UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

Facultad Introductoria a las Ciencias Informáticas

Departamento Programación

Modelo para la evaluación de la seguridad del Control de Acceso de los Sistemas de Información de centros productivos de la Universidad de las Ciencias Informáticas

Trabajo final presentado en opción al título de

Máster en Informática Aplicada

Autor: Ing. Maribel Silva Muñoz

Tutor: Dr C Efrén Vázquez Silva

Co-tutora: MSc Ruth Yurina Vega Cutiño

Ciudad de La Habana, Diciembre de 2014.

AGRADECIMIENTOS

A las personas que hicieron posible este trabajo con su apoyo y aliento: Jessie, Efrén, Juniel, Angel, Joelsy, Dovier.

A los especialistas: Yoanis, Yadier, Yasser, Julio.

A mis tutores, particularmente al profesor Efrén por su constancia, dedicación y tiempo.

Especialmente a mi hermana Maleini y a mi madre Maritza por existir, por apoyarme siempre para alcanzar mis metas, por estar de mi lado y preocuparse por mí, por haber sabido enfrentar muchas barreras de la vida y continuar hacia adelante…porque son todo para mí.

DEDICATORIA

A Jessie, que me alentó para que realizara este trabajo, que dedicó parte de su tiempo y esfuerzo en ayudarme, que fue siempre como una hermana para mí.

DECLARACIÓN JURADA DE AUTORÍA

Declaro por este medio que yo Maribel Silva Muñoz, con Carnet de Identidad 85123014573 soy la autora principal del trabajo final “Modelo para la evaluación de la seguridad del Control de Acceso de Sistemas de Información de centros productivos de la Universidad de las Ciencias Informáticas” desarrollada como parte de la Maestría Informática Aplicada y que autorizo a la Universidad de las Ciencias Informáticas a hacer uso de la misma en su beneficio, así como los derechos patrimoniales con carácter exclusivo.

Y para que así conste, firmo la presente declaración jurada de autoría en La Habana a los __ días del mes de _____ del año _____.

_____

Maribel Silva Muñoz

RESUMEN

El Control de Acceso permite restringir y auditar el acceso de los usuarios a los Sistemas de Información de las organizaciones a través de la concepción integrada de los procesos de Identificación y Autenticación, Autorización y Auditoría. Los directivos de las organizaciones tienen la necesidad de evaluar este mecanismo de manera que puedan tomar decisiones sobre la información almacenada.

En la Universidad de las Ciencias Informáticas la evaluación del mecanismo de Control de Acceso de los Sistemas de Información se realiza durante las pruebas de calidad que les realiza el Centro Nacional de Calidad de Software (Calisoft). En la actualidad no existe una solución para la evaluación que sea eficiente y contribuya a la toma de decisiones. Esto provoca dependencia tecnológica de la entidad proveedora del servicio, elevados costos y tiempo de evaluación, que la documentación del proceso sea escasa y que se requieran varios especialistas para llevarla a cabo.

La presente investigación propone un modelo que integra indicadores y criterios para evaluar de manera eficiente los procesos de Identificación y Autenticación, Autorización y Auditoría de los Sistemas de Información de centros productivos de la Universidad de las Ciencias Informáticas. El modelo contribuye a la integración y síntesis de controles para la evaluación, permite la mejora continua, la generalización y la medición descriptiva del proceso. Se presenta una guía para su aplicación y un sistema informático basado en un algoritmo de evaluación.

Palabras clave: Control de Acceso, Seguridad, Sistema de Información.

ABSTRACT

The Access Control allows to restrict and audit user access to the Information Systems of organizations through the integrated conception of Identification and Authentication, Authorization and Audit processes. The managers of organizations have the need to evaluate this mechanism so they can make decisions about the stored information.

In the University of Information Sciences the evaluation of the Access Control mechanism to Information Systems is carried out during quality tests performed at the National Center for Software Quality (Calisoft). At present there is no solution for this evaluation that can be efficient and that contributes to decision-making. This produces technological dependence with the entity providing the service, high costs and time of evaluation, a scarce process documentation and several specialists required to carry it out.

This research proposes a model that integrates indicators and criteria to efficiently assess Identification and Authentication, Authorization and Audit processes of Information Systems from productive centers of the University of Information Sciences. The model contributes to the integration and synthesis of controls for evaluation, enables continuous improvement, the generalization and the descriptive measurement of the process. A guide for its implementation and a computer system based on an evaluation algorithm are presented.

Keywords: Access Control, Security, Information Systems.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS Y TABLAS

INTRODUCCIÓN

Antecedentes y situación problemática.

En la actualidad la información es un activo de interés que contribuye a mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial de las organizaciones (Huerta, 2004). La información es clasificada según su valor, los requisitos legales, la sensibilidad y la criticidad para la organización (Broderick, 2006).

El uso de Tecnologías de Información ofrece medios para contribuir a la seguridad de la información de las organizaciones (ITGI, 2008). Los Sistemas de Información (SI) de las organizaciones alinean los procesos con un software que transforma los datos en información útil para la toma de decisiones (Laudon and Laudon, 2004). Estos sistemas permiten la recopilación de datos, tanto internos como externos; el almacenamiento, procesamiento y la transmisión de información a los directivos (Cañavate, 2003).

La certeza de poder confiar en la seguridad de los SI y en la información producida, posibilita la obtención de un retorno positivo de las inversiones en TI (Huerta, 2004). Garantizar que solo tengan acceso a un SI o a la información que este contiene, aquellos debidamente autorizados requiere de la identificación y autenticación de usuarios; la limitación de acceso, la monitorización de las acciones realizadas y a su sistema de auditoría (Comunicaciones, 2007).

Los directivos tienen la necesidad de evaluar los mecanismos de Control de Acceso de la información, de manera que puedan tomar decisiones sobre la seguridad de la misma. Esto contribuye al éxito de la política de seguridad de las organizaciones donde son implantados los SI (ITGI, 2008).

La UCI presenta una infraestructura de producción de software que se materializa en centros productivos, como son el Centro de Gobierno Electrónico (CEGEL) y el Centro de Informatización de Entidades (CEIGE) de la Facultad 3. En ellos se desarrollan los SI de diferentes organizaciones que informatizan procesos estratégicos para el gobierno cubano. La información que gestionan estos SI requiere de seguridad, protección contra pérdidas y accesos no autorizados.

Durante el año 2013 y principios del año 2014 en la universidad fueron identificados un conjunto de ataques informáticos como son: robo de contraseñas, ingeniería social, correo basura o mensaje basura y escaneo de puertos desde el exterior que provocaron daños al personal que labora en la organización y a los SI desarrollados en los centros productivos.

Introducción

La evaluación del mecanismo de Control de Acceso de los SI de centros productivos de la UCI se realiza durante las pruebas de calidad que les realiza Calisoft. En la actualidad no existe una solución propia de los centros para la evaluación que sea eficiente y contribuya a la toma de decisiones. Esto provoca dependencia tecnológica de la entidad proveedora del servicio, elevados costos y tiempo de evaluación, que la documentación del proceso sea escasa y que se requieran varios especialistas para llevarla a cabo.

Según una encuesta realizada (preguntas 1 y 2, Anexo 1) se pudo constatar que durante el proceso de evaluación se utilizan los controles de seguridad que proponen la ISO/IEC 9126, la ISO/IEC 25000, la Guía de Pruebas v3.0 de OWASP (2008) y la Resolución 127 del MIC. Este mecanismo se encuentra alineado con La Política de Seguridad Informática de la UCI y tiene el objetivo de conocer cuán seguros son los procesos de Identificación y Autenticación, Autorización y Auditoría de los SI.

En el proceso de evaluación de la seguridad del Control de Acceso de los SI interviene un conjunto de especialistas de Calisoft. La evaluación se basa en chequear una lista que incluye los requisitos de seguridad del SI que se evalúa. El software es objeto de la revisión de cada uno de los elementos de la lista así como de pruebas manuales o automatizadas que reflejan el cumplimiento o no de un total de 15 indicadores para la evaluación del sistema. Los 15 indicadores fueron definidos en la propia entidad evaluadora y reflejan requisitos de seguridad que debe cumplir el sistema en su totalidad. Los indicadores son generales, no se encuentran clasificados por los procesos del Control de Acceso.

La evaluación de la seguridad del Control de Acceso de los SI de centros de la UCI presenta algunos problemas que limitan la eficiencia y su potencial de éxito:

- Adoptar uno u otro modelo de manera independiente o incluso la integración de algunos modelos de evaluación que existen en la actualidad, no contribuye a la obtención de un mecanismo integral y balanceado para la medición del desempeño de los procesos de Identificación y Autenticación, Autorización y Auditoría de un SI que apoye la mejora continua del mecanismo de Control de Acceso de los SI de centros de la UCI.
- No contar con un marco de gestión basado en un enfoque común de mejores prácticas y gestión de servicios en entornos organizacionales influye negativamente en la manera en que los directivos de las organizaciones donde sean desplegados estos SI debieran entender y definir los riesgos.

- No contar con un marco de gestión basado en un enfoque común de mejores prácticas y gestión de servicios en entornos organizacionales provoca irregularidades en el momento de definir las áreas objetivo y las áreas de proceso en las que deben incidir la seguridad del Control de Acceso de los SI, en el análisis de la capacidad de identificar brechas para mejorar la gestión de estas áreas, así como en el monitoreo de los resultados de las mejoras que pudieran ser implementadas en las organizaciones.
- De manera general se prescinde de la gestión integrada de objetivos de control, mejores prácticas en dominios y procesos de TI para la evaluación de los mecanismos de Control de Acceso de los SI de centros productivos de la UCI. Esto no posibilita la obtención de un modelo de madurez acorde a marcos de control interno de implantación a nivel internacional (ITGI, 2008).

Considerando la problemática existente, el **problema científico** se formula de la siguiente manera:

¿Cómo evaluar de manera eficiente la seguridad del Control de Acceso de los Sistemas de Información de centros productivos de la Universidad de las Ciencias Informáticas?

Para darle una solución al problema se plantea como **objetivo general**: Desarrollar un modelo que integre indicadores y criterios para evaluar de manera eficiente los procesos de Identificación y Autenticación, Autorización y Auditoría de los Sistemas de Información de centros productivos de la Universidad de las Ciencias Informáticas.

El **objeto de estudio** lo constituye la seguridad de los Sistemas de Información y el **campo de acción** en el que se enmarca la investigación es precisamente la evaluación de la seguridad del Control de Acceso de Sistemas de Información de centros productivos de la Universidad de las Ciencias Informáticas.

La investigación a realizar será de tipo **correlacional** ya que es posible conocer la relación que existe entre las variables de investigación. Es necesario que las organizaciones que adoptan el modelo para la evaluación posean una evaluación más eficiente de los Sistemas de Información que aquellas que no lo utilizan. Se persigue la evaluación de criterios y la utilización de algoritmos de evaluación con el fin de obtener una evaluación cualitativa de la seguridad del Control de Acceso de Sistemas de Información de centros productivos de la UCI.

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

- Elaborar el marco teórico conceptual de la investigación, relacionado con las tecnologías más utilizadas para la evaluación de la seguridad del Control de Acceso de los SI.
- Definir los indicadores y criterios para evaluar la seguridad del Control de Acceso de los SI de centros productivos de la UCI.
- Integrar indicadores y criterios de evaluación en el modelo.
- Desarrollar un Sistema Informático para la Evaluación de la seguridad del Control de Acceso de los SI de centros productivos de la UCI que facilite la aplicación del modelo propuesto.
- Validar el modelo mediante su aplicación en los SI de centros productivos de la UCI y la consulta a un grupo de expertos.

Una vez analizada la literatura para conformar el marco teórico se formula la siguiente **hipótesis de investigación**: Si se desarrolla un modelo que integre indicadores y criterios de evaluación aumentará la eficiencia de la evaluación de la seguridad del Control de Acceso de Sistemas de Información de centros productivos de la Universidad de las Ciencias Informáticas.

Para dar cumplimiento al objetivo propuesto se han combinado diferentes métodos así como procedimientos teóricos y empíricos, en la búsqueda y procesamiento de la información.

Dentro de los **métodos teóricos** empleados destacan el hipotético – deductivo para definir la hipótesis de la investigación y proponer nuevas líneas de trabajo relacionadas con la evaluación de los procesos de Identificación y Autenticación, Autorización y Auditoría para determinar la seguridad del Control de Acceso de los Sistemas de Información de centros productivos de la Universidad de las Ciencias Informáticas. El método análisis – síntesis fue utilizado para descomponer el problema de investigación en el estudio por separado de los procesos de Identificación y Autenticación, Autorización y Auditoría de los SI, para luego integrarlos de forma coherente en la solución general del problema planteado, y el método sistémico para lograr que todos los elementos de la estructura y concepción de la solución funcionen como un todo, lo que representa la expresión de su comportamiento. El método histórico - lógico fue empleado en el estudio del comportamiento y evolución de las posiciones respecto a indicadores y criterios de evaluación de los procesos de Identificación y Autenticación, Autorización y Auditoría para evaluar la seguridad del Control de Acceso de los SI de centros productivos de la UCI.

Los **métodos empíricos** empleados fueron el análisis de documentos en la consulta de la literatura especializada, con el objetivo de extraer la información necesaria para definir los escenarios que deben cubrir los modelos para la evaluación de la seguridad del Control de

Acceso de los SI de centros productivos de la UCI. El método experimental fue empleado con el objetivo de explicar cómo influye el modelo propuesto a los SI de centros de la UCI que forman parte de la muestra de aquellos que no lo hacen.

Muestreo

Población: La población seleccionada para la investigación esta constituida por los SI del centro productivo CEGEL de la Facultad 3.

Muestra: La muestra seleccionada para la investigación fue el conjunto de cinco de los SI pertenecientes al centro productivo CEGEL de la Facultad 3 a cuya información se tiene acceso. La muestra representa el 71.42% de la población, seleccionada mediante muestreo no probabilístico.

Diseño de la investigación

La estrategia de la investigación estuvo basada en el diseño de un pre-experimento con pre y post prueba con un solo grupo. Esto con el objetivo de analizar si la variable independiente (Indicadores y criterios de evaluación integrados en un modelo) influye en la variable dependiente (Eficiencia de la evaluación de la seguridad del Control de Acceso de Sistemas de Información de centros productivos de la Universidad de las Ciencias Informáticas) y la razón a la que se debe.

Instrumentos para la medición de la variable dependiente

La recolección de los datos implicaría el uso de un Cuestionario. Este es aplicado directamente a los participantes, quienes lo contestan de manera individual. En la investigación las muestras son los resultados de comparar los indicadores de usabilidad establecidos para la variable dependiente en los SI del centro productivo CEGEL de la Facultad 3 antes y después de la aplicación del modelo. Para determinar el grado de coincidencia de los expertos con relación a los indicadores fue aplicado el test de concordancia de Kendall. Además, se precisa del uso del tabulador Excel y la herramienta STATGRAPHICS para el análisis estadístico de los datos.

Dominio e indicadores de las variables a medir

Las variables que conforman la hipótesis de investigación son las siguientes:

Variables independientes: Indicadores y criterios de evaluación integrados en un modelo.

Variable dependiente: Eficiencia de la evaluación de la seguridad del Control de Acceso de Sistemas de Información de centros productivos de la Universidad de las Ciencias Informáticas.

La Tabla 1 y la Tabla 2 muestran la operacionalización de las variables.

Tabla 1. Operacionalización de la variable independiente. Fuente: Elaboración propia.

Variable independiente	**Dimensión**	**Indicadores**	**Unidad de Medida**
Indicadores y criterios de evaluación integrados en un modelo	Criterios de evaluación definidos	Criticidad	No crítico [1] Poco crítico [2] Crítico [3] Muy crítico [4]
		Efectividad para la evaluación del Control de Acceso	Sí/No
	Capacidad de generalización a una gran variedad de los SI	Utilización de indicadores y criterios de evaluación	Sí/No
		Tolerancia a soluciones propias	Sí/No

Tabla 2. Operacionalización de la variable dependiente.

Variable dependiente	**Dimensión**	**Indicadores**	**Unidad de Medida**
Eficiencia de la evaluación de la seguridad del Control de Acceso de los SI de centros productivos de la UCI	Usabilidad	Cantidad de especialistas que son necesarios para la evaluación de la seguridad del Control de Acceso	Más de 6 especialistas 2-6 especialistas 1 especialista
		Tiempo para generar la evaluación de la seguridad del Control de Acceso	Más de 6 horas 1-6 horas 0-60 minutos

El **resultado esperado** de la investigación lo constituye el Modelo, basado en indicadores y criterios de evaluación de la seguridad del Control de Acceso de Sistemas de Información de centros productivos de la Universidad de las Ciencias Informáticas.

El **aporte teórico** de la investigación lo constituye el modelo para la evaluación de la seguridad del Control de Acceso de Sistemas de Información de centros productivos de la Universidad de las Ciencias Informáticas basado en indicadores y criterios de evaluación.

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

- Conjunto de indicadores para la evaluación de los procesos de Identificación y Autenticación, Autorización y Auditoría de los SI de centros productivos de la UCI.
- Guía para la aplicación del modelo propuesto.
- Sistema para la Evaluación del Control de Acceso (SIECA) basado en un algoritmo de evaluación.
- Especificaciones y configuraciones necesarias para la implementación del SIECA.

Estructura del documento

El documento se encuentra estructurado en tres capítulos que se describen brevemente a continuación:

- El primer capítulo, “Fundamentación Teórica”, tiene como objetivo analizar los diferentes aspectos teóricos relacionados con la evaluación de la seguridad del Control de Acceso de los SI de centros productivos de la UCI. Además se analizan y adoptan los principales conceptos que facilitan el estudio y compresión de la temática. El capítulo concluye con la especificación de los escenarios no resueltos relacionados con la evaluación de los procesos de Identificación y Autenticación, Autorización y Auditoría para determinar la seguridad del Control de Acceso.
- En el segundo capítulo, “Modelo para la evaluación de la seguridad del Control de Acceso de los SI de centros productivos de la UCI” se describen los componentes que forman parte de la propuesta, así como la guía de aplicación del modelo.
- En el tercer capítulo, “Validación del modelo” se presentan los resultados obtenidos como parte de la aplicación del modelo en los SI de centros productivos de la UCI. El capítulo concluye con la valoración del aporte e impacto de los resultados a partir de la aplicación del modelo en entornos reales.

