Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC 27002

Diana C. Franco
Universidad de los Llanos, Villavicencio, Colombia, dfranco@unillanos.edu.co

Cesar D. Guerrero
Universidad Autónoma de Bucaramanga, Bucaramanga, Colombia, cguerrer@unab.edu.co

RESUMEN

La gestión de la seguridad de la información es un factor cada vez más determinante en la competitividad de las organizaciones. La gestión del riesgo y el aseguramiento de la información se apoyan en la aplicación de normas internacionales como el estándar ISO/IEC 27002. El proceso de implementación de la norma y su gestión permanente se facilita a través del uso de software que en la actualidad es mayoritariamente comercial. La restricción de idioma, poca documentación y limitada disponibilidad de software abierto que se ajuste a requerimientos particulares de organizaciones en el contexto latinoamericano, limita la aplicación de la norma y la efectividad de su uso. Este artículo presenta una plataforma web abierta denominada *SGCSI* que permite apoyar la gestión de controles de seguridad de la información de acuerdo con el estándar ISO 27002. Tras la evaluación comparativa del uso de la plataforma por parte de expertos y aprendices en seguridad, se pudo evidenciar su efectividad en la auditoria sobre el cumplimiento de los 32 objetivos de control establecidos por la norma.

Palabras claves: ISO/IEC 27002, seguridad de la información, auditoría de seguridad.

ABSTRACT

The information security management is an increasingly decision factor in the competitiveness of organizations. Risk management and information assurance are based on the application of international standards such as ISO/IEC 27002. The process of implementation of the standard and its management is facilitated through the use of software that currently is mostly commercial. Language restrictions, little documentation, and limited availability of open software to fit particular requirements of organizations in the Latin-American context, limits the application of the standard and the effectiveness of its use. This paper presents an open software web platform called SGCSI that supports the management of information security controls in accordance with the ISO 27002 standard. After a comparative evaluation of the use of the platform by security experts and trainees, it is shown the effectiveness in the audit about the compliance of the 32 control objectives established by the standard.

Keywords: ISO/IEC 27002, information security, security audit.

1. INTRODUCCIÓN

En el ejercicio profesional, muchos administradores de seguridad se limitan a realizar algunas actividades de protección aisladas, a su vez, un alto porcentaje de organizaciones no realiza ningún tipo de prueba de seguridad al año. Esto se da en gran parte porque las herramientas de administración de seguridad existentes son complejas a la hora de configurar, administrar, están ligadas a la plataforma operativa, son genéricas, con restricciones de idioma, sin la documentación, ni acceso a los códigos fuentes, no enfocadas en las necesidades de la región ni en el tipo de organización y además algunas son costosas. Este artículo se origina desde esta necesidad identificada, enmarcada por la ausencia de herramientas que apoyen la gestión de controles de seguridad de la información, basadas en directrices o normas internacionales, como el estándar ISO 27002, en organizaciones de la región Orinoquia y otras a nivel colombiano y latinoamericano.

De igual manera se pretende que se convierta en una herramienta académica para el aprendizaje y desarrollo de prácticas de laboratorio en programas académicos asociados con seguridad informática; generando una solución pedagógica y tecnológica que apoye procesos de aprendizaje autónomos y asistidos.

En la sección 2 se presenta el estado del arte de investigaciones y herramientas orientadas a apoyar la gestión de la seguridad de la información. La sección 3 presenta la metodología desarrollada para construir la plataforma web. Posteriormente, en la sección 4 se presenta el análisis del diagnóstico realizado con estudiantes y expertos en seguridad informática como base para el desarrollo de la herramienta. La sección 5 muestra la herramienta y su funcionalidad y finalmente en la sección 6 se presentan conclusiones y trabajos futuros.

2. ESTADO DEL ARTE

Según Knapp, et al (2009), se han definido algunos modelos de buenas prácticas, sin embargo están más dirigidos hacia "la creación de una cultura de seguridad de la información facilitando el pensamiento conceptual y la argumentación del recurso humano en las organizaciones", que a una definición estricta y especifica de políticas centradas en la seguridad de procesos corporativos de los diferentes tipo de organización y su interrelación con el recurso humano.

En el contexto internacional existen modelos estandarizados para buenas prácticas de seguridad como ISO 27002, OSSTMM, COBIT, entre otros y mecanismos basados en software para implantación de Sistemas de Gestión de Seguridad de Información (SGSI); estos son muy globales y genéricos (ver Tabla 1).

