RILCO
Revista de Desarrollo Sustentable, Negocios, Emprendimiento y Educación

Año 2 Número 12
Octubre 2020
ISSN 2695-6098

METODOLOGÍA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LOS ASPECTOS MÁS RELEVANTES DE LA NORMA CUBANA NC ISO IEC 27001:2016

Ing. Yailín Rojas Pupo,
yailin@ncholguín.cu
Oficina Territorial de Normalización de Holguín, Cuba

MSc. Pedro Francisco Tamayo García,
calidad@enpa.hlg.minag.cu
Empresa de Proyectos e Ingeniería del MINAG Holguín, Cuba

DraC Maira Moreno Pino,
mayramp188@gmail.com
Universidad de Holguín

Para citar este artículo puede utilizar el siguiente formato:

Yailín Rojas Pupo, Pedro Francisco Tamayo García y Maira Moreno Pino (2020): "Metodología para la gestión de la seguridad de la información basada en los aspectos más relevantes de la norma cubana NC ISO IEC 27001:2016", Revista de Desarrollo Sustentable, Negocios, Emprendimiento y Educación RILCO DS, n. 12 (octubre2020). En línea:
https://www.eumed.net/rev/rilcoDS/12/gestion-seguridad-informacion.html

RESUMEN

Muchas organizaciones, a raíz del avance tecnológico, no pueden garantizar la seguridad de la información, situación que trae como consecuencia la presencia de amenazas y riesgos de seguridad. El presente trabajo se encaminó a desarrollar una metodología para la gestión de la seguridad de la información, aplicando técnicas de seguridad alineadas con el estándar NC ISO IEC 27001,con el objetivo de analizar, evaluar, controlar y reducir los riesgos, para preservar la confidencialidad, asegurando que accedan a la información aquellos que estén autorizados, que la información y sus métodos de procesamiento sean exactos y asegurando que los usuarios autorizados tengan acceso a esta y a sus activos asociados cuando lo requieran. Se desarrolla una herramienta informática que cumple con las buenas prácticas y controles establecidos en la norma cubana NC ISO IEC 27002, para evaluar el nivel de seguridad de la información, con el fin de diagnosticar el sistema, identificar vulnerabilidades y evaluar los riesgos que se detecten, aplicando los controles necesarios que reduzcan los niveles de riesgos y proponiendo medidas hacia su mejora.

Palabras claves: Gestión de la información, seguridad de la información, vulnerabilidad, riesgos, amenazas.

ABSTRACT

Many organizations, due to technological progress, cannot guarantee the security of information, a situation that results in the presence of threats and security risks. The present work aimed to develop a methodology for information security management applying security techniques aligned with the NC ISO IEC 27001 standard under the objective of analyzing, evaluating, controlling and reducing risks, to preserve confidentiality ensuring that Those who are authorized access the information, that the information and its processing methods are accurate and ensuring that authorized users have access to it and its associated assets when required. A computer tool is developed that complies with the good practices and controls established in the Cuban standard NC ISO IEC 27002 to assess the level of information security, in order to diagnose the system, identify vulnerabilities and assess the risks that are detected, applying the necessary controls that reduce risk levels and proposing measures towards their improvement.

Keywords: Information management, information´s security, vulnerability, risks, threats.

INTRODUCCIÓN

El avance de las Tecnologías de la Información y las Comunicaciones (TIC) durante los inicios del presente siglo, ha creado una dependencia tal para el desarrollo de las actividades de cualquier organización (empresa, organismo estatal, organización social, entre otras) que el no poder contar con estas tecnologías en un momento determinado provoca un verdadero desastre, el cual, en función de su magnitud puede traer consigo incluso la desaparición de la propia organización. Debido a la existencia de este riesgo se ha convertido en un aspecto estratégico vital de la política de las organizaciones, garantizar la seguridad de la información (SI).

Las actuales sociedades avanzadas son denominadas frecuentemente sociedades de la información, pues el volumen de datos que es procesado, almacenado y transmitido es inconmensurablemente mayor que en cualquier época pretérita.

