Universidad de Holguín

FACULTAD
CIENCIAS EMPRESARIALES
Y ADMINISTRACIÓN

DEPARTAMENTO DE INGENIERÍA INDUSTRIAL

MÁESTRIA EN INGENIERÍA INDUSTRIAL

PROCEDIMIENTO PARA IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN COMO CONTRIBUCIÓN A LA CALIDAD DE LA INFORMACIÓN DE LOS SERVICIOS DE CONSULTORÍA. APLICACIÓN EN EL CIGET DE HOLGUÍN

TESIS PRESENTADA EN OPCIÓN AL TÍTULO ACADÉMICO DE

MÁSTER EN INGENIERÍA INDUSTRIAL

MENCIÓN CALIDAD

Autor: Ing. Yudelkis Olivera Argota

Tutora: Dr. C Mariluz Llanes Font

HOLGUÍN, 2019

RESUMEN

La información se ha convertido en uno de los más importantes activos de la organización. Hoy en día la preocupación no es solo ser productivos y generar nuevos productos o servicios sino también el de protegerse ante cualquier tipo de ataque. Asegurar la disponibilidad, la confidencialidad e integridad de la información es una garantía que debe brindar la organización, como atributos para elevar la calidad de los servicios y el valor de sus activos, razón que amerita una correcta gestión de la seguridad mediante procesos documentados y conocidos.

En la investigación, se analizan diferentes enfoques a través del uso de métodos teóricos y empíricos, con el objetivo de desarrollar un procedimiento para implementar un sistema de gestión de seguridad de la información normalizado en el Ciget de Holguín que contribuya a elevar la calidad de los servicios de consultoría. El mismo adopta como referencia la norma cubana ISO/IEC 27001:2016. El procedimiento consta de seis fases y quince pasos, donde se definen las etapas, objetivos, pasos y técnicas necesarias a utilizar para su desarrollo.

Como resultados de la aplicación parcial del procedimiento, se lograron resultados como la conformación de un equipo gestor que garantice el diseño, la implementación, control y mejora del sistema. Se logró ganar en cultura de gestión de seguridad por parte de los trabajadores y se realizó un inventario de activos de información.

CONTENIDO

INTRODUCCIÓN

La informatización de la sociedad a todos los niveles es una necesidad que se acrecienta en correspondencia con el desarrollo científico y tecnológico, con énfasis en la información que se requiere para abordar el crecimiento en diferentes ramas del saber, lo cual es posible a partir del desarrollo de las nuevas tecnologías de la informática y la comunicación, e incluye tanto a los países desarrollados como a los subdesarrollados entre los que se incluye Cuba, que además está sometida a un bloqueo que impide la adquisición de medios y equipos necesarios para la mayor calidad en las investigaciones necesarias para el desarrollo económico social.

A escala nacional e internacional diversos autores tratan el tema de la información y sus diversas aristas, sin embargo no todos coinciden en relación con la manera de utilizarla, protegerla y asegurarla a partir de las necesidades de los actores sociales que la solicitan a las entidades que tienen como objeto social prestar servicio en tal sentido, esta investigación comparte los postulados referidos por Vilalta & Espinosa (2008), Bauer, Pavlov & Karakaneva (2011), Bernroider & Chudzikowski (2017) y Hussain (2017) donde plantean que la información se ha convertido en uno de los más importantes activos de la organización.

Los autores precitados refieren además que existe la necesidad de gestionar adecuadamente aquella con la que habitualmente se trabaja. En las organizaciones de consultoría empresarial, este tema se hace más evidente por la misión que los mismos desarrollan, la información no se encuentra presente solo en sus procesos de gestión internos, sino que manipulan datos que forman parte de la gestión integral de otras organizaciones. La calidad de los servicios se estar vinculada con una información integral y disponible para ser utilizada, así como un control de la misma para que los datos con carácter confidencial solo sean utilizados por las personas con privilegios de uso, eso implica que no solo hay que saber cómo gestionar la información interna de la organización, sino saber manipular aquellas que son provistas por terceros.

Independientemente de la forma que tome o los medios por los que se comparta o almacene la información y los procesos que la apoyan, esta debe protegerse de forma adecuada. Por lo que la disponibilidad, integridad y confidencialidad de la misma pueden ser esenciales para mantener la gestión, competitividad, rentabilidad, cumplimiento de la legalidad e imagen organizacional. Hoy en día la preocupación de una organización no es solo el de ser productivos y el de generar nuevos productos o servicios sino también el de protegerse ante cualquier tipo de ataque.

Numerosas son las empresas internacionales que en la actualidad acentúan sus bases en servicios que se relacionan con la seguridad de la información, entre ellas se encuentran DUX Diligens, Sebgon, Integridata, Áudea, todas tienen como finalidad la del desarrollo de consultoría de seguridad con base en mejores prácticas de la industria.

La investigación sostiene que la gestión de seguridad de la información (GSI) es la mejor manera de supervisar, controlar, revisar periódicamente el trabajo de la organización al tener en cuenta que, proporciona una dirección de las actividades relacionadas. El uso de estándares internacionales como la ISO 27001 aporta una guía metodológica para el logro efectivo de la misma.

La seguridad de la información en Cuba, según el sitio institucional de las fuerzas armadas revolucionarias (2014), tiene como condición necesaria garantizar la disponibilidad, confidencialidad e integridad que este necesita emplear para su desarrollo y defensa; se impide el empleo ilegal o pernicioso del espacio informativo nacional y se garantiza la divulgación de la verdad sobre la revolución cubana así como las amenazas o agresiones a que es sometida.

Por otra parte la protección de la Información en el país juega un papel importante en materia de seguridad, por tal motivo se declaran normas, procedimientos, leyes y decretos que regulan lo que se vincula a la seguridad de la información, entre ellos sobresalen el decreto ley 221 de los archivos de la república de Cuba, Resolución 127/2007 Reglamento de seguridad para las tecnologías de la información , Decreto Ley No. 199/1999 del Consejo de Estado, Decreto No. 281 (Reglamento para la Implementación y Consolidación del Sistema de Dirección y Gestión Empresarial Estatal), Documentos Rectores de la Ciencia y la Innovación Tecnológica (2001), Política Nacional de Información (2008) y la familia de normas ISO 27001.

Si bien el país declara la importancia de la información y la necesidad de incentivar las medidas de control sobre esta, la seguridad de la información es asumida de manera desarticulada, siendo tratada desde una perspectiva del control de la seguridad informática en las empresas, observada como un simple tema de cumplimiento legal o un simple problema técnico.

La seguridad informática es un proceso que se encuentra inmerso dentro la seguridad de la información, pero no abarca todo lo que esta plantea, pues intenta proveer de medidas de a otros medios donde se localice la información, no solo la tecnológica sino incluso proporciona medidas con respecto a las personas que la manipulan.

Según datos de la oficina territorial de normalización, en el territorio de la provincia Holguín, hasta principios del año 2019, no existen organizaciones con el Sistema de Gestión de la Seguridad de la Información (SGSI) certificado a partir de la norma cubana (NC) ISO/IEC 27001:2016, adoptada por Cuba para garantizar la GSI, por lo que la búsqueda de alternativas dirigidas a su concreción es una necesidad para las entidades comprometidas con ello, tal es el caso del Centro de Información y Gestión Tecnológica de Holguín en lo adelante Ciget, organización perteneciente al CITMA, especializada en prestar servicios de consultoría empresarial, propiedad industrial y gestión del conocimiento al sector estatal y privado para

favorecer la toma de decisiones, la solución de problemas y el desempeño de las organizaciones a través de una adecuada gestión de la información.

Al tratarse de una organización de gestión de información, la misma maneja datos que en ocasiones son sensibles, por lo cual debe ser protegida ya sea para garantizar las exigencias de los clientes, así como evitar la fuga de información que pueda ser utilizada de manera inadecuada por personas o instituciones ajenas a la organización.

El Ciget se inserta en el cumplimiento de estas normativas para el control de la seguridad de la información donde establece como uno de sus principales activos imprescindibles en el logro de sus objetivos estratégicos a la Información, es por ello que la alta dirección a partir del año 2015 como parte de los procesos de perfeccionamiento de los sistemas internos fomenta las actividades para el aseguramiento de esta, sin embargo solo cuenta con procedimientos para el control de la seguridad informática, obviándose en ocasiones lo relacionado con la gestión de la información en los servicios científico técnicos en detrimento de la calidad a que se aspira.

A partir de la revisión de auditorías, autocontroles, entrevistas y diagnósticos previos realizados condujo a determinar que existen insuficiencias que limitan la seguridad de la información tales como:

- Escasa cultura organizacional e involucramiento en relación con la gestión de la seguridad de la información.
- La organización no cuenta con procedimientos documentados que permitan una correcta gestión de auditoría en seguridad.
- Insuficientes mecanismos que permitan centralizar y asegurar la disponibilidad de la información para todos los trabajadores.
- Débil identificación de los riesgos sobre seguridad de la información y su implicación con la calidad de los servicios.
- No existencia de un sistema de gestión de seguridad de la información amparado en sistemas normalizados que permitan generar una organización más flexible con altas posibilidades de responder a un entorno cada vez más cambiante.

