K. Scarfone, M. Barrett, and C. Johnson, "NIST SP 800-117: Guide to Adopting and Using the Security Content Automation Protocol (SCAP)." National Institute of Standards and Technology, Jul-2010.

[10] G. García, "Principales deficiencias en las redes nacionales." Oficina de Seguridad para las Redes Informáticas (OSRI), Dec-2010.

[11] R. A. Martin, "Making security measurable and manageable," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, 2009, pp. 1–9.

[12] D. B. Lacquement, T. Sager, and P. Bartock, "An introduction to security automation," *IAnewsletter*, vol. 14, no. 4, 2011.

[13] D. Schmidt, "Security automation: a new approach to managing and protecting critical information," *IAnewsletter*, vol. 13, no. 1, 2010.

[14] 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.

[15] ISO/IEC, "ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management." International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2005.

[16] MIC, "Resolución 127/2007 MIC. Reglamento de seguridad para las tecnologías de la información." Ministerio de la informática y las comunicaciones (MIC), 2007.

[17] R. Montesino, “Gestión de la seguridad informática: de la teoría a la práctica,” in *IX Seminario Iberoamericano de Seguridad en las Tecnologías de la Información*, La Habana, Cuba, 2009.

[18] J. Cano, “Un concepto extendido de la mente segura: pensamiento sistémico en seguridad informática.” Criptored, 2005.

[19] B. von Solms, “Information Security – The Fourth Wave,” *Computers & Security*, vol. 25, no. 3, pp. 165-168, May. 2006.

[20] NIST, “NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations.” National Institute of Standards and Technology, Aug-2009.

[21] ISF, “The Standard of Good Practice for Information Security.” Information Security Forum (ISF), 2007.

[22] V. Aceituno, “ISM3: Information security management maturity model v2.0.” ISM3 Consortium, 2007.

[23] ITGI, “Control Objectives for Information and Related Technology (COBIT 4.1).” IT Governance Institute (ITGI), 2007.

[24] OGC, “Information Technology Infrastructure Library (ITIL v3).” Office of Government Commerce UK (OGC), 2007.

[25] PCI SSC, “Payment Card Industry Data Security Standard (PCI DSS).” Payment Card Industry Security Standards Council (PCI SSC), 2010.

[26] HHS, “Health Insurance Portability and Accountability Act (HIPAA) - Security Rule.” Department of Health and Human Services US (HHS), 2003.

[27] BSI, “IT Baseline Protection Catalog.” German Federal Office for Security in Information Technology (BSI), 2005.

[28] DSD, “Australian Government Information Security Manual (ISM).” Department of Defense. Australian Government, Sep-2012.

[29] CSIS, “Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines v3.0.” Center for Strategic and International Studies (CSIS), 2011.

[30] ISACA, “An Introduction to the Business Model for Information Security.” Information Systems Audit and Control Association (ISACA), 2009.

[31] S. Kraemer, P. Carayon, and J. Clem, “Human and organizational factors in computer and information security: Pathways to vulnerabilities,” *Computers & Security*, vol. 28, no. 7, pp. 509-520, Oct. 2009.

[32] S. Kraemer and P. Carayon, “Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists,” *Applied Ergonomics*, vol. 38, no. 2, pp. 143–154, 2007.

[33] D. Ashenden, “Information Security management: A human challenge?,” *Information Security Technical Report*, vol. 13, no. 4, pp. 195-201, Nov. 2008.

[34] C. Ormella, “El factor gente y la seguridad de la información,” presented at the SeguInfo, 2010.

[35] S. Kraemer, P. Carayon, and J. F. Clem, “Characterizing violations in computer and information security systems,” in *Proceedings of the 16th Triennial Congress of the International Ergonomics Association*, 2006.

[36] W. Baker and L. Wallace, “Is Information Security Under Control?: Investigating Quality in Information Security Management,” *IEEE Security and Privacy*, vol. 5, no. 1, pp. 36-44, Jan. 2007.

[37] ITGI, “Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit.” IT Governance Institute (ITGI), 2008.

[38] J. Clinch, “ITIL V3 and Information Security.” Office of Government Commerce UK (OGC), May-2009.

[39] “Optimizing ISO/IEC 27001 using O-ISM3.” The Open Group, Jul-2012.

[40] J. S. Broderick, “ISMS, security standards and security regulations,” *Information Security Technical Report*, vol. 11, no. 1, pp. 26-31, Jan. 2006.

[41] M. M. Eloff, “A Multi-dimensional Model for Information Security Management,” PhD Thesis, 2000.

[42] D. Trcek, “An integral framework for information systems security management,” *Computers & Security*, vol. 22, no. 4, pp. 337-360, 2003.

[43] J. Tudor, “Information Security Architecture,” 2000.

[44] B. Tomhave, “The Total Enterprise Assurance Management (TEAM) Model: A unified approach to information assurance management,” MSc. Thesis, George Washington University, 2006.

[45] I. Tashi and S. Ghernouti-Hélie, “A Security Management Assurance Model to holistically assess the Information Security posture,” presented at the International Conference on Availability, Reliability and Security (ARES), 2009.

[46] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, “Introduction to the OCTAVE® Approach.” Carnegie Mellon University, 2003.

[47] MINHAP, “MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.” Ministerio de Hacienda y Administraciones Públicas, Gobierno de España, Oct-2012.

[48] ISO/IEC, “ISO/IEC 27005: Information technology - Security techniques - Information security risk management.” International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2008.

[49] NIST, “NIST SP 800-30 rev1: Guide for Conducting Risk Assessments.” National Institute of Standards and Technology, Sep-2012.

[50] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson, “NIST SP 800-55: Performance measurement guide for information security.” National Institute of Standards and Technology, 2008.

[51] M. Masera and I. N. Fovino, “Security metrics for cyber security assessment and testing.” Joint Research Centre of the European Commission, Aug-2010.

[52] A. Jaquith, *Security metrics: replacing fear, uncertainty, and doubt*. Upper Saddle River NJ: Addison-Wesley, 2007.

[53] L. Hayden, *IT security metrics a practical framework for measuring security & protecting data*. New York: McGraw Hill, 2010.

[54] W. Jansen, “Directions in security metrics research.” National Institute of Standards and Technology (NIST), Apr-2009.

[55] S. L. Pfleeger and R. K. Cunningham, “Why Measuring Security Is Hard,” *IEEE Security and Privacy*, Aug. 2010.

[56] ISO/IEC, “ISO/IEC 27004: Information technology - Security techniques - Information security management systems – Measurements.” International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2009.

[57] D. A. Chapin and S. Akridge, “How can security be measured?,” *Systems Control Journal*, vol. 2, 2005.

[58] R. Savola, “Towards a security metrics taxonomy for the information and communication technology industry,” in *Proceedings of the International Conference on Software Engineering Advances*, 2007.

[59] R. Barabanov, *Information security metrics: state of the art*. Swedish Civil Contingencies Agency (MSB), 2011.

[60] CIS, “CIS Security Metrics.” Center for Internet Security, 2010.

[61] S. Y. Nof, *Springer Handbook of Automation*. Springer, 2009.

[62] N. Agoulmine, *Autonomic network management principles: from concepts to applications*. London: Academic, 2010.

[63] P. Horn, “Autonomic Computing: IBM’s Perspective on the State of Information Technology.” IBM Research, 2001.

[64] IBM, “An architectural blueprint for autonomic computing.” IBM Research, 2005.

[65] IBM, “IBM Tivoli Management Framework.” [Online]. Available: http://www-01.ibm.com/software/tivoli/products/mgt-framework/. [Accessed: 20-Aug-2012].

[66] B. McLarnon, P. Robinson, P. Milligan, and P. Sage, “Introducing automated management through iteratively increased automation and indicators,” in *12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops*, Dublin, Ireland, 2011, pp. 1116-1121.

[67] J. Famaey, S. Latre, J. Strassner, and F. De Turck, “A hierarchical approach to autonomic network management,” in *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*, Osaka, 2010, pp. 225-232.

[68] S. Dobson et al., “A survey of autonomic communications,” *ACM Transactions on Autonomous and Adaptive Systems*, vol. 1, no. 2, pp. 223-259, Dec. 2006.

[69] R. Mortier and E. Kiciman, “Autonomic network management: some pragmatic considerations,” in *Proceedings of the 2006 SIGCOMM workshop on Internet network management - INM ’06*, Pisa, Italy, 2006, pp. 89-93.

[70] J. Strassner, N. Agoulmine, and E. Lehtihet, “FOCALE - A Novel Autonomic NetworkingArchitecture,” in *Latin American Autonomic Computing Symposium (LAACS)*, Campo Grande, MS, Brazil, 2006.

[71] D. Raymer, S. van der Meer, and J. Strassner, “From Autonomic Computing to Autonomic Networking: An Architectural Perspective,” in *Fifth IEEE Workshop on Engineering of Autonomic and Autonomous Systems (ease 2008)*, Belfast, Northern Ireland, 2008, pp. 174-183.

[72] H. Hamdi, A. Bouhoula, and M. Mosbah, “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.

[73] A. A. Hassan and W. M. Bahgat, “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.

[74] A. Ouda, H. Lutfiyya, and M. Bauer, “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.

[75] R. Abassi and S. G. E. Fatmi, “An Automated Validation Method for Security Policies: The Firewall Case,” in *2008 The Fourth International Conference on Information Assurance and Security*, Naples, Italy, 2008, pp. 291-294.

[76] N. Damianou, N. Dulay, E. Lupu, and M. Sloman, “The ponder policy specification language,” *Policies for Distributed Systems and Networks*, pp. 18–38, 2001.

[77] Gaeil Ahn, Seungyong Yoon, Kiyoung Kim, and Jongsoo Jang, “Security policy decision for automation of security network configuration,” in *9th Asia-Pacific Conference on Communications (IEEE Cat. No.03EX732)*, Penang, Malaysia, pp. 1057-1061.

[78] H. T. Tian, L. S. Huang, Z. Zhou, and Y. L. Luo, “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.

[79] H. Shahriar and M. Zulkernine, “Automatic Testing of Program Security Vulnerabilities,” in *2009 33rd Annual IEEE International Computer Software and Applications Conference*, Seattle, Washington, USA, 2009, pp. 550-555.

[80] A. Al-Ayed, S. M. Furnell, D. Zhao, and P. S. Dowland, “An automated framework for managing security vulnerabilities,” *Information Management & Computer Security*, vol. 13, no. 2, pp. 156-166, 2005.

[81] Y. Takamatsu, Y. Kosuga, and K. Kono, “Automated detection of session management vulnerabilities in web applications,” in *2012 Tenth Annual International Conference on Privacy, Security and Trust*, Paris, France, 2012, pp. 112-119.

