REVISTA CUBANA
DE TRANSFORMACIÓN DIGITAL

RNPS 2487 • ISSN 2708-3411
Vol. 3 • Nro. 3 • julio-septiembre 2022 • e181

ARTÍCULO ORIGINAL

Herramienta para auditorías de seguridad informática

Tool for Computer Security Audits

Laritza González Miranda
larygm88@gmail.com • https://orcid.org/0000-0002-5731-8269
EMPRESA DE APLICACIONES INFORMÁTICAS, DESOFT PINAR DEL RÍO, CUBA

Raidel Rodríguez Romeu
rirro@upr.edu.cu • https://orcid.org/0000-0003-4268-2073
UNIVERSIDAD DE PINAR DEL RÍO, CUBA

Rigoberto Samuel Rodríguez Romeu
rigosam83@gmail.com • https://orcid.org/0000-0003-2303-2665
CENTRO PROVINCIAL DE MEDICINA DEPORTIVA, PINAR DEL RÍO, CUBA

Recibido: 2022-09-21 • Aceptado: 2022-10-30

RESUMEN

El tema de seguridad informática en nuestro país se ha convertido en pilar fundamental, pues el Estado tiene como una de sus actividades priorizadas la informatización de la sociedad cubana, garantizando de manera eficiente y eficaz la ciberseguridad. Por tal motivo, se han realizado actualizaciones a nuestra base legal, aprobándose nuevos decretos-ley que regirán estos procesos. No obstante, se hace necesario establecer un marco de trabajo que permita estandarizar las auditorías de seguridad informática con basamento en lo legislado. Cuba no cuenta con una norma específica para la seguridad informática, ni para realizar auditorías relacionadas con este tema; solo existen como patrón los decretos leyes, las resoluciones y la metodología por la que se diseña el Sistema de Gestión de Seguridad Informática, elaborado por la Oficina de Seguridad para las Redes Informáticas. Esta investigación se propone elaborar un *software* que permite estandarizar el proceso de auditoría de seguridad informática en el país, tomando como referencia lo estipulado internacionalmente y contextualizándolo a la realidad cubana, teniendo como soporte la legislación vigente. La investigación es de tipo descriptiva y en ella se utilizó Scrum como marco de trabajo, específicamente la versión *Guía Scrum 2020.* Como resultado, brinda aportes tanto en lo metodológico como en lo práctico. El primero

de ellos está dado por la elaboración de la guía para la realización de auditorías de seguridad informática, mientras que lo segundo se evidencia en el diseño y la implementación de un *software* que automatiza el proceso y brinda retroalimentación a los usuarios.

Palabras clave: auditoría de seguridad informática, ciberseguridad, guía metodológica, seguridad informática, sistema de gestión de seguridad informática.

ABSTRACT

The issue of computer security in our country has become a fundamental pillar, since the State has as one of its prioritized activities the computerization of Cuban society, guaranteeing cybersecurity efficiently and effectively. For this reason, updates have been made to our legal basis, approving new Decree-Laws that will govern these processes. However, it is necessary to establish a framework that allows standardizing computer security audits based on what is legislated. Cuba does not have a specific standard for computer security or to carry out audits related to this issue, there are only decree laws, resolutions and the methodology by which the Computer Security Management System prepared by the Office of Security for Computer Networks. This research aims to develop software that allows standardizing the computer security audit process in the country, taking as a reference what is stipulated internationally and contextualizing it to the Cuban reality, having as support the current legislation. The research carried out is descriptive, and Scrum was used as a framework, specifically the Scrum Guide 2020 version. As results, it provides contributions both methodologically and practically. The first of them is given by the elaboration of the guide for carrying out computer security audits, while the second is evidenced in the design and implementation of software that automates the process and provides feedback to users.

Keywords: *computer security audits, cybersecurity, methodological guide, computer security, computer security management systems.*

INTRODUCCIÓN

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad

de las operaciones. La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que estos van adquiriendo día a día habilidades más especializadas, que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior de la organización. La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de ello, han ido aumentando las acciones poco respetuosas hacia la privacidad y la propiedad de recursos y sistemas (Lawrence, B., Lawrence, G., & Martin, L., 2018).

Pero si se toman las medidas adecuadas, la gran mayoría de este tipo de ataques puede prevenirse, adoptando medidas de seguridad informática que incluyan, por ejemplo: la instalación de *software* legalmente adquiridos; la utilización de antivirus, *hardware* y *software* cortafuegos; el uso de contraseñas complejas y grandes; la capacitación de los usuarios en temas de ingeniería social y la utilización de técnicas y herramientas criptográficas (Mesquida & Mas, 2015).