Las insuficiencias referidas conducen a formular el siguiente **problema científico**: ¿Cómo implementar un SGSI normalizado en el Ciget de Holguín que contribuya a elevar la calidad de la información de los servicios de consultoría?

Para dar solución al problema de investigación se determinó la necesidad de incidir en el siguiente **objeto de la investigación**: la seguridad de la información. Para tratar de encontrar la solución al problema desde el objeto y el campo seleccionados se traza como **objetivo general de la investigación:** Desarrollar un procedimiento para implementar un SGSI normalizado en el

Ciget de Holguín que contribuya a elevar la calidad de la información de los servicios de consultoría.

Para consolidar el objetivo general se precisaron los **objetivos específicos** siguientes:

- Elaborar el marco teórico - práctico referencial de la investigación.
- Diseñar el procedimiento para la implementación de un SGSI como contribución a la calidad de la información de los servicios de consultoría.
- Aplicar parcialmente el procedimiento para la implementación del SGSI como contribución a la calidad de la información de los servicios de consultoría en el Ciget de Holguín.

Para incidir en el objeto declarado en pos de encontrar solución al problema se selecciona como **campo de acción**: los Sistemas de Gestión de Seguridad de la Información como contribución a la calidad de la información de los servicios de consultoría en el Ciget de Holguín.

Con el fin de predecir una respuesta que constituye la solución del problema y como tal, orientar y guiar el proceso investigativo, se plantea la siguiente **Idea a defender**: El desarrollo de un procedimiento para implementar el SGSI normalizado en el Ciget de Holguín contribuye a elevar la calidad de la información de los servicios de consultoría.

En el desarrollo de la investigación se utilizaron métodos teóricos y empíricos, así como técnicas y herramientas de la Ingeniería Industrial y otras especialidades afines. Dentro de los **métodos teóricos** se encuentran el análisis y síntesis de la información obtenida a partir de la revisión de literatura y documentación especializada, la redacción de las conclusiones y recomendaciones; el inductivo-deductivo propició llegar a generalizaciones y razonamientos después de conocer las interioridades de la seguridad de la información, además de analizar el sistema en el diseño y aplicación del procedimiento propuesto; el sistémico estructural para el desarrollo del mapa mental del marco teórico práctico de la investigación, el análisis de las interrelaciones entre la ISO/IEC 27001:2016 e ISO 9001:2015 para el establecimiento del paso 7, así como en la enfoque integral que se aplicó en el procedimiento. Los **métodos empíricos** se relacionan con la observación científica de los procesos y sus resultados a través de la organización. Se aplican técnicas como: entrevistas a trabajadores y especialistas de información en el territorio, observación directa, entre otras. Su aplicación sistémica permite el desarrollo exitoso de las diferentes etapas de la investigación y el alcance de los resultados previstos.

Para su presentación, esta tesis se estructura de la forma siguiente: un capítulo I, que contiene el marco teórico práctico referencial que sustenta la investigación; en el capítulo II, se describirá el instrumental metodológico desarrollado; un capítulo III, donde se mostrará la aplicación parcial del procedimiento en el Ciget de Holguín, así como conclusiones y recomendaciones derivadas de la investigación; la bibliografía consultada y finalmente, un grupo de anexos de necesaria inclusión, como complemento de la investigación realizada.

CAPÍTULO I. MARCO TEÓRICO PRÁCTICO REFERENCIAL DE LA INVESTIGACIÓN EN RELACIÓN CON LOS SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Este capítulo brinda el soporte teórico a la investigación, a través de la revisión de la literatura especializada, así como otras fuentes consultadas, con el objetivo de elaborar el estado del arte y de la práctica en el área de la seguridad de la información, que posibilite fundamentar las bases teóricas y prácticas de la investigación. El mapa mental para construir el marco teórico práctico se muestra en la figura 1.

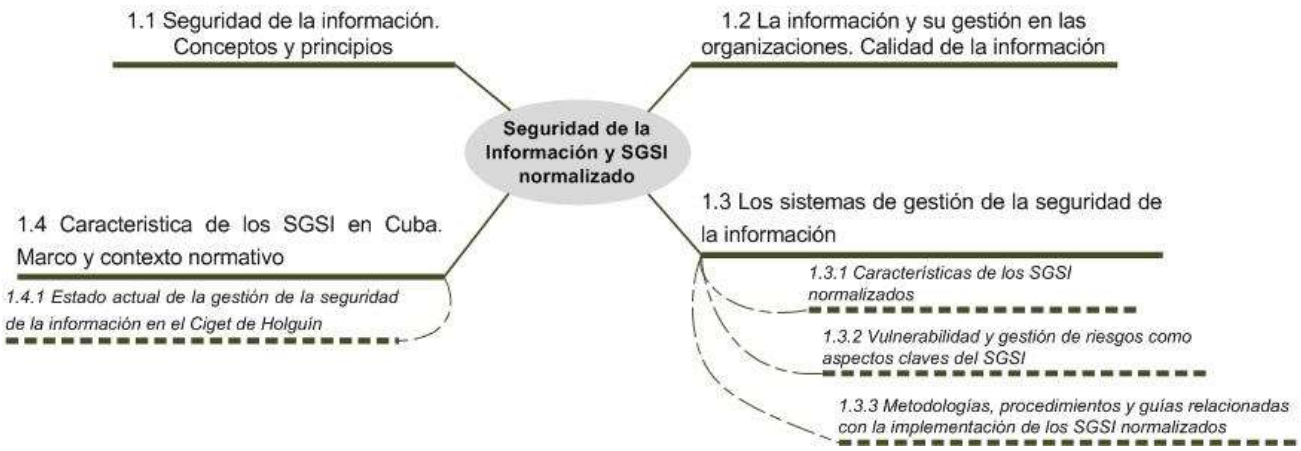


Figura 1. Mapa mental del marco teórico práctico de la investigación.

1.1 Seguridad de la información. Conceptos y principios

Según la Real Academia Española (RAE) seguridad se define como una cualidad cuando algo se encuentra seguro, que el mismo debe ser libre y exento de todo peligro, daño o riesgo, cierto, que no puede dudarse, firme o bien sujeto y que no falla o que ofrece confianza.

Al analizar la definición de seguridad según la RAE, se observa una total convergencia en relación con la seguridad de la información, sin embargo, una mayor precisión en tal sentido deviene de los fundamentos teóricos por los que transita la construcción del capítulo 1.

Seguridad de la información

Para Medina (2017) la seguridad de la información es una solución integrada que combina recursos organizacionales, procesos y tecnología. En la investigación se asume esta conceptualización al entenderse que los aspectos que le caracterizan están vigentes en las interioridades del problema que se investiga, aun cuando desde el punto de vista praxiológico no revela aportes que favorezcan una posible solución

La universidad de Veracruzana (2019) conceptualiza a la seguridad de la información, como un proceso integrado por estrategias, medidas preventivas y medidas reactivas que se ponen en

práctica en las instituciones para proteger la información y mantener su confidencialidad, disponibilidad e integridad de la misma. Esta conceptualización no tiene un sustento teórico, el abordaje se propone desde la praxis a través de diferentes vías que aunque se considera pueden ser una solución, no rebasan los criterios que según la investigación pueden dar mayor precisión en tal sentido, a través de un procedimiento. Así mismo sobre la base del mismo concepto anteriormente expuesto, se muestra en el sitio web "Evaluando Software.com" quienes afirman que la seguridad de la información empresarial es el conjunto de medidas que permitan mantener la calidad de la información en los tres principales pilares de seguridad.

Para Margaret (2016) la seguridad de la información es un conjunto de estrategias para administrar los procesos, herramientas y políticas necesarias para prevenir, detectar, documentar y contrarrestar las amenazas a la información digital y no digital. En esta conceptualización al igual que en la anterior prevalece el abordaje práctico, a través de la estrategia como vía de intervención.

Una importante reflexión lo constituye la pronunciada por Clastornik (2017) en conferencia de apertura de la 77ª edición de Segurinfo en Uruguay, donde señala que la seguridad de la información es parte de una transformación que se hace entre todos, la misma no constituye sólo un tema de tecnología sino también de un cambio cultural, de conceptualización y sensibilización del problema y gestión del cambio. Si bien no tiene un soporte teórico, si brinda una interesante reflexión para las organizaciones.

La NC ISO/IEC 27000:2016 define la seguridad de la información como la "preservación de la confidencialidad, integridad y disponibilidad de la información". Si bien no caracteriza el objeto de estudio, si define el objetivo que se persigue con la misma.

De igual forma se asume lo referido por Iriarte (2006) en relación con la seguridad de la información, al plantear que la misma tiene que ser un proceso continuo que implica el accionar de todo el personal de la organización a través de procedimientos, políticas y controles, las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener.