- Finalmente se presentan las conclusiones y recomendaciones de la investigación.

CAPÍTULO 1: FUNDAMENTACIÓN TEÓRICA

1.1 Introducción.

En el presente capítulo se expone el marco teórico-referencial del trabajo. En el mismo se abordan los conceptos asociados al dominio del problema. Se presentan los indicadores y criterios de evaluación asociados a los procesos de Identificación y Autenticación, Autorización y Auditoría para evaluar la seguridad del Control de Acceso de los SI de centros productivos de la UCI. Se realiza un análisis crítico de cada uno de estos elementos.

1.2 Características generales de la evaluación de la seguridad del Control de Acceso de los Sistemas de Información.

Al realizar una investigación que aborde los conceptos de seguridad del Control de Acceso de los SI son inevitables las confusiones sobre la relación que se establece entre cada uno de ellos. Esto provoca interpretaciones inadecuadas sobre el área en la que se incide y los resultados que se pretenden obtener.

Para facilitar el estudio de la bibliografía son necesarias, en consideración de la autora de la presente investigación, definiciones relacionadas con el tema de la investigación. La seguridad, el Control de Acceso y la evaluación de la seguridad del Control de Acceso de los SI presentan características útiles que contribuyen a la comprensión y al desarrollo del trabajo.

1.3 Sistema de Información de las organizaciones.

Los SI son un conjunto de herramientas que combinan las TI (hardware y software) con procedimientos que permiten suministrar información a los directivos de una organización. Contribuyen a resolver problemas que se presentan con regularidad y ofrecen, de forma periódica, reportes para el soporte de decisiones basados en las actividades que tienen lugar en las organizaciones (Senn, 2001). Son usados en entornos orientados a la administración de procesos en las organizaciones y se desarrollan considerando el modelo Desarrollo Rápido de Aplicaciones (DRA por sus siglas en Inglés) que comprende las fases de: Modelado de Gestión, Modelado de Datos y Modelado de Procesos (Pressman, 2005).

1.4 Dominio de Seguridad.

Un Dominio de Seguridad es un grupo acotado de usuarios y bienes protegidos, a los que se aplica una sola política de Control de Acceso ejecutada por un único administrador de seguridad

(ITU-T, 1996). Está formado por una autoridad y una Política de Seguridad. Define un conjunto de actividades sujetas a la política de seguridad que es administrada por la autoridad del dominio de seguridad establecido. La Política de Seguridad limita las actividades de los elementos sujetos a la misma, ya sea exigiendo ciertas acciones o mediante la prohibición de ciertas actividades.

1.5 Control de Acceso.

El Control de Acceso es el proceso de restringir y auditar el acceso de los usuarios (persona, rol, sistema, entre otros) a los recursos (información, sistema, objetos, ficheros, entre otros) gestionados por un SI, a través de la concepción integrada de los procesos de Identificación y Autenticación, Autorización y Auditoría (Comunicaciones, 2007).

El Control de Acceso posee cuatro procesos fundamentales (Rivest, 1992):

- La **Identificación** es la acción por parte de un usuario de presentar su identidad a un sistema; generalmente se usa un identificador de usuario. Establece que el usuario es responsable de las acciones que realice el sistema.
- La **Autenticación** es la verificación de que el usuario que intenta identificarse es válido; usualmente se implementa con una contraseña en el momento de iniciar una sesión.
- La **Autorización** es el proceso que permite determinar si un sujeto identificado y autenticado tiene acceso al recurso solicitado. Posibilita la ejecución de operaciones específicas, dependiendo de sus derechos de acceso configurados con antelación. La política de autorización debe ser gestionada por el administrador o agente de seguridad responsable de apoyar y llevar a cabo la política de seguridad en la organización.
- La **Auditoría** es el proceso de registro y análisis de todas las acciones ejecutadas por los sujetos sobre los recursos a través de un SI. La auditoría es un aspecto crítico para identificar violaciones, debilidades, amenazas, predecir comportamientos y oportunidades de mejoras que apoya en la toma de decisiones en las organizaciones.

1.6 Evaluación de la seguridad del Control de Acceso.

La evaluación de la seguridad del Control de Acceso considera el uso de las normas y estándares. A continuación se muestran los elementos esenciales de estos controles de seguridad de aplicación internacional.

- La **ISO/IEC 27002** y los documentos relacionados han contribuido a la normalización de las funciones de seguridad; establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización (Standard and techniques, 2005).
- La **ISO/IEC 15408 Criterio Común** (Astels et al.) constituye una guía útil para el desarrollo de productos y sistemas de TI con funciones de seguridad, así como para la adquisición de productos comerciales y sistemas con funciones de seguridad (SANS, 2013).
- Los **Objetivos de Control para la Información y la Tecnología relacionada** (COBIT por sus siglas en Inglés) propone un marco de trabajo de dominios y procesos que incluye un conjunto de buenas prácticas más enfocadas en el control que en la ejecución (Criteria, 2012).
- La **Biblioteca de Infraestructura de TI** (ITIL por sus siglas en Inglés) surge con el propósito de contribuir al proceso de Gestión de Seguridad de la Información (ISM por sus siglas en Inglés) así como garantizar que la seguridad de información se gestione con eficacia en todos los servicios y actividades de gestión de servicios (Garzaro, 2007).
- La **Publicación Especial 800-53 del NIST** propone un conjunto de controles de seguridad con el fin de que sean implementados en una organización para brindar protección a la información y a los SI de tipo federal (Standards., 2006).
- El **Proyecto de los 10 Mejores Elementos** que forman parte del Proyecto de Seguridad para Aplicaciones Web de Código Abierto (OWASP por sus siglas en Inglés) contribuye a aumentar la seguridad de aplicaciones mediante la identificación de algunos de los riesgos más críticos que enfrentan las organizaciones (OWASP, 2010).
- Las **guías de OWASP** contribuyen a la construcción y mantenimiento de aplicaciones seguras mediante la definición de un conjunto de guías gratuitas y abiertas, que están disponibles de manera detallada. Permiten mantener el enfoque de un problema general sin proporcionar suficiente información para encontrar, diagnosticar y resolver los problemas de seguridad (Foundation, 2008).
- La **Norma de Buenas Prácticas para la Seguridad de la Información** se enfoca en la seguridad de la información desde una perspectiva empresarial, proporcionando una base práctica para la evaluación de las medidas de seguridad de información de una organización. Contiene una amplia gama de características que cubre todo el espectro de

los arreglos que deben hacerse para mantener los riesgos dentro de los límites aceptables (Solms, 1998).

- La **Resolución 127/2007** proporciona vigencia al "Reglamento de Seguridad para las Tecnologías de la Información" según el Ministerio de la Informática y las Comunicaciones (MIC) de Cuba en el acuerdo No. 6058 del Comité Ejecutivo del Consejo de Ministros. Constituye un Reglamento de seguridad para las Tecnologías de la Información que tiene como objetivo establecer y regular el sistema para la Seguridad y Protección de la Información Oficial (Comunicaciones, 2007).
- El **Decreto Ley 281** introduce elementos a considerar para la gestión de la información, y la integración de los correspondientes sistemas informativos del Gobierno. Constituye un conjunto de disposiciones legales que establecen los principios para la integración del Sistema de Información del Gobierno determinado por su organización y funcionamiento (Estado, 2011).

1.6.1 Estándares de Identificación y Autenticación.

El proceso de Autenticación se lleva a cabo con el propósito de asegurar la identidad del usuario. La elección de una determinada tecnología para la gestión de la autenticación condiciona el resto de los procesos de Control de Acceso. A continuación se muestran los elementos esenciales de las soluciones de Identificación y Autenticación que constituyen estándares internacionales.

- La **Infraestructura de Clave Pública** (PKI por sus siglas en Inglés) define estándares que se usan en el intercambio de datos para garantizar la integridad, autenticidad, confidencialidad y en algunos casos el no repudio de la información. Provee algoritmos o estándares de seguridad (Choudhury et al., 2002; Komar, 2010).
- El estándar **X.509** define un formato de certificados general y flexible. Proporciona un conjunto de soluciones de aplicación en entornos de acceso a recursos protegidos que requieran intercambios de información por canales seguros y en repositorios de información. (Cánovas and Cánovas, 2002; IETF, 2002; ITU-T, 2005).
- La **Infraestructura de Clave Pública Simple** (SPKI por sus siglas en Inglés) provee un detallado formato de certificados y las reglas de procesamiento requeridas para su implementación. Aplica el cifrado de clave pública (Ellison et al., 1999).

- El estándar **Abierto de Privacidad Bastante Buena** (OpenPGP por sus siglas en Inglés) define los protocolos de empaquetamiento requeridos para construir y procesar mensajes de correo electrónico que usan el estándar PGP mediante el cifrado de clave pública a una red de confianza sin existencia de un directorio global (Garfinkel, 1995) (Zimmerman, 1995).
- El estándar **S/MIME** incluye la habilidad de etiquetar los mensajes de correo de acuerdo a su nivel de seguridad, así como de solicitar y obtener un recibo firmado como prueba de la recepción de un mensaje enviado previamente (COMER, 1995).
- El estándar **IPSec.** define un conjunto de componentes esenciales de la arquitectura de seguridad para proveer autenticidad, integridad y confidencialidad. Posibilita la autenticación basada en certificados X.509 (Davis, 2001).
- La **especificación Capa de Transporte Seguro** (TLS por sus siglas en Inglés) crea un canal seguro entre la fuente y el destino en la capa de transporte, proporcionando autenticación basada en certificados, integridad de la información y confidencialidad de los datos (Dierks and Allen, 1999).
- El **Protocolo de Acceso Simple a Objetos** (SOAP por sus siglas en Inglés) describe mensajes enviados de un programa a otro. Es el protocolo que los servicios web utilizan para la comunicación (Brown et al., 2001; Hurwitz et al., 2007).
- La **Especificación de Gestión de Claves** (XKMS por sus siglas en Inglés) define una sintaxis para el cifrado y la firma digital (Werner, 2001). Provee distintas modalidades de intercambio de mensajes entre los servicios XKMS y sus clientes (Wangham et al., 2005).
- El **estándar Kerberos** es un estándar cuyo funcionamiento se basa en un servicio de autenticación central que es la autoridad de autenticación. A través de los llamados *ticket* los servidores de recursos pueden probar que el usuario ha sido autenticado mediante un servicio de autenticación confiable (Estéban, 2004; R. Alfieri, 2003).
- El **servicio de Pasaporte** es un sistema de autenticación basado en la Web. Se compone de tres entidades: servidor de pasaporte, los comerciantes en línea, y los clientes (Kormann and Rubin, 2000; Thurrott, 2001).
- La **Prueba Pública y Automática de Turing** (CAPTCHA por sus siglas en Inglés) constituye un método basado en los Puntos Débiles del Reconocimiento Óptico de Caracteres (OCR por sus siglas en Inglés) (G. and J., 2003; IEEE, 2004).

1.6.2 Estándares de Autorización.

El proceso de Autorización incluye el conjunto de usuarios con diferentes roles que requieren obtener acceso a la información bajo determinadas circunstancias. A continuación se muestran los elementos esenciales de las soluciones de Autorización que constituyen estándares internacionales.

- La **Infraestructura Simple de Seguridad Distribuida** (SDSI por sus siglas en Inglés) ofrece una arquitectura con requerimientos tanto de autenticación como de autorización. SPKI permite gestionar la delegación en el servicio de autorización. La propuesta SPKI/SDSI es un lenguaje de gestión de confianza en sistemas descentralizados (Rivest and Lampson, 1996).
- El **Lenguaje de Marcado de Aserción de Seguridad** (SAML por sus siglas en Inglés) está basado en XML para intercambiar información de autenticación y autorización entre dominios de seguridad, proporcionando identidad y servicios a través de mecanismos de Inicio de Sesión Únicos (SSO, por sus siglas en Inglés) (OASIS, 2005; R. Alfieri, 2003).
- El **proyecto Shibboleth** proporciona acceso a la información empleando una infraestructura de autorización basada en el lenguaje SAML. Permite la transmisión segura de los atributos de usuario del dominio de origen al dominio del proveedor del recurso (Cantor, 2005).
- El **Punto de Acceso a los Proveedores de Información** (PAPI por sus siglas en Inglés) posibilita la gestión del Control de Acceso entre proveedores de recursos o información y usuarios finales de la Web (Rojo. and López, 2001).
- El **proyecto Alianza Libertad** como solución abierta y federada de autenticación unificada se encarga de la gestión de identidades basado en SAML para servicios web mediante la definición de un marco para el establecimiento de federaciones de identidades en Internet (Cantor and Kemp, 2003).
- La **Autenticación Remota para Marcado de Servicio de Usuario** (RADIUS por sus siglas en Inglés) define un protocolo para centralizar la autenticación y autorización, así como el Control de Acceso para el protocolo de Interfaz de Línea Serie (SLIP por sus siglas en Inglés) y el protocolo Punto a Punto (PPP por sus siglas en Inglés) (Rigney et al., 2000).
- El protocolo **TACACS+** suministra información de contabilidad detallada, una administración flexible y configurable mediante comandos desde el propio servidor de RADIUS. Permite

separar las opciones de autenticación y autorización, así como el cifrado de mensajes completos (Estéban, 2004; Finseth, 1993).

- El protocolo **DIAMETER** especifica toda la información intercambiada entre las partes mediante atributos de pares de valores. Está basado en un modelo directo de servidor que soporta entrega en tiempo real de información de contabilidad (Calhoun et al., 2005; P. Calhoun, 2003).
- El protocolo **Privacidad para Redes Inalámbricas** (WEP por sus siglas en Inglés) es un protocolo de encriptación basado en el algoritmo de encriptación RC4 que proporciona un nivel de seguridad aceptable solo para usuarios domésticos y aplicaciones no críticas (Lehembre, 2006).
- El estándar de **Punto de Acceso Protegido dos** (WPA2 por sus siglas en Inglés) se corresponde con el estándar 802.11i. Está basado en el Algoritmo de Encriptación Estándar (AES por sus siglas en Inglés) para el cifrado de bloque y autenticación (Moffat Mathews, 2007).

1.6.3 Estándares de Auditoría.

El proceso de Auditoría se encarga de la revisión correspondiente por parte de la administración de las actividades realizadas por usuarios de los sistemas. Proporciona una mejora continua del sistema de seguridad informática. A continuación se muestran los elementos esenciales de las soluciones de Auditoría que constituyen estándares internacionales.

- El **Comité de Organizaciones Patrocinadoras sobre el control interno** (COSO por sus siglas en Inglés) conforma un marco de control interno que incluye aspectos para la segregación de funciones, el autocontrol de arriba hacia abajo, el costo menor que beneficio, la eficacia, la confiabilidad y la documentación (Moeller, 2007).
- La **Ingeniería Dirigida por Modelos** (MDE por sus siglas en Inglés) le otorga merecida importancia a la gestión de la trazabilidad. Permite definir el uso de la información de trazabilidad, las operaciones de gestión sobre la información de trazabilidad, y las características a tener en cuenta para soportar trazabilidad según el modelo (Schmidt, 2006).
- La **Interfaz de Sistemas Operativos Portables** en la versión POSIX.1q de 2000 proporciona una interfaz que permite recabar información sobre las acciones realizadas por

los programas de usuario y el propio sistema operativo, tales como cambios de contexto, llamadas al sistema u otros eventos definidos por el usuario (POSIX, 2000).

1.7 Soluciones para la evaluación del Control de Acceso.

La evaluación requiere del análisis de métricas y algoritmos para medir el desempeño del SI en cuanto a la seguridad de su mecanismo de Control de Acceso. A continuación se muestran las soluciones de aplicación internacional que contribuyen a la evaluación de la seguridad.

- Las **métricas de seguridad** que define el Centro de Seguridad de Internet (CIS por sus siglas en Inglés) están centradas en el esfuerzo involucrado en los procesos de seguridad, tales como el esfuerzo para reparar una vulnerabilidad de manera que se contribuya a la eficiencia y su impacto beneficie la organización (CIUREA, 2009). A pesar de su gran aceptación a nivel internacional los indicadores propuestos abarcan sólo algunos controles de seguridad informática tales como la gestión de incidentes, de vulnerabilidades y parches.
- El **Sistema de Puntuación de Vulnerabilidades Comunes** (CVSS por sus siglas en Inglés) es un estándar abierto que se aplica universalmente a cualquier vulnerabilidad informática y permite obtener una evaluación del riesgo asociado (NIST, 2007). A pesar de que proporciona a los usuarios una representación clara e intuitiva de una vulnerabilidad y una taxonomía común para la descripción (Mell et al., 2007) sus métricas base consideran mayormente la Autenticación como proceso del Control de Acceso, no siendo así los procesos de Autorización y Auditoría.
- La **Técnica Ajustada de Puntuación de Riesgos de Negocio** (BAR por sus siglas en Inglés) clasifica defectos de seguridad de acuerdo a su tipo de vulnerabilidad, el grado de riesgo y posible impacto (Barabanov et al., 2011; Jaquith, 2002). A pesar de que permite clasificar defectos de seguridad por su respectivo tipo de seguridad, el método mide impacto y riesgo en el negocio. No considera indicadores o criterios asociados a los procesos de Identificación y Autenticación, Autorización y Auditoría.

1.7.1 Lógica de Puntuación de Preferencias.

El algoritmo **Lógica de Puntuación de Preferencias** (LSP por sus siglas en Inglés) fue propuesto en 1996 por Dujmovic (Dujmovi'c, 1996). Se utiliza para evaluar y seleccionar sistemas complejos de hardware y software. El proceso de evaluación LSP permite determinar claramente cuáles son los requerimientos que deben cumplir los sistemas, los principales atributos a evaluar y los rangos de valores que éstos pueden tomar. Estos atributos son

llamados Variables de Performance, cada una de ellas es transformada en una Preferencia Elemental al aplicarle el correspondiente Criterio Elemental.

En el algoritmo LSP una Variable de Performance mediante la aplicación de un Criterio Elemental es transformada en valores que pertenecen al intervalo [0, 1] (Preferencia Elemental). Estos valores representan el grado de satisfacción de los requerimientos, 0 cuando no satisface el requerimiento, 1 cuando los satisface plenamente.