[82] J. Yoon and W. Sim, “Implementation of the automated network vulnerability assessment framework,” in *2007 Innovations in Information Technologies (IIT)*, Dubai, United Arab Emirates, 2007, pp. 153-157.

[83] G. Koschorreck, “Automated Audit of Compliance and Security Controls,” in *2011 Sixth International Conference on IT Security Incident Management and IT Forensics*, Stuttgart, Germany, 2011, pp. 137-148.

[84] M. N. Alsaleh and E. Al-Shaer, “SCAP based configuration analytics for comprehensive compliance checking,” in *2011 4th Symposium on Configuration Analytics and Automation (SAFECONFIG)*, Arlington, VA, USA, 2011, pp. 1-8.

[85] M. Lopes, A. Costa, and B. Dias, “Automated network services configuration management,” in *2009 IFIP/IEEE International Symposium on Integrated Network Management-Workshops*, New York, NY, USA, 2009, pp. 140-143.

[86] W. Enck et al., “Configuration management at massive scale: system design and experience,” *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 3, pp. 323-335, Apr. 2009.

[87] P. Goldsack et al., “The SmartFrog configuration management framework,” *ACM SIGOPS Operating Systems Review*, vol. 43, no. 1, p. 16, Jan. 2009.

[88] E. Al-Shaer, W. Marrero, A. El-Atawy, and K. ElBadawi, “Network configuration in a box: towards end-to-end verification of network reachability and security,” in *2009 17th IEEE International Conference on Network Protocols*, Plainsboro, NJ, USA, 2009, pp. 123-132.

[89] S. Neelakantan et al., “An architecture for self-configuration of network for QoS and security,” in *2009 First International Communication Systems and Networks and Workshops*, Bangalore, India, 2009, pp. 1-5.

[90] H. Chen, Y. B. Al-Nashif, G. Qu, and S. Hariri, “Self-Configuration of Network Security,” in *11th IEEE International Enterprise Distributed Object Computing Conference (EDOC 2007)*, Annapolis, MD, USA, 2007, pp. 97-97.

[91] J. Schonwalder, M. Bjorklund, and P. Shafer, “Network configuration management using NETCONF and YANG,” *IEEE Communications Magazine*, vol. 48, no. 9, pp. 166-173, Sep. 2010.

[92] A. Erkan, “An automated tool for information security management system,” MSc. Thesis, Middle East Technical University, 2006.

[93] Kun Sun, S. Jajodia, J. Li, Yi Cheng, Wei Tang, and A. Singhal, “Automatic security analysis using security metrics,” in *2011 - MILCOM 2011 Military Communications Conference*, Baltimore, MD, USA, 2011, pp. 1207-1212.

[94] S. Quinn, D. Waltermire, C. Johnson, K. Scarfone, and J. Banghart, “NIST SP 800-126: The Technical Specification for the Security Content Automation Protocol (SCAP).” National Institute of Standards and Technology, 2009.

[95] S. Radack and R. Kuhn, “Managing Security: The Security Content Automation Protocol,” *IT Professional*, pp. 9–11, 2011.

[96] J. Banghart, S. Quinn, and K. Stine, “Security automation from a NIST perspective,” *IAnewsletter*, vol. 14, no. 4, 2011.

[97] B. Potter, “Security automation,” *Network Security*, vol. 2007, no. 9, pp. 18-19, Sep. 2007.

[98] D. Waltermire, S. Quinn, K. Scarfone, and A. Halbardier, “NIST SP 800-126 Rev. 2: The Technical Specification for the Security Content Automation Protocol (SCAP) Version 1.2.” National Institute of Standards and Technology, Sep-2011.

[99] R. Montesino and Y. Mesa, “Automatización en la gestión de la seguridad informática,” in *X Seminario Iberoamericano de Seguridad en las Tecnologías de la Información*, La Habana, Cuba, 2011.

[100] “Validation Program - The Security Content Automation Protocol (SCAP) - NIST.” [Online]. Available: http://scap.nist.gov/validation/. [Accessed: 30-Aug-2012].

[101] E. Al-Shaer, “Security automation research: challenges and future directions,” *IAnewsletter*, vol. 14, no. 4, 2011.

[102] R. Montesino and S. Fenz, “Automation Possibilities in Information Security Management,” in *2011 European Intelligence and Security Informatics Conference*, Athens, Greece, 2011, pp. 259-262.

[103] D. Linthicum, *Enterprise application integration*. Reading Mass.: Addison-Wesley, 2000.

[104] R. Gleghorn, “Enterprise application integration: a manager’s perspective,” *IT Professional*, vol. 7, no. 6, pp. 17-23, Nov. 2005.

[105] K. Renholm, “Enterprise Application Integration. An Investigative Case Study.,” MSc. Thesis, KTH Electrical Engineering, 2011.

[106] S. Izza, “Integration of industrial information systems: from syntactic to semantic integration approaches,” *Enterprise Information Systems*, vol. 3, no. 1, 2009.

[107] C. Rong, “Preliminary exploration on enterprise application integration based on message-oriented middleware,” in *2011 International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Xianning, China, 2011, pp. 4273-4276.

[108] G. Qing-rui and Z. Hai-tao, “Research of using SOA build enterprise application integration strategy,” in *2010 2nd IEEE International Conference on Information Management and Engineering*, Chengdu, China, 2010, pp. 435-438.

[109] Xiulong Pan, Wei Pan, and Xiao Cong, “SOA-based enterprise application integration,” in *2010 2nd International Conference on Computer Engineering and Technology*, Chengdu, China, 2010, pp. V7-564-V7-568.

[110] X. He, H. Li, Q. Ding, and Z. Wu, “The SOA-Based Solution for Distributed Enterprise Application Integration,” in *2009 International Forum on Computer Science-Technology and Applications*, Chongqing, China, 2009, pp. 330-336.

[111] W. He and Xu, “Integration of Distributed Enterprise Applications: A Survey,” *IEEE Transactions on Industrial Informatics*, 2012.

[112] Y. Du, W. Peng, and L. Zhou, “Enterprise Application Integration: An Overview,” in *2008 International Symposium on Intelligent Information Technology Application Workshops*, Shanghai, China, 2008, pp. 953-957.

[113] L. D. Xu, “Enterprise Systems: State-of-the-Art and Future Trends,” *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 630-640, Nov. 2011.

[114] J. Thompson, Y. V. Natis, M. Pezzini, D. Sholler, R. Altman, and K. Iijima, “Magic Quadrant for Application Infrastructure for Systematic Application Integration Projects.” Gartner, Jun-2012.

[115] M. Nicolett and K. M. Kavanagh, “Critical Capabilities for Security Information and Event Management Technology.” Gartner, May-2011.

[116] D. R. Miller, S. Harris, A. A. Harper, S. VanDyke, and C. Blask, *Security Information and Event Management (SIEM) Implementation*. McGraw-Hill, 2011.

[117] “AlienVault Unified SIEM system description.” AlienVault, 2010.

[118] M. Nicolett and K. M. Kavanagh, “Magic Quadrant for Security Information and Event Management.” Gartner, May-2011.

[119] J. Shenk, *SANS Sixth Annual Log Management Survey Report*. SANS, 2010.

[120] H. Karlzén, “An Analysis of Security Information and Event Management Systems,” MSc. Thesis, Chalmers University of Technology, 2009.

[121] A. Chuvakin, “SIEM: Moving Beyond Compliance.” RSA, 2010.

[122] W. K. Edwards, E. S. Poole, and J. Stoll, “Security automation considered harmful?,” in *Proceedings of the 2007 Workshop on New Security Paradigms*, 2008, pp. 33–42.

[123] R. Montesino and S. Fenz, “Information security automation: how far can we go?,” presented at the Sixth International Conference on Availability, Reliability and Security (ARES), Vienna, Austria, 2011.

[124] R. Montesino, S. Fenz, and W. Bajula, “SIEM-based framework for security controls automation,” *Information Management & Computer Security*, vol. 20, no. 4, Jul. 2012.

[125] V. Verendel, “Quantified security is a weak hypothesis,” in *Proceedings of the 2009 workshop on New security paradigms workshop - NSPW ’09*, Oxford, United Kingdom, 2009, p. 37.

[126] W. S. Torgerson, *Theory and Methods of Scaling*. New York: Wiley, 1958.

[127] L. A. Ramírez and A. M. Toledo, “Algunas consideraciones acerca del método de evaluación utilizando el criterio de expertos.” 2005.

ANEXOS

Anexo 1: Productos SCAP validados por el NIST

Compañía	Nombre del producto	Validación otorgada
ca technologies	CA IT Client Manager	FDCC Scanner Authenticated Configuration Scanner
the CENTER for INTERNET SECURITY	CIS - Configuration Audit Tool	FDCC Scanner
eEye Digital Security®	Retina	FDCC Scanner Authenticated Configuration Scanner Authenticated Vulnerability and Patch Scanner Unauthenticated Vulnerability Scanner
McAfee	Policy Auditor	FDCC Scanner Authenticated Configuration Scanner Authenticated Vulnerability and Patch Scanner
Microsoft	System Center Configuration Manager	FDCC Scanner
nCircle	Configuration Compliance Manager	FDCC Scanner Authenticated Configuration Scanner Authenticated Vulnerability and Patch Scanner
symantec™	Control Compliance Suite	FDCC Scanner Authenticated Configuration Scanner Authenticated Vulnerability and Patch Scanner
TENABLE Network Security®	Security Center	FDCC Scanner Authenticated Configuration Scanner Authenticated Vulnerability and Patch Scanner Unauthenticated Vulnerability Scanner

Anexo 2: Controles automatizables en ISO/IEC 27002

No.	ID	Control
1	7.1.1	Inventory of assets
2	8.3.3	Removal of access rights
3	9.1.2	Physical entry controls
4	9.2.2	Supporting utilities
5	10.1.2	Change management
6	10.3.1	Capacity management
7	10.4.1	Controls against malicious code
8	10.5.1	Information back-up
9	10.6.1	Network controls
10	10.7.1	Management of removable media
11	10.7.4	Security of system documentation
12	10.8.4	Electronic messaging
13	10.9.3	Publicly available information
14	10.10.1	Audit logging
15	10.10.2	Monitoring system use
16	10.10.3	Protection of log information
17	10.10.4	Administrator and operator logs
18	10.10.5	Fault logging
19	10.10.6	Clock synchronization
20	11.2.2	Privilege management
21	11.2.3	User password management
22	11.3.2	Unattended user equipment
23	11.4.2	User authentication for external connections
24	11.4.3	Equipment identification in networks
25	11.4.4	Remote diagnostic and configuration port protection
26	11.4.6	Network connection control
27	11.4.7	Network routing control
28	11.5.1	Secure log-on procedures
29	11.5.2	User identification and authentication
30	11.5.3	Password management system
31	11.5.5	Session time-out
32	11.5.6	Limitation of connection time
33	12.3.2	Key management
34	12.4.3	Access control to program source code
35	12.5.3	Restrictions on changes to software packages
36	12.6.1	Control of technical vulnerabilities
37	13.1.1	Reporting information security events
38	14.1.3	Developing and implementing continuity plans including information security
39	15.2.2	Technical compliance checking