La seguridad de la información está orientada a reforzar la credibilidad de los servicios y de esta forma proporcionar la confianza adecuada frente a los clientes. Al referirse al término de seguridad de la información en la actualidad, la mayoría de los usuarios lo relacionan con el tema de la seguridad informática o ciberseguridad, quienes lo asumen como un mismo concepto, cuando en realidad existen aspectos que las distinguen según lo plantean diferentes autores, tal como aparece en la siguiente tabla:

Seguridad de la Información	**Seguridad informática**	**Ciberseguridad**
Se ocupa de la seguridad	Es el proceso de tomar medidas	Atienden en dos pliegues.

básica que incluye el armado de estrategias de seguridad de la información, estándares / políticas, gestión de riesgos, intrusión, solución de detección, conciencia de seguridad y enmarcar la defensa en capas que incluirá ingeniería, diseño y endurecimiento de cortafuegos.	preventivas físicas y de software para proteger la infraestructura de red subyacente del acceso no autorizado, mal uso, mal funcionamiento, modificación, destrucción o divulgación indebida, creando así una plataforma segura para que las computadoras, los usuarios y los programas realicen sus tareas permitidas.	Investigación de incidentes: incluya la función de realizar análisis forense, realizar recuperación de datos, informar métricas de seguridad y tomar instantáneas de imágenes y discos.
Los especialistas en seguridad de la información se centran en diseñar, implementar y mantener una política de seguridad integral con el objetivo de resguardar toda la información de la organización, independientemente del formato en que se encuentre.	Los especialistas en seguridad informática se centran en la protección interna al mantener una estrecha vigilancia de las contraseñas, los firewalls, el acceso a Internet, el cifrado, las copias de seguridad y más. Su objetivo principal es proteger la información interna mediante la supervisión del comportamiento de los trabajadores y el acceso a la red.	Los especialistas en ciberseguridad se centran en las amenazas externas buscando hackers que intenten infiltrarse en la red y obteniendo información sobre posibles ataques futuros.
Preserva los activos de información sin importar su forma o estado (formato digital, en forma física, así como la manera no representada, como pueden ser las ideas o el conocimiento de las personas).	Salvaguarda los activos de información en formato digital y los sistemas informáticos que los procesan y almacenan, indistintamente si están interconectados o no.	Protege cualquier cosa en el ámbito cibernético.
Involucra la seguridad de la información física.	No se ocupa de la información física.	No se ocupa de la información en papel.
Se ocupa de la protección de datos contra cualquier forma de amenaza.	Se ocupa de los peligros de la información electrónica.	Se ocupa de los peligros en el ciberespacio.
Trabaja contra el acceso, divulgación, uso, modificación, interrupción o destrucción no autorizados de la información.	Vela contra el acceso, divulgación, uso, modificación, interrupción o destrucción no autorizados de la información digital.	La ciberseguridad se esfuerza contra los delitos cibernéticos y los fraudes cibernéticos.

Estas tres disciplinas son distintas, pero comparten como objetivo común la protección de la información. La diferencia entre ellas está en el tipo de recurso que incide cada una. La

seguridad informática y ciberseguridad se centran en proteger la información digital e infraestructuras tecnológicas, mientras que la seguridad de la información está relacionada con proteger la información como activo estratégico, independientemente de si se mantiene digitalmente o no. Los rasgos que definen cada una permiten encontrar puntos de convergencia, lo que asegura que la seguridad de la información constituye un todo único, que integra diferentes factores y elementos.

El análisis de las conceptualizaciones de seguridad de la información revela elementos que convergen entre todas las definiciones. Para el desarrollo de esta investigación se asumirá que una información se considera segura cuando a través de los medios desplegados a través de estrategias que permitan identificar, valorar y gestionar la información como activo de la organización para preservar la confidencialidad, integridad, disponibilidad, autenticidad, responsabilidad, no repudio y fiabilidad de la misma.

A continuación se despliegan conceptos de los principios de seguridad que serán adoptados, para un mejor entendimiento de los mismos.

Confidencialidad

Según la RAE es la condición cuando se hace o se dice en la confianza de que se mantendrá la reserva de lo hecho o lo dicho.

En relación con la seguridad de la información varios autores consultados conceptualizan la confidencialidad como:

la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona. Ávila (2013)

Pérez & Gardey (2013) lo abordan como una propiedad de la información que pretende garantizar el acceso sólo a las personas autorizadas. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a ésta información.

Por otra parte en artículo de la Biblioteca de la CEPAL (2019) aporta un elemento distinto cuando refiere que la confidencialidad es al acuerdo del investigador con el participante acerca de cómo se manejará, administrará y difundirá la información privada de identificación. La propuesta de investigación debe describir las estrategias para mantener la confidencialidad de los datos identificables, incluidos los controles sobre el almacenamiento, la manipulación y el compartir datos personales. En esta conceptualización se entiende al investigador como el cliente y como participante a la organización que presta el servicio.

En tanto en la NC ISO/IEC 27001:2016 la confidencialidad garantiza que la información no sea accesible para personas no autorizadas.

Integridad

Según la RAE la integridad se alcanza cuando algo no carece de ninguna de sus partes.

El Instituto Nacional de Ciberseguridad de España (Incibe, 2018) declara que la integridad de la información hace referencia a que la misma sea correcta y esté libre de modificaciones y errores.

La NC ISO/IEC 27001:2016 refiere que la integridad protege la información y los sistemas para que no sean modificados por personas no autorizadas; asegura que los datos sean precisos y confiables.

Disponibilidad

La RAE define a la disponibilidad como algo que se puede disponer libremente de ella o que está lista para usarse o utilizarse. Otros conceptos relacionados con este son:

Los autores Suhail & Quadri (2016) hacen referencia a la disponibilidad de la información como la capacidad de hacer que la información y los recursos físicos y lógicos relacionados sean accesibles según sea necesario, cuando se necesiten y dónde se necesiten.

Por su parte la disponibilidad de acuerdo a la NC ISO/IEC 27001:2016 garantiza que las personas autorizadas puedan acceder a la información cuando sea necesario y que todos los medios de almacenamientos se mantengan adecuadamente y se actualicen y/o modifiquen en dependencia de las necesidades de la empresa.

La disponibilidad de la información acarrea en la gestión y la forma en que la organización pueda desenvolverse ante la ocurrencia de un incidente de seguridad. Ante la presión por asegurar la continuidad del negocio la elaboración de planes de contingencias se han convertido en imprescindibles.

Autenticidad

LA REA lo identifica como:

- Acreditado como cierto y verdadero por los caracteres o requisitos que en ello concurren.
- Consecuente consigo mismo, que se muestra tal y como es. Es una persona muy auténtica.
- Certificación con que se testifica la identidad y verdad de algo.
- Copia autorizada de alguna orden, carta, etc.

En la (NC ISO 27000:2016) se define como la propiedad de que una entidad es lo que dice ser. Por otra parte Arias (2018) añade que la misma puede ser aplicada a usuarios, procesos, sistemas e información

Responsabilidad

Según la definición más acertada de la REA, la responsabilidad es la capacidad existente en todo sujeto activo de derecho para reconocer y aceptar las consecuencias de un hecho realizado libremente.

Para Xiaoxia (2012) es el cumplimiento de las obligaciones, o el cuidado al tomar decisiones o realizar algo. La responsabilidad es también el hecho de ser responsable de alguien o de algo.

No repudio

En la NC ISO 27000:2016 se define como la capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron

Para Castillo (2017), esta se caracteriza porque al emisor garantiza que la información fue entregada y ofrece una prueba al receptor del origen de la información recibida: ¿Se ha enviado/recibido esto realmente? Es decir, un mensaje tiene que ir firmado (emisor) y, quien lo firma, (receptor) no puede negar que el mensaje lo envió otra persona distinta. Este último aspecto o principio tiene como fin último proteger a la organización de que un solo cliente interno pueda adquirir, manipular, alterar o destruir información y con ello ocasionar una situación grave de crisis.

Fiabilidad

La RAE define a la fiabilidad como que ofrece seguridad o buenos resultados. Creíble, fidedigno, sin error. Con fiabilidad nos referimos a que los datos que obtenemos sean consistentes y reales.

La NC ISO 27000:2016 la precisa como la propiedad relativa a la consistencia en el comportamiento y en los resultados deseados

Los principios anteriormente mencionados son conocidos mundialmente, quienes permanecen vigentes en el tiempo, pero las metodologías de cumplimiento cambian continuamente con la evolución de la tecnología y el desarrollo constante de nuevas vulnerabilidades y amenazas. Los esfuerzos continuos son esenciales para garantizar el cumplimiento de estos principios de la información en todo momento.

En relación con los postulados anteriores los autores Imbaquingo, Pusdá, & Jácome (2017) consideran que antes de que exista una falla de seguridad que afecte cualquiera de estos, debe haber un riesgo de seguridad que en su momento no se detectó. Es por ello, la necesidad de la aplicación de controles de seguridad que protege contra todo aquello que pueda causar un incidente de seguridad, criterios con los que concuerda esta investigación por considerar que los mismos tienen una incidencia directa en relación con la seguridad de la información

1.2 La información y su gestión en las organizaciones. Calidad de la información

La gestión de la información ha evolucionado desde la década de los 80 a partir de un extenso número de conceptos y aplicaciones y que responden a las condiciones actuales de las

organizaciones y de la sociedad. Para comprender su significado se asumen los conceptos de Woodman (1985) y Rowley (1998), que sin importar los varios años desde su concepción, reflejan cada uno desde diferentes ópticas una idea general de lo que constituye la gestión de la información.