No obstante, es importante recalcar que un componente relevante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red, lo cual puede garantizarse mediante la ejecución de auditorías de seguridad informáticas (Ramalingam, Arun, & Anbazhagan, 2018).

Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización del *software* y la adquisición de *hardware*, hacen necesario que los sistemas estén continuamente verificados mediante auditoría, la cual permite conocer en el momento de su realización cuál es la situación exacta de los activos de información en cuanto a protección, control y medidas de seguridad.

La auditoría de seguridad informática es el estudio que comprende un análisis y una gestión de sistemas, para identificar y, posteriormente, corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, los servidores y las redes de comunicaciones (Azán, Y., Bravo, L., Rosales, W., Trujillo, D., García, E. y Pimentel, A, 2014).

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Actualmente, existe un gran número de aplicaciones destinadas a auditar diferentes procesos empresariales, los cuales se centran mayormente en análisis estadísticos y financieros. También existen investigaciones que proponen aplicaciones destinadas a auditar determinados *software*, como los relacionados con la gestión de proyectos. Otros detectan vulnerabilidades relacionadas con sitios web, atendiendo fundamentalmente a su confección lógica y a la codificación, así como aplicaciones que permiten realizar auditorías a sistemas gestores de bases de datos. Existe una gama muy amplia de *software*, que escanean la red en busca de vulnerabilidades desde diferentes puntos de vista, por ejemplo, buscando puertos abiertos, *software* y sistemas operativos instalados y explotan las vulnerabilidades que estos presentan, brindando al usuario un análisis de las vulnerabilidades detectadas y desplegando medidas en aras de erradicarlas.

En nuestro país existe un *software* denominado «Diógenes», desarrollado por el Grupo de Investigación y Desarrollo de la Oficina de Seguridad para las Redes Informáticas (OSRI), el cual está basado en la derogada Resolución 127 de 2007, del Ministerio de las Comunicaciones.

La Empresa de Aplicaciones Informáticas, Desoft, cuenta con un *software* denominado Suit de Seguridad Informática, que permite detectar fundamentalmente los equipos conectados en la red y alertar sobre cambios de *hardware*.

Los sistemas mencionados anteriormente no satisfacen las necesidades de automatización del proceso que se investiga, ya que ninguno aporta una solución abarcadora a la problemática de la auditoría y no se ajustan a la legislación vigente en nuestro país.

Recientemente fue actualizada nuestra base legal, aprobándose los Decretos-Ley N° 370/2018 sobre la Informatización de la Sociedad en Cuba y el N° 360/2019 sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional, a partir de los cuales se han aprobado resoluciones que establecen metodologías de trabajo. (Ministerio de Comunicaciones, 2019).

Ambos decretos y las resoluciones derivadas constituyen actualmente las líneas bases sobre las que deben desempeñarse los procesos correspondientes a la informática y las telecomunicaciones. No obstante, se hace necesario establecer un marco de trabajo que permita estandarizar la auditoría de estos procesos basado en lo legislado. Cuba no cuenta con una norma específica para la seguridad informática, ni para realizar auditorías relacionadas con este tema, solo existen como patrón los decretos leyes y las resoluciones. La metodología por la que se diseña el Sistema de Gestión de Seguridad Informática (SGSI), elaborado por la Oficina de Seguridad para las Redes Informáticas (OSRI), también ha sido modificada y aprobada en la Resolución 129/2019 (Ministerio de Comunicaciones, 2019), por lo que debe tomarse como patrón para guiar las auditorías.

Existe un gran número de guías para realizar auditorías de seguridad informática, que se encuentran dispersas por todo el país. Cada empresa que audita la seguridad informática asume una serie de aspectos que se deben revisar, tomando como referencia la resolución derogada 127/2007. Muchas de estas empresas asumen el rol de auditores para chequear el funcionamiento de la actividad informática internamente; otras, autorizadas por el Ministerio de las Comunicaciones, brindan servicios de auditoría a terceros, pero tampoco cuentan con una guía estándar ni completamente actualizada para desempeñar estas funciones. Otro aspecto de interés relacionado con la falta de una guía metodológica estándar de trabajo, es la forma de evaluación de los resultados de estas auditorías, pues no se aplican sistemas de medición adecuados. La mayoría están basados en la experiencia del auditor y todos los aspectos que chequean se evalúan de igual forma, sin establecer ponderaciones según el grado de importancia de sus activos informáticos. Todos estos aspectos crean una gran incertidumbre en el personal que atiende la actividad informática en las empresas, ante la realización de auditorías, lo cual influye negativamente a la hora de asumir el rol de Especialista de Seguridad Informática. Sin saber exactamente qué aspectos serán revisados durante una auditoría, ni la

forma correcta en la que deben realizar actividades y procedimientos, es muy difícil mantener en funcionamiento el SGSI.