Además, no sólo el volumen sino la importancia de esta información para el desarrollo económico y social, no tiene parangón con la que tuvo en cualquier otra época. De hecho, en la actualidad, las empresas consideran que la información es un bien más de su activo y en muchos casos prevalece sobre los restantes.

Con la llegada de nuevas tecnologías,organizaciones de todos los sectores económicos se ven en la necesidad de abordar un proceso donde se adopten los controles y procedimientos más efectivos (Solarte, Rosero, & del Carmen Benavides, 2015) y coherentes con la estrategia de negocio al cual se debe dar prioridad basado en estándares, modelos y normas internacionales que, a través de una serie de mejores prácticas, proporcione una adecuada gestión que les permita asegurar, tanto interna como externamente, que se está realizando una gestión eficaz de la información que garantice la confidencialidad, integridad y disponibilidad de los sistemas de información e informáticos. Una de

las normas más reconocidas es la NC ISO IEC 27001:2016 que establece las guías, procedimientos y procesos para gestionarla apropiadamente, mediante un proceso de mejoramiento continuo, esto es conocido como Sistema de Gestión de la Seguridad de la Información (SGSI).

Es necesario el desarrollo de una metodología para la implementación de los controles dentro del SGSI que proteja los activos de manera rentable, a partir de un análisis de riesgos que determine qué activos se tratan de proteger, de qué se quieren proteger y por qué.

Como objetivo general de la investigación se plantea: Diseñar una metodología para la gestión de la SI que permita analizar, evaluar, controlar y reducir los riesgos para preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de las principales técnicas de seguridad existentes.

METODOLOGÍA

En el proceso de la investigación se utilizaron métodos teóricos y empíricos:

Teóricos:

Históricos - lógico: se utiliza para realizar análisis lógicos de la situación problemática, para su comportamiento histórico evolutivo y para la construcción del marco teórico y práctico de la investigación.

Analítico - sintético: Para analizar y sintetizar la información que se necesita a partir de la revisión de bibliografías, para el tratamiento y resumen de la información y la elaboración de conclusiones.

Empíricos:

La observación directa para caracterización del problema.

Revisión documental en literaturas especializadas.

Términos y definiciones (Fuente:(NC-ISO-IEC-27000, 2016))

Información: Conjunto organizado de datos procesados.

Activo: Cualquier información o elemento relacionado con el tratamiento de la misma que tenga valor para la organización.

Amenaza: Cualquier evento que pueda causar un daño a un sistema de información, pueden provocar ataques a sistemas informáticos, redes, instalaciones etc.

Vulnerabilidad: Fallo o debilidad en un sistema de información que puede quedar expuesta a una amenaza.

Control: Medidas de seguridad para evitar o minimizar la pérdida o falta de disponibilidad debido a las amenazas que actúan por una vulnerabilidad asociada a la amenaza.

Riesgo: efecto de la incertidumbre sobre los objetivos de la seguridad de la información.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Seguridad de información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de gestión: Conjunto de elementos interrelacionados o interactivos de una organización para establecer políticas, objetivos y procesos para alcanzar esos objetivos.

DESARROLLO DEL TEMA

La siguiente metodología está alineada con los principales aspectos de la norma cubana NC ISO IEC 27001, que promueve la adopción de un sistema basado en enfoque de procesos por lo que se puede decir que es coherente con el ciclo de gestión PHVA (Planear, Hacer, Verificar, Actuar) de Walter Andrew Shewhart, más popularizado por William Edwards Deming, con el fin de establecer, implementar, aplicar, dar seguimiento, mantener y mejorar el SGSI de una organización. Está compuesta por cuatro (4) etapas secuenciales como se muestra en la figura 1, las cuales serán detalladas para poder comprender los pasos a desarrollar. Como un requisito fundamental para cumplir los objetivos previstos se tiene que contar con el respaldo de la alta dirección a partir de un proyecto que incorpore personas, tiempo y recursos.

Se desarrolla una herramienta informática como apoyo a los proceso de revisión y actualización del SGSI.