Rowley (1998) plantea que "la gestión de información es promover la eficacia organizacional al elevar las potencialidades de la organización para cumplir con las demandas del ambiente interno y externo en condiciones tanto dinámicas como estables".

Woodman (1985) que "la gestión de información son toda actividad relacionada con obtener la información correcta, en la forma adecuada, para la persona indicada, al costo correcto, en el momento y lugar oportuno, para tomar la acción precisa". El concepto deja a relucir los elementos que inciden en la gestión de información, los mismos deben de contar con mecanismos de control que permita una adecuada gestión. Así mismo se indica en lo conceptualizado por Ponjuán (2014), quien indica que, la gestión de información es "un proceso estratégico que tiene lugar en una organización de cualquier tipo y abarca todos los procesos, actividades y componentes, manteniendo una estrecha relación con el sistema que lo rige".

Por lo antes enunciado, es posible declarar que para que exista el tratamiento y administración de la información en una organización, deben incurrir elementos que interactúan para procesar los datos y dan lugar a información más elaborada. De acuerdo a la investigación de autores como Lugones (2013), Hernández (2014), Mayra (2014) y García, F., & García, A. (2018) estos se clasifican en: personas, datos, actividades o técnicas de trabajo y recursos materiales.

Las personas constituyen el equipo humano y profesional que lleva a cabo los avances, los logros y los errores de la organización. Son quienes interactúan con la información extraída de los datos. En el ámbito de seguridad de la información autores como Said, Abdullah, Uli & Abidin (2014) fundamentan que su gestión requiere, como mínimo, la participación de todos los empleados en la organización. En la actualidad son muchos los que manifiestan a las personas como el principal factor de vulnerabilidad Bursztein (2014), por lo que según Garrido (2016) el compromiso en relación a la misa por parte de los empleados, es la mejor herramienta de prevención de pérdidas de una organización. Así, mismo, el autor declara que los empleados, al sentirse comprometidos con la seguridad de la organización y al estar capacitados serán un aliado muy importante, convirtiéndose en actor para cumplir y hacer cumplir las normas establecidas, Moreno (2015) añade que un buen plan de concienciación de los usuarios es una prioridad para las organizaciones.

Por su parte, los datos son las porciones de información donde reside todo el valor. El control y preservación de la misma constituye la razón fundamental de la gestión de la seguridad de la información.

Las actividades o técnicas de trabajo son el conjunto de acciones, operaciones o procedimientos, materiales o intelectuales ejecutadas por una persona o unidad administrativa como parte de una función asignada, para cumplir una tarea específica. La seguridad de la información debe estar vinculada en la ejecución de la misma, la que debe responder por el manejo correcto de los flujos de información que se conciban. En esta clasificación se podría recoger el software como una actividad automatizada destinada a recoger los datos, almacenarlos, procesarlos y analizarlos.

Y por último, los recursos materiales de una organización son todos los bienes tangibles de los que dispone a la hora de llevar a cabo la actividad. Entre estos puede haber infraestructura, materias primas, terrenos, material de oficina, equipos informáticos, vehículos, entre otros. Jauregui (2014), por tal motivo, por tal sentido, los controles a los medios físicos desde el inicio de su vida útil, debe estar insertada en los procesos de gestión de la seguridad de la información.

Con el advenimiento de las TIC las organizaciones han modificado su estructura organizacional adaptando sus procesos a los nuevos cambios que se presentan dentro y fuera de la misma. Las mismas han sustituido gradualmente el respaldo físico de su documentación por el digital (ej. El 93% de los documentos corporativos son creados electrónicamente. Espona (2015). El uso de las TIC permite el desarrollo de mayor flexibilidad y dinamismo, así aportar soluciones que apoyan los procesos internos y externos. Sin embargo, se exponen a los nuevos peligros que representa el almacenamiento electrónico o en línea, ya que, si no se toman las medidas preventivas adecuadas, cualquiera podría tener acceso a su información incluso a miles de kilómetros de distancia. En tal sentido la seguridad de la Información debe ser un medio de control que en gran medida incide sobre los dispositivos electrónicos.

1.2.1 La seguridad de la información como contribución a alcanzar la calidad de la misma

Las organizaciones dependen de sus clientes y por lo tanto deberían comprender sus necesidades, satisfacer sus requisitos y exceder sus expectativas. Los principios de calidad de Deming, Ishikawa, Juran y Crosby se usan para mejorar la calidad de los productos; también en la actualidad se emplean estos principios en la administración de la información.

Cualquier organización aspira a proporcionar productos y/o servicios de calidad a sus clientes. Se habla de calidad al tratar los objetivos estratégicos de las organizaciones,

independientemente del tipo, sector, etc. De acuerdo a la norma ISO 9000:2015, una organización orientada a la calidad promueve una cultura que da como resultado comportamientos, actitudes, actividades y procesos para proporcionar valor mediante el cumplimiento de las necesidades y expectativas de los clientes y otras partes interesadas pertinentes. Para los autores Buitrago, Bonilla & Murillo (2012) la seguridad de la información es responsabilidad de la organización al ser el apoyo de las industrias en el control de calidad de sus procesos y productos, planteando como objetivo asegurar resultados confiables a los clientes.

Tomando como referencia que los datos son los principios por donde se desarrollará la información, los autores Vilalta & Espinosa (2008) en su aportación de una Metodología para el diagnóstico de la calidad de los datos, reflejan la importancia de la seguridad en la calidad de los datos, al desplegar una etapa completamente de la metodología propuesta a "Garantizar la seguridad del dato", enfatizando que los datos que almacenan las empresas y todo tipo de organizaciones de cualquier sector son información valiosísima de los ciudadanos que se tiene la obligación de proteger.

Existen diversos conceptos de calidad de la información y que ya alcanzan el status de estándares internacionales y que demuestran la existencia de algunos principios que responden a la seguridad de la información. A continuación se despliegan algunas de estas.

Maravilhas (2015) en su investigación declara que para ser considerada de calidad, la información debe presentar criterios como son: *integridad, accesibilidad, exactitud, precisión*, objetividad, consistencia, relevancia, *puntualidad* y transparencia.

Según Dávila (2003) el manejo de la calidad de la información se da desde la captura de la misma. Se debe de trabajar en función de validación de los mismos, que permita al sistema ayudar en la revisión de la *validez de los datos* que se están incorporando. Una conceptualización de gran importancia y repercusión en la investigación, dado que la misma declara que los datos de entrada son un importante eslabón para alcanzar la calidad. Es por ello que se deben aplicar técnicas de recepción de datos que permitan que los mismos tengan la integridad y confiabilidad que se desea para alcanzar los resultados propuestos.

Lo antes mencionado se refuerza en lo declarado por Olivé (2012) quien determina que la calidad será alcanzada de acuerdo al grado en que los métodos de medición utilizados para preparar la información pueda representar lo que el cliente quiere saber (*relevancia de la información*), los métodos fueron aplicados de manera competente y los resultados se han mostrado de manera veraz (*fiabilidad o credibilidad de la información*).

Los autores Nor, Zaidi & Hussin (2018) definen que la calidad de la información solo puede implementarse a través de la *tecnología***,** el *conocimiento* y las *redes de relaciones*. Si bien esta no constituye una conceptualización teórica, precisa los puntos focales a los que habría de aplicar acciones de seguridad con el fin de garantizar su efectividad.

La Dra. Espona(2015), en su investigación "Calidad de Información: una nueva herramienta para la investigación" argumenta sobre la metodología para evaluar la Calidad de Información emitida por el Instituto de Tecnología de Massachusetts (MIT) quienes analizan este tema y plantean la existencia de al menos 15 dimensiones o aspectos destacados de la información que condicionan su calidad. Según la investigación la Calidad de la información (CI) se encuentran desplegados en:.

- Disponibilidad: relacionada con accesible para ser utilizado en el momento que se disponga y sobre cómo están protegidos del uso no autorizado. Incluye la dimensión de *accesibilidad* y *seguridad de acceso.*
- Presentación: la información debe ser comprendida y entendida, donde se deben considerar atributos como el idioma, el soporte, las unidades de medida y la codificación. Asimismo, se deben buscar la concisión y la consistencia metodológica de los datos. Incluye las dimensiones de *interpretabilidad, facilidad de comprensión, consistencia representacional* y *representación concisa*.
- Contexto: evalúa la relación entre los datos y las circunstancias en que serán utilizados. Los datos deben tener relación con el tema en cuestión y estar actuales. Incluye cinco dimensiones: *valor agregado*, *relevancia*, *oportunidad*, *completa* y *cantidad de datos*.
- Intrínseco: está relacionado con la calidad propia de la información y no de la fuente en donde se encuentra auto contenida. Incluye las dimensiones: *credibilidad*, *precisión*, *objetividad* y *reputación*.