Es por eso que esta investigación pretende estandarizar el proceso de auditorías de seguridad informática. La primera fase del trabajo se centró en la elaboración de la guía metodológica, que constituye la base del *software* que automatizará todo el proceso, el cual será desarrollado en la segunda fase, actualmente en proceso.

De este modo se puede definir como problema de la investigación: ¿Cómo optimizar el proceso de auditorías de seguridad informática en las organizaciones laborales cubanas?

El objetivo es optimizar el proceso de auditorías informáticas en las organizaciones laborales cubanas, mediante la elaboración de una guía metodológica y un *software* que la automatice.

Esta investigación resulta novedosa, ya que se diseña por primera vez en la provincia un *software* vinculado con la realización de auditorías de seguridad informática, cumpliendo con los parámetros establecidos en las normas y los estándares internacionales, y con las resoluciones y decretos-ley vigentes en nuestro país. Las auditorías de seguridad informática se optimizan con la utilización de la guía metodológica y el *software*, ya que disminuirá considerablemente el tiempo de entrega de los resultados y humanizará en gran medida el trabajo del equipo de auditoría, permitiéndoles realizar evaluaciones de forma estandarizada, sin recurrir a sus propias apreciaciones. El *software* podrá ser utilizado como una guía orientadora, válida no solo para personal experto en temas de auditorías de seguridad informática, sino que permitirá a profesionales de las ciencias de la computación diseñar y mejorar SGSI.

El aporte metodológico de la investigación está dado por la elaboración de una guía que estandarice el proceso de auditorías de seguridad informática en las organizaciones laborales cubanas, posibilitando la evaluación de la entidad auditada a partir de un criterio unificado que no dependa solo de la percepción del auditor.

El aporte práctico está dado por el diseño y la implementación de un *software*, que evalúa a las organizaciones laborales con respecto a la seguridad informática y que brinda una retroalimentación a los usuarios, basándose en recomendaciones para mantener e implementar buenas prácticas en este campo.

METODOLOGÍA

La presente investigación es de tipo descriptiva, ya que persigue describir el comportamiento de una serie de variables relacionadas con el funcionamiento de la seguridad informática, mediante la realización de auditorías de seguridad informática en las organizaciones laborales, con el objetivo de determinar las vulnerabilidades y brindar recomendaciones para minimizar su impacto negativo.

Esta investigación responde a un diseño no experimental, ya que las variables no han sido manipuladas deliberadamente por el investigador, sino que se ha observado el fenómeno tal y como se da en su ambiente natural, para luego analizarlo. También es necesario señalar que se

ha realizado la recolección de información en un momento y en un tiempo determinados; su propósito es describir variables y analizar su incidencia e interrelación en un lapso dado, por lo cual, los diseños de investigación de tipo no experimental se ubican dentro de los estudios transversales o transaccionales.

Para poder desarrollar la investigación fue necesario el empleo de diferentes métodos científicos, procedentes del nivel teórico, entre los que se encuentran el histórico-lógico, sistémico-estructural y análisis-síntesis.

El método histórico-lógico se vincula al conocimiento de las distintas etapas de los objetos en su sucesión cronológica, su evolución y desarrollo, así como sus conexiones históricas fundamentales. Se empleó en esta investigación con el objetivo de poder describir la evolución de las auditorías de seguridad informática, sus características y etapas principales, así como para conocer cuáles son sus tendencias básicas. También permitió investigar y analizar la implementación y puesta en práctica de otros proyectos informáticos realizados con propósitos similares.

Se necesitó además la utilización del método análisis-síntesis, porque mediante este fue posible descomponer el problema en las diversas partes que lo componen y así poder estudiarlas de modo multifacético. Este método también permitió comprender toda la estructura y delimitar los aspectos que resultan esenciales para la comprensión del fenómeno. A través de la síntesis se pudieron revelar las relaciones esenciales y las características generales de las auditorías de seguridad informática, las normas y regulaciones establecidas a nivel internacional y nacional, extraer conclusiones válidas para la investigación y sistematizar el conocimiento científico. Este método contribuyó además a la elaboración de una guía metodológica.