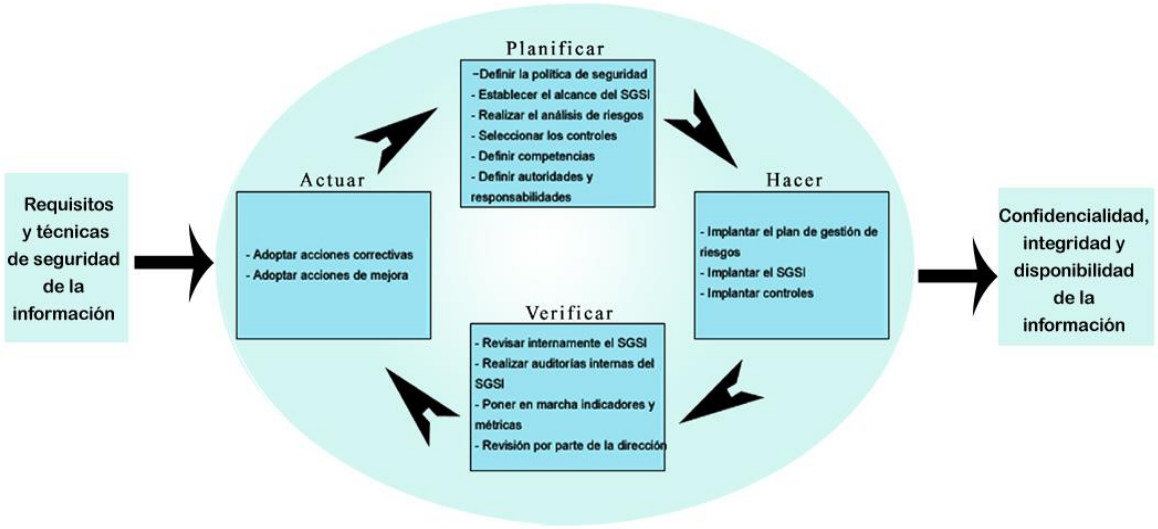

Figura 1. Ciclo PHVA aplicada a la gestión de la seguridad de la información basada en los aspectos más relevantes de la norma cubana NC ISO IEC 27001:2016.

1- Etapa 1. Planificación de un SGSI

En esta primera etapa se analizan y se crean las condiciones oportunas para el desarrollo y la futura implantación del SGSI; teniendo en cuenta los objetivos estratégicos de la organización se realizan un estudio del estado actual del sistema, con el objetivo de fijar las fallas de seguridad y determinar las necesidades según los activos de información que se quieren proteger y sus riesgos asociados para a partir de ahí precisar políticas, objetivos y procedimientos para aplicar un proceso de gestión de riesgos de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.

1.1 Definir la política de seguridad

La dirección establecerá una política de SI en correspondencia con los objetivos de la entidad y demostrará su apoyo y compromiso para la mejora continua del SGSI proveyendo un marco para definir los objetivos de SI.

La política del SGSI debe: estar disponible como información documentada, ser comunicada a todo el personal, estar disponible para las partes interesadas de manera apropiada, accesible y comprensible.

La dirección asegurará que el establecimiento de la política y los objetivos de la SI sean compatibles con la dirección estratégica de la organización y con las regulaciones y leyes vigentes. Es importante tener en cuenta que la política general de SI es una sola, pero a un nivel inferior debería apoyarse en políticas sobre temas específicos (NC-ISO-IEC-27002, 2016), que profundicen en la implantación de controles y que estén estructurados para atender las necesidades de determinados grupos dentro de la organización, ejemplo de estas políticas son: Control de acceso, clasificación de la información, uso adecuado de activos, transferencia de información, copias de respaldo. En algunas organizaciones se utilizan otros términos para estas políticas como normas, directivas o reglas.

Estas políticas deben ser comunicadas a los empleados y terceras partes relevantes de forma entendible y accesible al lector al que va dirigida.

1.2 Alcance del SGSI

La organización debe determinar los límites y la aplicabilidad del SGSI, entender las necesidades y expectativas de sus partes interesadas relacionadas a la SI para establecer su alcance, la misma debe estar documentada y disponible para todo el personal.