Para la autora el alcanzar la calidad de la información la misma debe cumplir con cada una de estas dimensiones, por lo que a través del principio de disponibilidad, se demuestra la importancia que la autora le confiere a la seguridad de la información

En la investigación de Spanevello (2012), que es referenciada por Espona (2015), ofrecen 10 razones de acuerdo a estudios efectuado en proyectos de Calidad de la Información en organizaciones líderes internacionales, que dan origen a problemas con los datos. En la siguiente tabla se expresan estos, y se ofrece por cada condición las posibles incidencias de los principios de seguridad de la información que puedan provocar los problemas que son sugeridos por los autores:

	Condición	**Problemas con la calidad de los datos**	**Vinculación con la Seguridad**

1	Múltiples fuentes de datos	Diferentes valores para el mismo dato Información inconsistente Tiempo perdido para reconciliar datos	Puede estar vinculada a la falta de: Integridad, Disponibilidad y Fiabilidad de la información
2	Subjetividad en la producción de información	Información imprecisa y poco confiable es ingresada y utilizada	Puede estar vinculada a la falta de: Autenticidad, Integridad, Fiabilidad
3	Recursos de cómputos limitados	Incapacidad de obtener información oportunamente Información oculta o no disponible	Puede estar vinculada a la falta de: Disponibilidad
4	Accesibilidad vs seguridad	Los mecanismos de seguridad son barreras para la accesibilidad.	Puede estar vinculada a la falta de: Disponibilidad
5	Distintas codificaciones para los mismos datos	Datos difíciles de entender que no son utilizados en el contexto correspondiente.	Puede estar vinculada a la falta de: Confidencialidad, Responsabilidad
6	Representación de datos complejas	Limitada capacidad de análisis de imágenes y textos almacenados digitalmente	Puede estar vinculada a la falta de: Responsabilidad
7	Volumen de datos	Imposibilidad de obtener datos oportunamente debido a la dificultad que acarrea el procesamiento de gran cantidad de información	Puede estar vinculada a la falta de: Disponibilidad, Fiabilidad, Responsabilidad
8	Reglas de ingreso demasiado restrictivas o pasadas por alto	Información perdida, distorsionada o poco confiable	Puede estar vinculada a la falta de: Confidencialidad, Disponibilidad
9	Necesidad de datos cambiantes	Incoherencia entre la información disponible y las necesidades para su uso	Puede estar vinculada a la falta de: Disponibilidad, Fiabilidad
10	Sistemas heterogéneos distribuidos	Información inconsistente, difícil de acceder y de resumir	Puede estar vinculada a la falta de: Disponibilidad, Integridad

De acuerdo a lo enunciado existe incidencia de la seguridad en la calidad de la información que a su vez tributaría a mejorar la calidad del servicio. Hay que subrayar que el lograr que la información sea segura no garantiza la calidad de la misma, pero si, es una contribución que ayuda a alcanzarla.

1.3 Los sistemas de gestión de seguridad de la información

El SGSI es la mejor manera de supervisar, controlar, revisar periódicamente el trabajo de la organización en materia de seguridad de la información, proporcionando una dirección de las actividades relacionadas con la seguridad de la información en respuesta a los factores de

cambio por agentes internos o externos. Todo individuo dentro de la organización debe aceptar su responsabilidad para mejorar el SGSI. *Robles & Rodríguez (2006)*

Los autores Pulido & Mantilla (2016) plantean que el SGSI es un conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

1.3.1 Características de los SGSI normalizado

La norma universalmente más conocida y aplicada en materia de seguridad de la información es la ISO 27001:2013, y actualizada a los estándares nacionales en el 2016, la misma puede ser aplicada a cualquier tipo de organización, independientemente del tamaño y el sector al que pertenecen.

Esta norma es consistente con las mejores prácticas descritas en ISO/IEC 27002 y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

La NC ISO/IEC 27001:2016 es la encargada de definir los distintos requisitos necesarios para el establecimiento, la implantación, la correcta operatividad, el monitoreo, la revisión, el mantenimiento y la mejora del sistema de gestión de seguridad de la información, así como los controles de seguridad que se deben llevar a cabo en cualquier organización. A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares, estructurada en 6 partes. La NC ISO/IEC 27001:2016 es la única de esta serie que puede ser certificada, la misma brinda la documentación que es requerida para una certificación de cumplimiento de todos los requisitos.

La ISO 27001:2016 como norma de SGSI, establece en total 50 acciones que deben cumplirse y que se determinan en 130 requisitos.

Dentro de la implementación de la norma ISO/IEC 27001:2016, los requisitos de la norma ISO 27002 resulta un instrumento de importancia como guía de buenas prácticas para implantar controles y que garantizarán la seguridad de la información gracias a sus recomendaciones, y a su vez constituye el instrumento que se debe seguir si se desea certificar el SGSI de la organización con la NC ISO/IEC 27001:2016. Con esta, se definen objetivos de control y gestión que deberán perseguirse por las organizaciones, las que se distribuyen en dominios que abarcan de una forma integral todos los aspectos que deben tenerse en cuenta por las organizaciones.

Una de las fortalezas y claves del éxito de la nueva ISO/IEC 27001:2016 es que la compatibilidad con otras normas internacionales cuya estructura está relacionada, construida y documentada, en relación a las normas de gestión: serie ISO 9000 para la gestión de la calidad,

norma NC ISO 14001:2015 para sistemas de Gestión Medioambiental o la NC ISO 19011: 2018, que proporciona las directrices para las auditorias de sistemas de gestión.

Ventajas de la NC ISO/IEC 27001:2016

La certificación del SGSI ayuda a las organizaciones a desarrollar y mejorar su rendimiento.

- Es una Norma con Reconocimiento Internacional.
- Eficiencia en la gestión de la empresa, al tomarse medidas para minimizar los riesgos que se asocien a la gestión de la información.
- Solvencia empresarial, por disponer de un sistema que garantiza la confidencialidad, integridad y disponibilidad de la información.
- Continuidad, como consecuencia de la implantación de planes de continuidad de negocio que evitan paradas no deseadas de la actividad empresarial.
- Mejora de la imagen de la empresa, al evidenciar su compromiso con la seguridad de la información propia y de clientes.

En la investigación, se asume los postulados en la NC ISO/IEC 27001:2016, por considerarla una estrategia empresarial para lograr futuras certificaciones en materia de seguridad de la información.

Documentos obligatorios y registros que son requeridos en la NC ISO/IEC 27001:2016

Para cumplir con la norma NC ISO/IEC 27001:2016 se hace necesario elaborar una lista de documentos. A continuación se listas los que son adaptados al objeto de investigación.

El alcance del sistema de gestión de seguridad de la información (cláusula 4.3)

Política de seguridad de la información (cláusulas 5.2)

Apreciación del riesgo de seguridad de la información (cláusula 6.1.2)

- Criterios de aceptación y apreciación del riesgo (cláusula 6.1.2 a)
- Lista de riesgo, identificación de dueños (cláusula 6.1.2 c)
- Probabilidad de ocurrencia y niveles de riesgos, consecuencias de materializarse el riesgo (cláusula 6.1.2 d)

Tratamiento del riesgo (cláusula 6.1.3)

- Opciones de tratamiento de riesgo, Controles de implementación (cláusula 6.1.3 b)
- Declaración de aplicabilidad (cláusula 6.1.3 d)
- Plan de tratamiento de riesgo (cláusula 6.1.3 e y 6.2)

Objetivos de seguridad de la información (cláusulas 6.2)

Competencias de los trabajadores *(Influye formación y acciones de cumplimiento, tutorías, contratación de personas competentes, Se evidencia a través de registros)* (cláusulas 7.2)

Planes para alcanzar los objetivos de seguridad (cláusula 8.1)

Plan de auditoría interna y resultados de revisión (cláusula 9.2) (*Se evidencia a través de registros*)

Resultados de la Revisión por Dirección (cláusula 9.3) (*Se evidencia a través de registros*)

Resultados de acciones correctivas (cláusula 10.1) (*Se evidencia a través de registros*)

Según el Anexo A de la norma deben incluirse deben contar con los siguientes documentos. Algunos documentos del anexo son obligatorios sólo si existen riesgos que impliquen su implantación. A continuación se listas los mismos:

- Definición de roles y responsabilidades de seguridad (cláusulas A.7.1.2 y A.13.2.4)
- Inventario de activos (cláusula A.8.1.1)
- Uso aceptable de los activos (cláusula A.8.1.3)
- Política de control de acceso (cláusula A.9.1.1)
- Procedimientos de operación para gestión de TI (cláusula A.12.1.1)
- Registros de las actividades de usuario, excepciones y eventos de seguridad (cláusulas A.12.4.1 y A.12.4.3) (*Se evidencia a través de registros*)
- Política de transferencia de información (cláusulas A.13.2.1, A.13.2.2, y A.13.2.3)
- Principios de ingeniería de sistemas seguros (cláusula A.14.2.5)
- Política de seguridad para proveedores (cláusula A.15.1.1)
- Procedimiento para gestión de incidentes (cláusula A.16.1.5)
- Procedimientos de Continuidad de negocio (cláusula A.17.1.2)
- Requerimientos legales, regulatorios y contractuales (cláusula A.18.1.1)

1.3.2 Vulnerabilidad y gestión de riesgos como aspectos claves del SGSI

En la nueva sociedad actual se conoce que toda organización se encuentra constantemente expuesta a riesgos, por lo que es declarado por muchos autores que la seguridad total es un concepto imposible de alcanzar Phillips (2013), por su parte Incibe (2015) declara que la seguridad de la información garantiza la continuidad de la organización y previene o minimiza el posible daño del impacto del riesgo.