Tabla 1. Contrastación de los sistemas de apoyo a SGSI existentes

Herramienta	BABEL	E-PULPO	MEYCOR COBIT KP	SECUWARE SECURITY	GLOBALSGSI	GXSGSI	GAP ISO 27001	SECURIA SGSI
Creador	ÁRTICA	INGENIA	DATASEC	SECUWARE	AUDISEC	SIGEA	SIGEA	SECURIA
Licencia	Open Source	GNU GPL v2	Comercial	Comercial	Comercial	Comercial	Comercial	GPL v2
Sistemas operativos en los que funciona	GNU/Linux, IBM AIX, Sun Solaris, OpenSolaris, SPARC, Windows	GNU/Linux	Windows	Windows	Windows	Windows	Windows	GNU/Linux, Windows
Estándares de seguridad	SOX/LOPD, ISO 27001, COBIT	ITIL, LOPD, ENS, ISO 27001, ISO 27002, ISO 20000	ISO I27001, COBIT, ISO 27002, ISO 20000, COSO I, COSO II	Ninguno. Suite empresarial para proteger la información en el puesto de trabajo.	ISO 27001	UNE 71502, ISO 27001	ISO 27001, ISO 27002	ISO 27001
Gestión documental	✓	✓	✓	×	✓	×	×	✓
Gestión de incidencias	✓	✓	✓	×	✓	✓	×	✓
Auto-evaluación de controles	✓	×	✓	×	✓	×	×	✓

Como se puede observar en la Tabla 1, las tendencias en la mayoría de herramientas de software existentes para el apoyo de la administración de información de los Sistemas de Información (SI) de una organización son propias de firmas de auditoría, son restringidas y costosas. Al ser desarrolladas por este tipo de firmas, la licencia es de tipo comercial, lo cual restringe en cierta manera su uso debido a los altos costos de licenciamiento. También se ha detectado que todas están basados en el estándar ISO 27001 y algunas tienen incorporados otros estándares como COBIT, ITIL, LOPD, pero son muy pocas las que están directamente relacionadas con ISO 27002. Con respecto a la plataforma operativa, se evidencia que tan solo dos herramientas funcionan en sistemas GNU/Linux y que la mayoría vienen solo con soporte a sistemas comerciales. De otro lado, se ha identificado que

funcionalidades como la gestión documental, la gestión de incidencias y la auto-evaluación de controles deben ser aspectos comunes y mínimos con los cuales debe contar una herramienta de este tipo.

Aparte de las herramientas analizadas, se conocen trabajos relacionados con ISO/IEC 27002; como el caso de Iqbal, et al (2009) en el que se presentan los aspectos a tener en cuenta para el desarrollo de una base de datos que permita un uso eficaz de la norma ISO/IEC 27002. Se analiza el uso de la norma y también investiga un método sistemático para la construcción de bases de datos de normas ISO para la seguridad de la información. Dentro de las consideraciones básicas analizaron que los usuarios de la base de datos deben estar clasificados como usuarios finales y un usuario administrador, donde los usuarios finales son los administradores de seguridad de la información de la organización y desarrolladores de SGSI mientras que el administrador establece y administra la base de datos. Definieron para la base de datos usos básicos y avanzados, dentro de los cuales se encuentran: especificación del perfil de estándar, recuperación de términos y definiciones, referenciar las diferencias entre las versiones del estándar, apoyo en la verificación de controles de seguridad y renovación automática de esos controles.

Klaic, et al (2011) brinda una visión del estado actual y tendencias en el campo de los métodos y herramientas para el apoyo a los procesos de planificación, implementación y ejecución de la política de seguridad de la información.

El trabajo de Horváth, et al (2009) está relacionado con la experiencia de un caso de aplicación de controles de seguridad basados en ISO/IEC 27002 para organizaciones pequeñas, en el cual se aplican específicamente 88 de los 133 controles. Establece que no necesariamente se deben aplicar todos los controles a una empresa, ya que esto depende de la naturaleza, tamaño, objetivos de la organización.

En el contexto regional y nacional, son escasos los antecedentes de herramientas de administración de información de controles de seguridad informática. Esto se evidencia aún más porque "Más del 66% de las empresas en Colombia no cuentan con una política de seguridad definida formalmente" (Almanza et al., 2010) y es necesario fortalecer estos aspectos ya que "las regulaciones nacionales e internacionales llevarán a las organizaciones en Colombia a fortalecer los sistemas de gestión de seguridad de la información…" (Almanza et al., 2010). Por su lado, el Ministerio de Comunicaciones a través del Plan nacional de TIC Colombia 2010-2019, también contempla la relevancia del sector de la seguridad informática, donde plantea la asignación de recursos para invertir en el Proyecto "Seguridad informática para el sector público y privado" cuyo objetivo es "Establecer lineamientos generales y prácticos en los temas de seguridad de la información desde la perspectiva del ciudadano; de la experiencia técnica y administrativa de las organizaciones, los estándares y las buenas prácticas; y de la protección de infraestructura crítica de la nación" (Ministerio de Comunicaciones, 2010). Lo cual evidencia también la necesidad de desarrollar trabajos desde el sector investigativo en ésta área.