Anexo 3: Controles automatizables en NIST SP 800-53

No.	ID	Control
1	AC-2	Account Management
2	AC-7	Unsuccessful Login Attempts
3	AC-8	System Use Notification
4	AC-9	Previous Logon (Access) Notification
5	AC-10	Concurrent Session Control
6	AC-11	Session Lock
7	AC-17	Remote Access
8	AC-18	Wireless Access
9	AC-21	User-Based Collaboration and Information Sharing
10	AU-6	Audit Review, Analysis, and Reporting
11	AU-7	Audit Reduction and Report Generation
12	AU-8	Time Stamps
13	AU-11	Audit Record Retention
14	AU-12	Audit Generation
15	AU-14	Session Audit
16	CA-2	Security Assessments
17	CA-7	Continuous Monitoring
18	CM-2	Baseline Configuration
19	CM-3	Configuration Change Control
20	CM-5	Access Restrictions for Change
21	CM-6	Configuration Settings
22	CM-8	Information System Component Inventory
23	CP-6	Alternate Storage Site
24	CP-7	Alternate Processing Site
25	CP-9	Information System Backup
26	IA-2	Identification and Authentication (Organizational Users)
27	IA-3	Device Identification and Authentication
28	IA-5	Authenticator Management
29	IA-7	Cryptographic Module Authentication
30	IR-4	Incident Handling
31	IR-5	Incident Monitoring
32	IR-6	Incident Reporting
33	MP-2	Media Access
34	MP-4	Media Storage
35	PE-3	Physical Access Control
36	PE-6	Monitoring Physical Access
37	PE-8	Access Records
38	PE-11	Emergency Power
39	PE-12	Emergency Lighting
40	PE-13	Fire Protection
41	PE-14	Temperature and Humidity Controls
42	RA-5	Vulnerability Scanning
43	SA-7	User-Installed Software

44	SA-10	Developer Configuration Management
45	SC-5	Denial of Service Protection
46	SC-7	Boundary Protection
47	SC-12	Cryptographic Key Establishment and Management
48	SC-14	Public Access Protections
49	SC-17	Public Key Infrastructure Certificates
50	SC-20	Secure Name /Address Resolution Service (Authoritative Source)
51	SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)
52	SC-22	Architecture and Provisioning for Name/Address Resolution Service
53	SC-23	Session Authenticity
54	SC-24	Fail in Known State
55	SC-30	Virtualization Techniques
56	SI-2	Flaw Remediation
57	SI-3	Malicious Code Protection
58	SI-4	Information System Monitoring
59	SI-5	Security Alerts, Advisories, and Directives
60	SI-7	Software and Information Integrity
61	SI-8	Spam Protection
62	SI-13	Predictable Failure Prevention

Anexo 4: Métricas de seguridad informática propuestas en el modelo GAISI

1. Inventario de activos

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

Pregunta: ¿Se encuentran debidamente registrados todos los dispositivos conectados a la red de datos?

Métrica 1.1: Cantidad de equipos desconocidos conectados a la red

Origen de los datos:
- Sistema de escaneo de red: proporciona el listado de equipos conectados a la red.
- Sistema de inventario de activos: proporciona el listado de equipos inventariados.

Fórmula:

$$[Cantidad\ de\ equipos\ conectados\ a\ la\ red - Cantidad\ de\ equipos\ conectados\ a\ la\ red\ que\ están\ inventariados]$$

Frecuencia de medición: Diaria

Pregunta: ¿Las estaciones de trabajo tienen instaladas las aplicaciones autorizadas?

Métrica 1.2: Porciento de equipos con software no autorizado

Origen de los datos:
- Sistema de inventario de activos: proporciona el listado de software instalado en cada equipo y la cantidad de equipos inventariados.
- Política de software autorizado: proporciona el listado de software autorizado.

Fórmula:

$$\left[\frac{Cantidad\ de\ equipos\ con\ software\ no\ autorizado}{Cantidad\ de\ equipos} * 100\right]$$

Frecuencia de medición: Diaria

2. Gestión de usuarios

Objetivo: garantizar la correcta activación, modificación y eliminación de cuentas de usuarios de las tecnologías de la información.

Pregunta: ¿Se eliminan correctamente las cuentas de los usuarios que causan baja de la institución?

Métrica 2.1: Cantidad de cuentas de usuarios que no pueden ser asociadas con algún proceso o área de la institución.

Origen de los datos:
- Directorio: proporciona el listado de las cuentas de usuarios activas.
- Base de datos de recursos humanos: proporciona el listado de trabajadores activos.

Fórmula:

$$[Cantidad\ de\ cuentas\ de\ usuario\ activas - Cantidad\ de\ trabajadores\ activos]$$

Frecuencia de medición: Semanal

Pregunta: ¿Son deshabilitadas las cuentas de usuarios que no poseen actividad en determinado período de tiempo?

Métrica 2.2: Cantidad de cuentas de usuarios que permanecen activas sin ser usadas por más de 30 días.

Origen de los datos:
- Directorio: proporciona el listado de las cuentas de usuarios que no han tenido actividad en determinado período de tiempo

Fórmula:

$$[Cantidad\ de\ cuentas\ \text{sin}\ actividad\ en\ 30\ días]$$

Frecuencia de medición: Diaria

3. Gestión de trazas

Objetivo: 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.

Pregunta: ¿Las trazas de los sistemas son almacenadas en una localización centralizada?

Métrica 3.1: Porciento de sistemas que almacenan trazas de seguridad en una localización centralizada.

Origen de los datos:
- Sistema de almacenamiento de trazas: proporciona el listado de los sistemas con trazas almacenadas.
- Sistema de inventario de activos: proporciona el listado de los sistemas inventariados.

Fórmula:

$$\left[\frac{Cantidad\ de\ sistemas\ con\ trazas\ almacenadas}{Cantidad\ de\ sistemas\ inventariados} * 100\right]$$

Frecuencia de medición: Semanal

Pregunta: ¿Las trazas son conservadas por el tiempo establecido?

Métrica 3.2: Tiempo de conservación de las trazas.

Origen de los datos:
- Sistema de almacenamiento de trazas: proporciona el tiempo de almacenamiento de las trazas

Fórmula:

$$[Tiempo\ de\ almacenamiento\ de\ las\ trazas]$$

Frecuencia de medición: Mensual

4. Monitorización de los sistemas

Objetivo: realizar un monitoreo constante de los sistemas para detectar ataques informáticos, falta de disponibilidad de las aplicaciones, y modificaciones a la información.

Pregunta: ¿Existe algún comportamiento anormal en los intentos de ataques informáticos que se producen desde el exterior?

Métrica 4.1: Cantidad de intentos de ataques (por hora) a la DMZ

Origen de los datos:
- Sistema de detección de intrusos de red (IDS): proporciona las alertas sobre intentos de ataques recibidos.

Fórmula:

$$\left[\frac{Cantidad\ de\ alertas * 60}{Tiempo\ transcurrido\ en\ minutos\ entre\ la\ primera\ y\ última\ alerta}\right]$$

Frecuencia de medición: Diaria

Pregunta: ¿Las aplicaciones críticas se encuentran disponibles todo el tiempo?

Métrica 4.2: Porciento del tiempo en que los sistemas críticos se encuentran disponibles

Origen de los datos:
- Sistema de monitoreo de disponibilidad: proporciona el intervalo de tiempo en que las aplicaciones monitoreadas han estado disponibles.
- Análisis de riesgos: proporciona el listado de los sistemas críticos.

Fórmula:

$$\left[\frac{Tiempo\ de\ disponibilidad\ del\ sistema}{Tiempo\ total} * 100\right]$$

NOTA: para este caso se toma el sistema de la peor condición, o sea, el que haya estado disponible el menor tiempo.

Frecuencia de medición: Semanal

5. Protección contra programas malignos

Objetivo: Emplear mecanismos de protección contra programas malignos que se encuentren constantemente actualizados, para detectar y erradicar código malicioso.
Pregunta: ¿Las estaciones de trabajo poseen el antivirus autorizado por la institución?
Métrica 5.1: Porciento de equipos con el antivirus autorizado instalado
Origen de los datos: - Sistema de inventario de activos: proporciona el listado de los equipos inventariados. - Kit de administración del sistema antivirus: proporciona el listado de los equipos que tienen el antivirus instalado.
Fórmula: $$\left[\frac{Cantidad\ de\ equipos\ con\ el\ antivirus\ instalado}{Cantidad\ de\ equipos\ inventariados} * 100\right]$$
Frecuencia de medición: Diaria
Pregunta: ¿El antivirus se encuentra constantemente actualizado?
Métrica 5.2: Porciento de equipos con el antivirus desactualizado
Origen de los datos: - Kit de administración del sistema antivirus: proporciona el listado de los equipos que tienen el antivirus instalado y desactualizado.
Fórmula: $$\left[\frac{Cantidad\ de\ equipos\ con\ el\ antivirus\ desactualizado}{Cantidad\ de\ equipos\ con\ el\ antivirus\ instalado} * 100\right]$$
Frecuencia de medición: Diaria
6. Detección de vulnerabilidades y gestión de parches
Objetivo: 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.
Pregunta: ¿Poseen vulnerabilidades los diferentes sistemas de la institución?
Métrica 6.1: Cantidad de vulnerabilidades críticas detectadas
Origen de los datos: - Sistema de escaneo de vulnerabilidades: proporciona el listado de las vulnerabilidades detectadas y su clasificación
Fórmula: $$[Cantidad\ de\ vulnerabilidades\ críticas\ detectadas]$$
Frecuencia de medición: Semanal
Métrica 6.2: Porciento de equipos con vulnerabilidades críticas
Origen de los datos: - Sistema de escaneo de vulnerabilidades: proporciona el listado de los equipos con vulnerabilidades detectadas y su clasificación.
Fórmula: $$\left[\frac{Cantidad\ de\ equipos\ con\ vulnerabilidades\ críticas}{Cantidad\ de\ equipos\ escaneados} * 100\right]$$
Frecuencia de medición: Semanal
Pregunta: ¿Las vulnerabilidades de los sistemas son detectadas y solucionadas con agilidad?
Métrica 6.3: Tiempo medio de mitigación de vulnerabilidades
Origen de los datos: - Sistema de escaneo de vulnerabilidades: proporciona listados con los resultados de varios escaneos que contienen las vulnerabilidades detectadas y las fechas de los escaneos.
Fórmula:

$$\left[\frac{\sum_1^n (Fecha\ en\ la\ que\ se\ corrigió\ -\ Fecha\ en\ la\ que\ se\ detectó\ la\ vulnerabilidad)}{n}\right]$$

n: cantidad de vulnerabilidades

Frecuencia de medición: Mensual

Pregunta: ¿Existen sistemas con parches pendientes de aplicar?