Otro método del nivel teórico empleado fue el sistémico-estructural, que permitió poder llegar a modelar el *software* a través de un estudio sobre las auditorías de seguridad informática y de los elementos que la componen. Esto permitió poder comprender la lógica de trabajo de los expertos que las realizan, modelar los datos necesarios para el diseño de la base de datos, así como para procesar la información recopilada y analizarla en aras de brindar resultados, retroalimentar a los usuarios y evaluar la entidad auditada mediante el *software*.

Del empleo de estos métodos correspondientes al nivel empírico se empleó la técnica de la entrevista en profundidad, aplicada a los expertos que realizan este tipo de auditorías, gracias a las cuales se pudo llegar a conocer el sistema de trabajo de los métodos, así como sus principales problemas y necesidades informáticas. Los datos obtenidos fueron de significativo interés para la elaboración de la guía metodológica, ya que eran imposibles de obtener por otra vía. También se utilizó el método de análisis de documentos para revisar todo lo relacionado con la base legal vigente en nuestro país y las normativas a nivel internacional, y para analizar todo lo existente en materia de *software*, relacionado con el tema de la investigación.

Como marco de trabajo para el desarrollo del *software* se utilizó Scrum, que es un marco ligero de ayuda a personas, equipos y organizaciones, que les permita generar valor a través de soluciones adaptables para problemas complejos (Schwabe & Sutherland, 2020). Entre las ventajas que proporciona, destacan gestión regular de las expectativas del cliente, resultados

anticipados, flexibilidad y adaptación respecto a las necesidades del cliente o cambios en el mercado, gestión sistemática del retorno de inversión, mitigación sistemática de los riesgos del proyecto, productividad y calidad, alineamiento entre el cliente y el equipo de desarrollo y, por último, fomenta la motivación del equipo de trabajo con buenas prácticas colaborativas, lo que permite obtener mejores resultados y aumentar la productividad(proyectosagiles.org, 2008).

En Scrum se realizan entregas parciales y regulares del producto final, priorizadas por el beneficio que aportan al receptor del proyecto. Por ello, Scrum está especialmente indicado para proyectos en entornos complejos, donde se necesita obtener resultados rápido, donde los requisitos son cambiantes o poco definidos, y la innovación, la competitividad, la flexibilidad y la productividad, fundamentales.

RESULTADOS

Como resultado se presenta una guía metodológica que permite realizar las auditorías de seguridad informática en las diferentes organizaciones laborales, y una primera fase del desarrollo de la herramienta informática que automatiza el proceso de auditoría de seguridad informática en Cuba y brinda retroalimentación a los usuarios. Se diseñó la base datos para la captura de la información y algunas de las principales funcionalidades asociadas a los módulos de la aplicación, relacionados con la entrada de la información sobre las empresas auditadas y los resultados de las auditorías realizadas.

La guía metodológica abarca todos los aspectos de la seguridad informática que se deben controlar en una entidad y que están regulados por las normas vigentes en el marco legal de seguridad informática en Cuba. Esa guía se ha estructurado en ocho secciones, las cuales se deben realizar según el orden presentado y pueden ser ejecutadas por personal experto en temas de auditorías de seguridad informática que provienen de otras instituciones, como la OSRI o las empresas dedicadas a brindar estos servicios, por ejemplo, Desoft. También puede ser aplicada por el personal de la empresa designado para implementar el SGSI.

1. Diagnóstico inicial: en esta sección se revisan los resultados obtenidos en el control previo si es que existe algún registro, se chequea todo lo relacionado con la presencia de la entidad en la red nacional e Internet, teniendo en cuenta la información que muestran. Además, se verifica que cuentan con los documentos de autorización para el uso de la red de datos y los servicios registrados. Por último, se analiza si el objeto social de la entidad con su misión y visión se corresponde con los procesos que se desarrollan en esta y con la utilización de los bienes informáticos.
2. Estrategia y planificación del Sistema de Seguridad de las TIC: se verifica nivel de responsabilidades relacionadas con la seguridad informática y si el personal conoce sus deberes y derechos, se chequea que existen plazas específicas para controlar toda la actividad y que cuentan con un SGSI implementado y en funcionamiento.