3. METODOLOGÍA

Para el desarrollo de la herramienta objeto de este artículo, se planteó un proceso secuencial a través de unas fases estructuradas desde el análisis de la información recopilada sobre software de apoyo a la implementación de SGSI, la identificación de las funcionalidades más relevantes de los sistemas existentes, el desarrollo del sistema web y la verificación de la operación del sistema en un escenario real. Las fases se articularon adecuadamente al cumplimiento de los objetivos durante el proceso investigativo. A continuación se detalla el proceso:

3.1 ANÁLISIS DE INFORMACIÓN

Una vez realizado el proceso de búsqueda en bases de datos digitales y literatura relevante sobre SGSI, se analizó la literatura recopilada dando como resultado la detección de las funcionalidades que debe tener un sistema de apoyo de este tipo con respecto a los sistemas existentes. Este análisis, permitió además, la elaboración del estado del arte y el marco conceptual del proyecto.

3.2 IDENTIFICAR LAS FUNCIONALIDADES DE SISTEMAS EXISTENTES

En esta fase se identificaron las funcionalidades de mayor relevancia en sistemas existentes para apoyo a la verificación de controles de seguridad informática, a través de la aplicación de un instrumento tipo encuesta que permitió recolectar información de expertos en seguridad informática.

El instrumento de medición fue diseñado y montado en una plataforma de gestión de encuestas en línea. Fue diligenciado por 24 expertos de la región y de la ciudad de Bogotá, pertenecientes a organizaciones del sector educativo, sector gobierno, sector financiero, entre otros.

El instrumento contempló 10 aspectos relacionados con la caracterización de la organización, la gestión de seguridad de la información llevada en las organizaciones, la identificación de funcionalidades más relevantes para este tipo de sistemas, así como la formación que se está brindando desde las universidades a los profesionales en esta área.

3.3 DESARROLLAR EL SISTEMA WEB

Se definieron los requerimientos técnicos del sistema web y funcionalidades más relevantes como la gestión documental, la gestión de incidencias y la auto-evaluación de controles. Presenta las siguientes características:

- Fue desarrollado 100% con software libre.
- Requiere mínimas características de hardware y software.
- Basado en el estándar internacional ISO 27002.
- Dirigido tanto a grandes como a pequeñas organizaciones.
- No presenta altos costos económicos para su adquisición debido a que es software libre.
- Se tiene en cuenta el tipo de empresa (educativa, industrial, energética, agropecuaria, financiera, etc.) para el proceso de auditoría.
- Presenta una interfaz amigable, es un sistema de libre acceso y está orientado a la web.
- Es un sistema robusto y confiable.
- Presenta una metodología propia para llevar a cabo un proceso de auditoría.

También en esta fase, se diseñaron los diagramas de casos de uso, el modelo entidad relación, las interfaces y formatos de entrada y salida de datos; así como el desarrollo general del sistema en un ambiente web.

3.4 VERIFICAR LA OPERACIÓN DEL SISTEMA

El escenario real para la realización de pruebas definido fue una organización de tipo educativo como lo es el Centro de Informática de la Facultad de Ciencias Básicas e Ingeniería de la Universidad de los Llanos. En esta fase se verificó la operación del sistema realizando pruebas de funcionamiento, portabilidad y manejo de excepciones. Así como la interpretación de los resultados obtenidos.

4. ANÁLISIS DE LAS ENCUESTAS REALIZADAS

Se realizaron encuestas a los actores involucrados, de donde se logró obtener los requerimientos funcionales de la herramienta desarrollada y se identificaron los aspectos generales con respecto al aprendizaje de temáticas relacionadas con la seguridad de la información en las organizaciones.

4.1 ANÁLISIS DE LA ENCUESTA REALIZADA A LOS ESTUDIANTES

La cantidad total de encuestas diligenciadas fue 29. La mayoría de encuestados son estudiantes que ya han terminado materias, incluso pueden ser recién egresados. Y esto ha influido en que los resultados tengan una perspectiva desde un ambiente laboral. Más de la mitad de los encuestados ha realizado prácticas de laboratorio sobre gestión de seguridad informática; sin embargo frente al uso de herramientas para este tipo de prácticas, más del 50% indica que no ha manejado herramienta alguna. Esto se debe a que muy posiblemente éstas prácticas fueron llevadas a cabo de forma manual, apoyadas en algún tipo de hoja de cálculo.

Desde el punto de vista del aprendizaje de estas temáticas, se evidencia un alto número de estudiantes que se ven afectados por falencias en la realización de laboratorios, como se muestra en la Figura 1; se puede percibir que la falta de herramientas en esta área aporta a esta tendencia. De igual manera es significativo el porcentaje reflejado por la falta de bases sólidas; desde el punto de vista pedagógico, el proceso de formación en este tipo de aspectos tecnológicos debe equilibrar adecuadamente la teoría y la práctica, lo que se puede explicar desde el ítem "realización de pocas prácticas".