Métrica 6.4: Porciento de equipos con parches de seguridad críticos pendientes de instalación

Origen de los datos:

- Sistema de gestión de parches: proporciona el listado de los sistemas que tienen parches pendientes de instalación y su clasificación

Fórmula:

$$\left[\frac{Cantidad\ de\ equipos\ con\ parches\ críticos\ pendientes}{Cantidad\ total\ de\ equipos} * 100\right]$$

Frecuencia de medición: Semanal

Pregunta: ¿Los parches son aplicados con la agilidad necesaria?

Métrica 6.5: Tiempo medio de aplicación de los parches de seguridad

Origen de los datos:

- Sistema de gestión de parches: proporciona el listado de los parches aplicados y las fechas en que se aplicaron los mismos

Fórmula:

$$\left[\frac{\sum_1^n \sum_1^m (Fecha\ en\ la\ que\ se\ aplicó\ el\ parche\ -\ Fecha\ en\ la\ que\ se\ publicó\ el\ parche)}{n}\right]$$

m: cantidad de parches
n: cantidad total de equipos

Frecuencia de medición: Mensual

7. Configuraciones de seguridad y cumplimiento de políticas

Objetivo: 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.

Pregunta: ¿Las configuraciones de seguridad de los diferentes sistemas está acorde con las políticas definidas en la institución?

Métrica 7.1: Porciento de equipos acorde con la imagen y configuraciones de seguridad definidas.

Origen de los datos:

- Sistema de chequeo de configuraciones: proporciona el resultado de la verificación de las configuraciones de los equipos con respecto a un patrón definido.

Fórmula:

$$\frac{Cantidad\ de\ equipos\ con\ configuraciones\ incorrectas}{Cantidad\ total\ de\ equipos} * 100$$

Frecuencia de medición: Mensual

Pregunta: ¿Poseen configuraciones seguras los sistemas según patrones de referencia internacionales?

Métrica 7.2: Puntuación (benchmark) de seguridad promedio (de acuerdo a patrones internacionales)

Origen de los datos:

- Sistema de chequeo de configuraciones: proporciona la puntuación alcanzada por los equipos al chequear sus configuraciones con respecto a patrones de referencia internacionales.

Fórmula:

$$\left[\frac{\sum_1^n Puntuación\ alcanzada\ por\ el\ equipo}{n}\right]$$

n: cantidad total de equipos

Frecuencia de medición: Trimestral

8. Respaldo de información

Objetivo: realizar frecuentemente copias de respaldo de la información y los sistemas, que posibiliten la recuperación ante la ocurrencia de algún incidente.

Pregunta: ¿Se respalda la información de los sistemas críticos?

Métrica 8.1: Porciento de sistemas críticos respaldados

Origen de los datos:

- Sistema de copias de respaldo: proporciona el listado de los sistemas con información respaldada
- Análisis de riesgos: proporciona el listado de los sistemas críticos

Fórmula:

$$\frac{Cantidad\ de\ sistemas\ críticos\ con\ información\ respaldada}{Cantidad\ de\ sistemas\ críticos} * 100$$

Frecuencia de medición: Mensual

Pregunta: ¿La información respaldada posee la actualidad necesaria para una recuperación efectiva?

Métrica 8.2: Última fecha en la que todos los respaldos se realizaron de forma exitosa

Origen de los datos:

- Sistema de copias de respaldo: proporciona el listado de los sistemas con información respaldada, las fechas en que se realizaron las mismas y los errores ocurridos.

Fórmula:

$$[Última\ fecha\ en\ la\ que\ no\ se\ reportaron\ errores]$$

Frecuencia de medición: Diaria

9. Seguridad física

Objetivo: 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.

Pregunta: ¿Los equipos operan a una temperatura adecuada?

Métrica 9.1: Temperatura promedio de operación de los sistemas

Origen de los datos:

- Sistema de monitoreo: proporciona la temperatura de operación de los sistemas en diferentes momentos de tiempo

Fórmula:

$$\left[\frac{\sum_1^n Temperatura\ de\ operación\ del\ sistema}{n}\right]$$

n: cantidad de mediciones

Frecuencia de medición: Semanal

Pregunta: ¿Los fallos eléctricos han provocado afectación en los sistemas?

Métrica 9.2: Cantidad de fallos de corriente eléctrica (por semana)

Origen de los datos:

- Sistema de gestión de la UPS: proporciona información sobre los fallos de corriente.

Fórmula:

$$[Cantidad\ de\ fallos\ de\ corriente]$$

Frecuencia de medición: Semanal

10. Gestión de incidentes

Objetivo: establecer un sistema de gestión de incidentes de seguridad informática que incluya la detección, análisis, contención, solución y recuperación de los incidentes.

Pregunta: ¿Se han producido muchos incidentes de seguridad informática?

Métrica 10.1: Cantidad de incidentes de seguridad informática (por semana)

Origen de los datos:

- Sistema de gestión de incidentes: proporciona información sobre los incidentes de seguridad informática con sus fechas de ocurrencia, detección y solución.

Fórmula:

$$[Cantidad\ de\ incidentes\ detectados\ en\ una\ semana]$$

Frecuencia de medición: Semanal

Pregunta: ¿Los incidentes de seguridad informática son detectados y solucionados con agilidad?

Métrica 10.2: Tiempo medio de detección de incidentes

Origen de los datos:

- Sistema de gestión de incidentes: proporciona información sobre los incidentes de seguridad informática con sus fechas de ocurrencia, detección y solución.

Fórmula:

$$\left[\frac{\sum_1^n (Fecha\ en\ la\ que\ se\ detectó\ el\ incidente\ -\ Fecha\ en\ la\ que\ ocurrió\ el\ incidente)}{n}\right]$$

n: cantidad de incidentes

Frecuencia de medición: Mensual

Métrica 10.3: Tiempo medio de solución de incidentes

Origen de los datos:

- Sistema de gestión de incidentes: proporciona información sobre los incidentes de seguridad informática con sus fechas de ocurrencia, detección y solución.

Fórmula:

$$\left[\frac{\sum_1^n (Fecha\ en\ la\ que\ se\ solucionó\ el\ incidente\ -\ Fecha\ en\ la\ que\ se\ detectó\ el\ incidente)}{n}\right]$$

n: cantidad de incidentes

Frecuencia de medición: Mensual

Anexo 5: Script para la sincronización del Directorio Activo con las bases de datos de recursos humanos.

Sincronizar_directorio.py

```
#!/usr/bin/python
# coding: utf-8

import MySQLdb
import sys
import os
import ldap
import active_directory
import win32com
import win32com.client
import smtplib

msg_template2 = """\
To: %s
From: %s
Subject: Solapin incorrecto en el Directorio Activo
Content-Type: text/plain; charset="UTF-8"

Su usuario (%s) tiene un solapin (%s) en el Directorio Activo que no
coincide o no existe con los registrados en los sistemas primarios
(Akademos, Capital Humano, Tercerizados)
UD dispone de 3 dias para acudir al Nodo Central con su solapin, pasado ese
tiempo su usuario será deshabilitado.

Servicios Telematicos UCI.
"""


def conectar_ldap():
# Se conecta al AD
        ld = ldap.initialize('ldap://10.0.0.2')
        user = "xxxxxxxxxxxxxxxx"
        password = "yyyyyyyyyyyyyyyyyy"
        try:
                ld.simple_bind_s(user, password)
                print "conectado al AD"
                return ld
        except:
                print "error al conectarse"
                return "no"

def buscar_todos_ad():
# Busca todos los username del AD y sus respectivos solapines
# Busca todos los que no tienen solapin en el AD
        for user in active_directory.search_ex("SELECT
            sAMAccountName,postOfficeBox  FROM 'LDAP://OU=UCI Domain
            Users,DC=uci,DC=cu' WHERE objectCategory='Person'"):
```

```
                temp_solapa = str (user.postOfficeBox)
                username = str (user.sAMAccountName)
                #esto es para limpiar la salida del AD
                if temp_solapa != "None":
                        a,b=temp_solapa.split("u")
                        c,d=str(b).split(",)")
                        e=str(c).strip("'")
                        solapin = e

                        solapines_ad.append(solapin)
                        diccionario_AD.setdefault(solapin, username)
                        directorio.append(str (user.sAMAccountName))
                else:
                        sin_solapin.append(username)
        return diccionario_AD, solapines_ad, sin_solapin, directorio

def buscar_todos_activos():
# Devuelve todos pareja username, solapin que estén activos
# Devuelve todos los solapines activos
        conn = MySQLdb.connect (host = "dbserver1.uci.cu", user = "xxxxxx",
                                passwd = "yyy", db = "UCI_Autenticacion_v2")
        cursor = conn.cursor ()
        consulta = "SELECT username,ExpedienteId from GatewayUsers WHERE
                    IsActive = '1'"
        cursor.execute (consulta)
        resultado = cursor.fetchall ()

        # a[0]  ----->  solapin IdExp
        # a[8]  ----->  username

        for a in resultado:
                #print a[0]
                b = a[0]
                #print b
                #print a[1]
                c = a[1]
                #print c
                #raw_input ()
                diccionario_PA.setdefault(b,c)
                #print diccionario_PA
                solapines_activos.append(a[1])
                usuarios_activos.append(a[0])
                #print a[0]
                #print a[4]
        return diccionario_PA, solapines_activos, usuarios_activos

if __name__ == "__main__":
# Definiciones de listas y variables
        # Este tendra todos los solapines que esten activos
        solapines_activos = []
        #Este tendra los usuarios que no tienen solapin en el AD
        sin_solapin = []
        #Este tendra los solapines de los usuarios segun el AD
        solapines_ad= []
```

```
        #Todos los username del AD
        todos_username = []
        #Todos los usuarios del AD
        directorio = []
        #Pareja SOLAPIN-USERNAME Active Directory
        diccionario_AD = {}
        #Pareja SOLAPIN_USERNAME Pasarela de Autenticacion
        diccionario_PA = {}
        #comodin
        resultado = []
        #Este tendra las bajas UCI
        deserticons = []
        #username activos segun Pasarela
        usuarios_activos = []
        #notificados
        nottificados = []

        # Conectar con el servidor de correo y el LDAP
        smail = smtplib.SMTP(mailhost)
        conectar_ldap()


        buscar_todos_ad()
        buscar_todos_activos()

# Buscar los usernames que estan en el AD y no en Pasarela
        for user in directorio:
                if user not in usuarios_activos:
                        deserticons.append(user)

# Buscar los solapines de los username que salieron como resultado del paso
# anterior
        for user in deserticons:
                a = active_directory.find_user(user)
                solapin = a.postOfficeBox
                if solapin in solapines_activos:
                        deserticons.remove(user)

# Notificar por correo que el username no aparece o tiene solapin mal
        for z in deserticons:
                user = active_directory.find_user(z)
                sola = user.postOfficeBox
                k = str(user.mail)
                if k != "None":
                        smail.sendmail(from_address, k, msg_template2 %
                                        (k, from_address, z, str(sola)))
                        print user.DisplayName

# Tratamiento de los usuarios posibles bajas. Moverlos para la OU ghost

        for user in deserticons:
                me = active_directory.find_user(user)
                destination_ou.com_object.MoveHere(str(me.as_string()),
                                                   str(me.Name))
```