La apreciación de los riesgos de seguridad de la información y el proceso de tratamiento recogido en esta norma se alinean con los principios y directrices genéricas definidos en la NC ISO 31000:2018.

Según la NC ISO 31000:2018 el riesgo es el efecto de la incertidumbre sobre los objetivos. El efecto es la desviación respecto a lo previsto, siendo positivo, negativo o la combinación de ambos, y puede abordar, crear o resultar en oportunidades y amenazas. Mientras tanto, los objetivos pueden tener diferentes aspectos y categorías, y se pueden aplicar a diferentes

niveles. En el contexto de SGSI, la NC ISO/IEC 27001:2016 define que el riesgo se relaciona con la posibilidad de que las amenazas exploten vulnerabilidades de un activo o grupo de activos de información y causen daño a la organización.

Los autores Martins & dos Santos (2010) plantea, que para minimizar el impacto de los riesgos, se debe establecer una correcta identificación de las amenazas y el análisis de las vulnerabilidades de los activos organizacionales que soportan los flujos de información". Todo esto se debe de crear de una forma clara y que responda a los criterios específicos que se desean.

De acuerdo a Londoño (2014) las vulnerabilidades son los elementos que, al ser explotados por amenazas, afectan la confidencialidad, disponibilidad e integridad de la información de un individuo u organización, estos dependen de la forma en que se organizó el ambiente en que se maneja la información. El autor declara que la existencia de puntos débiles en la organización, se relacionan con la presencia de elementos que perjudican el uso adecuado de la información y del medio en que la misma se utiliza o transmite.

Los autores Bogdanel & Fotache (2015) declaran que las amenazas son la probabilidad de que se materialice aprovechando una vulnerabilidad y produciendo un daño o impacto, e Incibe (2017) añade que las vulnerabilidades o las amenazas, por separado, no representan un peligro, pero si se juntan, se convierten en un riesgo.

Proteger los bienes de las organizaciones exige la combinación de diversas prácticas, tanto culturales, como de disciplina y entrenamiento de los usuarios. La gestión de riesgos se presenta como una actividad clave para el resguardo de los activos de información de una organización.

El análisis de riesgo es el proceso de identificación de factores que tienen influencia sobre la seguridad de la información. Los autores Pavlov & Karakaneva (2011) exponen cuatro resultados principales para establecer una evaluación de riesgos, los mismos son:

- Determinar las amenazas a la misión de la organización
- Priorizar los niveles de riesgo
- Definir controles y medidas de protección
- Desarrollo de un plan de acción para la implementación de estas medidas.

Para establecer los riesgos se han de considerar además aspectos técnicos, organizativos, de recursos humanos y de cumplimiento legal. Incibe (2015).

Las medidas de seguridad que se implementen, deben disminuir los riesgos, y con esto, disminuir el impacto para los activos, y por tanto, para la organización.

De acuerdo a Pavlov & Karakaneva (2011), el proceso de gestión de riesgos proporciona el cumplimiento entre los objetivos comerciales o misiones y la necesidad de la organización protección de activos de manera efectiva.

Según el autor Del Peso y citado por Rayme (2007), a la hora de implantar medidas de seguridad, es preciso tener hecha una clasificación de la información conociendo lo que realmente debemos proteger y lo que no, y no adoptando medidas iguales para todo nuestro patrimonio informacional, cuando, en muchos casos, parte de él no merece que realicemos ningún gasto de seguridad, Por ello, la información, como activo de cualquier organización, ha de ser clasificada según el grado de sensibilidad e importancia para la misma y, en base a ello, poder definir la que debe ser protegida y con qué niveles. El autor también expresa que los inventarios de activos ayudan a garantizar la vigencia de una protección eficaz de los recursos de información. El proceso de constituir un inventario de activos es un aspecto importante de la gestión de riesgos. Para Rayme y que se sostiene en la investigación cada activo debe ser claramente identificado y su propietario y clasificación en cuanto a seguridad deben ser tratados y documentados, junto con la ubicación vigente del mismo.

Se han desarrollado diferentes estándares o modelos internacionales centrados en la gestión de riesgos, altamente difundidos en la actualidad. Entre ellos se destacan: OCTAVE, MAGERIT, MEHARI, NIST SP 800-30, CORAS, CRAMM, COBIT o ISO 31000. Todos ellos orientados a ser una guía para las organizaciones en brindar estrategias y consejos para desarrollar un mayor grado de madurez en la seguridad de la información; sin embargo, la implementación de alguno de ellos, requiere consideraciones adicionales. En el anexo 5 se muestra una tabla comparativa con las ventajas y desventajas que presentan las antes mencionadas.

Como uno de los objetivos que se pretende alcanzar en esta investigación, es la selección de un marco de referencia que permita la gestión de los riesgos de la organización. Tras evaluar el entorno en que se manifiesta el objeto de estudio, las ventajas y desventajas de alguna de las metodologías existentes, se propone la norma NC ISO 31000:2018, adaptada a los modelos nacionales.

Figura 2. Proceso de Gestión de Riesgo.
NC ISO 31000:2018

Su selección se enfatizó en el grado en que la misma puede estar integrada en todas las prácticas y procesos de la organización, pudiéndose aplicar a

cualquier tipo de riesgo, ya sea por su naturaleza, causa u origen, no solo así a la seguridad de la información. La gestión del riesgo debería formar parte de toda la organización, y su accionar debe dirigirse a identificarlos todos independientemente del tipo de proceso al que se encuentre integrado y no ser independiente de ellos.

La ISO 31000:2018, establece pautas que deben ser integradas para hacer un control eficaz del riesgo. Esta norma brinda los principios y las directrices genéricas sobre la gestión del riesgo, y puede ser utilizada por cualquier organización pública, privada o gubernamental. Por lo tanto, no es específica para ninguna industria o sector.

El esquema o proceso de la ISO 31000:2018 para la gestión del riesgo es el siguiente:

Alcance, contexto, criterios: Identificar y definir el ambiente político, social, económico, legal y organizativo dentro del cual se lleva a cabo la actividad, el proceso, la decisión, etc. incluyendo el desarrollo de los criterios, políticas y estrategias de riesgos.

Evaluación del riesgo: La evaluación del riesgo es el proceso global de identificación, análisis y valoración del riesgo. La manera de aplicar este proceso no solo depende del contexto del proceso de gestión del riesgo, sino también de los métodos y técnicas utilizadas para realizar la apreciación del riesgo.

Tratamiento del riesgo: Identifica, evalúa y selecciona las opciones de tratamiento de los riesgos, tomando en consideración la relación costo-beneficio, las medidas que se necesitan aplicar para ayudar a minimizar los riesgos inaceptables y/o su impacto, y preparar e implementar planes de acción.

Comunicación y Consulta: Comunica de forma eficaz a todas las partes interesadas en el proceso de identificar y enfrentar los riesgos y ayuda a tomar decisiones más acertadas.

Seguimiento y Revisión: El contexto y otros factores pueden variar a lo largo del tiempo y podrían cambiar o invalidar la valoración del riesgo. Debe darse un seguimiento continuo y revisión, para que la valoración del riesgo pueda actualizarse cuando sea necesario. Las responsabilidades para la creación y revisión de la evidencia y documentación debe definirse y documentarse.

1.3.3 Metodologías, procedimientos y guías relacionadas con la implementación de los SGSI normalizados

Numerosos autores, como Barbosa(2005); Cosachov(2006); Villena(2006); Nakrem(2007); Navarro(2007); Rayme(2007); Andrés & Gómez(2009); Pallas(2009); Buitrago, Bonilla & Murillo(2012); Aguirre & Aristizabal(2013); Carazo(2013); Guevara(2013); Baldecchi(2014); Bustamante & Osorio(2014); Macen(2014); Villena(2014); Bermúdez & Bailón(2015);

Bolivar(2015); Gorriti(2015); Guzmán(2015); Solarte, Enriquez & Benavides(2015); Talavera(2015); Paillacho(2015); Santofimio & Manrique(2015); Tibaquira(2015); Baca(2016); Chaparro(2016); Espinosa, García & Giraldo(2016); Delvasto(2016); Merino & Torres(2017); Muñoz(2017); Buesaquillo, Lopez & Garcia (2017); Bustamante, Fuertes, Diaz &Toulqueridis(2017); Cuervo(2017); Gallegos & Murillo(2017); Landázuri(2017); Lozano(2017); Torres(2017); Cely(2018) han sentado sus investigaciones en la formulación de acciones que contribuyan a mejorar la seguridad de la información en organizaciones. Algunos como Solarte, Enriquez & Benavides (2015), Paillacho (2015), Delvasto (2016) y Espitia (2018 han abordado metodologías para la gestión de riesgos e incidentes de seguridad, quienes lo ven como la principal fuente para el control de la seguridad de la información.