El SGSI debe formar parte y estar integrado con los procesos de la organización (NC-ISO-IEC-27001, 2016). La alta dirección debe precisar en qué actividades de la organización se desea implantar el SGSI, teniendo en cuenta las cuestiones externas e internas que son pertinentes para cumplir con los objetivos propuestos y que se ajusten a las necesidades de la organización. Como primera medida las primeras áreas y procesos que se deben considerar son aquellas que por sus funciones y responsabilidades ayudan en primera instancia a dar cumplimiento a la misión institucional (ISOTools Excellence, 2014); (Espinosa, 2014), las cuáles posteriormente y en algunos casos se debe determinar si existen ámbitos del negocio, ya sea porque difieren en tamaño, por el número de empleados y números de clientes o por su ubicación, ya que existen organizaciones que cuentan con varias sedes y pueden ir desde un proceso a un conjunto de procesos, de uno a varios servicios, por el volumen de información manejada o porque sus diferentes activos no precisen de la implantación de un protocolo de seguridad.

1.3 Realizar el análisis de riesgos

Para realizar un análisis de riesgos es necesaria una metodología que se ajuste a las necesidades de la organización, debe ser comprobable en el tiempo, que demuestre evolución en la implementación de controles a la hora de reducirlos y determinar el criterio de riesgo aceptable, es decir definir en qué nivel se aceptan, en cuál se aplican controles y en cuál se transfiere. Se deben

identificar los dueños de los riegos, ya que necesariamente los dueños de los activos de la organización no son los dueños de los riesgos, por lo que es necesario durante la realización del análisis contar con la colaboración de diversas áreas de la organización que podría estar integrado por:

- Dirigentes y funcionarios, que a los diferentes niveles responden por los activos de información que se procesan en las tecnologías.
- Personal de informática, que domina los aspectos técnicos necesarios para la implementación de los controles de seguridad.
- Profesionales de protección a partir de su responsabilidad en la custodia de los activos de la organización.

Esta metodología estaría compuesta por diferentes etapas comenzando por la recogida y preparación de la información, la identificación, clasificación y valoración de los activos a proteger, análisis de las principales amenazas, determinar cuáles son las áreas con una mayor incidencia, determinar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas, identificar el impacto para la entidad que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo para, a partir de este punto, determinar las necesidades de protección mediante la evaluación de riesgos que estaría orientada a la evaluación de las posibles consecuencias y el impacto que puedan causar a la entidad, determinar los niveles del mismo y posteriormente analizarlo.

Tratamiento de los riesgos

Una organización puede afrontar el riesgo básicamente de cuatro formas diferentes: eliminarlo, reducirlo, trasladarlo o asumirlo (Valencia & Alzate, 2017), según se muestra en la figura 2.

Asumir el riesgo: Se acepta la pérdida probable y se elabora un plan para su manejo.

Reducir el riesgo: Implica tomar medidas de prevención para disminuir el riesgo como medidas de protección para disminuir el impacto.

Transferir el riesgo: Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones.

Evitar el riesgo: Se toman medidas para evitar su presencia.

Figura 2: Gestión de riesgos.

1.4 Seleccionar los controles

Con el objetivo de que cada riesgo identificado previamente quede cubierto y pueda ser auditable, la norma NC ISO/IEC 27001:2016 establece en su última versión hasta 114 puntos de control, que

son un conjunto de acciones, documentos, medidas, procedimientos a adoptar para dar cumplimiento a los objetivos de la organización, que se dividen por las políticas de SI y controles operacionales. Los controles son medidas de seguridad orientadas a mitigar los riesgos encontrados en el análisis de estos de manera que se encuentren por debajo del nivel asumido por la organización.

Cada empresa, según su parecer, puede añadir más puntos de control si lo considera conveniente, así como personalizarlos para adaptarlos a su propio plan de control operacional, pero siempre debe estar alineados a lo que pide la norma. Los controles seleccionados por la organización serán recogidos en un documento llamado declaración de aplicabilidad donde se comparan los controles seleccionados con los del anexo A de la NC ISO IEC 27001 y se justifiquen las inclusiones de los 114 controles, estén implementados o no y la justificación de las exclusiones. A continuación en la tabla 1 se muestra un ejemplo.

Tabla 1: Ejemplo de declaración de aplicabilidad.