Anexo 6: Conectores desarrollados para la integración de WSUS y Bacula

WSUS.cfg

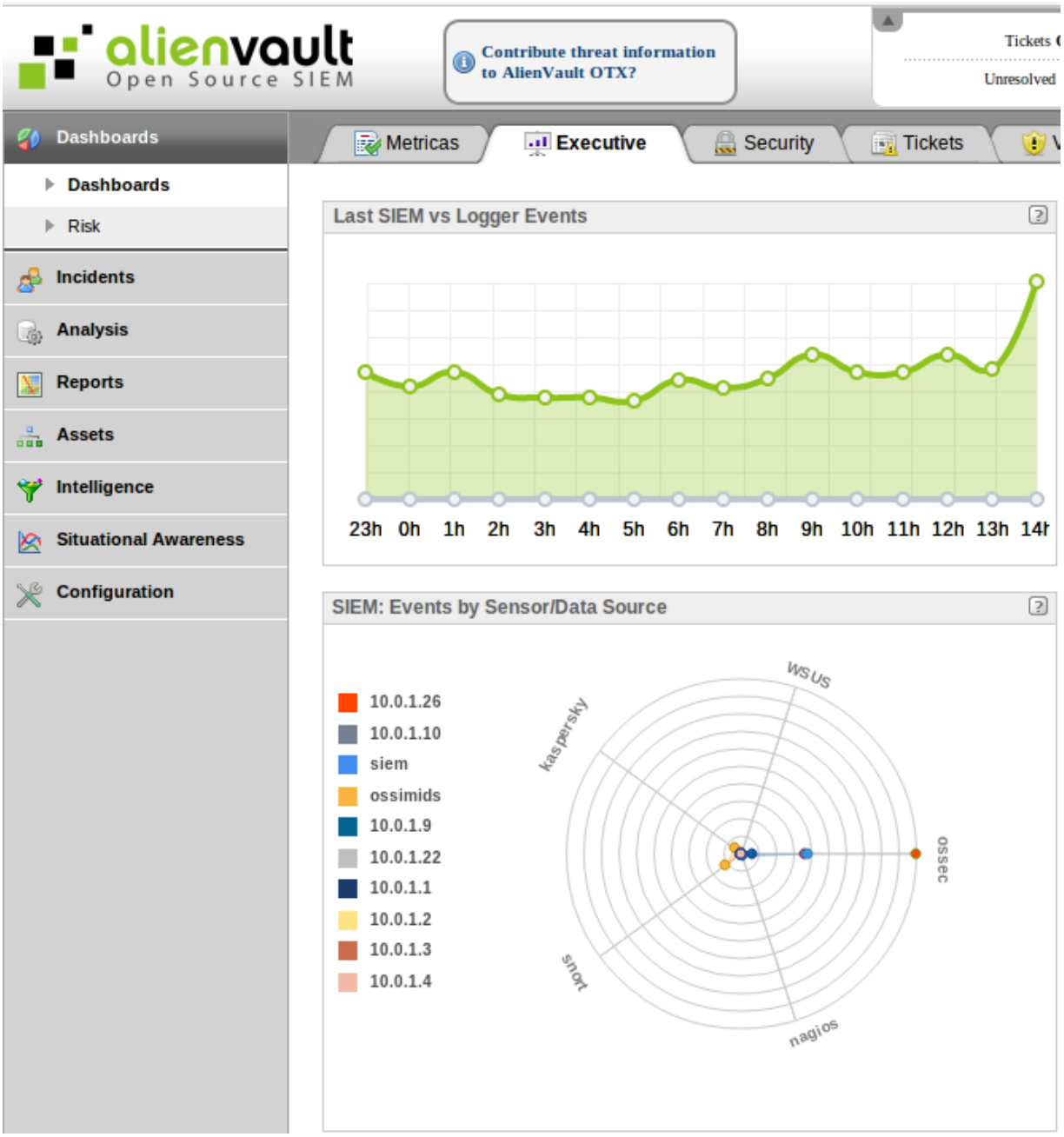
```
[DEFAULT]
plugin_id=20014

[config]
type=detector
enable=yes

process=syslogd   ; -r || -u
start=no    ; launch plugin process when agent starts
stop=no     ; shutdown plugin process when agent stops
startup=/etc/init.d/%(process)s start
shutdown=/etc/init.d/%(process)s stop

source=log
location=/var/log/ossim-wsus.log

create_file=false

[snare-nxlog-format-wu-events]

event_type=event
regexp="(?P<date>\w{3}\s+\d{1,2}\s\d\d:\d\d:\d\d)\s+(?P<host>\S+)(#011|\s+)
MSWinEventLog(#011|\s+)(\d+)(#011|;|\s+)([\w/]+)(#011|;|\s+)([\w/]+)(#011|\
s+|;)(?P<windowsdate>\w{3}\s\w{3}\s+\d{1,2}\s\d{1,2}:\d{1,2}:\d{1,2}\s\d{4}
)(#011|;|\s+)(?P<sid>\d+)(#011|;|\s+)(Windows Server Update
Services)(#011|;|\s+)([\w/]+)(#011|;|\s+)([\w/]+)(#011|;|\s+)(?P<severity>[
\w_]+)(#011|;|\s+)(?P<hostname>[\w.]+)(#011|;|\s)([\w/\s.]+)(#011|;|\s+)(#0
11|;|\s+)(?P<msg_event>.*.)(#011|;|\s+)(.*)|#015"

date={normalize_date($date)}
plugin_id=20014
plugin_sid={$sid}
src_ip={resolv($host)}
username={$user}
userdata1={$hostname}
userdata2={$severity}
userdata3={$msg_event}
```

Bacula.cfg

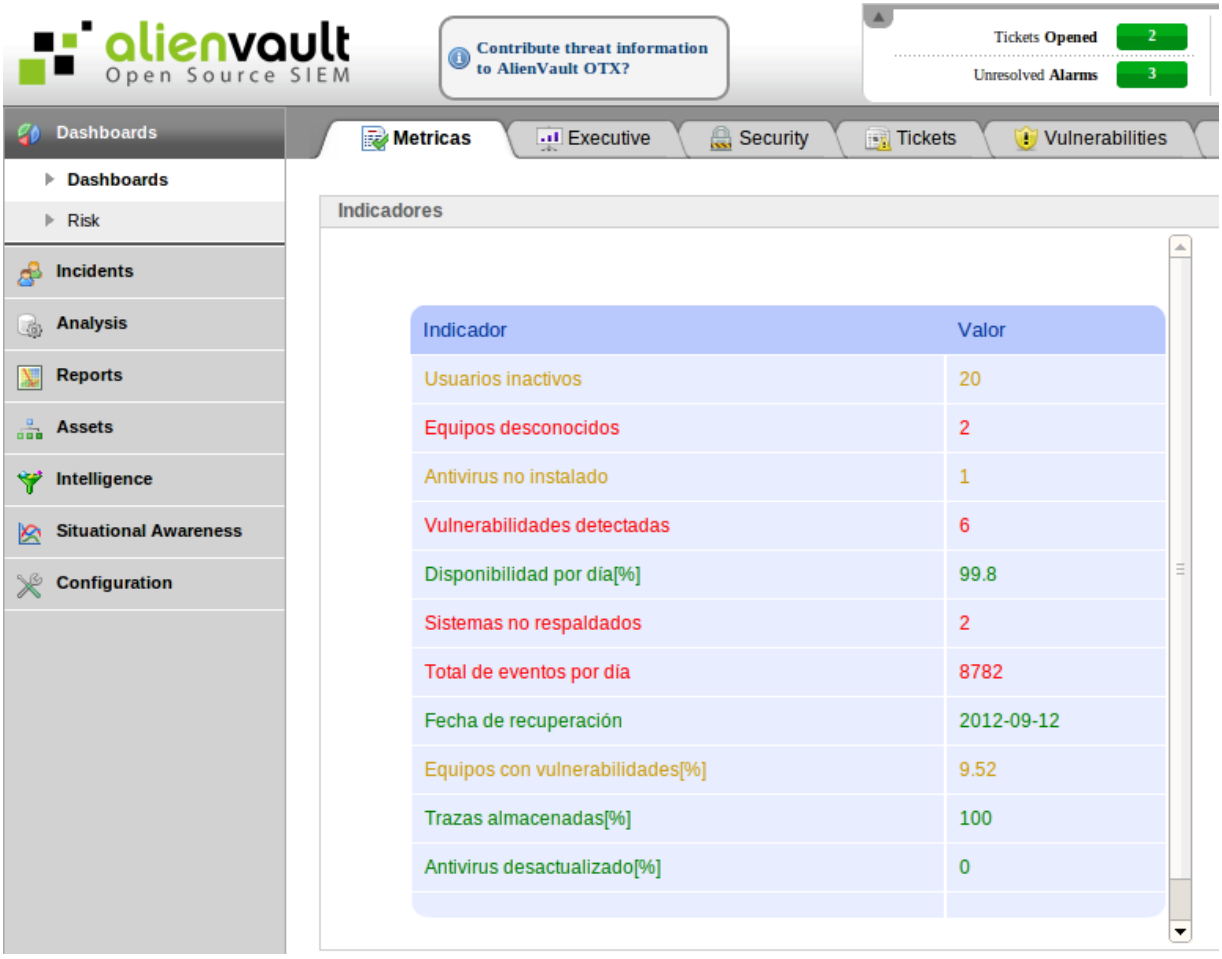
```
[DEFAULT]
plugin_id=20012

[config]
type=detector
enable=yes

source=database
source_type=mysql
source_ip=10.0.0.x
source_port=3306
user=xxxx
password=yyyyyyy
db=bacula
sleep=60

process=
start=no
stop=no
[translation]
Warning=2
Error=3
Fatal error=4

[start_query]
query="select LogId from Log order by LogId DESC LIMIT 1;"
regexp=

[query]
query="select Log.LogId, Log.JobId ,Log.Time,Log.LogText, Job.ClientId,
Job.Name,TRIM(SUBSTRING_INDEX(SUBSTRING_INDEX(Log.LogText,':',2),':',-1))
as severity from Log inner join Job on Job.JobId = Log.JobId where
Log.LogId > $1  and
TRIM(SUBSTRING_INDEX(SUBSTRING_INDEX(Log.LogText,':',2),':',-1)) REGEXP
'Error|Warning|Fatal' ORDER BY Log.LogId asc;"
regexp=
ref=0
plugin_sid={translate($6)}
date={normalize_date($2)}
userdata1={$0}
userdata2={$1}
userdata3={$4}
userdata4={$5}
userdata5={$6}
log= Bacula message time: {$2}, Job ID:{$1} ,Text: {$3}
```