Las Preferencias Elementales constituyen los parámetros de la Función de Criterio del LSP. Esta función retorna un único indicador global, que es el grado de satisfacción de los requerimientos del sistema en general.

1.8 Escenarios no cubiertos por los modelos existentes para la evaluación de la seguridad del Control de Acceso de los SI de centros productivos de la UCI.

Las incapacidades para gestionar con eficiencia la evaluación de la seguridad de los procesos de Identificación y Autenticación, Autorización y Auditoría en los escenarios descritos anteriormente, constituyen las causas fundamentales del fracaso de muchas organizaciones. La autora de la presente investigación consideró que los escenarios fundamentales no cubiertos por los modelos de evaluación de la seguridad del Control de Acceso son los siguientes:

1. No existe un lenguaje común para comunicar las metas, objetivos y resultados de evaluación a los profesionales de auditoría, informática y otras disciplinas.
2. No existe un método para medir si el mecanismo de evaluación satisface los requisitos de la UCI como organización.
3. Es insuficiente el desarrollo de políticas claras y mejores prácticas para la administración de los SI hacia un enfoque de mejores prácticas para la evaluación.
4. No existen objetivos de control agrupados por procesos o dominios de evaluación.
5. No se lleva a cabo la gestión dinámica de normas, estándares, guías, recomendaciones, resoluciones y decretos de manera que puedan ser implementados y se mantengan actualizados.
6. No se asegura que las actividades críticas puedan ser monitoreadas y medidas, de modo que los problemas puedan ser identificados y que las medidas correctivas puedan ser adoptadas en los diferentes SI.

7. No se miden los resultados estableciendo un mecanismo de puntuación para medir el desempeño actual y monitorear los resultados de las evaluaciones de los SI de centros productivos de la UCI.
8. No existen infraestructuras para la evaluación de manera que se facilite, apoye la creación y el intercambio de información entre los SI.

Las carencias identificadas en los modelos de evaluación, incrementados por la falta de integración entre sus componentes, constituyen los antecedentes fundamentales de la presente investigación.

En el capítulo siguiente se describen los componentes que se integran en un modelo para la evaluación de la seguridad del Control de Acceso de los SI de centros productivos de la UCI. La definición del modelo cubre los escenarios descritos anteriormente.

1.9 Conclusiones parciales.

Sobre la fundamentación teórica se concluye lo siguiente:

- La evaluación de la seguridad del Control de Acceso contribuye a orientar y determinar las prioridades, además de las acciones de gestión adecuadas para la administración de los riesgos concernientes a la seguridad de la información.
- La gestión de la seguridad de los procesos de Identificación y Autenticación, Autorización y Auditoría presenta soluciones que incluyen lenguajes, certificados, protocolos, estándares, proyectos, modelos, algoritmos, etcétera para la evaluación de la seguridad del Control de Acceso de los SI de centros productivos de la UCI.
- Los escenarios no cubiertos por los modelos de evaluación existentes permitió constatar que las normas, estándares y protocolos implementados no contribuyen a la gestión eficiente del proceso de evaluación.

CAPÍTULO 2: MODELO PARA LA EVALUACIÓN DE LA SEGURIDAD DEL CONTROL DE ACCESO DE LOS SI DE CENTROS PRODUCTIVOS DE LA UCI.

2.1 Introducción.

En el presente capítulo se describen los componentes que se integran en un modelo para la evaluación de los SI de centros productivos de la UCI. Se presentan los principios y bases del modelo, así como la guía para facilitar la adopción y aplicación del mismo.

2.3 Modelo para la Evaluación de la Seguridad del Control de Acceso.

Los modelos de evaluación no cubren los ocho escenarios relacionados con la evaluación de la seguridad del Control de Acceso de los SI de centros productivos de la UCI, tal y como se describe en el capítulo anterior. Esto ocasiona que el proceso de evaluación no sea eficiente según normas, estándares, guías, recomendaciones, resoluciones y decretos, provocando que no se consideren métricas y algoritmos de evaluación de aplicación internacional.

El Modelo para la Evaluación de la Seguridad del Control de Acceso de los SI de centros productivos de la UCI (MECA) provee una solución a los escenarios no cubiertos por los modelos existentes en la actualidad.

La interrelación de los componentes del modelo permite evaluar eficientemente los procesos de Identificación y Autenticación, Autorización y Auditoría. La Figura 1 muestra los componentes del modelo, así como su integración para llevar a cabo la evaluación.

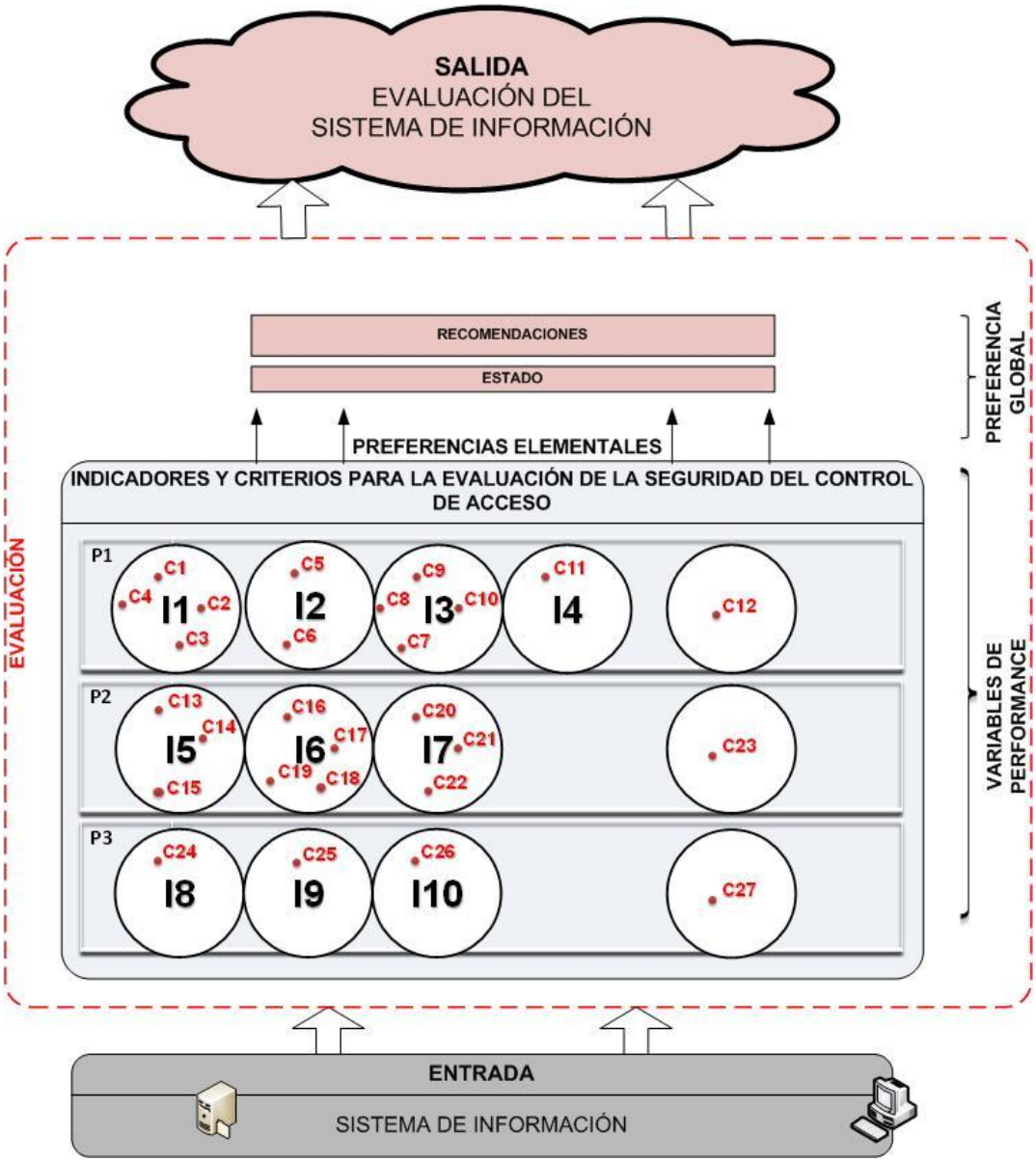

Figura 1. Modelo para la Evaluación de la seguridad del Control de Acceso (Fuente: Elaboración propia).

El MECA posee las siguientes características generales:

- Se definen **10 indicadores** para la evaluación. Estos indicadores sintetizan los controles de las principales directrices en el área de la evaluación de la seguridad del Control de Acceso de aplicación internacional.
- Se definen **27 criterios** medibles que describen las diferentes soluciones de Control de Acceso y contribuyen a la evaluación de los procesos de Identificación y Autenticación, Autorización y Auditoría.

- El proceso de evaluación se realiza mediante la adaptación del **algoritmo LSP** a las condiciones del modelo permitiendo conocer el estado (Bajo, Medio o Alto) de cada uno de los procesos del Control de Acceso y conocer sobre los criterios que incidieron en los resultados obtenidos.

La entrada del modelo es la información proveniente de los SI de centros productivos de la UCI que utilizan un mecanismo de Control de Acceso de la información.

Las salidas del modelo se reflejan en el estado de los procesos de Identificación y Autenticación, Autorización y Auditoría de los SI y en las recomendaciones derivadas del análisis de los resultados de la evaluación.

2.4 Principios del modelo.

El modelo se sustenta en un conjunto de principios para garantizar que su aplicación sea exitosa. Estos principios son los siguientes:

- **Evaluar un SI** implica que el sistema a evaluar posee las características de todo SI desarrollado en centros productivos de la UCI.
- **Evitar la selección de responsables de la evaluación que no sean especialistas de seguridad** se basa en la selección del responsable de la evaluación partiendo de su conocimiento sobre el mecanismo de Control de Acceso del SI (especialista de seguridad que participó en el desarrollo de la solución de Control de Acceso o posee conocimiento sobre su implementación en el SI).
- **Evaluar la totalidad de los criterios** requiere que el responsable de la evaluación del SI determine el grado de cumplimiento de la totalidad de los criterios para la evaluación.
- **Evaluar la totalidad de los indicadores** requiere que el responsable de la evaluación del SI determine el grado de cumplimiento de la totalidad de los indicadores para la evaluación.
- **Análisis cualitativo y por procesos** mediante la determinación de un estado Bajo, Medio o Alto para cada uno de los procesos y las recomendaciones basadas en la identificación de los indicadores y criterios que incidieron en el estado obtenido.
- **Evitar análisis superficiales de la evaluación** requiere de un análisis que refleje la valoración general del proceso de evaluación: indicadores y criterios que afectan la evaluación de manera que se contribuya a la mejora de la seguridad del Control de Acceso del SI.

- **Disponer de la documentación del proceso de evaluación de la seguridad del Control de Acceso** requiere de la disponibilidad de la información asociada al proceso de evaluación y de su acceso autorizado por parte de los directivos de la organización.

2.5 Bases del modelo.

La integración de indicadores y criterios para la evaluación de la seguridad de los procesos de Identificación y Autenticación, Autorización y Auditoría de los SI de centros productivos de la UCI requiere que el modelo esté basado en:

- La **Integración** de los controles para la evaluación.
- La **Síntesis** de los controles para la evaluación del Control de Acceso de los SI de centros productivos de la UCI.
- La **Medición Descriptiva** del estado actual de los procesos del Control de Acceso del SI, a partir de la evaluación y medición del grado de cumplimiento de los criterios e indicadores para la evaluación de la seguridad de los procesos de Identificación y Autenticación, Autorización y Auditoría.
- La **Mejora Continua** para propiciar que la evaluación pueda verse como un conjunto de actividades que contribuyan a la mejora continua de los SI que sean evaluados.
- La **Generalización** para que el modelo sea aplicable a una gran variedad de los SI de centros productivos de la UCI.

2.6 Componentes del modelo.

Considerando los principios y las bases descritos anteriormente, el modelo permite integrar los componentes para evaluar la seguridad del Control de Acceso de los SI de centros productivos de la UCI. A continuación se ofrece una explicación detallada de los componentes del modelo.

2.6.1 Indicadores para la evaluación de la seguridad del Control de Acceso.

En el campo de la evaluación de la seguridad del Control de Acceso existen pocas investigaciones que abordan la temática de la evaluación de los procesos de Identificación y Autenticación, Autorización y Auditoría. Un ejemplo ilustrativo de la selección de indicadores para la evaluación del Control de Acceso son los 45 indicadores propuestos en la tesis doctoral de Oiner Gómez Baryolo, que contribuyen a evaluar la seguridad de las soluciones de Control de Acceso de SI en entornos multidominios (Baryolo, 2012).

El análisis de la investigación del Dr C Oiner Gómez Baryolo (Baryolo, 2012) así como la revisión de normas, estándares, guías, recomendaciones, resoluciones y decretos contribuyeron a la definición de los indicadores para la evaluación.

Los 10 indicadores definidos constituyen una agrupación y síntesis de los controles para la evaluación de la seguridad de los procesos de Identificación y Autenticación, Autorización y Auditoría identificados en los estándares internacionales y en resoluciones cubanas.

- **I1. Empleo de estándares para el intercambio de información.** Para cumplir este indicador el sistema que se evalúa debe implementar estándares para el intercambio de mensajes de identificación y autenticación usando criptografía. Ejemplo: Kerberos, SPKI, OpenPGP, EDIFACT, AC X.509 (PKI X.509, S/MIME, IPSec, TLS, WAP, SOAP, WSDL, UDDI, WS Security, X.500, LDAP, XACML, XKMS), entre otros.
- I2. Empleo de métodos criptográficos y mecanismos seguros de comunicación (envío, recepción y almacenamiento de información sensible). Para cumplir este indicador el sistema que se evalúa debe implementar algoritmos o estándares reconocidos como por ejemplo: TDES, AES (RIJNDAEL, RC6, SERPENT, MARS), entre otros.
- **I3. Empleo de soluciones para la federación de identidades entre dominios**. Para cumplir este indicador el sistema que se evalúa debe implementar estándares que permiten la identificación y autenticación de usuarios externos que pertenecen a otro dominio, así como el soporte a mecanismos de SSO como por ejemplo: Passport, Shibboleth, Liberty Alliance, PAPI, entre otros.
- **I4. Empleo de pruebas desafío-respuesta en los eventos donde se necesite determinar cuándo el usuario es una persona o no**. Para cumplir este indicador el sistema que se evalúa debe implementar la Prueba Pública y Automática de Turing (CAPTCHA por sus siglas en Inglés) para identificar a máquinas y humanos.
- **I5. Empleo de estándares para la representación de la información de autorización.** Para cumplir este indicador el sistema que se evalúa debe implementar estándares para la gestión de la información de autorización como por ejemplo: SPKI/SDSI, SAML, entre otros.
- **I6. Empleo de protocolos para la gestión de autorización de la red.** Para cumplir este indicador el sistema que se evalúa debe implementar estándares para la gestión de la información de autorización de la red como por ejemplo: TACACS+, RADIUS, DIAMETER, WEP, WPA, entre otros.

- **I7. Empleo de estándares de Control de Acceso de la red**. Para cumplir este indicador el sistema que se evalúa debe implementar mecanismos de Control de Acceso de la red como por ejemplo: 802.1X, PANA, EAP, entre otros.
- **I8. Empleo de controles internos propuestos por marcos de trabajo de aplicación internacional.** Para cumplir este indicador el sistema que se evalúa debe implementar controles internos propuestos por marcos de trabajo de aplicación internacional como por ejemplo: COSO, entre otros.
- **I9. Empleo de modelos para la gestión de la trazabilidad.** Para cumplir este indicador el sistema que se evalúa debe implementar modelos para la gestión de la trazabilidad como por ejemplo: MDE, entre otros.
- **I10. Empleo de estándares para la gestión de trazas**. Para cumplir este indicador el sistema que se evalúa debe implementar estándares para la gestión de trazas. Ejemplo: POSIX 1003.1q, entre otros.

La Tabla 3 muestra la relación entre los indicadores I1, I2, I3 e I4 y los controles de ISO/IEC 27002, NIST SP 800-12, NIST SP 800-53, Proyecto OWASP de 10 Mejores Elementos y en su Manual de Prueba, Resolución 127/2007 del Ministerio de la Informática y las Comunicaciones de Cuba y el Decreto Ley 281 de los cuales fueron extraídos.

Tabla 3. Relación de los indicadores I1, I2, I3 e I4 y los controles de evaluación de la seguridad del Control de Acceso. (Fuente: elaboración propia).

Normas o Estándares, Recomendaciones y Resoluciones (INDICADORES 1, 2, 3 y 4)								
ISO/IEC 17799	**ISO/IEC 15408**	**NIST PUB 800-53**	**NIST PUB 800-12**	**FIPS PUB 140-2**	**OWASP Top 10 2010**	**OWASP Guía Prueba 2008**	**COBIT 4.1**	**Res. 127/2007 MIC**
11.5.2, 11.5.5, 11.5.6	FMT: _MOF, _MSA, _MTD, _REV, _SAE, _SMF, _SMR	AC (2.14.16	10.2, 10.4	4.3	A3	4.4.3,4.4.4,4.4.5	DS5.3, DS5.4	Acuerdo No. 3736. Acuerdo No. 6058

11.5.3, 11.2.3, 11.3.1	FCS: _CKM,_ COP	-	19.1,19.2	4.1, 4.7.1,4.7.2,4.7.3, 4.7.4,4.7.5,4.7.6	A8	4.4.1	DS5.8	Acuerdo No. 3736. Acuerdo No. 6058
11.4.2	FCO:_NRO, _NRR	AC 5, 6, 16, 21, 22	-	-	A3	-	DS5.3	Acuerdo No. 3736. Acuerdo No. 6058
-	-	-	-	-	-	4.4.8	-	-

La

Tabla 4 muestra la relación entre los indicadores I5, I6 e I7 y los controles de la ISO/IEC 27002,

Normas o Estándares, Recomendaciones y Resoluciones (INDICADORES 5, 6 y 7)							
ISO/IEC 17799	**ISO/IEC 15408**	**NIST PUB 800-53**	**FIPS PUB 140-2**	**OWASP Top 10 2010**	**OWASP Guía Prueba 2008**	**COBIT 4.1**	**Res. 127/2007 MIC**
11.1.1, 11.2, 11.2.2, 11.2.4, 11.6, 11.6.1, 11.6.2	FTA: _LSA,_MCS,_ SSL	AC1,3,4,5,10, 11, 12, 14, 15	4.3	A3,A7	4.6,4.6.3,4.5		Acuerdo No. 3736. Acuerdo No. 605
11.3.2, 11.1.1, 11.2, 11.2.2, 11.2.4, 11.6, 11.6.1, 11.6.2	FTP: _ITC, _TRPFPR: _ANO,_PSE	AC1,3, 4,5,10,11, 12,14, 15,22	-	A9,A10	4.6,4.6.3,4.5	DS5.10, DS5.11	Acuerdo No. 3736. Acuerdo No. 605
11.4.3, 11.4, 11.4.5, 11.1 11.4.6, 11.4.7, 11.4, 11.4.1, 11.6.2	FTP:_ITC, _TRP FPR: _ANO,_PSE	AC-17,AC-18, AC-19,AC-20, AC-21,AC-22, AC-18	-	A9,A10	-	DS5.10, DS5.11	Acuerdo No. 3736. Acuerdo No. 605

el NIST SP 800-12, el NIST SP 800-53, el Proyecto OWASP de 10 Mejores Elementos y en su Manual de Prueba, la Resolución 127/2007 del Ministerio de la Informática y las Comunicaciones de Cuba y el Decreto Ley 281 de los cuales fueron extraídos.