El estudio y revisión de sus principales aportes y limitaciones se lleva a cabo a partir del análisis de 10 variables tratadas por los autores, seleccionadas a partir de las deficiencias detectadas y principios presentes en la NC ISO/IEC 27001:2016, que constituyen interés para la investigación: enfoque normalizado , entrenamiento y conciencia, inventarios de activos, gestión de riesgos , manejo de incidentes, auditorias, revisión por la dirección, mejora, estructura de la documentación y registros del sistema.

Se elaboró una matriz binaria donde se analizó la relación o no de las variables en los enfoques metodológicos (anexo 1). A partir del análisis de correlaciones de distancia con la utilización de la medida Jaccard, se obtuvo como resultado en el estudio entre autores y variables un 50,77% de densidad de la red.

Al realizar el análisis por variables, la red muestra una relación media entre ellas, destacándose las más tratadas: enfoque normalizado, inventarios de activos, gestión de riesgos y auditorias. En cuanto a las variables menos trabajadas en los modelos y procedimientos fueron: estructura de la documentación y registros del sistema. Paralelamente se realizó la validación de la red utilizando el análisis de conglomerados jerárquico por variables (Anexo 1.1), al realizar un corte en el dendograma a la distancia de cinco, se corrobora la existencia de dos grupos y un elemento aislado. El primer grupo compuesto por las variables con mayor representatividad en las propuestas estudiadas y otro con las variables con menor incidencia, la “mejora” queda trabajado como un elemento aislado.

Pallas (2009) ofrece una metodología de implantación de un SGSI en un grupo empresarial jerárquico, siendo el objetivo de la misma: armonizar el SGSI de la empresa subordinada con el de la empresa principal del grupo empresarial. Se destacan conceptos y principios teóricos que contribuyen al estudio del objeto de la investigación. Se carece de acciones para llevar a cabo el diagnóstico de la organización, capacitación al personal. Se incursiona en la aplicación de

técnicas de grafos para la valoración de activos, pero su aplicación complejiza el modo de proceder para la valoración del mismo. La implementación no se adecua a esta investigación.

Solarte, Enriquez & Benavides (2015) ofrecen aspectos relevantes, pero solo análisis y evaluación de riesgos, explica la forma de proceder para dar cumplimiento a cada fase, etapa y tareas correspondientes. Si bien brinda detalles de materiales de consulta y utilización, los aspectos formulados solo abarcan el diagnóstico. Los instrumentos de trabajo propuestos, no se adecuan al objetivo de la investigación.

Por otra parte, Guzmán (2015) elaboró una metodología para la seguridad de tecnologías de información y comunicaciones sustentada en una institución privada de salud. La misma brinda información sobre los objetivos que se pretende conseguir en casa etapa planificada, no así en cómo lograr dichas acciones, además soporta alto número de documentos innecesarios que hacen extensos los pasos propuestos para cada etapa, perdiendo precisión y objetividad. Contiene elementos que son afines a esta investigación, pero carece de estrategias y acciones que permitan gestionar los riesgos que se desean mitigar.

Paillacho (2015) formula un modelo de gestión de riesgo en entidades gubernamentales, el mismo se despliega en dominios (establecimiento del contexto, valoración, tratamiento aceptación, comunicación, monitoreo y revisión del riesgo) cubriendo las cláusulas emitidas en la Norma ISO 27005. Se explican el modo de cumplir las etapas planificadas, mediante la utilización de ejemplos prácticos, centrándose en las deficiencias de su campo de acción, razón que debilita su implementación en otras organizaciones. Se centra en los riesgos que inciden en la información digital. No se presentan acciones para mitigar los riesgos, siendo esta una de los principales objetivos a perseguir en la investigación.

Bartnes (2015) en su tesis doctoral ofrece conocimientos sobre factores que afectan las actividades en la gestión de incidente de seguridad de la información y retos para la mejora. La tesis aporta conocimientos teóricos, no así acciones prácticas que permitan alcanzar el objetivo propuesto.

Por su parte Santofimio & Manrique (2015), ofrecen técnicas de evaluación del riesgo para determinar la viabilidad del proyecto en la etapa de formulación, se facilita de forma coherente criterios de apreciación del riesgo, que se adaptan a los requisitos organizativos y que recoge la variable calidad como aspecto para cuantificar el valor del riesgo. Estos principios son asumidos por la investigación.

Delvasto (2016) propone un una metodología desglosadas en 5 etapas: planeación y preparación, detección y reporte del incidente, evaluación y decisión, respuesta y lecciones aprendidas. En la misma se explica la forma de proceder ante un incidente de seguridad, pero

no responde a todo el ciclo de gestión de la seguridad de la Información. Esta investigación aporta el modo de proceder ante la ocurrencia de incidentes.

Chaparro (2016) ofrece un plan de Implementación de la ISO/IEC 27001:2013, la investigación es asumida desde la práctica, donde los pasos desplegados se sustentan en el resultado de acciones. Carece de una estructura esquemática que viabilice el entendimiento de los pasos a seguir y lo que hay que realizar en cada uno de estos. No se muestran acciones relacionadas con compromisos de los trabajadores, creación de grupo gestor y acciones de mejora.

Espitia (2018) ofrece una metodología de análisis y evaluación de riesgos aplicados a la seguridad de la información bajo la norma ISO/IEC 27001, en el mismo se ofrecen pautas para determinar las vulnerabilidades, amenazas, análisis de los riesgos y su diagnóstico, así como controles para el diseño del SGSI que incluya políticas y procedimientos para mitigar los riesgos. La investigación solo hace alusión a un aspecto vinculante con el SGSI, la misma no incluye las etapas de diagnóstico, diseño y documentación, entrenamiento y control.

De forma general, se concluye que los enfoques estudiados tienen como ventajas fundamentales:

- Resaltan los beneficios de la seguridad de la información en las organizaciones.
- Se evidencia la generalización del enfoque normalizado a través de la ISO/IEC 27001, para la implementación de los SGSI.
- Se identifican como etapas representativas la gestión de riesgos, diseño e implantación, control y evaluación.
- Existe alta representatividad de la gestión de riesgos, aplicado para ellos metodologías como Octave, Magerit, Cobit e ISO 31000.

Se aprecian también limitaciones que trazan las pautas para elaborar esta investigación:

- Presentan un abordaje práctico, limitándose al campo de acción, lo que dificulta su aplicación en otras organizaciones.
- Alto número de investigaciones que no definen técnicas y herramientas para la aplicación de cada fase, etapa o paso.
- Se conceptualiza a la gestión de riesgo como fase fundamental de desarrollo, excluyendo etapas del proceso de gestión de la seguridad de la información.
- No se identifican de forma explícita la contribución de la seguridad de la información a la calidad de los servicios.
- Los principales aportes relacionados con la SGSI a través del sistema normalizado ISO/IEC 27001 se presentan a nivel internacional. Ha sido débilmente trabajada en el contexto organizacional cubano.

Por lo que, se considera en la bibliografía consultada queda débilmente tratada un procedimiento para implementar un sistema de gestión de seguridad de la información que se identifique e incorpore actividades en los SGC para contribuir a la calidad de la información de los servicios, adaptada al marco legal reglamentario de Cuba, estableciendo el orden lógico para su consecución emitiendo las entradas, técnicas y/o herramientas de trabajo, contextos de desarrollo y salidas para cada una de las etapas.

1.4 Características de los SGSI en Cuba. Marco y contexto normativo

En materia de seguridad de la información en Cuba existen diferentes regulaciones que determinan acciones a ser cumplidas y que responden a la seguridad de la información en las organizaciones.

De acuerdo al análisis documental de las legislaciones vigentes, en materia de seguridad de la información existen lagunas jurídicas que hacen que las organizaciones no presten interés a la implementación de un sistema de seguridad de la información.

Según la resolución ministerial 127 /2015 – “Cada entidad que haga uso para el desempeño de su actividad de las tecnologías de la información está en la obligación de diseñar, implantar y mantener actualizado, un sistema de seguridad informática…” -

Por otra parte se encuentra el decreto ley no. 221 que rigen la actividad archivística, donde se determinan las acciones a tener en cuenta con la información que se almacena en formato de papel. Pero, no existe un procedimiento o guía para el desarrollo de esta actividad.

Las acciones en materia de seguridad de la información en Cuba se encuentran aisladas y son implementadas como procesos independientes.