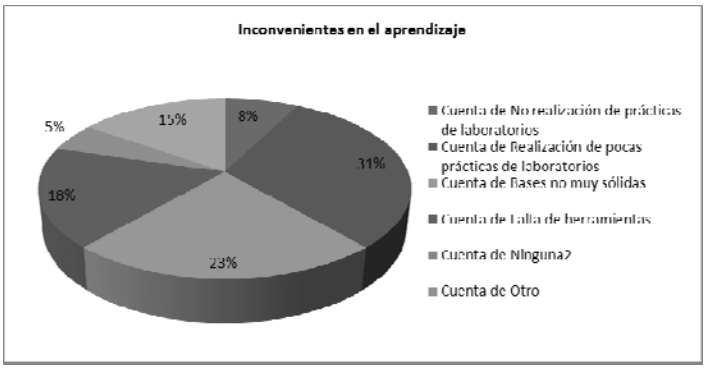


Figura 1. Inconvenientes de aprendizaje sobre seguridad de información

4.2 ANÁLISIS DE LA ENCUESTA REALIZADA A EXPERTOS EN GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La cantidad total de encuestas diligenciadas fue 24. En la Figura 2 se identifica el sector al que pertenece la organización donde labora el experto que ha diligenciado la encuesta. Se puede apreciar que el 38% de las organizaciones pertenece al sector educativo, que el 13% hacen parte del sector gobierno y que el 12% corresponde al sector financiero. Lo que permite un interesante análisis de la manera como se está asumiendo la gestión de la seguridad de la información en organizaciones de este tipo.

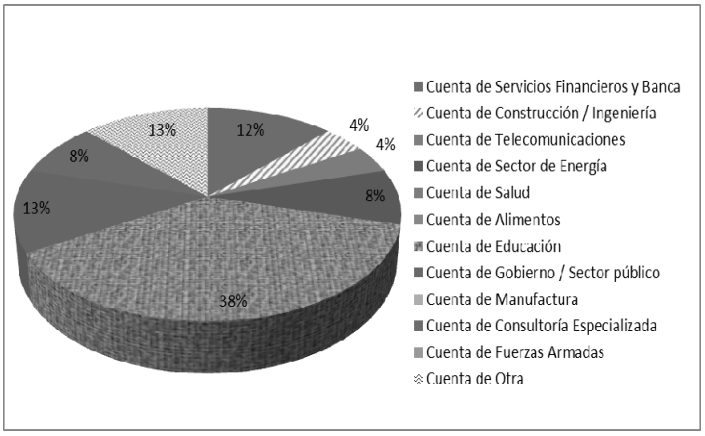


Figura 2. Sector de la organización

A pesar de que se reconoce la importancia de la gestión, hace falta mayor compromiso frente al establecimiento y aplicación de políticas de seguridad definidas. Tan solo el 38% de las organizaciones cuenta con un procedimiento definido para tal fin. Un 29% de ellas ha iniciado un proceso de desarrollo y el 33% no tiene ningún apolítica de seguridad definida.

Se ha evidenciado (ver Figura 3) que las pocas organizaciones que realizan esa verificación de controles no se apoyan de herramienta de software alguna, por tanto, se podría intuir que lo están haciendo de una forma manual apoyados tal vez de una hoja de cálculo. Tan solo una organización utiliza una herramienta como SEGURIA

SGSI, la cual es software libre; lo que demuestra que el uso de herramientas comerciales está supeditado al costo y tal vez a la complejidad tecnológica que las caracteriza.

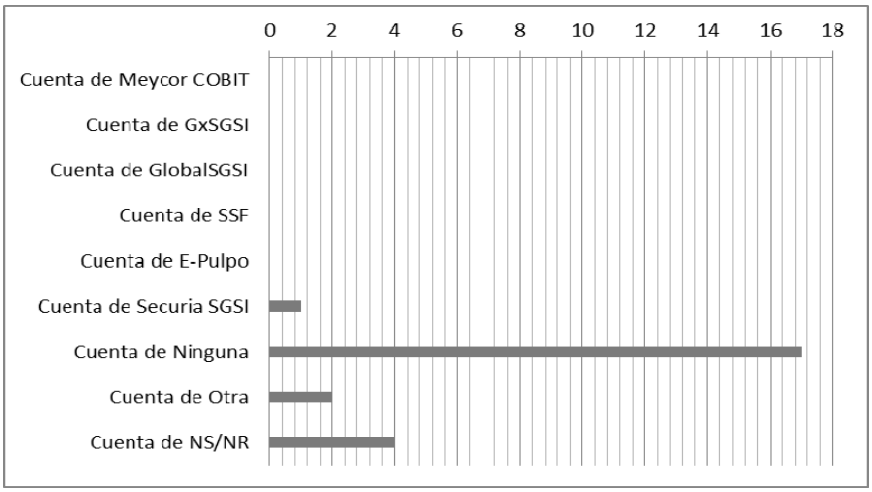


Figura 3. Herramienta de software que utiliza para la verificación de controles

Es importante resaltar que dentro de las funcionalidades relevantes con las que debe contar una herramienta de apoyo a la gestión de seguridad de la información, se encuentra en alto grado la gestión de hallazgos y evidencias, la administración de controles y la generación de reportes, como se muestra en la Figura 4. Lo que ha permitido que la herramienta desarrollada deba contar indiscutiblemente con estas opciones.