Anexo 7: Capturas de pantalla del sistema OSSIM instalado en la UCI

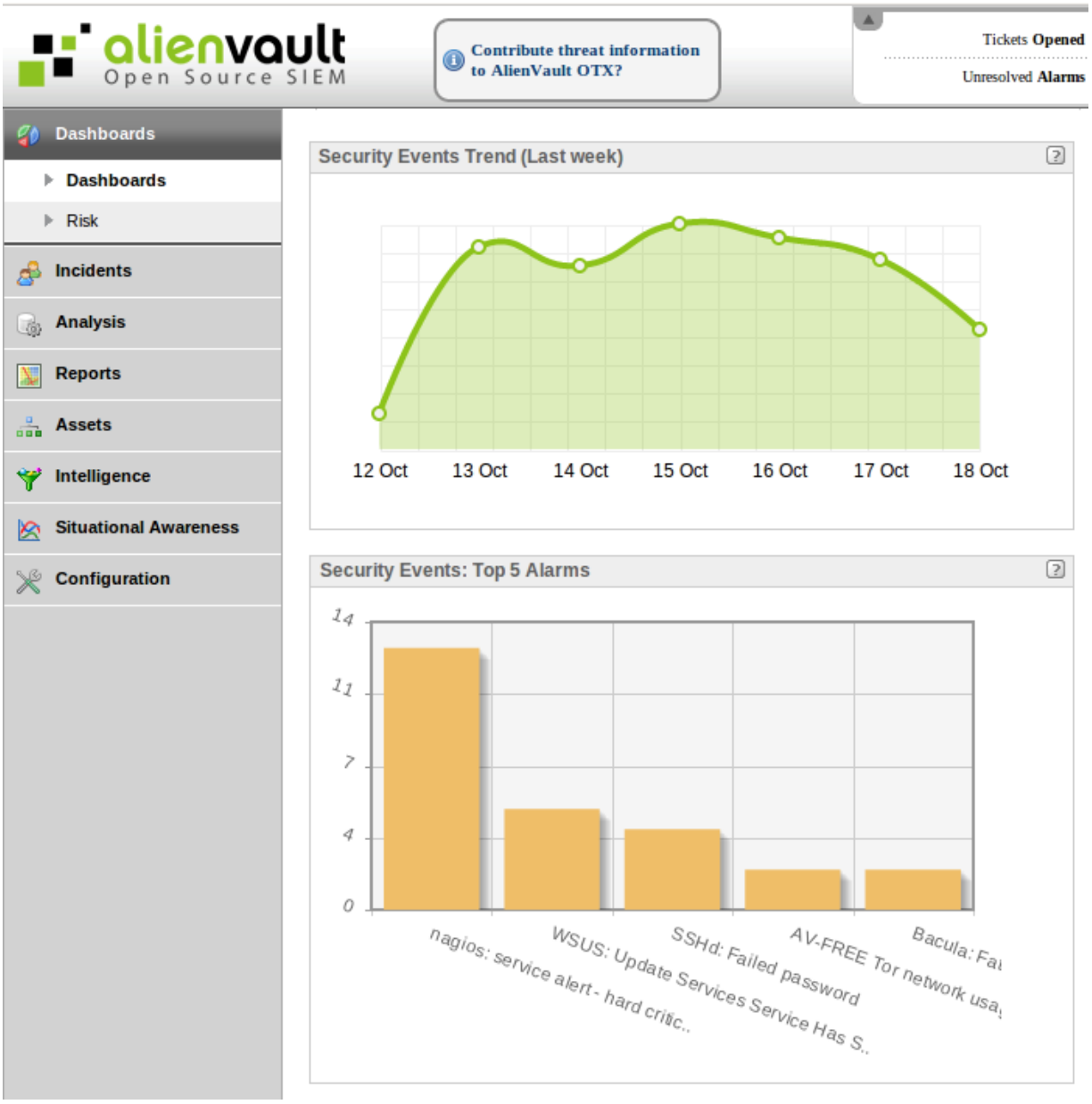
Panel ejecutivo de OSSIM donde se aprecian diferentes sistemas integrados



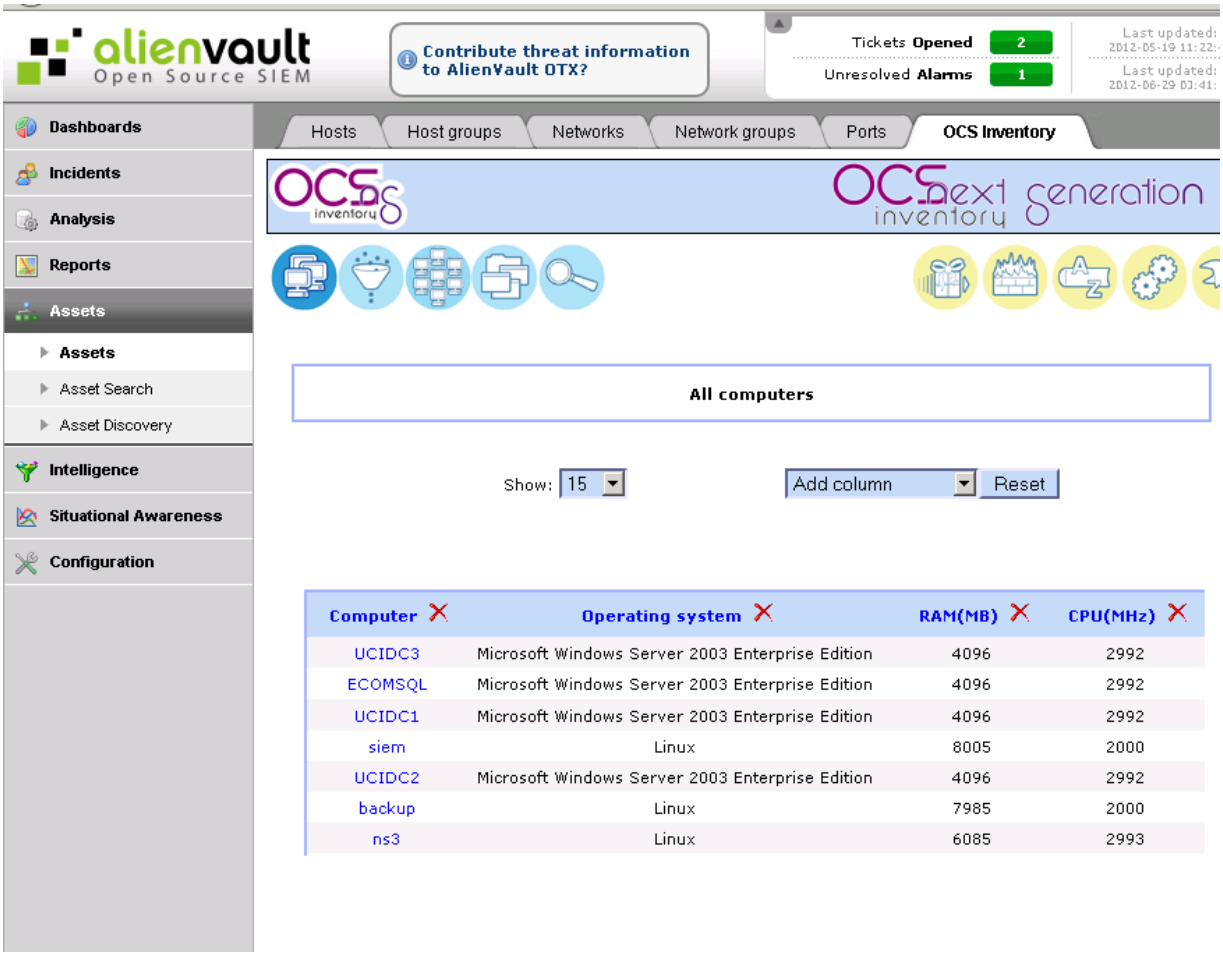
Métricas de seguridad informática del modelo GAISI mostradas en OSSIM