Normas o Estándares, Recomendaciones y Resoluciones (INDICADORES 5, 6 y 7)							
ISO/IEC 17799	**ISO/IEC 15408**	**NIST PUB 800-53**	**FIPS PUB 140-2**	**OWASP Top 10 2010**	**OWASP Guía Prueba 2008**	**COBIT 4.1**	**Res. 127/2007 MIC**

11.1.1, 11.2, 11.2.2, 11.2.4, 11.6, 11.6.1, 11.6.2	FTA: _LSA,_MCS,_ SSL	AC1,3,4,5,10, 11, 12, 14, 15	4.3	A3,A7	4.6,4.6.3,4.5		Acuerdo No. 3736. Acuerdo No. 605
11.3.2, 11.1.1, 11.2, 11.2.2, 11.2.4, 11.6, 11.6.1, 11.6.2	FTP: _ITC, _TRPFPR: _ANO,_PSE	AC1,3, 4,5,10,11, 12,14, 15,22	-	A9,A10	4.6,4.6.3,4.5	DS5.10, DS5.11	Acuerdo No. 3736. Acuerdo No. 605
11.4.3, 11.4, 11.4.5, 11.1 11.4.6, 11.4.7, 11.4, 11.4.1, 11.6.2	FTP:_ITC, _TRP FPR: _ANO,_PSE	AC-17,AC-18, AC-19,AC-20, AC-21,AC-22, AC-18	-	A9,A1 0	-	DS5.10, DS5.11	Acuerdo No. 3736. Acuerdo No. 605

Tabla 4. Relación de los indicadores I5, I6 e I7 y los controles de evaluación de la seguridad del Control de Acceso. (Fuente: Elaboración propia).

La Tabla 5 muestra la relación entre los indicadores I8, I9 e I10 y los controles de la ISO/IEC 27002, el NIST SP 800-12, el NIST SP 800-53, el Proyecto OWASP de 10 Mejores Elementos y en su Manual de Prueba, la Resolución 127/2007 del Ministerio de la Informática y las Comunicaciones de Cuba y el Decreto Ley 281 de los cuales fueron extraídos.

Tabla 5. Relación de los indicadores I8, I9 e I10 y los controles de evaluación de la seguridad del Control de Acceso. (Fuente: Elaboración propia).

	Normas o Estándares, Recomendaciones y Resoluciones (INDICADORES 8, 9, 10)						
ISO/IEC 17799	**ISO/IEC 15408**	**NIST PUB 800-53**	**NIST PUB 800-12**	**OWASP Top 10 2010**	**OWASP Guía Prueba 2008**	**COBIT 4.1**	**Res. 127/2007 MIC**
11.5.1	FAU:_ARP, _GEN, _SAA, _SAR, _SEL, _STG	AC 7,8, 9,13	18.2	-	-	DS5.5, DS5.6	Acuerdo No. 3736. Acuerdo No. 6058.
11.5.1	FAU:_ARP, _GEN, _SAA, _SAR, _SEL, _STG	AC-7,8, 9,13	18.2	-	-	DS5.5, DS5.6	Acuerdo No. 3736. Acuerdo No. 6058.
11.5.1	FAU: _ARP,_GE N,_SAA, _SAR,	AC - 7,8 ,9,	18.2	-	-	DS5.5, DS5.6	Acuerdo No. 3736. Acuerdo No.

	_SEL,_STG	13					6058.

2.6.2 Criterios para la evaluación de la seguridad del Control de Acceso.

- Los 10 indicadores del modelo agrupan un conjunto de criterios de evaluación. Es importante señalar que aunque los 10 indicadores para la evaluación de la seguridad de los procesos de Identificación y Autenticación, Autorización y Auditoría están descritos en diferentes normas, estándares, guías, recomendaciones, resoluciones y decretos (como muestran la Tabla 3, la
- **Tabla 4** y la Tabla 5), el enfoque de síntesis de los mismos así como sus relaciones en el

- **Normas o Estándares, Recomendaciones y Resoluciones (INDICADORES 5, 6 y 7)**

ISO/IEC 17799	**ISO/IEC 15408**	**NIST PUB 800-53**	**FIPS PUB 140-2**	**OWASP Top 10 2010**	**OWASP Guía Prueba 2008**	**COBIT 4.1**	**Res. 127/2007 MIC**
11.1.1, 11.2, 11.2.2, 11.2.4, 11.6, 11.6.1, 11.6.2	FTA: _LSA,_MCS,_ SSL	AC1,3,4,5,10, 11, 12, 14, 15	4.3	A3,A7	4.6,4.6.3,4.5		Acuerdo No. 3736. Acuerdo No. 605
11.3.2, 11.1.1, 11.2, 11.2.2, 11.2.4, 11.6, 11.6.1, 11.6.2	FTP: _ITC, _TRPFPR: _ANO,_PSE	AC1,3, 4,5,10,11, 12,14, 15,22	-	A9,A10	4.6,4.6.3,4.5	DS5.10, DS5.11	Acuerdo No. 3736. Acuerdo No. 605
11.4.3, 11.4, 11.4.5, 11.1 11.4.6, 11.4.7, 11.4, 11.4.1, 11.6.2	FTP:_ITC, _TRP FPR: _ANO,_PSE	AC-17,AC-18, AC-19,AC-20, AC-21,AC-22, AC-18	-	A9,A1 0	-	DS5.10, DS5.11	Acuerdo No. 3736. Acuerdo No. 605

modelo, constituyen aportes de la presente investigación.

Los 27 criterios de evaluación que se presentan a continuación están agrupados por indicadores; fueron identificados a partir del estudio documental y un cuestionario realizado a los expertos de las principales entidades rectoras en el área de la Seguridad Informática en Cuba (Anexo 2). Los criterios describen las diferentes soluciones de Control de Acceso que se utilizan en la actualidad y contribuyen a la evaluación de los procesos de Identificación y Autenticación, Autorización y Auditoría. Las soluciones de Control de Acceso desarrolladas por

especialistas de las propias organizaciones están representadas por los criterios C12, C23 y C27.

Criterios de evaluación del indicador I1:

- C1. Implementación del estándar Kerberos.
- C2. Implementación del estándar OpenPGP.
- C3. Implementación del estándar EDIFACT.
- C4. Implementación del estándar AC X.509 (PKI X.509, S/MIME, IPSec, TLS, WAP, SOAP, WSDL, UDDI, WS Security, X.500, LDAP, XACML, XKMS).

Criterios de evaluación del indicador I2:

- C5. Implementación de algoritmos de cifrado simétrico (DES-TDES, RC2/RC4/RC5/RC6, AES, IDEA, SEAL, Blowfish, Serpent).
- C6. Implementación de algoritmos de cifrado asimétrico (Diffie-Hellman, RSA, DSA, ElGamal, Rabin).

Criterios de evaluación del indicador I3:

- C7. Implementación del estándar Passport.
- C8. Implementación del estándar Shibboleth.
- C9. Implementación del estándar Liberty Alliance.
- C10. Implementación del estándar PAPI.

Criterio de evaluación del indicador I4:

- C11. Implementación de la prueba CAPTCHA.

Criterio de evaluación adicional:

- C12. Implementación de una solución propia de la organización para la gestión de la Identificación y Autenticación.

Criterios de evaluación del indicador I5:

- C13. Implementación del estándar SPKI/SDSI.
- C14. Implementación del estándar SAML.

- C15. Implementación del estándar TACACS+.

Criterios de evaluación del indicador I6:

- C16. Implementación del estándar RADIUS.
- C17. Implementación del estándar DIAMETER.
- C18. Implementación del estándar WEP.
- C19. Implementación del estándar WPA.

Criterios de evaluación del indicador I7:

- C20. Implementación del estándar 802.1X.
- C21. Implementación del estándar PANA.
- C22. Implementación del estándar EAP.

Criterio de evaluación adicional:

- C23. Implementación de una solución propia de la organización para la gestión de la Autorización.

Criterio de evaluación del indicador I8:

- C24. Implementación del marco de trabajo COSO.

Criterio de evaluación del indicador I9:

- C25. Implementación del modelo MDE.

Criterio de evaluación del indicador I10:

- C26. Implementación del estándar POSIX 1003.1q.

Criterio de evaluación adicional:

- C27. Implementación de una solución propia de la organización para la gestión de la Auditoría.

2.6.3 Algoritmo LSP adaptado para la evaluación de un SI.

La evaluación de un SI es cualitativa. Las entradas del algoritmo (Variables de Performance), su procesamiento (Preferencias Elementales) y el resultado final de la evaluación (Preferencia

Global) son definidos en el contexto de la evaluación de un SI. A continuación se describen los pasos para la evaluación según el MECA.

Evaluación de un SI.

La evaluación de un proceso es cuantitativa y se determina a partir de la evaluación de los criterios de evaluación del proceso. Está basada en los conceptos de Variables de Performance, Preferencias Elementales y Preferencia Global adaptados de la siguiente manera:

- **Variables de Performance:** Son los criterios de evaluación con los que cumple el sistema que se evalúa.
- **Preferencias Elementales**: Conforman las Evaluaciones de Criterios y el Estado del Proceso.
- **Evaluaciones de Criterios**: Se obtienen mediante funciones que dividen la criticidad de cada Variable de Performance entre la suma de las criticidades de todos los criterios del proceso expresadas en su máximo valor. En términos matemáticos, el valor de una Preferencia Elemental de un criterio *i-ésimo* (c_i) se expresa como Ec_i y se determina mediante la fórmula:

- $$Ec_i = g(c_i) = Cc_i / \sum_{i=0}^{i=n} c_i \qquad (3)$$

  Donde Ec_i es la Preferencia Elemental de c_i, g es la función que divide la criticidad de c_i entre la suma de las criticidades de todos los criterios del proceso expresadas en su máximo valor (c = 4), Cc_i es la criticidad de c_i y n representa la cantidad de criterios del proceso.

- La criticidad de un criterio de evaluación se obtiene mediante el cálculo de la media de las criticidades asignadas por los expertos. En términos matemáticos, la criticidad C de un criterio *i-ésimo* se determina mediante la fórmula:

- $$Cc_i = \sum_{j=0}^{j=n} Ce_j / n \qquad (4)$$

- Donde Cc_i es la criticidad de c_i, Ce_j es la criticidad asignada por el especialista *j-ésimo* a c_i y n es el número de especialistas que evaluaron los 27 criterios de evaluación.
- **Estado del proceso:** Se obtiene mediante la representación de las Evaluaciones de Criterios en una escala de intervalos. En términos matemáticos, el estado *i* de un proceso *j*

se expresa como G_{ij} y se determina mediante la fórmula: $G_{ij} = h(L_{ij})$ donde G_{ij} es el estado *i* del proceso *j*, *h* es la función que permite representar en una escala de intervalos las evaluaciones de los criterios del proceso *j*. El procedimiento para representar las Evaluaciones de Criterios del proceso en una escala de intervalos se describe detalladamente en el epígrafe siguiente. El valor o estado G_{ij} de un proceso puede ser Bajo, Medio o Alto.

- **Preferencia Global:** Se expresa como N_{pi} y describe las recomendaciones basadas en el estado del proceso evaluado. Las recomendaciones expresan los criterios de evaluación que afectaron el resultado obtenido por el proceso evaluado.

Representación de las evaluaciones de los criterios de un proceso en una escala de intervalos.

Un proceso de Identificación o Autenticación, Autorización y Auditoría, al ser evaluado, obtiene un estado de Bajo, Medio o Alto. La evaluación cualitativa de un proceso consta de 5 pasos que se describen a continuación:

- **Paso 1 Determinación de los intervalos que corresponden a las evaluaciones Bajo, Medio y Alto:** Consiste en definirlos intervalos de Bajo [0; 0.33), Medio [0.33; 0.66) y Alto [0.66; 1] a partir de la división proporcional de una escala de intervalos con valores extremos de mínimo en 0 y máximo en 1.
- **Paso 2 Representación de las evaluaciones:** Consiste en representar las Evaluaciones de Criterios en la escala de intervalos construida en el *Paso 1*.
- **Paso 3 Identificación del estado (Alto, Medio o Bajo):** Consiste en identificar el intervalo (Bajo [0; 0.33), Medio [0.33; 0.66) o Alto [0.66; 1]) en el que se encuentran representadas la mayor cantidad de evaluaciones de los criterios del proceso.
- **Paso 4 Recomendaciones:** Consiste en mostrar los criterios de evaluación que incidieron en el resultado (estado de Bajo, Medio o Alto) obtenido.

La Figura 2 muestra la adaptación del algoritmo LSP para la evaluación de un proceso como se ha descrito anteriormente.

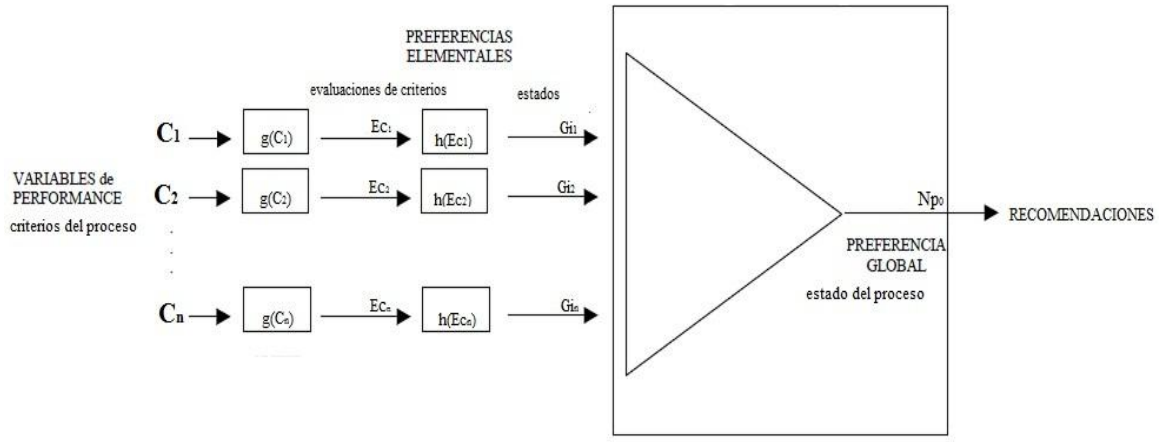

Figura 2. Adaptación del algoritmo LSP para la evaluación de un SI. (Fuente: elaboración propia).

2.7 Guía para la aplicación del modelo.

Para facilitar la aplicación del modelo fue necesario desarrollar una guía compuesta de tres etapas orientadas a la caracterización y descripción de la organización a la que pertenece el SI, la realización del proceso de evaluación y el almacenamiento de la información generada durante el mismo. Esas etapas se conforman de varios pasos. A continuación se describen detalladamente cada una de estas etapas y sus pasos.

Etapa 1 Diagnóstico inicial: El diagnóstico inicial tiene el objetivo de obtener una visión general de la estructura de la organización: procesos, personas y tecnologías. La etapa incluye la realización de cinco pasos. Se utilizan listas de chequeo para conocer sobre el estado de la organización y el análisis de los resultados del diagnóstico.

- **Paso 1.1 Diagnóstico inicial de los procesos:** Tiene el objetivo de conocer sobre el dominio y la gestión de procesos de la organización.
    1. Lista de Chequeo
    2. ¿Qué tipo de procesos tienen lugar en la organización?
    3. ¿Cuáles procesos de la organización son críticos?
- **Paso 1.2 Diagnóstico inicial de las personas:** Tiene el objetivo de conocer sobre el rol y la responsabilidad de las personas que forman parte de la organización.
    4. Lista de Chequeo
    1. ¿Qué rol o roles desempeñan las personas en la organización?

- **Paso 1.3 Diagnóstico inicial de la tecnología:** Tiene el objetivo de conocer sobre el tipo de tecnología que se utiliza en la organización y su funcionalidad.

    2. Lista de Chequeo

    1. ¿Qué procesos de la organización requieren el uso de TIC?
    2. ¿Qué responsabilidad ocupa la tecnología en la gestión de los procesos de la organización?

- **Paso 1.4 Diagnóstico inicial sobre la seguridad del Control de Acceso:** Tiene el objetivo de conocer sobre los procesos asociados a la seguridad del Control de Acceso y su interrelación en el SI de la organización. El diagnóstico se basa en la información protegida, en los controles de seguridad y en el procedimiento de evaluación de la seguridad empleados en la organización.

    3. Lista de Chequeo

    1. ¿Qué controles de seguridad se utilizan para la evaluación del SI de la organización?
    2. ¿Cómo se realiza la evaluación del Control de Acceso del SI de la organización?
    3. ¿Qué personas participan? ¿Qué roles ocupan en la organización?
    4. ¿Qué tipo de resultado se obtiene?
    5. ¿Qué análisis de la evaluación se realiza?
    6. ¿Qué registro de la evaluación se realiza?