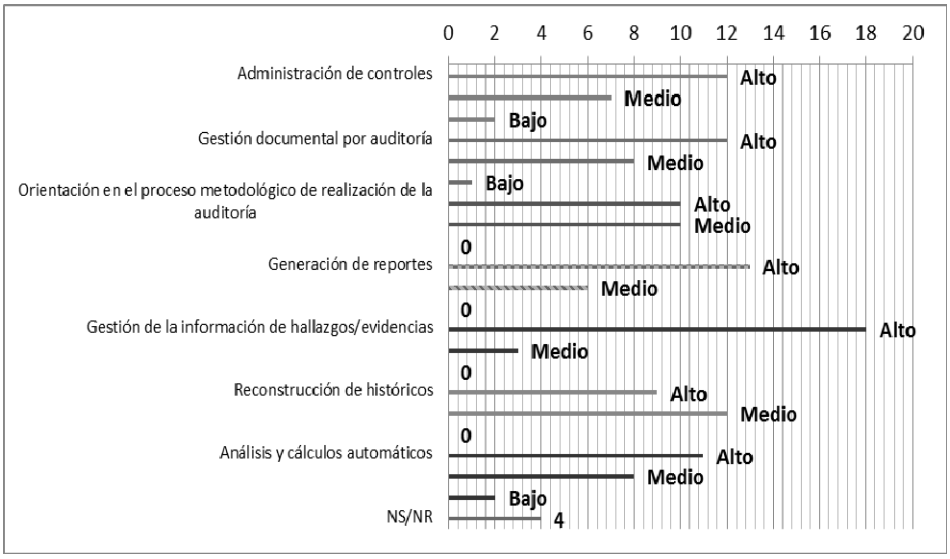


Figura 4. Grado de importancia de las funcionalidades que debería tener la herramienta a desarrollar

Teniendo en cuenta la Figura 5, con respecto a la formación de profesionales en Seguridad de la Información, la mayoría de organizaciones considera que se debe prestar mayor atención a este tema desde las universidades, quienes son las llamadas a suplir estas necesidades a través de la inclusión de cursos o asignaturas en el área dentro de sus planes de estudio en pregrado, ofrecimiento de cursos especializados o programas de posgrado; así como incentivar y promover nuevos trabajos de investigación e innovación en el área.

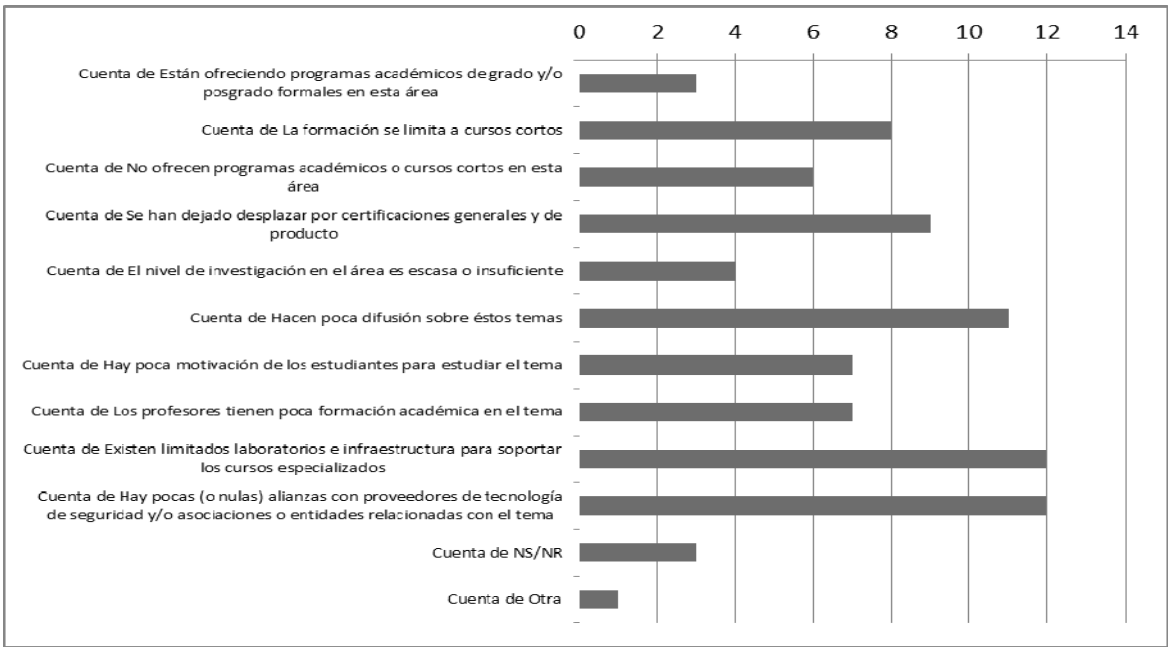


Figura 5. Concepto sobre la formación de profesionales en Seguridad de la Información que se está impartiendo en las universidades