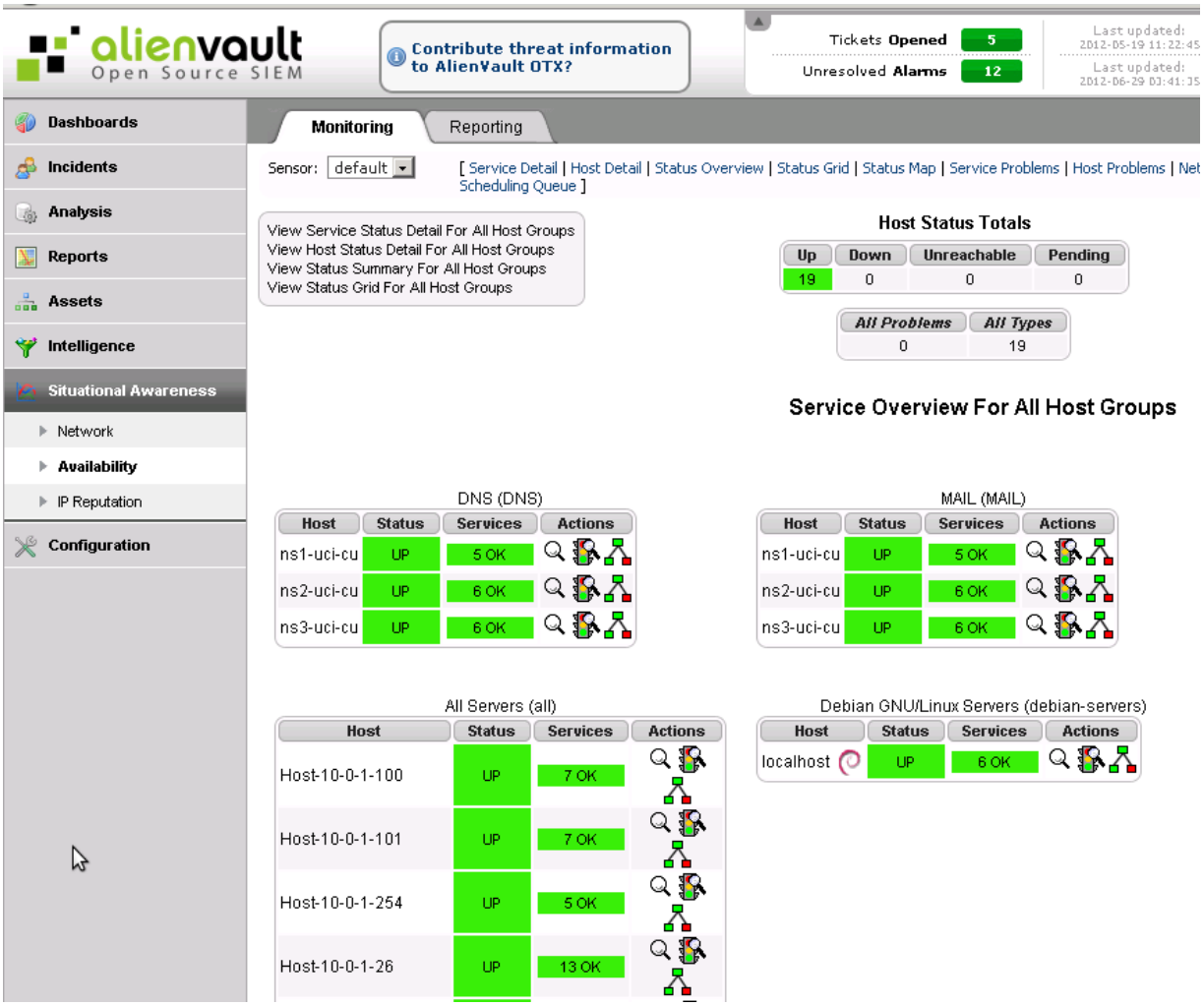
Gráficos de eventos y alarmas de OSSIM



OCS Inventory integrado en OSSIM



NAGIOS integrado en OSSIM



Anexo 8: Procedimiento para la determinación del nivel de competencia de los expertos

La competencia de los expertos se determina por el **coeficiente K,** el cual se calcula de acuerdo con la opinión del candidato sobre su nivel de conocimiento acerca del problema que se esta resolviendo y con las fuentes que le permiten argumentar sus criterios.

El coeficiente K se calcula por la siguiente expresión: **K = ½ (Kc + Ka)**

Kc: Es el coeficiente de conocimiento o información que tiene el experto acerca del problema, el cual es calculado sobre la base de la valoración del propio experto en una escala de 0 a 10 y multiplicado por 0.1 de modo que:

- El valor 0 indica absoluto desconocimiento de la problemática que se evalúa.
- El valor 1 indica pleno conocimiento de la referida problemática.

El experto deberá marcar una cruz en la casilla que estime pertinente según su autovaloración del nivel de conocimiento que posee en el tema tratado.

0	1	2	3	4	5	6	7	8	9	10

Ka: Es el coeficiente de argumentación o fundamentación de los criterios del experto, determinado como resultado de la suma de los puntos alcanzados a partir de una tabla patrón.

La tabla patrón forma parte del cuestionario que se le plica a los candidatos a expertos y en la misma estos reflejan el grado de influencia de las fuentes mediante las cuales han asimilado los conocimientos sobre el tema objeto de valoración.

FUENTES DE ARGUMENTACIÖN	Grado de influencia de cada una de las fuentes en sus criterios		
	ALTO (A)	MEDIO (M)	BAJO (B)
Investigaciones teóricas o experimentales relacionadas con el tema.	0.3	0.2	0.1
Experiencia obtenida en la actividad profesional.	0.5	0.4	0.2
Trabajos de autores nacionales.	0.05	0.05	0.05
Trabajos de autores extranjeros.	0.05	0.05	0.05
Conocimiento del estado actual del problema en el país y en el extranjero.	0.05	0.05	0.05

Intuición	0.05	0.05	0.05
TOTAL	**1**	**0.8**	**0.5**

Al experto se le presenta esta tabla sin cifras, orientándole que marque con una (x) sobre las fuentes que han influido más en su conocimiento de acuerdo con los niveles ALTO (A), MEDIO (M) y BAJO (B). Posteriormente utilizando los valores de la tabla patrón para cada una de las celdas marcadas por el experto, se calcula el número de puntos obtenidos en total.

Finalmente se determina el coeficiente de competencia K de modo que:

Si $0{,}8 < K \leq 1$ el experto tiene competencia alta.
Si $0{,}5 \leq K < 0{,}8$ el experto tiene competencia media.
Si $0 \leq K < 0{,}5$ el experto tiene competencia baja.

Anexo 9: Cuestionario aplicado al grupo de expertos

Sector al que pertenece: Académico: ___ Empresarial: ___ Gubernamental: ___

Grado científico: _____ Años de experiencia en seguridad informática: ____

Certificaciones obtenidas relacionadas con seguridad informática:_____

Cantidad de publicaciones científicas relacionadas con la seguridad informática:____

Cantidad de eventos científicos en los que ha participado:____

1. Evalúe el modelo propuesto con respecto a los siguientes criterios (asigne valores del 1 al 5):

   1 – No cumple, 2 – Casi no cumple, 3 – Cumple, 4 – Cumple en buena medida, 5 – Cumple excelentemente

Criterio	Significado	Evaluación
Automatización	Posibilita la automatización de gran cantidad de controles	
Integración	Permite la gestión integrada de los controles	
Síntesis	Presenta una adecuada síntesis de los controles automatizables	
Medición objetiva	Permite una medición objetiva de la efectividad de los controles	
Mejora continua	Posee un enfoque de gestión y de procesos continuos	
Generalidad	Es aplicable a una gran variedad de organizaciones	

2. Exprese su conformidad con respecto a la selección de los 10 macro-controles automatizables propuestos en el modelo. Utilice la escala de valores (1 - 5) de acuerdo a los siguientes criterios:

   1 - En total desacuerdo, 2 - Casi en desacuerdo, 3 - Parcialmente de acuerdo, 4 - Mayormente de acuerdo, 5 - Completamente de acuerdo

No.	Macro-control	Conformidad
1	Inventario de activos	
2	Gestión de usuarios	
3	Gestión de trazas	
4	Monitoreo de los sistemas	
5	Protección contra programas malignos	
6	Detección de vulnerabilidades y gestión de parches	
7	Configuraciones de seguridad y cumplimiento de políticas	
8	Respaldo de información	

9	Seguridad física	
10	Gestión de incidentes	

2.1. Añadiría algún otro control a la lista anterior: __ Sí __ No

En caso afirmativo, ¿cuál o cuáles serían? _____

_____

3. ¿Considera que los indicadores propuestos reflejan la efectividad de los 10 macro-controles de seguridad informática definidos en el modelo? Conteste Sí o No para cada indicador.

No.	Macro-control	Indicador	¿Efectividad?
1	Inventario de activos	Cantidad de equipos desconocidos conectados a la red	
		Porciento de equipos con software no autorizado	
2	Gestión de usuarios	Cantidad de cuentas de usuarios que no pueden ser asociadas con algún proceso o área de la institución	
		Cantidad de cuentas de usuarios que permanecen activas sin ser usadas por más de 30 días.	
3	Gestión de trazas	Cantidad de sistemas que almacenan las trazas de seguridad en un servidor centralizado	
		Tiempo de conservación de las trazas	
4	Monitoreo de los sistemas	Cantidad de intentos de ataques (por hora) a la DMZ	
		Porciento del tiempo en que los sistemas críticos se encuentran disponibles	
5	Protección contra programas malignos	Porciento de equipos con el antivirus autorizado instalado	
		Porciento de equipos con el antivirus desactualizado	
6	Detección de vulnerabilidades y gestión de parches	Cantidad de vulnerabilidades críticas detectadas	
		Porciento de equipos con vulnerabilidades críticas	
		Tiempo medio de mitigación de vulnerabilidades	
		Porciento de equipos con parches de seguridad críticos pendientes de instalación	
		Tiempo medio de aplicación de los parches de seguridad (desde su publicación hasta la instalación)	
7	Configuraciones de seguridad y cumplimiento de políticas	Porciento de equipos acorde con la imagen y configuraciones de seguridad definidas	
		Puntuación (*benchmark*) de seguridad promedio (de acuerdo a patrones internacionales)	
8	Respaldo de información	Porciento de sistemas críticos respaldados	
		Última fecha en la que todos los respaldos se realizaron de forma exitosa	
9	Seguridad física	Temperatura promedio de operación de los sistemas	

		Cantidad de fallos de corriente (por semana)	
10	Gestión de incidentes	Cantidad de incidentes de seguridad informática (por semana)	
		Tiempo medio de detección de incidentes (desde que ocurrió hasta su registro en el sistema)	
		Tiempo medio de solución de incidentes (a partir de que son reportados)	

3.1. ¿Añadiría algún otro indicador? __ Sí __ No

En caso afirmativo, ¿cuál o cuáles serían? _____

_____

4. ¿Considera que con la aplicación del modelo aumentaría la efectividad de los controles de seguridad informática?

__ Mucho __ Bastante __ Algo __ Casi nada __ Nada

5. ¿Considera que con la aplicación del modelo disminuiría la complejidad de la gestión de la seguridad informática?

__ Mucho __ Bastante __ Algo __ Casi nada __ Nada

6. ¿Desea añadir algún otro comentario sobre el modelo propuesto?