- **Paso 1.5 Análisis de resultados**: Tiene el objetivo de realizar un análisis sobre el diagnóstico de la organización para determinar la factibilidad de la evaluación. Consiste en describir si es posible o no llevar a cabo el proceso de evaluación sobre la base de la identificación del SI de la organización y del responsable de la evaluación.

    7. Lista de Chequeo

    1. ¿Puede ser definido el SI de la organización como un SI?
    2. ¿Existen los recursos humanos capacitados para la evaluación de la seguridad del Control de Acceso?

Etapa 2 Evaluación de la seguridad del Control de Acceso.

La evaluación tiene el objetivo de obtener el estado de los procesos de Identificación y Autenticación, Autorización y Auditoría del SI de la organización. Permite conocer las recomendaciones de la evaluación sobre la base de los criterios de evaluación que no fueron implementados en el SI. La etapa incluye la realización de 3 pasos en los que se describe el proceso para llevar a cabo la evaluación, así como el análisis de los resultados obtenidos.

- **Paso 2.1 Selección del responsable de la evaluación**: Permite la selección del responsable de la evaluación basado en el diagnóstico de las personas de la organización realizado durante la Etapa 1. El especialista debe haber participado en la implementación o tener conocimiento sobre la seguridad del SI.

    3. Lista de Chequeo

    1. ¿Cuál o cuáles roles asociados a la seguridad de la información ha desempeñado o desempeña dentro o fuera de la organización?
    2. ¿Qué nivel de experticia posee en el uso del SI de la organización?

- **Paso 2.2 Evaluación del SI**: Consiste en evaluar la seguridad del Control de Acceso de los procesos de Identificación y Autenticación, Autorización y Auditoría del SI. Determina el estado de un proceso de manera cualitativa en los términos de Bajo, Medio o Alto y genera recomendaciones basadas en los criterios que afectaron la evaluación.

    3. Lista de Chequeo

    1. ¿Cuáles fueron los estados de los procesos de Identificación y Autenticación, Autorización y Auditoría obtenidos en la evaluación?
    2. ¿Cuáles fueron las recomendaciones asociadas a los procesos de Identificación y Autenticación, Autorización y Auditoría obtenidas en la evaluación?

Etapa 3 Documentación de la evaluación de la seguridad del Control de Acceso.

La documentación de la evaluación consiste en formalizar el proceso de la evaluación mediante la documentación de cada una de las etapas y pasos de la guía de evaluación que fueron realizados. La etapa incluye la realización de un solo paso.

- **Paso 3.1 Documentación de la información de la evaluación**: Tiene el objetivo de almacenar la información obtenida en cada una de las etapas del proceso de evaluación referente a los resultados obtenidos, personas y tecnologías, incidencias, etc. Se describe el

medio de almacenamiento de la información así como los usuarios y roles que tienen acceso a la misma.

3. Lista de Chequeo

1. ¿Fueron almacenados los resultados de la aplicación de cada paso de la guía?
2. ¿Existe un mecanismo de copia de seguridad de la información almacenada?
3. ¿Están definidos los roles y usuarios que tienen acceso a la información de la evaluación?

Finalmente se analizan los resultados de la evaluación sobre la base de los criterios de evaluación que afectaron los resultados obtenidos. En caso de que estos últimos puedan ser mejorados de acuerdo al análisis realizado, se repite el proceso para obtener una nueva evaluación. En la Figura 3 se muestra la guía para la aplicación del modelo.

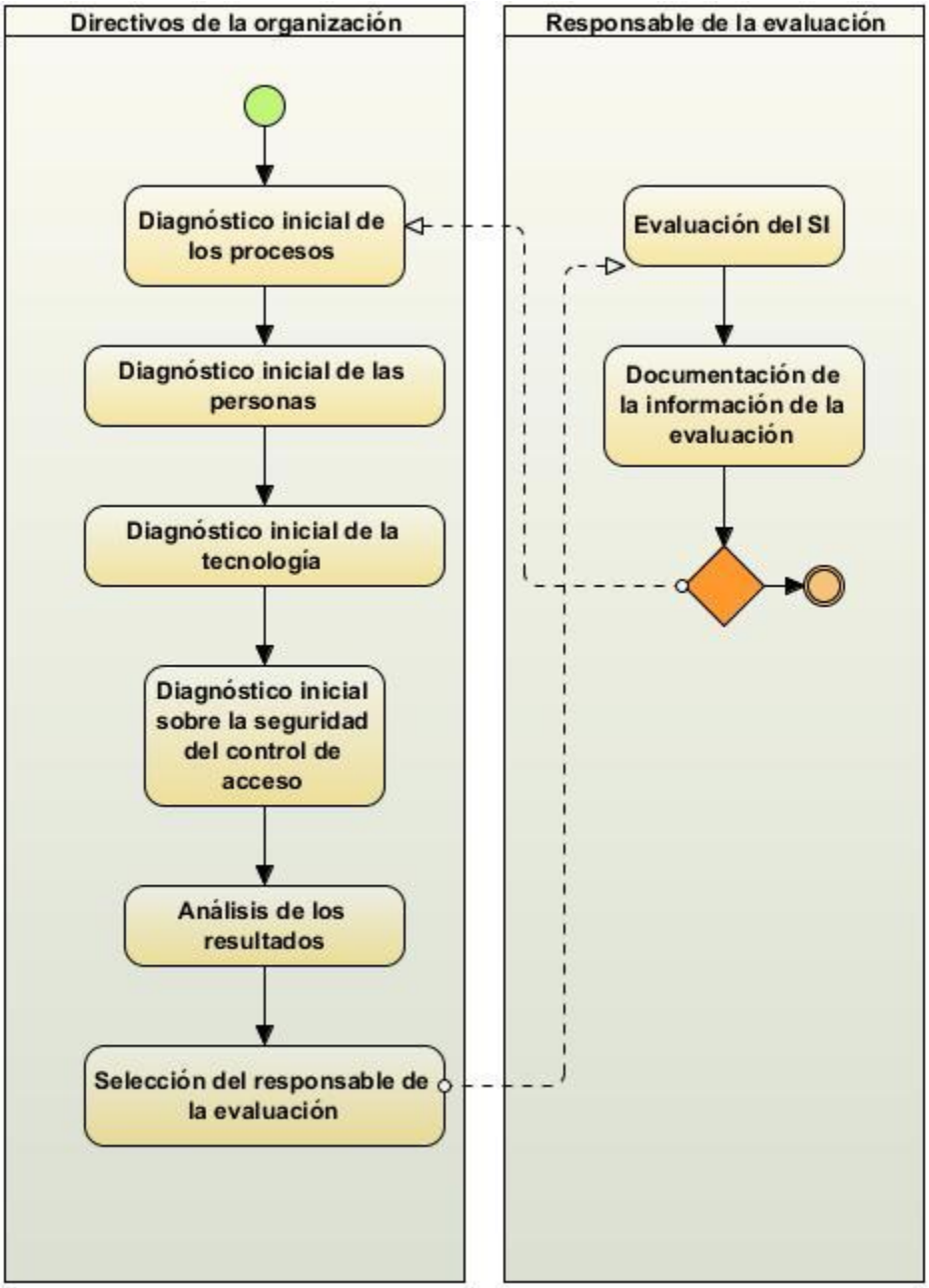

Figura 3. Diagrama de procesos de la guía para la aplicación del modelo. (Fuente: elaboración propia).

2.8 Sistema para la Evaluación del Control de Acceso.

La autora de la presente investigación, con el objetivo de facilitar la aplicación del modelo, desarrolló el Sistema para la Evaluación del Control de Acceso (SIECA). El SIECA constituye una solución informática para la evaluación. Esta herramienta utiliza los indicadores, criterios de evaluación y el algoritmo LSP adaptado para llevar a cabo la evaluación.

La evaluación de un SI, utilizando el SIECA, es por procesos. Esto permite identificar estados sobre la seguridad de la Identificación y Autenticación, Autorización y Auditoría, así como tomar decisiones en la organización sobre el mecanismo de Control de Acceso del SI. Sobre los estados que son alcanzados es posible realizar un análisis y generar recomendaciones.

- El SIECA asume los principios y las bases o restricciones del modelo. La solución informática está acorde a los lineamientos para el Perfeccionamiento de la Seguridad de las Tecnologías de la Información. La herramienta fue desarrollada utilizando software libre y sustituye la importación de servicios de auditoría informática y evaluación de la seguridad. Permite la agilidad en la implementación de controles para la evaluación y contribuye a la fiabilidad de los resultados de la evaluación. Las especificaciones y configuraciones necesarias para la implementación del SIECA (Anexo 5) contribuyen a la facilidad de su uso. La Figura 4 muestra la interfaz correspondiente al reporte de la evaluación.

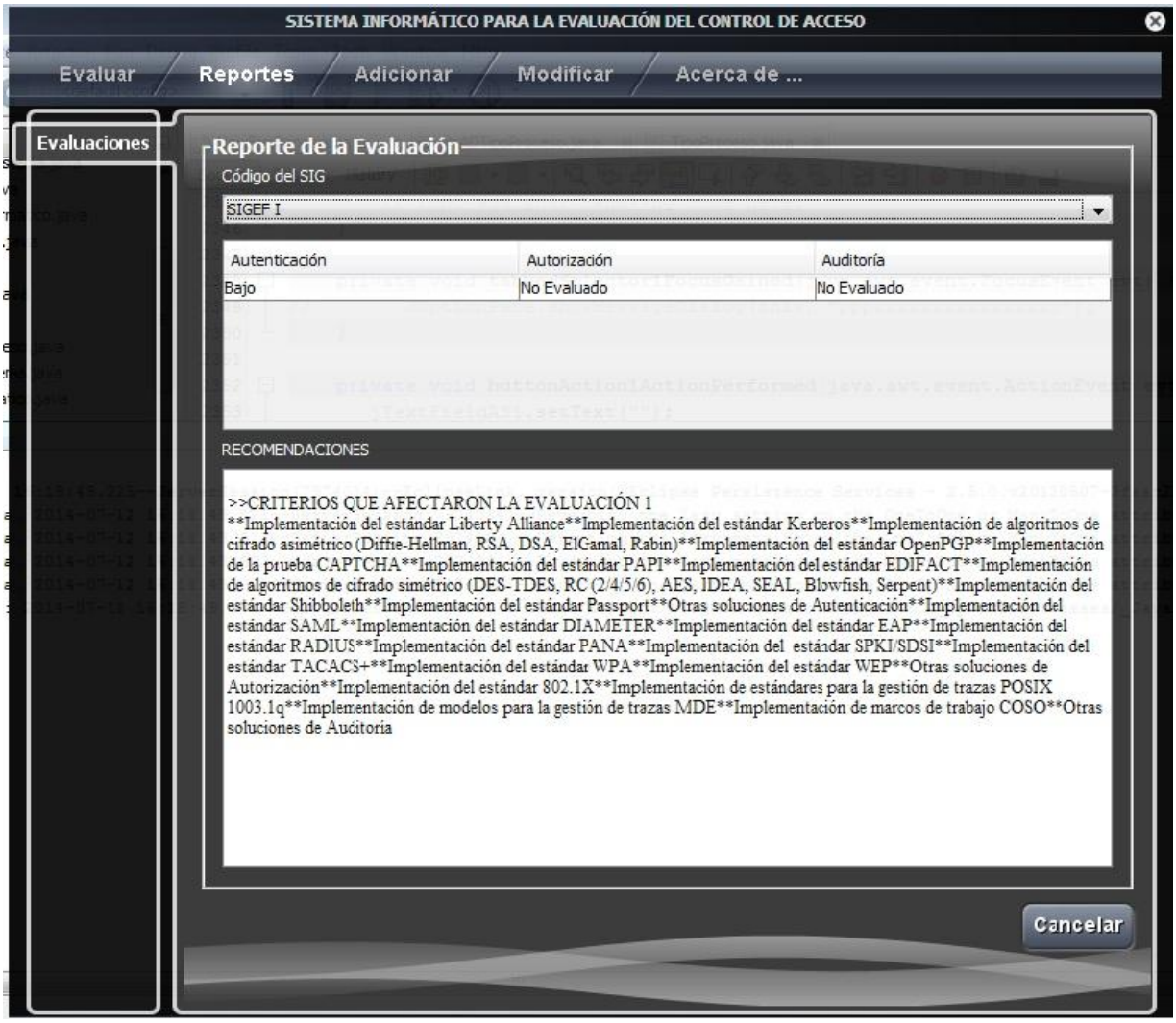

Figura 4. Reporte de la evaluación de la seguridad del Control de Acceso mediante SIECA. (Fuente: elaboración propia).

2.8.1 Pasos del MECA cubiertos por el SIECA.

Los pasos del modelo que son cubiertos por el sistema son aquellos que pueden ser informatizados mediante la utilización de los indicadores, criterios y el algoritmo LSP adaptado:

- El Paso 2 de la Etapa 2 ya que permite la aplicación de los controles de seguridad y el algoritmo LSP adaptado para la evaluación.
- El Paso 1 de la Etapa 3 sobre la documentación de la información relacionada con el proceso de evaluación ya que el SIECA almacena en una base de datos la información de la evaluación (datos generales del SI evaluado, fecha de la evaluación, estado de los procesos, recomendaciones realizadas, incidencias de la evaluación).

2.8.2 Pasos del MECA no cubiertos por el SIECA.

Los pasos del modelo que no son cubiertos por el SIECA son aquellos que se basan en actividades relacionadas con la labor humana. Para el desarrollo de estos pasos no es necesario el uso de herramientas informáticas:

- Los pasos 1, 2, 3, 4 y 5 de la Etapa 1 que permiten valorar la factibilidad de la evaluación sobre la base del diagnóstico de personas, tecnología, alcance y evaluación de la seguridad de la organización respectivamente.
- El Paso 1 de la Etapa 2 que corresponde a la selección del responsable de la evaluación que consiste en elegir a la persona de la organización con conocimiento sobre la seguridad de la información del SI.

2.9 Conclusiones parciales.

Sobre la elaboración del modelo propuesto por la autora se concluye lo siguiente:

- Define 10 indicadores para la evaluación de la seguridad de los procesos de Identificación y Autenticación, Autorización y Auditoría de los SI de centros productivos de la UCI, que permitieron agrupar y sintetizar las normas, estándares, guías, recomendaciones, resoluciones y decretos de controles de seguridad informática.

- El análisis de las soluciones para la gestión de los procesos de Identificación y Autenticación, Autorización y Auditoría permitió definir 27 criterios para la evaluación de los indicadores.
- La evaluación de la seguridad del Control de Acceso de los SI de centros productivos de la UCI fue posible por la adaptación del algoritmo LSP, basado en los conceptos de Variables de Performance, Preferencias Elementales y Preferencias Globales.
- La guía de aplicación del modelo, conformada por tres etapas y un conjunto de pasos, permitió la aplicación de los componentes del modelo.

CAPÍTULO 3: VALIDACIÓN DEL MODELO.

3.1 Introducción.

En el presente capítulo se realiza un análisis de la aplicación del modelo para la evaluación; se presentan la guía de validación diseñada y los resultados obtenidos en la ejecución de las actividades que la conforman.

3.2 Validación y análisis de los resultados.

El proceso de validación del modelo demuestra que este contribuye a la eficiencia de la evaluación. El MECA permite obtener soluciones eficientes para la evaluación, en comparación con los procedimientos y las guías de evaluación actuales que se utilizan en la UCI. El proceso de evaluación permite la aplicación de un conjunto de métodos científicos que se especifican en los siguientes epígrafes. La validación y el análisis de los resultados se basaron en los siguientes elementos:

- Análisis de la conformidad con el modelo de evaluación del MECA.
- Análisis de la contribución del modelo a la eficiencia de la evaluación del Control de Acceso de los SI de centros productivos de la UCI.
- Aplicación del modelo en cinco de los SI del CEGEL de la UCI.

3.2.1 Análisis de la conformidad con el modelo de evaluación del MECA.

Como parte de las acciones efectuadas para evaluar el potencial del modelo, se elaboró un cuestionario de cuatros preguntas (Anexo 2). El objetivo del cuestionario fue conocer la conformidad de expertos con el mecanismo de evaluación del MECA. Esto dado por la conformidad con los indicadores y criterios empleados. Los expertos seleccionados fueron cinco (Anexo 3) y el procedimiento para la selección de los mismos se describe brevemente a continuación.

Aplicación y resultados de la encuesta sobre la selección de los expertos para la evaluación de la seguridad del Control de Acceso.

Como parte del procedimiento para la selección de los expertos se contactaron a un conjunto de especialistas de seguridad provenientes de entidades que certifican la seguridad del Control de Acceso según normas, estándares, guías, recomendaciones, resoluciones y decretos. Los

especialistas seleccionados fueron aquellos que cumplieron con los requisitos que se describen a continuación:

- Más de 2 años en el trabajo con la Seguridad Informática.
- Dominio de normas, estándares, guías, recomendaciones, resoluciones y decretos actuales para la evaluación de la seguridad de los procesos de Identificación y Autenticación, Autorización y Auditoría y tener experiencia en su aplicación.
- Participación en la confección de Políticas de Seguridad y Auditorías Informáticas para la evaluación.
- Disposición para formar parte del grupo de expertos.
- Las entidades representadas en el proceso de validación del modelo fueron las siguientes:
- Centro Nacional de Calidad de Software (Calisoft).
- Universidad de las Ciencias Informáticas (UCI).
- Centro de Investigaciones de Tecnologías Integradas (XETID).

Aplicación y resultados del cuestionario sobre indicadores y criterios.

Las tres primeras preguntas del cuestionario (preguntas 1, 2 y 3, Anexo 2) estaban orientadas a validar la efectividad de los controles para la evaluación de los indicadores y los criterios de evaluación del modelo. Para ello se definió una escala de valores adecuada para garantizar la exactitud del criterio de los expertos. Se utilizó el modelo de Torgerson (Torgerson, 1958) para asignar un valor de escala a cada atributo. Las preguntas se describen brevemente a continuación:

- la primera pregunta permitió conocer la conformidad de los expertos con respecto a la selección de los 10 indicadores;
- la segunda pregunta permitió conocer si los criterios eran efectivos o no y su nivel de criticidad para la evaluación;
- la tercera pregunta permitió evaluar la eficiencia del modelo para la evaluación de los SI de centros productivos de la UCI;
- la cuarta pregunta permitió conocer comentarios adicionales sobre el modelo propuesto.