5. HERRAMIENTA SGCSI

Se ha desarrollado un sistema para la administración de controles de seguridad de la información basada en el estándar internacional ISO 27002, llamado SGCSI, un sistema web basado en software libre dirigido a empresas de los diferentes sectores: educativo, industrial, energético, agropecuario, financiero, entre otros; caracterizado por ser una herramienta con una interfaz amigable al usuario, desarrollada en el idioma español, de libre acceso y uso, orientada a la web, fundamentada en estándares internacionales. El sistema cuenta con tres (3) tipos de usuarios: administrador, empresa y auditor. A continuación se definen las funciones que cada uno puede realizar:

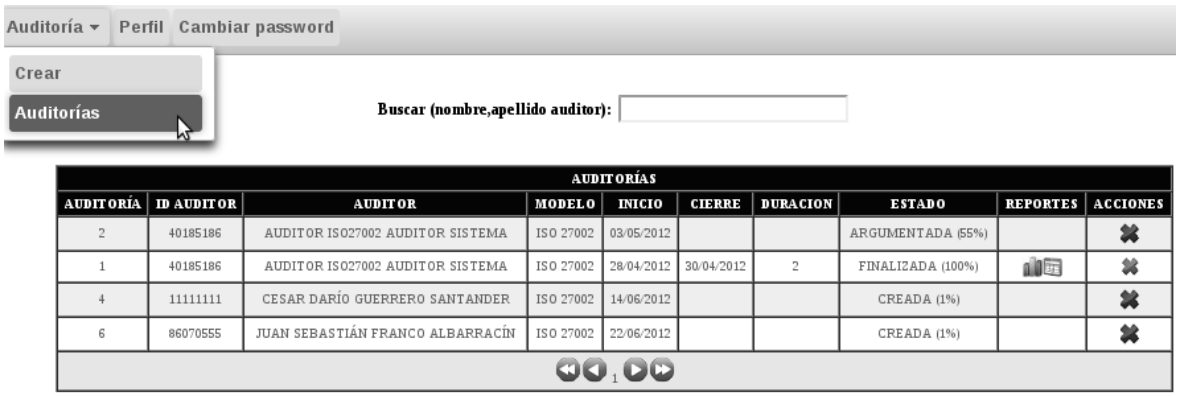
- **Usuario administrador:** administrador general del sistema, puede realizar tareas como: consultar y actualizar empresas y auditores. Además debe tener dominio en la administración del servidor, mantenimiento, supervisión, configuración y actualización del sistema.
- **Usuario empresa:** representante legal de una empresa a la que se le va a realizar el proceso de auditoría. Puede realizar tareas como: registrarse en el sistema, consultar y actualizar sus respectivos datos, crear y asignar auditores, crear, consultar y actualizar auditorías y generar reportes.
- **Usuario auditor:** profesional encargado de llevar a cabo el proceso de ejecución de la auditoría. Puede realizar tareas como: registrarse en el sistema, consultar y actualizar sus respectivos datos, consultar, ponderar, argumentar, valorar, cerrar auditorías, cargar insumos y generar reportes.

El sistema en su estructura le permite al oficial de seguridad abordar el proceso general de seguridad y auditoría referente a HPVA (Hacer – Planear – verificar - Actuar), sobre los diferentes dominios definidos en ISO/IEC 27002; donde se puede implementar éste estándar en organizaciones de los diferentes sectores de la sociedad (educativo, energético, textil, etc…). Una vez se obtengan los resultados de la auditoria el equipo de seguridad se centrará en la planeación y actuación, acorde a los reportes que genera SGCSI para la toma de decisiones.

En la Figura 6 se aprecia la interfaz principal que se presenta una vez se ejecuta el sistema en un navegador web sin haber iniciado sesión. Con las opciones del menú: Empresa y Auditor, se brinda la posibilidad de registrarse en el sistema, una vez registrado, el administrador general validará la información y habilita el acceso de los mismos.

Figura 6. Pantalla principal de SGCSI

Si por ejemplo se inicia sesión como usuario empresa, ésta tiene la opción de actualizar sus datos si así lo desea y la opción de crear procesos de auditorías, así como listarlos. En la Figura 7 se presenta la manera como aparecen los procesos de auditoría que tiene la empresa, indicando el código, el auditor asignado, la fecha de inicio y cierre, el tiempo de duración, el estado en el que se encuentra (creada, activada, ponderada, argumentada, valorada, cerrada, en periodo de reclamación o finalizada). Y finalmente la opción para generar los reportes gerencial y técnico.