N.	N. Control	Descripción	Implementados	Justificación
1	5.1.1	Políticas para la SI	Si	Es necesario establecer políticas de SI para gestionar los objetivos de SI en la organización
2	5.1.2	Revisión de las políticas para la SI	Si	Es necesario hacer revisiones de las políticas para la SI a intervalos planificados con el fin de asegurar que se mantenga su idoneidad, adecuación y eficacia
3	6.1.1	Roles y responsabi-lidades en SI	Si	Es necesario establecer roles y responsabilidades para la protección de los activos y para llevar a cabo procesos de seguridad específicos

Plan de tratamiento de riesgo

Es importante tener en cuenta que la elaboración de un plan de tratamiento de riesgos requiere un análisis de costo-beneficio de los controles a implementar y los techos presupuestales asignados para su elaboración, de allí la importancia de priorizar aquellos escenarios de riesgo que son más críticos para la organización.

El propósito del plan es documentar como será implementado, que sea consistente con las metas y objetivos de la organización en la planificación del proceso de gestión (Bertolín, 2008), (Avellaneda, 2011); (Castro & Bayona, 2011); (Nieves, 2017) incluyendo las razones del tratamiento, los beneficios que se esperan obtener, los responsables de su aprobación e implementación, los recursos que se necesitan, medidas de tratamiento, tiempo y programación de cada una de las actividades. A continuación en la tabla 2 se muestra un ejemplo de plan de tratamiento de riesgo.

Tabla 2: Ejemplo de plan de tratamiento de riesgo

N.	Amenaza	Vulnerabilidad	Activos	Dueño del riesgo	Clasificación riesgo	Medidas a implementar	Fecha ejecución
1	Ataque por virus informáticos	Falta de un antivirus	Área de servidores Estaciones de trabajo	Administrador de Red de la organización	Alta	- Instalación de antivirus en todas las PC de la organización con actualización diaria	May/2020

1.5 Definir competencias

La organización debe: determinar las competencias necesarias de las personas que realizan trabajos que afectan el cumplimiento de los objetivos de la organización en SI, debe asegurarse que el personal con el que cuenta tenga experiencia adecuada a la actividad a realizar o formación profesional afín, debe capacitar al personal cuando sea aplicable y evaluar la eficacia de las acciones llevadas a cabo, debe conservar la información documentada como evidencia de la competencia en SI del personal según su puesto o función en la organización.

1.6 Definir autoridades y responsabilidades

La alta dirección debe asegurarse de que las responsabilidades y autoridades se decidan según el puesto o función que realiza el personal pertinente, quien está autorizado a acceder a la SI y se comuniquen dentro de la organización. También la alta dirección puede asignar un responsable para informar sobre el comportamiento del SGSI dentro de la organización.

2- Etapa 2: Implementación del SGSI

Durante el proceso de implementación del SGSI se comienzan a gestionar los riesgos identificados mediante la aplicación de los controles seleccionados y las acciones apropiadas por parte del personal definido, los recursos técnicos disponibles en función de la seguridad y las medidas administrativas, de manera que se mantenga siempre el riesgo por debajo del nivel asumido por la propia entidad y esté en correspondencia con el cumplimiento de los objetivos de la organización.

La organización asegurará que el personal tenga conciencia de la necesidad e importancia de las actividades de SI que le corresponde realizar, garantizará la divulgación y comprensión de las políticas de seguridad implementadas, debe capacitar al personal según se implanten los procedimientos para así contribuir al logro de los objetivos del SGSI.

Se requiere además precisar el procedimiento de medición de la eficacia de los controles o grupos de controles seleccionados y especificar cómo se van a emplear estas mediciones, con el fin de evaluar su eficacia para producir resultados comparables y reproducibles y de esta forma determinar si las actividades de seguridad implementadas satisfacen las expectativas concebidas.