Análisis sobre la conformidad de los expertos con la selección de los indicadores.

Sobre la conformidad de los expertos con los 10 indicadores para la evaluación se obtuvieron los resultados que se muestran en la Figura 5.

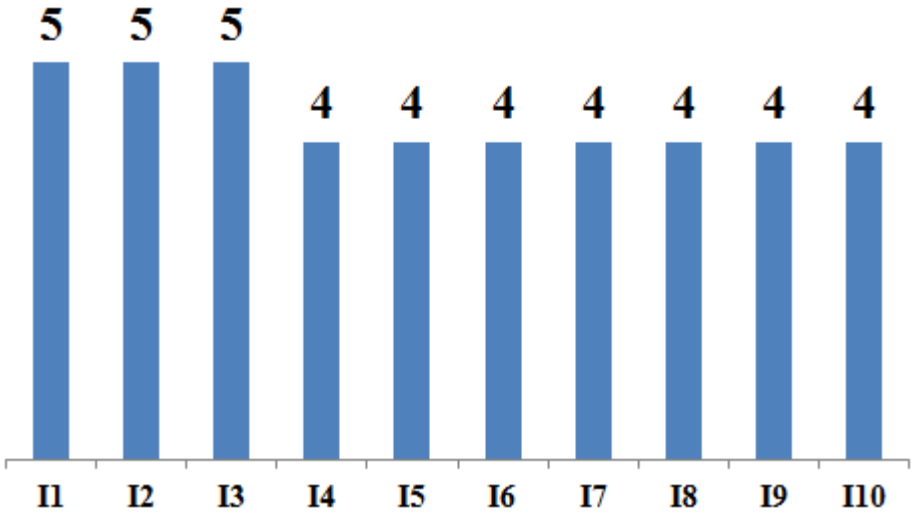

Figura 5. Evaluación de los indicadores por los expertos. (Fuente: elaboración propia).

- Los indicadores I1, I2 e I3 fueron evaluados de Completamente de Acuerdo por la totalidad de los expertos.
- Los indicadores I4, I5, I8 y I10 fueron evaluados de Mayormente de Acuerdo por la mayoría de los expertos.
- Los indicadores I6, I7 e I9 fueron evaluados de Parcialmente de Acuerdo por la mayoría de los expertos.
- No existieron indicadores con los cuales los expertos estuviesen en desacuerdo.

Para determinar el grado de coincidencia de los expertos con relación a los indicadores fue aplicada la prueba estadística Coeficiente de Concordancia de Kendall. La significancia estadística de las correlaciones estimadas (Valor–P= 0,504) indicó valores superiores a un nivel de significancia de 0,05. Se evidenció un acuerdo entre las opiniones de los especialistas, la mayoría de estos estuvieron conformes con los 10 indicadores y consideraron que no debían utilizarse otros indicadores en el modelo. Los estadígrafos básicos y de percentiles obtenidos se presentan en la Figura 6.

Correlaciones Kendall Rank

	E1	E2
E1		0,1516
		(27)
		0,5047
E2	0,1516	
	(27)	
	0,5047	

Figura 6. Estadígrafos obtenidos para el test de Kendall. (Fuente: elaboración propia).

Análisis sobre la efectividad de los criterios para la evaluación del Control de Acceso.

Sobre la efectividad de los criterios para evaluar los indicadores propuestos en el modelo se pudo constatar que la totalidad de los expertos consideraron que los 27 criterios reflejaban la efectividad de los indicadores para la evaluación y que debían ser considerados en el modelo.

Análisis sobre la criticidad de los criterios de evaluación.

Sobre la criticidad de los criterios de evaluación se obtuvieron los resultados que se muestran en la Figura 7.

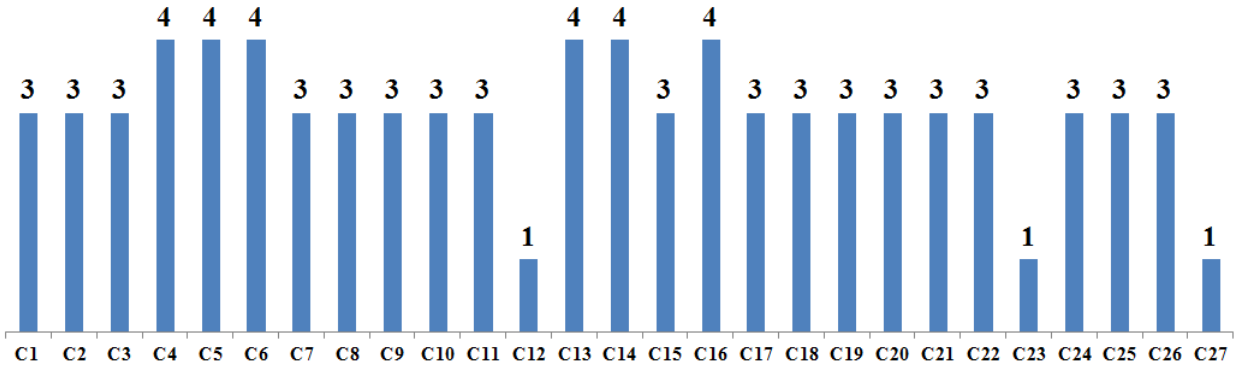

Figura 7. Evaluación de los criterios por los expertos. (Fuente: elaboración propia).

- Los criterios C4, C5, C6, C13, C14 y C16 fueron evaluados de Muy Críticos por la mayoría de los expertos.
- Los criterios C1, C2, C3, C7, C8, C9, C10, C11, C15, C17, C18, C19, C20, C21, C22, C24, C25 y C26 fueron evaluados de Críticos por la mayoría de los expertos.
- Los criterios C12, C23 y C27 fueron evaluados de No Críticos por la mayoría de los expertos.

Una vez procesada la información emitida por los expertos se pudo constatar que el nivel de criticidad de los criterios de evaluación estuvo mayormente entre los valores tres y cuatro. Este resultado evidenció la calidad en el proceso de síntesis de los indicadores y de agrupación de los criterios de evaluación. Además fue posible corroborar que no son críticas las soluciones de Control de Acceso que no reflejan el cumplimiento de normas, estándares, recomendaciones, resoluciones y decretos.

Análisis de la tolerancia a soluciones propias.

El tratamiento a soluciones de Control de Acceso, propias de los SI de las organizaciones, fue un requisito a considerar en el modelo. Los criterios de evaluación empleados consideraron la implementación de soluciones de Control de Acceso propias de todo SI que sea evaluado. Esto permitió mejorar objetivamente la eficiencia de la evaluación.

Existen aspectos que pudieran mejorarse, como por ejemplo que la producción de criterios de evaluación tiene un carácter estático, significando que el modelo propuesto necesita ser revisado periódicamente en la medida que surjan nuevas soluciones de Control de Acceso. El modelo podrá ser mejorado continuamente para obtener una mayor aproximación a los resultados esperados.

3.2.2 Análisis de la contribución del modelo a la eficiencia de la evaluación del Control de Acceso.

La aplicación del modelo propuesto evidenció una mejora de la eficiencia de la evaluación del Control de Acceso de los SI de centros productivos de la UCI. Para demostrar lo anterior se aplicó una encuesta de 4 preguntas a especialistas de seguridad (Anexo 4) de los SI de centros productivos de la UCI. La aplicación de la encuesta permitió realizar una comparación entre el procedimiento para evaluar un SI contratando los servicios de Calisoft y mediante el propio MECA.

Análisis del tiempo de respuesta.

La evaluación de los SI de centros productivos de la UCI que contratan los servicios de especialistas de Calisoft ocupa tiempos de hasta seis horas. Con la aplicación del modelo propuesto se logró disminuir estos tiempos. Para demostrar lo anterior fueron analizados los resultados de la aplicación de la encuesta analizada en este apartado (pregunta 3, Anexo 1). Se

compararon opiniones de los especialistas con relación al tiempo para la evaluación obtenida mediante la contratación de los servicios de terceros (Calisoft) y mediante el propio modelo.

Los encuestados manifestaron su opinión sobre el tiempo de respuesta de la evaluación seleccionando una de las posibles opciones:

- Más de 6 horas.
- 1 - 6 horas.
- 10 - 20 minutos.
- 20 - 50 segundos.

La comparación de las dos muestras independientes (Calisoft y MECA) permitió determinar si existían diferencias significativas entre las mismas. Los estadígrafos básicos y de percentiles obtenidos se presentan en la Figura 8.

Resumen Estadístico

	CALISOFT	*MECA*
Recuento	5	5
Promedio	200.0	23.0
Desviación Estándar	35.3553	2.0
Coeficiente de Variación	17.6777%	8.69565%
Mínimo	150.0	20.0
Máximo	240.0	25.0
Rango	90.0	5.0
Sesgo Estandarizado	-0.516398	-0.855816
Curtosis Estandarizada	-0.314028	-0.0855816

Figura 8. Estadígrafos obtenidos para el criterio tiempo de respuesta de las muestras CALISOFT y MECA. (Fuente: elaboración propia).

Los valores de sesgo y curtosis estandarizados estuvieron dentro del rango [-2,+2] indicando que los datos seguían una distribución normal. La media de los especialistas consideró que el tiempo de respuesta para evaluar la seguridad del Control de Acceso de los SIG mediante la contratación de los servicios de terceros (Calisoft) y con la ayuda del modelo varió de las horas a los minutos. Se apreció en los valores obtenidos una disminución de la desviación estándar lo que significó una mayor uniformidad en las opiniones de los encuestados sobre el tiempo de respuesta de la evaluación hacia la utilización del modelo propuesto.

Análisis sobre la cantidad de especialistas que son necesarios para la evaluación de la seguridad del Control de Acceso.

La aplicación del MECA logró disminuir en cantidad los especialistas para la evaluación de la seguridad del Control de Acceso. Para demostrar lo anterior fueron analizados los resultados de la aplicación de la encuesta analizada en este apartado (pregunta 4, Anexo 1).

Los encuestados manifestaron su opinión seleccionando una de las posibles opciones:

- Más de 6 especialistas.
- 2-6 especialistas.
- 1 especialista.

Los resultados obtenidos permitieron constatar que la evaluación de la seguridad de Calisoft requiere de seis especialistas de seguridad mientras que la evaluación mediante MECA solamente requiere el esfuerzo de uno de ellos. La aplicación del modelo contribuyó a la disminución de la cantidad de especialistas que intervienen en la evaluación de la seguridad del Control de Acceso de los Sistemas de Información de centros productivos de la UCI.

3.2.3 Aplicación del modelo en los SI de centros productivos de la UCI.

La aplicación del MECA se realizó siguiendo los pasos de la guía propuesta en el presente trabajo. El modelo fue aplicado a cinco de los SI del centro productivo CEGEL de la Facultad 3 que se especifican a continuación:

- Sistema de Gestión Fiscal Fase I (SIGEF I).
- Sistema de Gestión Fiscal Fase II (SIGEF II).
- Sistema de Informatización de los Tribunales Populares Cubanos (SITPC).
- Sistema de Informatización Registral de la Cámara de Comercio (SIRECC).
- Portal para el Consejo Nacional de Patrimonio Cultural (CNPC).

La selección de los SI se basó en los siguientes criterios de selección:

- Que implementaran alguno de los procesos del Control de Acceso basado en los modelos, estándares y protocolos más aplicados de la literatura.
- Que implementaran un conjunto considerable de procesos críticos del entorno de la organización correspondiente. En este sentido, debe considerarse que los SI seleccionados poseen un nivel crítico en cuanto a la seguridad de los procesos que informatizan.

- Que tuviesen resultados satisfactorios en la aplicación en entornos reales de los requisitos de seguridad establecidos.

Los SI seleccionados fueron evaluados previamente por Calisoft requiriéndose en el proceso un total de seis especialistas y más de seis horas para la evaluación de la seguridad del Control de Acceso en todos los casos.

En las próximas secciones se detallan las acciones realizadas en cada uno de los pasos de la guía para la evaluación de los SI usando el MECA así como la cantidad de especialistas y tiempo de evaluación requeridos.

Análisis de la aplicación del modelo en el SIGEF I.

Los resultados de la aplicación del modelo según las etapas y los pasos de la guía de evaluación en el SIGEF I se describen a continuación:

- La realización del Paso 1 de la Etapa 1 permitió conocer que el SIGEF I implementa procesos críticos de la Fiscalía General de la República, Fiscalía Provincial y Fiscalía Municipal de Cuba.
- La realización del Paso 2 de la Etapa 1 permitió conocer sobre la existencia de especialistas de seguridad que conocían las soluciones de Control de Acceso implementadas en el SI.
- La realización del Paso 3 de la Etapa 1 permitió clasificar como un SI al SI de la organización.
- La realización del Paso 4 de la Etapa 1 permitió confirmar que el modelo podía ser aplicado al SIGEF I.
- La realización del Paso 1 de la Etapa 2 permitió la selección del especialista Manuel Enrique Delgado Fernández como responsable de la evaluación.
- La realización del Paso 3 de la Etapa 2 permitió conocer sobre las recomendaciones de la evaluación. Estas detallaron el conjunto de criterios que afectaron la evaluación de la seguridad de los procesos.
- La realización del Paso 1 de la Etapa 3 permitió documentar el proceso de evaluación y almacenar la información en la base de datos del SIECA para ser consultada por los responsables de la evaluación y demás directivos de la organización.

En la Tabla 6 se muestran los resultados de la evaluación obtenidos con la realización del Paso 2 de la Etapa 2.

Tabla 6. Resultados de la evaluación del SIGEF I. (Fuente: elaboración propia).

Etapa/Estado	**Estado del proceso**		
	Identificación y Autorización	**Autorización**	**Auditoría**
Etapa 2 Paso 2	Bajo	No evaluado	No evaluado

Las recomendaciones obtenidas durante la realización del Paso 3 de la Etapa 2, sobre los criterios que afectaron la evaluación del proceso de Identificación y Autenticación, fueron: la implementación de los estándares Liberty Alliance, Kerberos y OpenPGP, los algoritmos de cifrado asimétricos (Diffie-Hellman, RSA, DSA, ElGamal, Rabin), la prueba CAPTCHA y otras soluciones de Autenticación propias de la organización.

La evaluación de la seguridad del SIGEF I usando MECA fue realizada por un especialista y tuvo una duración de 30 minutos.

Análisis de la aplicación del modelo en el SIGEF II.

Los resultados de la aplicación del modelo, según las etapas y pasos de la guía de evaluación, en el SIGEF II se describen a continuación:

- La realización del Paso 1 de la Etapa 1 permitió conocer que el SIGEF II implementa procesos críticos de la Fiscalía General de la República, Fiscalía Provincial y Fiscalía Municipal de Cuba.
- La realización del Paso 2 de la Etapa 1 permitió conocer sobre la existencia de especialistas de seguridad que conocían las soluciones de Control de Acceso implementadas en el SI.
- La realización del Paso 3 de la Etapa 1 permitió clasificar como un SI al SI de la organización.
- La realización del Paso 4 de la Etapa 1 permitió confirmar que el modelo podía ser aplicado al SIGEF I.
- La realización del Paso 1 de la Etapa 2 permitió la selección del especialista Héctor Fuentes Blanco como responsable de la evaluación.

- La realización del Paso 3 de la Etapa 2 permitió conocer sobre las recomendaciones de la evaluación. Estas detallaron el conjunto de criterios que afectaron la evaluación de la seguridad de los procesos.
- La realización del Paso 1 de la Etapa 3 permitió documentar el proceso de evaluación y almacenar la información en la base de datos del SIECA para ser consultada por los responsables de la evaluación y demás directivos de la organización.

En la Tabla 7 se muestran los resultados de la evaluación obtenidos con la realización del Paso 2 de la Etapa 2.

Tabla 7. Resultados de la evaluación del SIGEF II. (Fuente: elaboración propia).

Etapa/Estado	**Estado del proceso**		
	Identificación y Autorización	**Autorización**	**Auditoría**
Etapa 2 Paso 2	Bajo	Bajo	No evaluado

Las recomendaciones obtenidas durante la realización del Paso 3 de la Etapa 2,sobre los criterios que afectaron la evaluación del proceso de Identificación y Autenticación, fueron: la implementación de los estándares Liberty Alliance, Kerberos, OpenPGP, PAPI, EDIFACT, Shibboleth, Passport, DIAMETER, EAP, RADIUS, PANA, SPKI/SDSI, TACACS+, WPA, WEP y 802.1X; los algoritmos de cifrado asimétrico (Diffie-Hellman, RSA, DSA, ElGamal, Rabin); la prueba CAPTCHA y otras soluciones de Autenticación propias de la organización. En el caso del proceso de Autorización los criterios que afectaron la evaluación obtenida fueron la implementación de los estándares: DIAMETER, EAP, RADIUS, PANA, SPKI/SDSI, TACACS+, WPA, WEP y otras soluciones de Autorización propias de la organización.

La evaluación de la seguridad del SIGEF II usando MECA fue realizada por un especialista y tuvo una duración de 25 minutos.

Análisis de la aplicación del modelo en el SITPC.

Los resultados de la aplicación del modelo según las etapas y pasos de la guía de evaluación en el SITPC se describen a continuación:

- La realización del Paso 1 de la Etapa 1 permitió conocer que el SITPC implementa procesos críticos del Tribunal Supremo Popular, Tribunal Provincial y Tribunal Municipal de Cuba.
- La realización del Paso 2 de la Etapa 1 permitió conocer sobre la existencia de especialistas de seguridad que conocían las soluciones de Control de Acceso implementadas en el SI.

- La realización del Paso 3 de la Etapa 1 permitió clasificar como un SI al SI de la organización.
- La realización del Paso 4 de la Etapa 1 permitió confirmar que el modelo podía ser aplicado al SIGEF I.
- La realización del Paso 1 de la Etapa 2 permitió la selección del especialista Manuel Urquiza Rodríguez como responsable de la evaluación.
- La realización del Paso 3 de la Etapa 2 permitió conocer sobre las recomendaciones de la evaluación. Estas detallaron el conjunto de criterios que afectaron la evaluación de la seguridad de los procesos.