3. Empleo seguro de las TIC: sección donde se verifica que se lleva un control sobre los bienes informáticos de la entidad teniendo en cuenta su identificación, uso, controles de acceso, manejo por parte de personal capacitado, que se tiene documentado todo lo relacionado con las responsabilidades, los deberes y los derechos del personal encargado de las actividades de seguridad informática y redes, y de los usuarios de las TIC en general.
4. Infraestructuras críticas de las TIC: en esta sección se revisan cada una de las áreas que componen la entidad y que cuentan con bienes informáticos, para chequear que las medidas de seguridad implementadas se corresponden con lo establecido, tanto a nivel físico como lógico.
5. Protección antivirus: se revisan los procedimientos para el control de virus informáticos, a través de la utilización de los antivirus seleccionados por la dirección de la entidad y que cumplan con lo establecido en las normativas vigentes.
6. Seguridad de las operaciones: aquí se chequea todo lo relacionado con la autorización, para acceder a los diferentes servicios y sistemas con que cuenta la entidad, así como el procedimiento para conservar las trazas generadas por estos. Se revisan los métodos para asignar credenciales de usuarios y contraseñas, además de los procedimientos para realizar salvas de información.
7. Seguridad de las redes: en esta sección se audita todo lo relacionado con el uso de las redes de datos, tanto cableadas como inalámbricas, desde la verificación del estado de seguridad de los sistemas operativos utilizados en las PC y en los servidores, el control de las trazas de los principales eventos teniendo en cuenta el período establecido, así como la verificación de la correspondencia entre la arquitectura y configuración de la red con lo descrito en el plan de seguridad informática. Además, se utilizan herramientas para escanear la red en busca de vulnerabilidades y se verifica el estado de las conexiones físicas y lógicas.
8. Gestión de incidentes de seguridad informática: en esta última sección se analizan los procedimientos establecidos por la entidad para la identificación de incidentes de seguridad informática con las medidas que se deben tomar y las diferentes instancias a las que se debe informar en caso de la ocurrencia de alguno de los posibles eventos identificados.

Esta guía de trabajo está diseñada como un cuestionario, que consiste básicamente en una lista de preguntas para cada sección, mediante las cuales se pretende evaluar el grado de vulnerabilidad del SGSI de la entidad que está siendo auditada. Las respuestas negativas indican deficiencia o vulnerabilidad asociada al aspecto; las positivas, cumplimiento, y las de «no procede», que el aspecto no puede ser evaluado por las características de la entidad. Un ejemplo de ello se puede observar en la tabla 1, donde se presentan las preguntas para la sección diagnóstico inicial.

Además, en la guía metodológica se ofrecen indicaciones para evaluar las respuestas del cuestionario por secciones de manera general. Para ello se tomó como referencia lo estipulado en la Resolución 129 de 2019 Metodología para Sistema de Gestión de Seguridad Informática, en su sección Métodos de medición, donde establece que se puede definir un total de factores que se van a evaluar (K) y ver cuántos de ellos se cumplen (k), a través de la operación K/k.

Tabla 1. Cuestionario para sección diagnóstico Inicial

Sección 1: Diagnóstico inicial			
Preguntas	**Cumple**	**No Cumple**	**No Procede**
¿Tienen presencia en la red nacional e Internet?			
¿Cuentan con un perfil institucional en las redes sociales?			
¿La información de la entidad la publican a través de perfiles personales?			
¿Exponen información limitada o confidencial?			
¿Exponen su dominio de trabajo, direcciones de trabajo o FTP?			
¿Publican información acorde a lo estipulado en la base legal?			
¿Cuentan con la inscripción de sus redes y los servicios registrados?			
¿Cuentan con el documento emitido por la entidad UPTCER, perteneciente al Mincom, que acredita la inscripción de la red cableada e inalámbrica?			
¿Tienen servicios informáticos contratados con otras entidades?			

Durante el proceso de análisis para la confección de la guía metodológica, se determinó que la fórmula presentada anteriormente no se debía aplicar de manera lineal para evaluar un SGSI, porque el resultado final sería:«se cumple» o «no se cumple» con los aspectos evaluados; sin embargo, de esta manera no se tiene en cuenta que existen organizaciones a las cuales no se les pueden evaluar determinados aspectos, ya que no están presentes en estas, un ejemplo sería las empresas que no cuentan con redes o navegación internacional. Se decidió entonces modificar la fórmula de referencia, incluyendo una nueva variable: cantidad de preguntas que no proceden (C).

Al respecto, se sugiere calcular el índice de cumplimiento de la sección (ICS), mediante la siguiente fórmula:

$$ICS = K/ (k-C)$$

Donde K es la cantidad de preguntas cumplidas en la sección, k es el total de preguntas de la sección y C es la cantidad de preguntas que no proceden en la sección.