_____

_____

Anexo 10: Tablas resultantes del procesamiento del cuestionario aplicado a los expertos

Tabla A.10.1: Frecuencia (PRINCIPIOS)

PRINCIPIOS	5	4	3	2	1	TOTAL
Automatización	2	7	1	0	0	10
Integración	3	4	3	0	0	10
Síntesis	3	6	0	1	0	10
Medición objetiva	1	7	2	0	0	10
Mejora continua	4	4	2	0	0	10
Generalidad	4	5	1	0	0	10

Tabla A.10.2: Escala de los indicadores y puntos de corte (PRINCIPIOS)

PRINCIPIOS	5	4	3	2	Promedio	N - Prom.	
Automatización	-0.84	1.28	3.50	3.50	1.86	**-0.10**	4
Integración	-0.52	0.52	3.50	3.50	1.75	**0.01**	4
Síntesis	-0.52	1.28	1.28	3.50	1.39	**0.37**	**4**
Medición objetiva	-1.28	0.84	3.50	3.50	1.64	**0.12**	4
Mejora continua	-0.25	0.84	3.50	3.50	1.90	**-0.14**	4
Generalidad	-0.25	1.28	3.50	3.50	2.01	**-0.25**	4
Puntos de corte	**-0.61**	**1.01**	**3.13**	**3.50**	**1.76**	**= N**	

Tabla A.10.3: Frecuencia (MACRO-CONTROLES)

MACRO-CONTROLES	5	4	3	2	1	TOTAL
Inventario de activos	7	3	0	1	0	11
Gestión de usuarios	9	2	0	0	0	11
Gestión de trazas	8	3	0	0	0	11
Monitoreo de los sistemas	10	1	0	0	0	11
Protección malware	7	4	0	0	0	11
Vulnerabilidades y parches	9	2	0	0	0	11
Configuraciones y cumplimiento	7	4	0	0	0	11
Respaldo de información	5	3	3	0	0	11
Seguridad física	3	6	2	0	0	11
Gestión de incidentes	9	1	1	0	0	11

Tabla A.10.4: Escala de los indicadores y puntos de corte (MACRO-CONTROLES)

MACRO-CONTROLES	5	4	3	2	Promedio	N - Prom.	
Inventario de activos	0.35	1.34	1.34	3.50	1.63	**0.82**	4
Gestión de usuarios	0.91	3.50	3.50	3.50	2.85	**-0.40**	5
Gestión de trazas	0.60	3.50	3.50	3.50	2.78	**-0.33**	**5**
Monitoreo sistemas	1.34	3.50	3.50	3.50	2.96	**-0.51**	5
Protección malware	0.35	3.50	3.50	3.50	2.71	**-0.26**	5

Vulnerabilidades y parches	0.91	3.50	3.50	3.50	2.85	**-0.40**	5
Configuraciones y cumplimiento	0.35	3.50	3.50	3.50	2.71	**-0.26**	5
Respaldo información	-0.11	0.60	3.50	3.50	1.87	**0.58**	**4**
Seguridad física	-0.60	0.91	3.50	3.50	1.83	**0.62**	**4**
Gestión de incidentes	0.91	1.34	3.50	3.50	2.31	**0.14**	**5**
Puntos de corte	**0.50**	**2.52**	**3.28**	**3.50**	**2.45 = N**		

Anexo 11: Cuestionario aplicado a directivos y especialistas del MES y el MIC

1. Datos del encuestado (marque con una X):
   __ Directivo del área informática o de seguridad informática
   __ Administrador de la red
   __ Especialista de seguridad informática

2. Datos generales de la organización:
   2.1. Cantidad de computadoras:
   2.2. Cantidad de servidores:
   2.3. Cantidad de usuarios de las TIC:

3. Diga cuáles de los siguientes controles de seguridad informática, y en qué medida, están implementados en su organización, así como los sistemas que se utilizan para su gestión. Utilice la escala de valores (1 - 5) para especificar el nivel de implementación, donde uno significa que el control no está implementado y cinco significa que el control está automatizado. En el Anexo 1 se describe la escala de valores para cada control.

No.	Controles	Implementación (1 - 5)	Sistemas empleados
1	Inventario de activos		
2	Gestión de usuarios		
3	Gestión de trazas		
4	Monitoreo de los sistemas		
5	Protección contra programas malignos		
6	Detección de vulnerabilidades y gestión de parches		
7	Configuraciones de seguridad y cumplimiento de políticas		
8	Respaldo de información		
9	Seguridad física		
10	Gestión de incidentes		

4. ¿Se utiliza en la entidad algún sistema de gestión de eventos e información de seguridad (SIEM)?
   __ Sí __ No __ No sé

   4.1. En caso afirmativo diga el sistema SIEM que se utiliza: _____

5. ¿Se utiliza en su entidad algún sistema de indicadores que permita evaluar la efectividad de los controles de seguridad informática?
   __ Sí __ No __ No sé

   5.1. En caso afirmativo, ¿con qué frecuencia se actualizan y revisan los indicadores? (marque con una X)
   __ Diaria __ Semanal __ Mensual __ Trimestral __ Semestral
   __ Anual

6. Diga cuáles de los siguientes factores usted considera que contribuirían a aumentar la efectividad y disminuir la complejidad de la gestión de la seguridad informática. Utilice la escala de valores (1 - 5) de acuerdo a los siguientes criterios:

5 – Mucho 4 – Bastante 3 – Algo 2 – Casi nada
1 – Nada

Factores	**Aumenta efectividad**	**Disminuye complejidad**
Automatización de los controles de seguridad informática mencionados		
Integración de los diferentes sistemas y herramientas de seguridad informática en un sistema que permita una gestión centralizada		
Mayor cantidad de especialistas de seguridad informática		
Preparación y superación de los especialistas de seguridad informática		
Capacitación de los usuarios de las TIC en seguridad informática		
Mayor compromiso de la dirección de la entidad con la seguridad informática		
Asignación de un presupuesto mayor para la seguridad informática		

6.1. Mencione otros factores que usted considere:

_____

_____

Anexo 1 (del cuestionario): Escala de valores para determinar el nivel de implementación de los controles de seguridad informática

- Inventario de activos:
    1. No se lleva un control de activos fijos en la institución.
    2. Se tiene un control de medios básicos en general.
    3. Se tiene un control de medios básicos hasta el nivel de componentes (Procesador, memoria RAM, Disco duro)
    4. Se tiene un control de los equipos y el software instalado en los mismos.
    5. El inventario de los dispositivos, sistemas operativos y aplicaciones se realiza de forma automatizada.
- Gestión de usuarios:
    1. No existe un directorio centralizado.
    2. Existe un directorio pero los usuarios utilizan credenciales distintas para acceder a sistemas diferentes.
    3. La autenticación de las aplicaciones es integrada al directorio central y las contraseñas cumplen con parámetros de complejidad.
    4. Se revisa con cierta periodicidad las cuentas sin uso en un determinado período de tiempo y los usuarios que han causado baja de la entidad.
    5. Las cuentas del directorio son verificadas de forma automática contra la base de datos de recursos humanos.
- Gestión de trazas:
    1. No se almacenan trazas de seguridad o solo se conservan un período muy corto de tiempo.
    2. Las trazas de seguridad se almacenan localmente en diferentes servidores.
    3. Las trazas de seguridad se almacenan en una localización centralizada.
    4. Se utiliza un servidor Syslog para la gestión de trazas.
    5. Se utiliza un sistema SIEM para la gestión de trazas
- Monitoreo de los sistemas:
    1. No se tienen implementados sistemas de detección de intrusos (IDS), ni de chequeo de disponibilidad, ni de chequeo de integridad.
    2. Se tienen implementados IDS, o sistemas de chequeo de disponibilidad, o sistemas de chequeo de integridad.
    3. Se tienen implementados al menos dos de los siguientes sistemas: IDS, chequeo de disponibilidad, chequeo de integridad.
    4. Se tienen implementados IDS, sistemas de chequeo de disponibilidad y sistemas de chequeo de integridad.
    5. Se utiliza un sistema SIEM para correlacionar la información de los diferentes sistemas de monitoreo.

- Protección contra programas malignos:
    1. No se utilizan sistemas antivirus.
    2. Se utilizan sistemas antivirus en las computadoras de los usuarios finales.
    3. Se utilizan sistemas antivirus en las computadoras, servidores de correo y servidores proxy.
    4. Se utiliza un mismo software antivirus en toda la organización y este se actualiza desde un repositorio central.
    5. Se utilizan un software antivirus corporativo con un kit de administración centralizado.
- Detección de vulnerabilidades y gestión de parches:
    1. No existe un sistema de gestión de actualizaciones y parches para los sistemas operativos y aplicaciones utilizados en la institución.
    2. Se orienta a los usuarios que deben actualizar sus sistemas operativos y aplicaciones directamente de Internet.
    3. Se tiene un sistema centralizado que gestiona los parches de los sistemas operativos y aplicaciones propietarias. Se mantienen localmente repositorios de Linux actualizados.
    4. Se cuenta con un sistema de gestión de parches y se realizan escaneos de vulnerabilidades con determinada frecuencia a los diferentes sistemas.
    5. Se cuenta con un sistema de gestión de parches y se realizan escaneos de vulnerabilidades automáticos de forma programada a los sistemas críticos de la institución.
- Chequeo de políticas y configuraciones de seguridad:
    1. No existen políticas sobre las configuraciones mínimas de seguridad que deben tener los diferentes sistemas.
    2. Existen políticas sobre las configuraciones mínimas de seguridad de los diferentes sistemas.
    3. Se utilizan imágenes base, con las configuraciones de seguridad definidas, para la instalación de los sistemas operativos en los servidores y computadoras de la institución.
    4. Se utilizan guías de referencia internacionales para las configuraciones de seguridad de los diferentes sistemas operativos y aplicaciones.
    5. Se utilizan sistemas SCAP, con definiciones OVAL y XCCDF, para el chequeo de configuraciones de seguridad
- Respaldo de información:
    1. No se realizan respaldos de información.
    2. Las copias de respaldo se realizan de forma manual con determinada frecuencia.
    3. Los servidores realizan respaldos automáticos de información de forma independiente.
    4. Las copias de respaldo de todos los sistemas se almacenan centralizadamente en un servidor de respaldo.

5. Se utiliza un software único que gestiona de forma centralizada y programada las copias de respaldo de todos los sistemas.

- Seguridad física:
    1. No se tienen sistemas de respaldo eléctrico, detección de incendios, detección de intrusos o sistemas de control de acceso.
    2. Los locales tecnológicos están climatizados y existen sistemas de respaldo eléctrico.
    3. Los locales tecnológicos están climatizados, existen sistemas de respaldo eléctrico, detección de incendios y detección de intrusos.
    4. Se cumple con el ítem 2 y además se utilizan sistemas de control de acceso basados en tarjetas magnéticas, smart cards o dispositivos biométricos.
    5. Todos los sistemas de seguridad física son monitoreados mediante software en una consola central.
- Gestión de incidentes:
    1. No se gestionan los incidentes de seguridad informática.
    2. Existe un lugar donde las personas reportan por diferentes vías (teléfono, correo, e-mail) los incidentes de seguridad informática.
    3. Se llevan estadísticas y se generan reportes, con determinada frecuencia, de los incidentes reportados.
    4. Se utiliza un software de gestión de incidentes on-line, con un sistema de tickets, que permite dar seguimiento a los incidentes de seguridad informática.
    5. El sistema de gestión de incidentes está integrado con otras aplicaciones como IDS y escáner de vulnerabilidades, que abren tickets automáticos ante la detección de ataques y vulnerabilidades.