La realización del Paso 1 de la Etapa 3 permitió documentar el proceso de evaluación y almacenar la información en la base de datos del SIECA para ser consultada por los responsables de la evaluación y demás directivos de la organización.

En la Tabla 8 se muestran los resultados de la evaluación obtenidos con la realización del Paso 2 de la Etapa 2.

Tabla 8. Resultados de la evaluación del SITPC. (Fuente: elaboración propia).

Etapa/Estado	**Estado del proceso**		
	Identificación y Autorización	**Autorización**	**Auditoría**
Etapa2 Paso 2.	Bajo	Bajo	No evaluado

Las recomendaciones obtenidas durante la realización del Paso 3 de la Etapa 2, sobre los criterios que afectaron la evaluación del proceso de Identificación y Autenticación, fueron: la implementación de los estándares Liberty Alliance, Kerberos, OpenPGP, PAPI, EDIFACT, Shibboleth, Passport, DIAMETER, EAP, RADIUS, PANA, SPKI/SDSI, TACACS+, WPA, WEP y 802.1X; los algoritmos de cifrado asimétrico (Diffie-Hellman, RSA, DSA, ElGamal, Rabin); la prueba CAPTCHA y otras soluciones de Autenticación propias de la organización. En el caso del proceso de Autorización los criterios que afectaron la evaluación obtenida fueron la implementación de los estándares: DIAMETER, EAP, RADIUS, PANA, SPKI/SDSI, TACACS+, WPA, WEP u otras soluciones de Autorización propias de la organización.

La evaluación de la seguridad del SITPC usando MECA fue realizada por un especialista y tuvo una duración de 32 minutos.

Análisis de la aplicación del modelo en el SIRCC.

Los resultados de la aplicación del modelo según las etapas y pasos de la guía de evaluación en el SIRCC se describen a continuación:

- La realización del Paso 1 de la Etapa 1 permitió conocer que el SIRCC implementa procesos críticos de la Cámara de Comercio de Cuba.
- La realización del Paso 2 de la Etapa 1 permitió conocer sobre la existencia de especialistas de seguridad que conocían las soluciones de Control de Acceso implementadas en el SI.
- La realización del Paso 3 de la Etapa 1 permitió clasificar como un SI al SI de la organización.
- La realización del Paso 4 de la Etapa 1 permitió confirmar que el modelo podía ser aplicado al SIRCC.
- La realización del Paso 1 de la Etapa 2 permitió la selección del especialista Julio César Prieto Álvarez como responsable de la evaluación.
- La realización del Paso 3 de la Etapa 2 permitió conocer sobre las recomendaciones de la evaluación. Estas detallaron el conjunto de criterios que afectaron la evaluación de la seguridad de los procesos.
- La realización del Paso 1 de la Etapa 3 permitió documentar el proceso de evaluación y almacenar la información en la base de datos del SIECA para ser consultada por los responsables de la evaluación y demás directivos de la organización.

En la Tabla 9 se muestran los resultados de la evaluación obtenidos con la realización del Paso 2 de la Etapa 2.

Tabla 9. Resultados de la evaluación del SIRCC. (Fuente: elaboración propia).

Etapa/Evaluación	**Estado del proceso**		
	Identificación y Autorización	**Autorización**	**Auditoría**
Etapa 2 Paso 2	Bajo	No evaluado	No evaluado

Las recomendaciones obtenidas durante la realización del Paso 3 de la Etapa 2, sobre los criterios que afectaron la evaluación del proceso de Identificación y Autenticación,fueron: la implementación de los estándares Liberty Alliance, Kerberos, OpenPGP, PAPI, EDIFACT, Shibboleth, AC X.509 (PKI X.509, S/MIME, IPSec, TLS, WAP, SOAP, WSDL, UDDI, WS Security, X.500, LDAP, XACML, XKMS) y Passport; algoritmos de cifrado asimétrico (Diffie-

Hellman, RSA, DSA, ElGamal, Rabin) y otras soluciones de Autenticación propias de la organización.

La evaluación de la seguridad del SIRCC usando MECA fue realizada por un especialista y tuvo una duración de 24 minutos.

Análisis de la aplicación del modelo en el CNPC.

Los resultados de la aplicación del modelo según las etapas y pasos de la guía de evaluación en el CNPC se describen a continuación:

- La realización del Paso 1 de la Etapa 1 permitió conocer que el CNPC implementa procesos críticos Consejo Nacional del Patrimonio Cultural.
- La realización del Paso 2 de la Etapa 1 permitió conocer sobre la existencia de especialistas de seguridad que conocían las soluciones de Control de Acceso implementadas en el SI.
- La realización del Paso 3 de la Etapa 1 permitió clasificar como un SI al SI de la organización.
- La realización del Paso 4 de la Etapa 1 permitió confirmar que el modelo podía ser aplicado al CNPC.
- La realización del Paso 1 de la Etapa 2 permitió la selección del especialista Robin Sencial Terrero como responsable de la evaluación.
- La realización del Paso 3 de la Etapa 2 permitió conocer sobre las recomendaciones de la evaluación. Estas detallaron el conjunto de criterios que afectaron la evaluación de la seguridad de los procesos.
- La realización del Paso 1 de la Etapa 3 permitió documentar el proceso de evaluación y almacenar la información en la base de datos del SIECA para ser consultada por los responsables de la evaluación y demás directivos de la organización.

En la Tabla 10 se muestran los resultados de la evaluación obtenidos con la realización del Paso 2 de la Etapa 2 y el Paso 1 de la Etapa 4.

Tabla 10. Resultados de la evaluación de CNPC. (Fuente: elaboración propia).

Etapa/Evaluación.	**Estado del proceso**		
	Identificación y Autorización.	**Autorización.**	**Auditoría.**
Etapa 2 Paso 2.	Alto	Alto	Alto

No se obtuvieron recomendaciones durante la realización del Paso 3 de la Etapa 2 debido a que todos los procesos fueron evaluados de Alto.

La evaluación de la seguridad del CNPC usando MECA fue realizada por un especialista y tuvo una duración de 27 minutos.

3.4 Análisis sobre la evaluación de la seguridad del Control de Acceso.

El análisis por procesos de los SI evaluados se describe a continuación:

En el proceso de **Identificación y Autenticación** se pudo constatar que:

- No se implementan estándares para el intercambio de mensajes de Identificación y Autenticación en función de lograr mayor nivel de integración con otros sistemas.
- Existen SI que presentan deficiencias en la implementación de algoritmos criptográficos para el envío, recepción y almacenamiento de información sensible.

En el proceso de **Autorización** se obtuvo que:

- Existen deficiencias relacionadas con la implementación de estándares para el intercambio de mensajes de Autorización.
- La gestión de privilegios sobre los recursos del nivel de sistema y los recursos del nivel de base de datos se realiza de forma independiente.
- En necesario fortalecer el mecanismo de administración de sesiones de usuario.

En el proceso de **Auditoría** se pudo concluir que:

- Existen sistemas que no documentan eventos críticos sucedidos en el entorno organizacional.
- Existen sistemas que no proveen la gestión dinámica de registro de eventos.
- Existen SI cuyos datos carecen de la completitud necesaria, limitando los análisis sobre la seguridad del Control de Acceso del sistema.

Las carencias identificadas en cada uno de los procesos afectaron la evaluación de los SI que conformaron la muestra. Los estados de los procesos de Identificación y Autenticación así como de Autorización fueron mayormente de Bajo. El proceso de Auditoría fue mayormente no evaluado lo cual significó que no fue implementado en la mayoría de los sistemas de la muestra.

Las recomendaciones reflejaron el conjunto de soluciones de Control de Acceso no implementadas en cada uno de los procesos anteriormente descritos.

3.5 Valoración económica del modelo.

La realización del modelo tuvo una duración de 24 días hábiles e involucró a un especialista del centro CEGEL a tiempo completo. La tarifa horaria definida fue de 12 pesos/hora. El costo directo fue de $8502.56.

La evaluación mediante el MECA permitió la disminución de costos directos de materiales y de mano de obra en comparación con aquellos generados durante el proceso de evaluación de Calisoft. Contribuyó al ahorro de recursos monetarios destinados a la contratación de servicios de evaluación de la seguridad, la adquisición de las tecnologías necesarias así como los costos asociados a la depreciación de estas últimas.

3.6 Conclusiones parciales.

La aplicación del modelo propuesto evidenció su contribución a la eficiencia de la evaluación.

- El análisis de los métodos de validación empleados reflejaron que la evaluación es un aspecto difícil de medir debido a la ausencia de herramientas que permitan hacerlo.
- La aplicación del pre-experimento permitió constatar que la evaluación mediante el modelo contribuyó a la eficiencia de la evaluación de los SI que conformaron la muestra.
- La consulta a expertos permitió constatar que los especialistas coinciden en que el modelo es eficiente para la evaluación de los SI de centros productivos de la UCI.

CONCLUSIONES

Sobre los resultados obtenidos durante el desarrollo de la investigación se concluye lo siguiente:

- El análisis sobre los métodos científicos empleados permitió establecer que no existía ningún modelo para la evaluación de la seguridad del Control de Acceso de los SI de centros productivos de la UCI.
- El modelo propuesto permitió integrar y describir las relaciones entre los componentes que conformaron la evaluación de la seguridad del Control de Acceso.
- La aplicación del modelo a cinco de los SI del CEGEL de la Facultad 3 permitió constatar que se contribuyó a la disminución del tiempo y la cantidad de especialistas necesarios para la evaluación de la seguridad de los procesos de Identificación y Autenticación, Autorización y Auditoría.
- El modelo permitió la evaluación eficiente de la seguridad del Control de Acceso si se compara con los modelos, estándares y protocolos más aplicados en la actualidad según la bibliografía consultada.

RECOMENDACIONES

Se recomienda para la continuidad de la investigación y en particular para la mejora del modelo propuesto:

- Establecer un mecanismo para la gestión dinámica de indicadores y criterios de evaluación basado en soluciones novedosas para la evaluación de la seguridad del Control de Acceso.
- Especificar soluciones de Control de Acceso a partir del modelo propuesto para lograr su adaptabilidad a los diferentes escenarios, en función de la criticidad de los recursos utilizados.
- Establecer un mecanismo para la selección del responsable de la evaluación basado en competencias relacionadas con la seguridad del Control de Acceso de la información.

REFERENCIAS BIBLIOGRÁFICAS

ASTELS, D., MILLER, G. AND NOVAK, M. *The Practical Guide to Extreme Programming*. Edtion ed. USA, 2010. ISBN 0130674826

BARABANOV, R., KOWALSKI, S. AND YNGSTRÖM, L. Information Security Metrics State of the Art. DSV Report series, 2011 2011, vol. 11-007.

BARYOLO, O.G. CAEM: Modelo de Control de Acceso para Sistemas de Información en entornos multidominios. In *Tecnología.* La Habana: Universidad de las Ciencias Informáticas, 2012, vol. Doctor en Ciencias Técnicas, p. 122.

BRODERICK, J.S. ISMS, security standards and security regulations. Information Security Technical Report, 2006 2006, vol. 11, no. 1, p. 26-31.

BROWN, A., FOX, B., HADA, S., LAMACCHIA, B. AND MARUYAMA, H. SOAP Security Extensions: Digital Signature. In W3C. *W3C NOTE.* United States of America: International Business Machines Corporation, Microsoft, 2001, p. 7.

CALHOUN, P.R., ZORN, G., SPENCE, D. AND MITTON, D. Diameter Network Access Server Application. In *Request for Comments (RFC)* Network Working Group, 2005, p. 85.

CAÑAVATE, A.M. Sistemas de información en las empresas. Hipertext.net, 2003 2003, vol. 1, p. 27.

CÁNOVAS, O. AND CÁNOVAS, O. Propuesta de una infraestructura de clave pública y su extensión mediante un sistema de gestión distribuida de credenciales basado en delegación y roles. *Delegation in Distributed Systems: Challenges and Opportunities* [Type of Work]. 2002, vol. 66-67, pp. 4. Available from Internet:<rediris.com/difusion/publicaciones/boletin/66-67/ponencia14.pdf>.

CANTOR, S. Shibboleth Architecture. In. Ohio: The Ohio State University, 2005, vol. Working Draft 02, p. 19.

CANTOR, S. AND KEMP, J. Liberty Protocols and Schema Specification Version 1.1. Liberty Alliance Project. In. USA, 2003, p. 48.

CHOUDHURY, S., BHATNAGAR, K. AND HAQUE, W. *Public key infrastructure implementation and design*. Edtion ed.: John Wiley & Sons, Inc., 2002. ISBN 0764548794.

CIUREA, C. A Metrics Approach for Collaborative Systems. . Informatica Economica, 2009 2009, vol. 13, no. 2, p. 41-49.

COMER, D.E. Redes Globales de información con Internet y TCP/IP 1995, vol. 3, p. 517.

COMUNICACIONES, M.D.L.I.Y.L. Resolución No. 127/2007. In.: Gaceta Oficial, 2007, p. 2.

CRITERIA, C. Common Criteria for Information Technology Security Evaluation. In., 2012, p. 321.

DAVIS, C.R. *Ipsec: Securing Vpns* Edtion ed.: McGraw-Hill Professional ©2001, 2001. ISBN 0072127570.

DIERKS, T. AND ALLEN, C. The TLS Protocol. In *Request for Comments (RFC) 2246.* 1999, p. 80.

DUJMOVI'C, J. A Method for Evaluation and Selection of Complex Hardware and Software Systems. In *CMG 96 Proceedings.* 1996, vol. 1, p. 368--378.

ELLISON, C., FRANTZ, B., LAMPSON, B., RIVEST, R., THOMAS, B. AND YLONEN, T. SPKI Certificate Theory. In *Request for Comments (RFC) 2693.* Network Working Group, 1999, p. 43.

ESTADO, C.D. Decreto Ley 281/11 In. Cuba: Gaceta Oficial de la República de Cuba, 2011, vol. 010, p. 6.

ESTÉBAN, J.J.M. Metodología para la incorporación de medidas de seguridad en sistemas de información de gran implantación. Confianza dinámica distribuida y regulación del nivel de servicio para sistemas y protocolos de internet. . In. Madrid: Universidad de Madrid, 2004, vol. Doctor, p. 177.

FINSETH, C.A. An Access Control Protocol, Sometimes Called TACACS. In *Request for Comments (RFC) 1492.* University of Minnesota, 1993, p. 21.

FOUNDATION 2008.

G., M. AND J., M. Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA. In *Computer Vision and Pattern Recognition, 2003. Proceedings.*, 2003, vol. 1, p. 134-141.

GARFINKEL, S. *PGP: Pretty Good Practice*. Edtion ed. Unite States of America, 1995. ISBN 1-56592-098-8.

GARZARO, M.G. Information Technology Infrastructure Library (ITIL). 2007, vol. No. 218571-5638, no. 1, pp. 4.

HUERTA, A.V. 2004. El Sistema de Gestión de la Seguridad de la Información. Códigos de buenas prácticas de seguridad. La nueva norma UNE 71502. In *Proceedings of the UNE-ISO/IEC 17799*, Valencia, 30/09/2014 2004, G. S2 Ed., Valencia, 29.

HURWITZ, J., BLOOR, R., BAROUDI, C. AND KAUFMAN, M. *Service Oriented Archtecture for dummies*. Edtion ed. Indianápolis. Indiana: Wiley Publishing, Inc., 2007.

IEEE Distortion estimation techniques in solving visual CAPTCHAs. Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2004.

IETF. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. In *Standards Track* USA: Network Working Group, 2002, p. 129.

INFOBAE. Febrero, un mes plagado de ataques informáticos en los EEUU. In *Infobae.* Argentina: Tecno, 2013, vol. Tecno, p. 1.

ITGI. Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa. In. USA: ITGI, 2008, p. 130.

ITU-T. Data Networks and open system communications security. In *Information Technology - Open System Interconnection - Security Frameworks for Open System: Overview.* USA: ITU, 1996, p. 28.

ITU-T, I.I.-. Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks 2005.

JAQUITH, A. The Security of Applications: Not All Are Created Equal. In. New York, 2002, p. 12.

KOMAR, B. *Windows Server® 2008 PKI and Certificate Security*. Edtion ed.: O'Reilly Media, Inc., 2010. ISBN 0735646406.

KORMANN, D.P. AND RUBIN, A.D. Risks of the Passport Single Signon Protocol. In *Computer Networks.* Elsevier Science Press, 2000, vol. 33, p. 51-58.

LAUDON, K.C. AND LAUDON, J.P. *Sistemas de Información Gerencial*. Translated by M.I. SYSTEM. Edtion ed. Mexino: Pearson Educacion Inc., 2004. ISBN 0-13-101498-6.

LEHEMBRE, G. Seguridad Wi-Fi – WEP, WPA y WPA2. Hakin9 nro 1, 2006.

MELL, P., SCARFONE, K. AND ROMANOSKY, S. The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems. In NIST. *Computer Security.* EEUU: NIST, 2007, p. 27.

MOELLER, R.R. *COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework*. Edtion ed. Canada, 2007. ISBN 978-0-471-74115-2.

MOFFAT MATHEWS, R.H. Evolution of Wireless LAN Arquitecture to IEEE 802.11i (WPA2). 2007, pp. 6.

NIST NVD Common Vulnerability Scoring System Support NIST National Institute of Standards and Technology, 2007.

OASIS. eXtensible Access Control Markup Language (XACML) Version 2.0. In. USA, 2005, p. 47.

OWASP. The Ten Most Critical Web Application Security Risks. In *OWASP Top 10-2010 rc1.* Unite States of America: The Open Web Application Security Project, 2010, p. 21.

P. CALHOUN, J.L., E. GUTTMAN, G. ZORN, AND J. ARKKO Diameter Base Protocol. Request for Comments (RFC) 3588, 2003.

POSIX. Standard for Information technology-Portable Operating Systems Interface (POSIX®)-Part 1: System Application Program Interface (API). In *System Application Program Interface (API).* USA, 2000, p. 200.

PRESSMAN, R.S. *Ingeniería de Software. Un enfoque práctico*. Translated by D. INCE; edited by D. INCE. Edtion ed. USA: Darrel Ince, 2005.