AUDITORÍAS

AUDITORÍA	ID AUDITOR	AUDITOR	MODELO	INICIO	CIERRE	DURACION	ESTADO	REPORTES	ACCIONES
2	40185186	AUDITOR ISO27002 AUDITOR SISTEMA	ISO 27002	03/05/2012			ARGUMENTADA (55%)		
1	40185186	AUDITOR ISO27002 AUDITOR SISTEMA	ISO 27002	28/04/2012	30/04/2012	2	FINALIZADA (100%)		
4	11111111	CESAR DARÍO GUERRERO SANTANDER	ISO 27002	14/06/2012			CREADA (1%)		
6	86070555	JUAN SEBASTIÁN FRANCO ALBARRACÍN	ISO 27002	22/06/2012			CREADA (1%)		

1

Figura 7. Procesos de auditoría de la empresa

5.1 PROPUESTA METODOLÓGICA PARA LA REALIZACIÓN DE AUDITORÍAS DE SEGURIDAD

En el marco de esta investigación se ha planteado el diseño de una metodología que permita asumir práctica y eficientemente la verificación de controles de seguridad informática soportada desde un sistema que oriente el proceso de auditorías de seguridad. Es así como el sistema SGCSI desarrollado involucra en su estructura y funcionamiento las siguientes fases metodológicas:

- **Creación:** se refiere a la fase donde inicia el proceso de auditoría, el cual es creado por la empresa quien asigna el auditor respectivo que lo realizará, estableciendo la fecha de inicio y fin para el mismo.
- **Activación:** en la cual se autoriza la solicitud del gerente al administrador general para usar los recursos del sistema en la realización del proceso de auditoría.
- **Ponderación:** donde se asignan los niveles de importancia a cada aspecto de seguridad definido en el proceso de auditoría (dominios, objetivos de control y controles) respectivamente, teniendo en cuenta que

entre ellos no deben sobrepasar el 100% (ver Figura 8). Dentro del sistema, se permite la activación o no de un aspecto de seguridad específico cuando una empresa lo considere necesario.