Luego se procede a calcular el índice de cumplimiento del cuestionario (ICC):

$$ICC = \Sigma K/ (\Sigma k-\Sigma C)$$

Donde ΣK es el total que se obtiene al sumar las preguntas cumplidas en cada sección, Σk es el total que se obtiene al sumar todas las preguntas de cada sección y ΣC es el total que se obtiene al sumar las preguntas que no proceden en cada sección.

No se consideró pertinente diferenciar la importancia de los aspectos dentro de la guía metodológica, ya que esa importancia puede variar de una organización a otra y, por tanto, quedaría a la apreciación de quien realice la auditoría, conceder mayor peso a un aspecto que a otro, lo cual establece un sesgo en la evaluación.

Finalmente, el valor del ICS y del ICC se ubica dentro de los rangos establecidos (Resolución 129 de 2019), para obtener la evaluación cualitativa correspondiente a la sección o al cuestionario en general.

- Riesgo bajo: de 0 a 0,35
- Riesgo medio: de 0,36 a 0,59
- Riesgo: de 0,60 a 0,79
- Riesgo muy alto: de 0,80 a 1,0

Para el desarrollo del *software* se utilizó el marco de trabajo Scrum, el cual conlleva a la realización de un grupo de eventos que se describen a continuación (Schwabe & Sutherland, 2020):

1. Planificación del Sprint: establece el trabajo que se realizará. Este plan resultante es creado con la colaboración de todo el equipo.
2. Scrum diario: su propósito es inspeccionar el progreso hacia el objetivo del Sprint y adaptar la pila de este, según sea necesario, ajustando el próximo trabajo planeado.
3. Revisión del Sprint: el propósito de la revisión es inspeccionar el resultado del Sprint y determinar futuras adaptaciones. El equipo presenta los resultados de su trabajo a las partes interesadas y se discute el progreso hacia el objetivo del producto.
4. La retrospectiva del Sprint: su propósito es planificar formas de aumentar la calidad y la eficacia. Es el evento que concluye el Sprint.

Durante la ejecución de los Sprint se diseñó la base de datos según modelo entidad/relación (figura 1), la cual se implementó con el Lenguaje SQL.