2.1 Implantar el plan de gestión de riesgos

La implementación de un plan de gestión de riesgos está orientada principalmente a la clasificación de las alternativas para manejar los riesgos a que puede estar sometido un activo dentro de los procesos en una organización. Se establece una estructura bien definida, con controles adecuados a su conducción, mediante acciones factibles y efectivas desde la calificación, identificación, análisis, evaluación y tratamiento de los riesgos, descritos en esta metodología en la fase 1 de planificación, hasta acciones descritas en las fases 3 y 4 para el análisis y monitoreo del SGSI, las auditorías, las revisiones por parte de la dirección y la actualización del SGSI.

La organización debe conservar información documentada de los resultados obtenidos.

2.2 Implantar el SGSI

La implantación de un SGSI es una decisión estratégica que involucra a toda la organización, debe ser parte de su estructura y como tal se incorpore como parte de los procesos en aquellas actividades que requieren adecuados niveles de protección de la información, debe ser apoyada y dirigida desde la dirección.

El tiempo de implantación del SGSI varía en función del tamaño de la empresa, el estado inicial de la seguridad de la información y los recursos destinados a ello.

2.3 Implantar controles

Durante la implantación de los controles del SGSI es necesaria la participación de los jefes de procesos, pues es primordial que se determine si en las actividades que lo requieren los controles seleccionados cubren los riesgos que para ellas fueron identificados.

Para lograr la implantación de estos controles es necesario definir los plazos para su cumplimiento y el personal responsabilizado para su ejecución; puede que por falta de algunos recursos que alguno de ellos necesite para su ejecución se requiera de un tiempo adicional.

3- Etapa 3: Revisar internamente el SGSI

La alta dirección debe: realizar revisiones periódicas del SGSI, seleccionar al responsable de hacer el seguimiento y la medición, en qué período se realizará, a que procesos hacer seguimiento y que es lo que se va a medir. Es necesario ejecutar procedimientos de revisión mediante instrumentos de medición que posibiliten detectar errores de proceso, identificar fallos de seguridad de forma rápida y determinar las acciones a realizar, ejemplo: La revisión de las mediciones de la eficacia de los controles para verificar que no se produzcan nuevos riesgos de seguridad, revisar las evaluaciones, los tratamientos de riesgos y los procedimientos de detección y prevención de incidentes; también es necesario verificar si los resultados que se obtienen cumplen con lo que se estableció en los objetivos de la organización.

La organización debe conservar información documentada como evidencia de los resultados.

3.1 Realizar auditorías internas

El SGSI debe ser auditado regularmente a intervalos determinados por la alta dirección ya que muchas veces las personas no son conscientes de que están haciendo algo mal y de saberlo no quieren ser descubiertos y esto puede llegar a dañar a la organización. Es necesario planear un

programa de auditoría teniendo en cuenta la importancia de los procesos y el alcance de la misma, hay que tener en cuenta los resultados de las auditorías anteriores.

Para realizar el proceso de auditoría es de apoyo la norma NC ISO 19011 que establece las directrices para auditar sistemas de gestión.

3.2 Indicadores y métricas

Es necesario que los indicadores estén alineados con los objetivos de la organización. En esta etapa adquieren especial importancia los registros (evidencias) que dejan los diferentes controles, así como los indicadores que permiten verificar el correcto funcionamiento del SGSI (QUIRÓS, 2010), la organización definirá su criterio respecto a qué aspectos quiere controlar y medir y el periodo en que se van a medir. Existen dos tipos de indicadores o métricas, los indicadores clave del desempeño (KPI) cuando se quieren reflejan los resultados relevantes de la organización y los indicadores clave de riesgo (KRI) cuando una métrica muestra advertencia en relación a riesgos operacionales.

Ejemplo de indicadores KPI

- Establecer los activos críticos que afectan a la organización
- Mejora de la satisfacción de los clientes
- Divulgación de la política de seguridad a los empleados
- Tratamiento de eventos
- Implementación de controles

Ejemplo de indicadores KRI

- Medir incidentes de SI
- Copias de seguridad

3.3 Revisión por parte de la dirección

La alta dirección tiene la responsabilidadde revisar el SGSI a intervalos planificados para asegurarse de su conveniencia, adecuación y eficacia, teniendo en cuenta las acciones desde anteriores revisiones por la dirección. Debe conocer si el SGSI obtiene los resultados deseados y a partir de ahí tomar decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el SGSI.