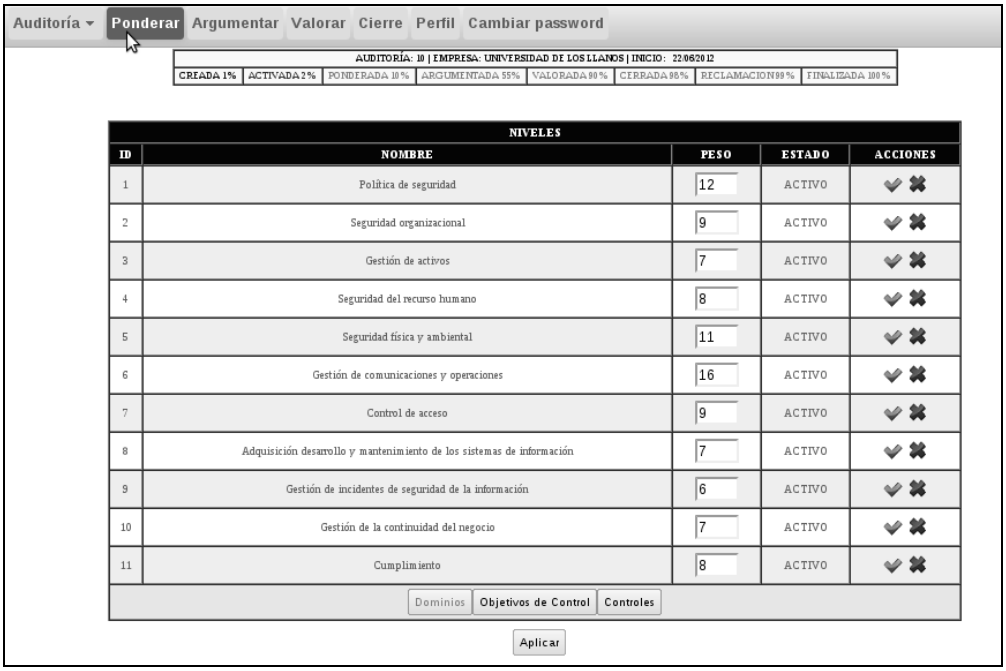


Figura 8. SGCSI - Ponderación

- **Argumentación:** en esta fase se administra la gestión de evidencias (insumos) que soportan el proceso, anexando las respectivas observaciones y sugerencias. El sistema permite adjuntar evidencias en cualquier formato de documento (.pdf, .doc., .odt, .jpg, …) ya que éstas pueden provenir de archivos de log, imágenes de dispositivos, fotografías, archivos de configuración, registros de actividades como realización de backup, listados de usuarios, etc.
- **Valoración:** se procede a asignar cuantitativamente una calificación al estado del cumplimiento del aspecto de seguridad definido en el proceso de auditoría, clasificándolo automáticamente en una escala de valoración cualitativa (alto, bueno, medio, regular, bajo) de 5 niveles, predefinida en el sistema, confines de agrupamiento para la generación de análisis y reportes sobre la gran cantidad de controles administrados.
- **Cierre:** el auditor finaliza el proceso de auditoría anexando las observaciones finales. Este cierre no es definitivo, ya que se puede presentar alguna apelación o reclamación.
- **Reclamación:** se refiere al evento de abrir nuevamente el proceso de auditoría terminado para realizar algún ajuste específico, procedente de aclaración o reclamación por un externo diferente al auditor, que implique reajustar la valoración de algún ítem. Este reajuste lo realiza el auditor.
- **Finalización:** en esta fase se cierra definitivamente el proceso de auditoría impidiendo cualquier evento de modificación de los datos generados y/o asignados durante el proceso. Debido a que a partir de esta se puede proceder a la generación del reporte gerencial y técnico.

Se ha verificado la operación del sistema desarrollado a través de un caso de aplicación en una organización de tipo educativo en la Orinoquia colombiana. Se realizó un análisis comparativo sobre dos métodos de manejo de la información generada por este proceso de auditoría realizado; el primero apoyado en una hoja de cálculo como Excel y el segundo a través del sistema desarrollado (SGCSI). Se logró evidenciar que los dos métodos de apoyo de manejo de información de la auditoría fueron de la misma precisión en los cálculos realizados (nivel de

cumplimiento de los 32 objetivos de control y el nivel de cumplimiento total); sin embargo, el método basado en hoja de cálculo presentó múltiples falencias sobre la integralidad y transversalidad del proceso de auditoría.

6. CONCLUSIONES Y TRABAJOS FUTUROS

El sistema puede evolucionar, en futuras versiones, con la adaptación de otros modelos o estándares de evaluación diferentes a ISO 27002, tales como OSSTMM y COBIT.

Implementar módulos de captura automática de información y análisis de evidencias (insumos), para cargar los datos de valoración dentro de la metodología diseñada en el proceso de auditoría.

Incluir de forma predefinida los valores ideales acorde al sector de la sociedad en la que actúan las diferentes organizaciones (financiero, educativo, industrial…).

Implementar un sistema de firmas digitales para proveer mayor confidencialidad sobre el sistema teniendo en cuenta el alto nivel de privacidad que deben mantener los datos administrados en el proceso de auditoría.

REFERENCIAS

Almanza, A., Cano, J. (2010). *Investigación - Encuesta nacional Seguridad informática en Colombia: Tendencias 2010*. De Colombia: Asociación Colombiana de Ingenieros de sistemas – ACIS. Recuperado en octubre de 2010. Disponible en: http://www.acis.org.co/fileadmin/Revista_115/investigacion.pdf

Colombia. Ministerio de Comunicaciones. (2010). *Plan Nacional de TIC´s 2010-2019.* Recuperado en octubre de 2010. Disponible en: http://www.colombiaplantic.org/docs/080409-Plan%20Nacional%20de%20TIC.pdf

Horváth, M.; Jakub, M. (2009). Implementation of security controls according to ISO/IEC 27002 in a small organization. Quality Innovation Prosperity, 13 (2), 48-54. Recuperado el 10 de octubre de 2011 de DOAJ - Directory of Open Access Journals. Disponible en:http://www.qip-journal.eu/files/2009/2009-2/QIP_2_2009_Horvath.pdf

Iqbal, A.; Horie, D.; Goto, Y.; Jingde Cheng. (2009). A Database System for Effective Utilization of ISO/IEC 27002. In Proceedings of the 2009 Fourth International Conference on Frontier of Computer Science and Technology (FCST '09). IEEE Computer Society, Washington, DC, USA, 607-612. Recuperado el 8 de octubre de 2011 de la base de datos IEEE Xplore Digital Library.

Knapp, K. J., Franklin Morris Jr., R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. Computers Security, 28(7), 493-508. Elsevier Ltd. Disponible en: http://linkinghub.elsevier.com/retrieve/pii/S0167404809000765

Klaic, A.; Hadjina, N. (2011). Methods and tools for the development of information security policy — A comparative literature review. MIPRO, 2011 Proceedings of the 34th International Convention , vol., no., pp.1532-1537, 23-27 May 2011. Disponible en: http://www.sinab.unal.edu.co:2365/stamp/stamp.jsp?tp=&arnumber=5967304&isnumber=5967009

Autorización y Renuncia

Los autores autorizan a LACCEI para publicar el escrito en las memorias de la conferencia. LACCEI o los editores no son responsables ni por el contenido ni por las implicaciones de lo que esta expresado en el escrito.