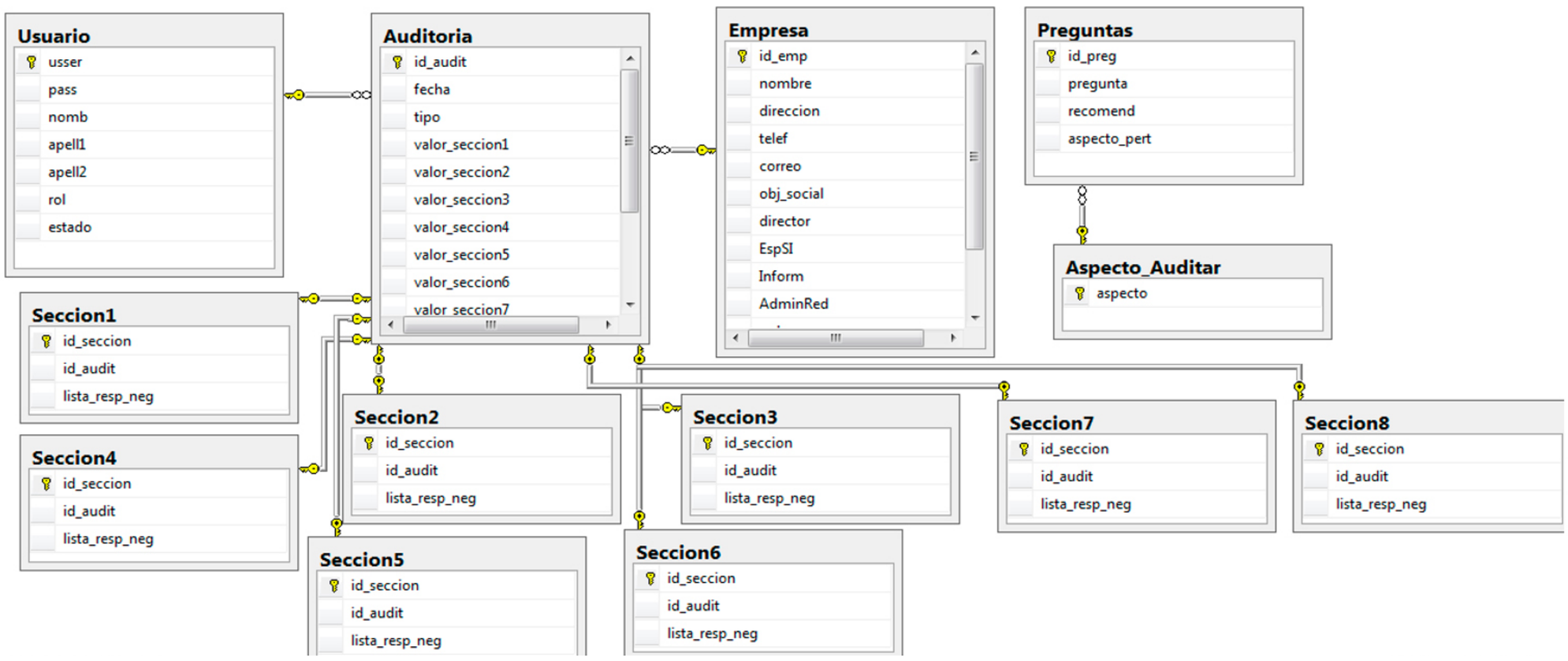

Figura 1 Diseño de la base de datos.

Además, se diseñaron las pantallas y formularios de la aplicación informática, así como las funcionalidades asociadas a los módulos de la aplicación relacionados con la entrada y procesamiento

de la información de las empresas y de las auditorías realizadas. También se realizaron pruebas de caja blanca a las funcionalidades terminadas.

DISCUSIÓN

En cuanto a las guías para la realización de auditorías de seguridad informática, son varias las empresas y organizaciones en Cubaque poseen procedimientos o guías para realizar ese proceso, entre ellas, la Empresa de Certificación de Seguridad y Protección (Acerprot), la Oficina de Seguridad para las Redes Informáticas (OSRI) y la Empresa de Aplicaciones Informáticas Desoft. También la mayoría de los ministerios y gobiernos provinciales tienen secciones encargadas de monitorear la seguridad informática en las entidades subordinadas. Todas estas guías o procedimientos tienen un alcance limitado, pues solo se centran en determinados elementos de la seguridad informática.

La guía metodológica que se propone en la investigación incluye los aspectos recomendados por los expertos que realizan este tipo de auditorías, lo cual la hace más abarcadora, así como toma en cuenta el marco de referencia la legislación vigente que recientemente ha sido aprobada en Cuba, elemento que la convierte en un referente actualizado, además de brindar un sistema de evaluación que permite unificar los criterios para que no dependa únicamente de la percepción del auditor y propone recomendaciones para mantener e implementar buenas prácticas en este campo.

La Empresa de Aplicaciones Informáticas Desoft en Pinar del Río, ha comenzado a utilizar esta guía metodológica como herramienta para realizar los diferentes servicios vinculados con la línea de producción de seguridad informática, como: asesoramiento para la elaboración del Plan de Seguridad Informática, las consultorías de las tecnologías informáticas y la detección de vulnerabilidades. Han sido varias las empresas que han contratado estos servicios, en las cuales se pudo validar la utilidad de la información obtenida, a través de la aplicación de la guía.

Por otra parte, se llevó a cabo un estudio del objeto de informatización del proceso de la auditoría a la seguridad informática, en el que hizo una revisión de otros *software* con temas afines. Entre los analizados se encuentra Diógenes, nombre de un *software* desarrollado por el Grupo de Investigación y Desarrollo de la OSRI, el cual verifica el estado de conformidad entre lo establecido oficialmente en la base legal de la seguridad de las tecnologías de la información y los controles implementados en una entidad.

Otro de los *software* fue el creado por la Empresa de Aplicaciones Informáticas Desoft, denominado Suit de Seguridad Informática, que permite identificar las PC conectadas a la red y el resto de dispositivos que se conecten a esta, y muestra alertas ante cambios de *hardware*. También permite ir actualizando algunos registros de seguridad informática de forma manual o automáticamente *(Productos / Desoft,* n.d.).

En el año 2013 se realizó una investigación titulada «Herramienta informática para la gestión de riesgos en TI», por el licenciado Luis Daniel Orta Cruz. El *software* obtenido, Riesgos

TI, propone una mejora al sistema Diógenes en su versión 2.0, siendo el cambio principal el uso de *software* libre para su implementación; pero está basado en la base legal anteriormente vigente en nuestro país, por lo que no está actualizado (Monografias.com, 2013).

De los sistemas informáticos mencionados ninguno aporta una solución abarcadora a la problemática de la auditoría, pues no se ajustan a la legislación vigente en nuestro país y no incluyen todos los aspectos que deben estar presentes en el proceso de auditorías de seguridad informática, que en Cuba se han convertido en pilar fundamental, ya que el Estado tiene como una de sus actividades priorizadas la informatización de la sociedad, aspecto que debe ir de la mano con garantizar de manera eficiente y eficaz la ciberseguridad.