La organización debe conservar información documentada como evidencia de los resultados.

4- Etapa 4: Actualización del SGSI

El SGSI debe mantenerse eficiente durante todo el tiempo adaptándose a los cambios internos de la organización, así como los externos del entorno. La organización deberá mejorar continuamente la idoneidad, adecuación y eficacia del SGSI, reaccionar ante las no conformidades cuando ocurran llevando a cabo las acciones de mejora y corrección, se debe establecer un plan, un responsable y un cronograma a ejecutar para atenuar o eliminar estas no conformidades, aplicando las medidas necesarias, revisando si las acciones correctivas adoptadas son eficaces y realizar los cambios necesarios al SGSI con el fin de mejorar y evitar que se repitan los problemas detectados.

5- Herramienta informática para diagnosticar el SGSI

El desarrollo de esta herramienta informática tiene como propósito funcional ofrecer a la organización la posibilidad de autoevaluar el SGSI. El software ofrece un cuestionario basándose en las técnicas de seguridad de la NC ISO IEC 27002 en las que la organización debe seleccionar a conciencia las respuestas, estas estarán asociadas a riesgos que pueden o no estar presentes en la organización dependiendo de su entorno de trabajo. A partir de ese punto se alinea cada riesgo con propuestas de posibles controles para reducirlos. Una vez respondido completamente el cuestionario brinda una calificación que caracteriza al sistema según sus resultados y ofrece recomendaciones para solucionar cada una de las no conformidades detectadas, siendo de gran apoyo en las etapas 3 y 4 de revisión y actualización del SGSI. Esta herramienta es una multimedia interactiva creada a través de los software Macromedia Director y Adobe Shockwave empleando el lenguaje de programación JavaScript y otros de carácter secundario.

CONCLUSIONES

Con el desarrollo de este trabajo se propone una metodología compuesta por cuatro etapas que conforman el proceso de diseño, implementación, revisión, seguimiento, mantenimiento y mejora de un SGSI basada en los aspectos más relevantes de la norma cubana NC ISO IEC 27001. Aporta un proceso metodológico que comienza por la recogida y preparación de la información, la identificación, clasificación y valoración de los activos a proteger mediante el análisis, la evaluación y la gestión de los riesgos que inciden sobre estos y los controles a implementar para gestionarlos o eliminarlos.

Para apoyar las etapas de revisión y mejora del sistema se hace uso de una herramienta informática que tiene como propósito funcional evaluar el nivel de seguridad de la información con el fin de diagnosticar el sistema, identificar vulnerabilidades y proponer medidas para solucionar los problemas detectados.

REFERENCIAS BIBLIOGRÁFICAS

1. Avellaneda, J. C. (2011). Medición de un SGSI: diseñando el cuadro de mandos.
2. Bertolín, J. A. (2008). Seguridad de la información. Redes, informática y sistemas de información: Editorial Paraninfo.
3. Castro, A. R., & Bayona, Z. O. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería, 16*(2), 56-66.
4. Espinosa, D., Martínez, J., & Amador, S. (2014). Gestión del riesgo en la seguridad de la información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la Metodología OCTAVE-S. Ingenierías USBMed, 5(2), 33-43
5. ISOTools Excellence. (2014). iso-27001-sistema-gestion-seguridad-información.
6. NC-ISO-IEC-27000. (2016). Tecnología de la información-técnicas de seguridad-sistemas de gestión de seguridad de la información-visión de conjunto y vocabulario.

7. NC-ISO-IEC-27001. (2016). Tecnología de la información-técnicas de seguridad-sistemas de gestión de seguridad de la información-requisitos.
8. NC-ISO-IEC-27002, O. (2016). Tecnología de información - Técnica de seguridad - Código de prácticas para controles de seguridad de la información.
9. Nieves, A. C. (2017). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma Iso/iec 27001: 2013.
10. QUIRÓS, AGUSTÍN L. (2010). Uso de la norma ISO/IEC 27004 para Auditoría Informátic.
11. Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL*, 28(5). 14-27.
12. Valencia, F. J. D., & Alzate, M. O. (2017). Implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. doi: 10.17013/risti.22.73–88