R. ALFIERI, R.C., V. CIASCHINI, L. DELL'AGNELLO, A. GIANOLI, F. SPATARO, F. BONNASSIEUX, P. BROADFOOT, G. LOWE, G. CORNWALL, J. JENSEN, D. KELSEY, A. FROHNER, D.L. GROEP, W. SOM DE CERFF, M. STEENBAKKERS, G. VENEKAMP, D. KOURIL, A. MC-NAB, O. MULMO, M. SILANDER, J. HAHKALA, AND K. LORENTEY. Managing dynamic user communities in a grid of autonomous resources. In Proceedings of Conference for Computing in High Energy and Nuclear Physics 2003.

RIGNEY, C., RUBENS, A., SIMPSON, W. AND WILLENS, S. Remote Authentication Dial In User Service (RADIUS). In *Request for Comments* IETF, 2000, p. 46.

RIVEST, R.L. The MD5 Message-Digest Algorithm. In *Request for Comments (RFC) 1321.* Cambridge, MA, 1992, vol. 2014, p. 21.

RIVEST, R.L. AND LAMPSON, B. SDSI { A Simple Distributed Security Infrastructure. 1996, pp. 37. Available from Internet:<http://www.schuba.com/christoph/pub/courses/it251-ss2001/papers/sdsi.pdf>.

ROJO., R.C. AND LÓPEZ, D.R. Papi: una propuesta de RedIris para el acceso ubicuo a recursos de información. In *El Profesional de la Información.* 2001, vol. 10, p. 11-14.

SANS. SANS Institute InfoSec Reading Room. In *THE COMMON CRITERIA ISO/IEC 15408– THE INSIGHT, SOME THOUGHTS, QUESTIONS AND ISSUES.* United States of America, 2013, p. 13.

SCHMIDT, D.C. Model Driven Engineering. *IEEE Computer Society* [Type of Work]. 2006, vol. 39, pp. 25-31. Available from Internet:<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.9720&rep=rep1&type=pdf>.

SENN, J.A. *Análisis y Deseño de Sistemas de Información* Translated by U. MCGRAW-HILL INC. Edtion ed. USA: McGraw-Hill, 2001. ISBN 0-07-056236-9.

SOLMS, R.V. *Information security management (3): the Code of Practice for Information Security Management (BS 7799)*. Edtion ed. British: MCB UP Ltd, 1998. 224 - 225 p.

STANDARD, I. AND TECHNIQUES, I.T.-S. Code of practice for information security management. International Standard

Information technology -Security techniques, ISO/IEC 2005., 2005.

STANDARDS., F.I.P. FIPS Publication 200: Minimum Security Requirements for Federal Information and Information System. . In *Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.* U.S, 2006, vol. Publication 200 p. 11.

THURROTT, P. Windows XP-Passport Integration. Windows & .NET Magazine, 2001.

TORGERSON, W.S. *Theory and methods of scaling*. Edtion ed. Michigan: Wiley, 1958.

WANGHAM, M.S., FRAGA, J.D.S., MELLO, E.R.D. AND MILANEZ, J. Um Modelo para o Gerenciamento Federado do SPKI/SDSI atrav´es do Servic¸o XKMS. In *Livro de Minicursos.* tele.sj.ifsc.edu.br, 2005, p. 14.

WERNER, G. Seguridad XML: Su Importancia en el E-Comercio. Advantage Security, 2001, p. 10.

ZIMMERMAN, P. *PGP User's Guide*. Edtion ed. Cambridge, 1995. ISBN 0-262-74017-6

ANEXOS

Anexo 1. Encuesta aplicada a evaluadores de la seguridad del Control de Acceso.

Encuesta a evaluadores de la seguridad del Control de Acceso

Nombre(s) y Apellidos: _____

Entidad/Organización en la que labora: _____

Rol que desempeña en la Entidad/Organización:_____

Años de experiencia en la evaluación de la seguridad: _____

Breve descripción

El Control de Acceso es el proceso de restringir y auditar el acceso de los usuarios (persona, rol, sistema, entre otros) a los recursos (información, sistema, objetos, ficheros, entre otros) gestionados por los Sistemas de Información (SI) de las organizaciones. Este mecanismo se lleva a cabo a través de la concepción integrada de los procesos de Identificación y Autenticación, Autorización y Auditoría.

La evaluación de la seguridad del Control de Acceso contribuye a orientar y determinar las acciones de gestión adecuadas para la administración de los riesgos concernientes a la seguridad de los SI de las organizaciones.

Desarrollo

1. ¿Se lleva a cabo en la entidad la evaluación de la seguridad de los procesos de Identificación y Autenticación, Autorización y Auditoría de los SI? __ Sí __ No
   1.1 En caso afirmativo, ¿puede describir brevemente este mecanismo de evaluación?

2. Exprese la utilización o no de las normas o estándares, recomendaciones, decretos, guía de buenas prácticas, resoluciones, metodologías o marcos de trabajo siguientes para la evaluación de la seguridad de los procesos de Identificación y Autenticación, Autorización y Auditoría de algunos de los SI de centros productivos de la UCI. Utilice la escala de valores (0 - 1) de acuerdo a los siguientes criterios: 0 – No se utiliza, 1 – Se utiliza.

Norma, recomendación, decreto, guía de buenas prácticas, resolución, metodología o marcos de trabajo	**Utilización (0-1)**
ISO/IEC 9126	
ISO/IEC 25000	
ISO/IEC 27002	
ISO/IEC 15408 Criterio Común	
COBIT	
ITIL	
NIST SP 800-53, 800-12	
FIPS PUB 140-2	
OWASP Top 10 – 2010, Guías de Pruebas de 2008	
Res. 127/2007 MIC	
Decreto Ley 281	

3. Indique qué tiempo se tarda en evaluar la seguridad del Control de Acceso de un SI.

Calisoft	MECA
( ) Más de 6 horas. Tiempo aproximado: ____	( ) Más de 6 horas. Tiempo aproximado: ____
( ) Entre 1 hora y 6 horas. Tiempo aproximado: ___	( ) Entre 1 hora y 6 horas. Tiempo aproximado: ___
( ) De 10 a 20 minutos. Tiempo aproximado: ___	( ) De 10 a 20 minutos. Tiempo aproximado: ___
( ) Entre 10 y 20 segundos.	( ) Entre 10 y 20 segundos.

4. Indique el grado de subjetividad de la evaluación de la seguridad del Control de Acceso de un SI.

Calisoft	MECA
( ) Bajo	( ) Bajo
( ) Medio	( ) Medio
( ) Alto	( ) Alto

Anexo 2. Cuestionario aplicado a expertos.

MODELO PARA LA EVALUACIÓN DEL CONTROL DE ACCESO

Cuestionario para Expertos

Nombre(s) y Apellidos _____

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

Grado científico: _____ Años de experiencia en Seguridad Informática: _____

Cargo: _____**Entidad**:_____**Certificaciones obtenidas relacionadas con la seguridad informática**: _____**Cantidad de publicaciones científicas relacionadas con la seguridad informática**:_____**Cantidad de eventos científicos en los que ha participado**: _____

Breve descripción

Las carencias identificadas en los modelos de evaluación de la seguridad del Control de Acceso de los SI de centros productivos de la UCI, incrementados por la falta de integración entre sus componentes, constituyen los antecedentes del Modelo para la Evaluación de la Seguridad del Control de Acceso (MECA). La interrelación de los componentes del modelo permite evaluar eficientemente los procesos del Control de Acceso. La Figura muestra los componentes del modelo, así como su integración para llevar a cabo la evaluación de la seguridad del Control de Acceso del SI de centros productivos de la UCI.

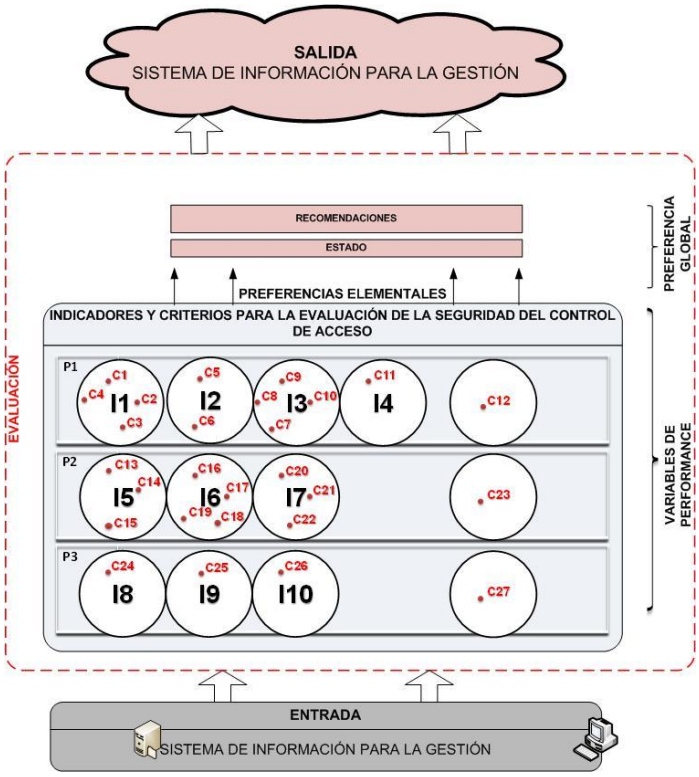

Figura 1. Modelo para la Evaluación del Control de Acceso.

El MECA posee las siguientes características generales:

- Se definen **10 indicadores** para la evaluación de la seguridad del Control de Acceso de los SI de centros productivos de la UCI. Estos indicadores sintetizan los controles de las principales directrices en el área de la evaluación de la seguridad del Control de Acceso de aplicación internacional.
- Se definen **27 criterios** medibles que describen las diferentes soluciones de Control de Acceso y contribuyen a la evaluación de los procesos de Identificación y Autenticación, Autorización y Auditoría.
- El proceso de evaluación se realiza mediante la adaptación del **algoritmo LSP** a las condiciones del modelo, lo cual permite conocer el estado (Bajo, Medio o Alto) de cada uno de los procesos del Control de Acceso y conocer sobre los criterios que incidieron en los resultados obtenidos.

Las entradas del modelo son conformadas por los SI de centros productivos de la UCI que informatizan procesos de diferentes organizaciones que utilizan un mecanismo de Control de Acceso de la información.

Las salidas del modelo se reflejan en el estado (Bajo, Medio o Alto) de los procesos de Identificación y Autenticación, Autorización y Auditoría de los SI y las recomendaciones derivadas del análisis de los resultados de la evaluación.

Desarrollo

1. Exprese su conformidad con respecto a la selección de los 10 indicadores para la evaluación de los procesos de Identificación y Autenticación, Autorización y Auditoría propuestos en el modelo. Utilice la escala de valores (1 - 5) de acuerdo a los siguientes criterios:

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

Indicador	**Evaluación (1-5)**
I1. Empleo de estándares para el intercambio de información.	
I2. Empleo de métodos criptográficos y mecanismos seguros de comunicación (envío, recepción y almacenamiento de información sensible).	
I3. Empleo de soluciones para la federación de identidades entre dominios.	
I4. Empleo de pruebas desafío-respuesta en los eventos donde se necesite determinar cuando el usuario es una persona o no.	
I5. Empleo de estándares para la representación de la información de autorización.	
I6. Empleo de protocolos para la gestión de autorización de la red.	
I7. Empleo de estándares de Control de Acceso de la red.	
I8. Empleo de controles internos propuestos por marcos de trabajo de aplicación internacional.	
I9. Empleo de modelos para la gestión de la trazabilidad.	
I10. Empleo de estándares para la gestión de trazas.	

1.1. ¿Añadiría algún otro indicador a la lista anterior? __ Sí __ No. En caso afirmativo, ¿cuál o cuáles serían?_____

2. Considera que los criterios de evaluación propuestos reflejan la efectividad de los 10 indicadores para la evaluación de los procesos de Identificación y Autenticación (A1), Autorización (A2) y Auditoría (A3) de los SI de centros productivos de la UCI propuestos en el modelo.

Conteste Sí o No para cada criterio.

2.1 Exprese el nivel de criticidad de los 27 criterios de evaluación agrupados en los 10 indicadores propuestos en el modelo. Utilice la escala de valores (1 - 4) de acuerdo a los siguientes criterios: No crítico (1), Poco crítico (2), Crítico (3), Muy crítico (4).

Indicador (Proceso)	**Criterios de Evaluación**	**¿Efectividad? (Sí-No)**	**Nivel de Criticidad (1-4)**
I1 (P1)	C1. Implementación del estándar Kerberos.		
	C2. Implementación del estándar OpenPGP.		

	C3. Implementación del estándar EDIFACT.		
	C4. Implementación del estándar AC X.509 (PKI X.509, S/MIME, IPSec, TLS, WAP, SOAP, WSDL, UDDI, WS Security, X.500, LDAP, XACML, XKMS).		
I2 (P1)	C5. Implementación de algoritmos de cifrado simétrico (DES-TDES, RC (2/4/5/6), AES, IDEA, SEAL, Blowfish, Serpent).		
	C6. Implementación de algoritmos de cifrado asimétrico (Diffie-Hellman, RSA, DSA, ElGamal, Rabin).		
I3 (P1)	C7. Implementación del estándar Passport.		
	C8. Implementación del estándar Shibboleth.		
	C9. Implementación del estándar Liberty Alliance.		
	C10. Implementación del estándar PAPI.		
I4 (P1)	C11. Implementación de la prueba CAPTCHA.		
*	C12. Otros.		
I5 (P2)	C13. Implementación del estándar SPKI/SDSI.		
	C14. Implementación del estándar SAML.		
	C15. Implementación del estándar TACACS+.		
I6 (P2)	C16. Implementación del estándar RADIUS.		
	C17. Implementación del estándar DIAMETER.		
	C18. Implementación del estándar WEP.		
	C19. Implementación del estándar WPA.		
I7 (P2)	C20. Implementación del estándar 802.1X.		
	C21. Implementación del estándar PANA.		
	C22. Implementación del estándar EAP.		
*	C.23.Otros.		
I8 (P3)	C24. Implementación de marcos de trabajo COSO.		
I9 (P3)	C25. Implementación de modelos para la gestión de trazas MDE.		
I10 (P3)	C26. Implementación de estándares para la gestión de trazas POSIX 1003.1q.		
*	C.27.Otros.		

*Criterio adicional. Este criterio representa las soluciones de Control de Acceso propias de los SI desarrolladas por la propia organización.

2.2 ¿Añadiría algún otro criterio a la lista anterior? __ Sí __ No

En caso afirmativo, ¿cuál o cuáles serían? _____

3. Evalúe el MECA. Utilice la escala de valores (1 - 5) de acuerdo a los siguientes criterios:

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

Criterio	Significado	Evaluación (1-5)
Integración	Permite la gestión integrada de los controles para la evaluación de la seguridad del Control de Acceso.	
Síntesis	Presenta una adecuada síntesis de los controles para la evaluación del Control de Acceso de los SI de centros productivos de la UCI.	
Mejora Continua	Posee un enfoque de gestión y de procesos continuos.	
Medición descriptiva	Describe adecuadamente el estado de la seguridad de los procesos del Control de Acceso del SI a partir de la criticidad de los criterios que cumple y las recomendaciones sobre aquellos que afectan la evaluación obtenida.	
Generalización	Es aplicable a una gran variedad de SI.	

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

Anexo 3. Expertos involucrados en la validación del cuestionario.

Nombre(s) y Apellidos	Entidad	Cargo	Años de Experiencia
Yadier Perdomo Cuevas	Centro de Identificación y Seguridad Digital	Subdirector	6
Yasser Azan Basallo	Centro de Telemática	Profesor	4
Darién García Tejo	Centro de Investigaciones de Tecnologías Integradas	Especialista	4

Anexo 4. Encuesta aplicada a evaluadores de la seguridad del Control de Acceso.

Encuesta a evaluadores de la seguridad del Control de Acceso

Nombre(s) y Apellidos: _____
Entidad/Organización en la que labora: _____
Rol que desempeña en la Entidad/Organización:_____
Años de experiencia en la evaluación de la seguridad: _____

Breve descripción

El Control de Acceso es el proceso de restringir y auditar el acceso de los usuarios (persona, rol, sistema, entre otros) a los recursos (información, sistema, objetos, ficheros, entre otros) gestionados por los Sistemas de Información (SI) de las organizaciones. Este mecanismo se lleva a cabo a través de la concepción integrada de los procesos de Identificación, Autenticación, Autorización y Auditoría.
La evaluación de la seguridad del Control de Acceso contribuye a orientar y a determinar las acciones de gestión adecuadas para la administración de los riesgos concernientes a la seguridad de los SI de las organizaciones.

Desarrollo

1. Indique qué tiempo se tarda en evaluar la seguridad del Control de Acceso de un SI.
2.

Calisoft	MECA
( ) Más de 6 horas. Tiempo aproximado: ___	( ) Más de 6 horas. Tiempo aproximado:
( ) Entre 1 hora y 6 horas. Tiempo aproximado: ___	( ) Entre 1 hora y 6 horas. Tiempo aproximado:
( ) De 10 a 20 minutos. Tiempo aproximado: ___	( ) De 10 a 20 minutos. Tiempo aproximado:
( ) Entre 10 y 20 segundos.	( ) Entre 10 y 20 segundos.

1. Indique la cantidad de especialistas que son necesarios para la evaluación de la seguridad del Control de Acceso de un SI.

Calisoft	MECA
( ) Más de 6 especialistas	( ) Más de 6 especialistas
( ) 2-6 especialistas	( ) 2-6 especialistas
( ) 1 especialista	( ) 1 especialista

Anexo 5. Recursos necesarios para la adopción del SIECA.

La adopción del SIECA implica el uso de recursos tecnológicos y humanos. Según la distribución de Gartner en (Rojo. and López, 2001) los recursos necesarios para la adopción del SIECA se especifican a continuación:

Clasificación	Recursos	Cantidad
Software	SIECA	1
	PostgreSQL 9.1	1
Hardware	Servidor	1
	Estación de trabajo	1
Personal	Especialista de seguridad	1
*Se asume que el servidor de base de datos puede ser instalado y configurado en la propia estación de trabajo donde sea ejecutado el SIECA.		