Con el *software* propuesto se pueden realizar auditorías de seguridad informática, tanto por auditores externos a las organizaciones laborales, como por el personal encargado de implementar y mantener actualizado el SGSI de cada entidad. Además de la evaluación obtenida en las secciones que lo componen y en su totalidad, se derivan recomendaciones sobre buenas prácticas que se deben desarrollar en materia de seguridad informática y elementos que ayudan a minimizar el impacto de las vulnerabilidades detectadas. También es importante señalar que incluye todos los aspectos que se deben tener en cuenta en la realización de las auditorías de seguridad informática y está basado en las leyes vigentes en Cuba en esta materia.

CONCLUSIONES

Se elaboró una guía metodológica que optimiza el proceso de auditorías a la seguridad informática y provee a los auditores de una herramienta capaz de evaluar con exactitud los diferentes Sistemas de Gestión de Seguridad Informática, a partir de la información que ellos mismos van chequeando. También permite que usuarios no expertos puedan ir retroalimentándose con los resultados obtenidos a partir de cada aplicación.

Con el *software* para auditorías de seguridad informática, se pone a disposición de empresas, organismos y ministerios, una herramienta informática que actualiza el trabajo de auditoría, pues está basado en la metodología utilizada por la OSRI en Cuba, la cual a su vez se basa en lo estipulado en las Normas ISO 27000 y 27001 de carácter internacional, y en nuestra base legal.

Por las características del sistema, este puede ser utilizado por el personal encargado de auditar temas de seguridad informática y por profesionales que quieran implementar un SGSI o mejorar el que tienen según las disposiciones establecidas.

Referencias bibliográficas

Azán Basallo, Y., Bravo García, L., Romero, W., Trujil Márquez, D., García Romero, E. y Pimentel Rivero, A. (2014). *Solución basada en el Razonamiento Basado en Casos para el apoyo a las auditorías informáticas a bases de datos.* Retrieved November 4, 2019, from http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992014000200004

Lawrence D., Bodin, Lawrence A., Gordon, & Martin P. Loeb (2018). Cybersecurity insurance and risk-sharing-Science Direct. Retrieved November 4, 2019, from Science Direct website: https://www.sciencedirect.com/science/article/pii/S0278425418302382

Mesquida, A. L., & Mas, A. (2015). Implementing information security best practices on *software* lifecycle processes: The ISO/IEC 15504 Security Extension. Computers & Security, 48, 19-34. https://doi.org/10.1016/j.cose.2014.09.003

Ministerio de Comunicaciones (2019). Resolución 128-2019 [Text]. Retrieved November 8, 2019, from Ministerio de Comunicaciones website: https://www.mincom.gob.cu/es/documento-legal/resolucion-128-2019

Ministerio de Comunicaciones (2019). GOC-2019-045 [Text]. Retrieved November 8, 2019, from Ministerio de Comunicaciones website: https://www.mincom.gob.cu/es/documento-legal/GOC-2019-045

Monografias.com, L.D.O.C. (2013). Herramienta informática para la gestión de riesgos en tecnologías de la información-Monografias.com. Retrieved November 11, 2019, fromhttps://www.monografias.com/trabajos99/herramienta-informatica-gestion-riesgos-tecnologias-informacion/herramienta-informatica-gestion-riesgos-tecnologias-informacion3.shtml

Oficina de Seguridad para las Redes Informáticas (OSRI). (n.d.). Retrieved March 15, 2022, fromhttps://www.osri.gob.cu/

Productos /Desoft. (n.d.). Retrieved April 5, 2022, fromhttps://www.desoft.cu/es/productos/166

proyectosagiles.org. (2008). Retrieved 11 30, 2022, from Proyectos Ágiles:https://proyectosagiles.org/beneficios-de-scrum/#:~:text=Los%20principales%20beneficios%20que%20proporciona,y%20basada%20en%20resultados%20tangibles

Ramalingam, D., Arun, S., & Anbazhagan, N. (2018). A Novel Approach for Optimizing Governance, Risk management and Compliance for Enterprise Information security using DEMATEL and FoM. Procedia Computer Science, 134, 365-370. https://doi.org/10.1016/j.procs.2018.07.197

Schwabe, K. y Sutherland, J. (2020). La Guía Definitiva de Scrum: Las Reglas del Juego. Retrieved from https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-Spanish-European.pdf