De acuerdo a la resolución 127 en su artículo 6: “El diseño del sistema de seguridad informática y la elaboración del plan de seguridad informática de cada entidad se realizarán en correspondencia con las metodologías establecidas al respecto por la oficina de seguridad para las redes informáticas, adscripta al ministerio de la informática y las comunicaciones.”. Esto induce a que las organizaciones tienen que medirse por cumplimiento de este, decretar la protección de las instalaciones informáticas y de la información en medios digitales, no así en otros medios donde se localice información como: impresos en papel, discos duros, e incluso medidas de seguridad respecto de las personas que la conocen.

Si se conoce que la seguridad informática constituye un elemento que puede medirse dentro de la seguridad de la información, las instituciones cubanas que deseen implementar la NC ISO/IEC 27001:2016 deben de tomar como punto de partida el diseño del Sistema de Seguridad Informática que se implementó.

1.4.1 Marco y contexto normativo en seguridad de la información en Cuba

En Cuba el proceso de normalización en el campo de la seguridad de la información se encuentra implícito en resoluciones, decretos y lineamientos que reflejan las acciones a acometer para determinadas aristas de la seguridad de la información en las organizaciones, además tiene como referencia las normas técnicas emitidas por organismos internacionales como la Organización Internacional de Normalización (ISO). A través del centro nacional de Normalización en la isla se realiza el proceso de generación y adopción de normas y estándares. Dentro de las principales normas legales a las que se encuentra sujeta la organización, y las que pueden afectar la gestión de la seguridad de información se encuentran:

- Política nacional de información. IDICT (2009).
  - Documentos Rectores de la Ciencia y la Innovación Tecnológica (2001): Sistema de Ciencia e Innovación Tecnológica, Política Nacional de Ciencia e Innovación Tecnológica
- Estrategia Nacional de Ciencia e Innovación Tecnológica
- Resolución No. 127/2007: Contiene el reglamento que establece los requerimientos que rigen la seguridad de las tecnologías de la información.
- Reglamento para la implementación y consolidación del sistema de dirección y gestión empresarial estatal (Art. 265, 574-575, 583-591, 632, 634-638, 641, 566)
- Plan de Informatización del IDICT 2018-2020
- Decreto ley no.221. De los archivos de la República de Cuba. Establece las normas y principios que rigen la actividad archivística en el territorio nacional.
- Decreto Ley 265/2009 (Consejo de Estado de la República de Cuba, 2009). “Del Sistema Nacional de Archivos de la República de Cuba”, establece las disposiciones generales para la protección del Patrimonio Documental de la Nación, así como las normas y principios que rigen la Gestión Documental en el territorio nacional.
- Resolución 41/2009. De la política de archivos y conservación de documentación/ Sistema Nacional de Archivos.
- Lineamientos de la Política Económica y Social del Partido y la Revolución. VI Congreso del PCC abril/2011
- Resolución No. 60/11 Normas del sistema de control interno.
- Guía de Ciberseguridad: documento emitido por el Ministerio de Comunicaciones de la República de Cuba, que ofrece una herramienta de autodiagnóstico, que permite realizar una evaluación de su nivel de ciberseguridad - a través de un breve y simple cuestionario - luego de lo cual se le presentan una serie de recomendaciones personalizadas.

A pesar del alto número de regulaciones que se desarrollan en torno a la seguridad de la información, no existe en realidad una concepción que unifique las diferentes aproximaciones o que recoja de manera consistente y coherente los distintos enfoques de esta.

La aproximación más cercana a la implementación de un sistema de seguridad de la información, está en base a lo declarado por la resolución 127, quién está relacionada con la confidencialidad, integridad y disponibilidad de la información, pero está, tratada por los ordenadores y las redes de datos. De acuerdo a esta resolución cada entidad que haga uso para el desempeño de su actividad de las tecnologías de la información está en la obligación de diseñar, implantar y mantener actualizado, un sistema de seguridad informática y quien a su vez declara que su diseño y la elaboración del plan asociado a este, se realizarán en correspondencia con la metodología establecida por la oficina de seguridad para las redes informáticas, adscripta al Ministerio de la Informática y las Comunicaciones.

Esta metodología describe las etapas para diseñar, implementar y operar el sistema de gestión de la seguridad informática, la cual se apoya por lo definido en la NC ISO/IEC 27001:2016, la misma presenta más de diez años de antigüedad, lo que diluye aspectos de actualidad internacional y que repercute en la seguridad de las organizaciones.

1.4.2 Estado actual de la gestión de la seguridad de la información en el Ciget de Holguín

En la actualidad es una entidad de interface subordinada al Instituto de Información Científico y Tecnológica (IDICT), del Ministerio de Ciencia, Tecnología y Medio Ambiente (CITMA), que tiene como encargo social la prestación de servicios especializados en información, servicios de gestión empresarial y propiedad industrial, para favorecer la toma de decisiones, la solución de problemas y el desempeño de las organizaciones.

La misión del centro está encaminada a ser una organización de la industria de la información y el conocimiento, que facilita la toma de decisiones, la solución de problemas y el desarrollo sostenible de sus clientes, con productos y servicios científicos, tecnológicos y ambientales de alto valor agregado.

Durante el periodo 2017-2018 se efectuaron 14 incidentes de seguridad internos, todos relacionados a la mala práctica y mal uso de los activos de información por parte de los trabajadores, en entrevistas efectuadas a 22 trabajadores de la organización el 90% de los mismos desconocían la existencia de políticas de seguridad, el 68 % aseguran no poseer respaldo de sus datos y el 55 % han sido víctima de un incidente de seguridad de la información, de los cuales solo el 25% de los mismos lo han notificado a las instancias superiores. Se reconocen los insuficientes conocimientos en relación a los actuales riesgos que

se presentan sobre la seguridad de la información y las formas de proceder ante la ocurrencia de un incidente.

La organización no cuenta con mecanismos eficientes de prevención y detención de incidentes, por medio de auditorías internas de seguridad, y que los mismos se presenten en procedimientos documentados que permitan una gestión eficaz y perdurable en el tiempo.

Existe poca reutilización de información complementaria generada de la prestación de servicios, debido a la no existencia de un sistema organizado para el almacenamiento y protección de la información utilizada, que en ocasiones se pierden.

Se cuenta con un plan de seguridad informática amparado en el reglamento de seguridad para las tecnologías de la información que sustenta las bases para minimizar los riesgos y garantizar la continuidad del sistemas y procesos informáticos, pero adolece de mecanismos definidos para el control de la seguridad, así como la no existencia de informes estructurados, para la revisión por la dirección, que recojan todo el acontecer anual de la seguridad en la organización, debilitando el funcionamiento de la seguridad.

La metodología actual para la evaluación de los riesgos identificados en el Ciget de Holguín, sustenta su análisis en la cuantificación económica a través de la tabla de valores confeccionada por los estados financieros. Se deja a la subjetividad de la experiencia de cada jefe de proceso y miembros del comité de prevención y control la valoración de aquellos riesgos que no son cuantificables económicamente, lo que limita una evaluación fiable del impacto de los mismos. En este sentido destaca el riesgo de la perdida de información documentada que para el caso particular de la organización es uno de los riesgos que tiene la mayor importancia porque ante su posible manifestación el impacto es grave. A pesar de esto, en la actualidad aún la entidad de forma general, no cuenta con una metodología que permita evaluar con exactitud los riesgos que no tienen determinado un valor económico para lograr un análisis y gestión adecuada de los mismos, lo que pudiera limitar la eficiencia y eficacia del sistema de control interno, en específico para el componente gestión y prevención de riegos.

No se cuentan con modelos a seguir en los flujos de información internas y externas que se genera de los procesos de consultoría empresarial que permita contar con un sistema seguro y que cumpla con las políticas claras que permitan gestionar los datos adecuadamente, facilitar su control, almacenamiento, distribución, recuperación, eliminación, clasificación, etc.

Conclusiones del capítulo

El análisis del estado del arte sobre el objeto de estudio permite arribar a las siguientes conclusiones parciales:

La seguridad de la información en las organizaciones está orientada en planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar la confidencialidad, integridad, disponibilidad, autenticidad, responsabilidad, no repudio y fiabilidad de la información que soporta los procesos de la organización.

La revisión de la literatura consultada manifiesta que la organización a través de la implementación de un SGSI permite definir los distintos requisitos necesarios para una gestión y control eficaz de la información como atributo que ayude a elevar y preservar la calidad de los servicios y de esta forma fortalecer la credibilidad y la confianza adecuada frente a los clientes.

En los autores consultados, se aprecian un abordaje práctico, limitándose al campo de acción de las investigaciones, lo que dificulta su aplicación en otros contextos. Existen carencias en técnicas y herramientas para la aplicación de cada fase, etapa o paso, además de abordar la gestión de riesgo como fase fundamental de desarrollo, excluyendo etapas del proceso de gestión de la seguridad de la información.

Las insuficiencias encontradas en el Ciget de Holguín en relación a la gestión de la seguridad de la información justifica el desarrollo de la investigación científica propuesta.

CAPITULO II. PROCEDIMIENTO PARA IMPLEMENTAR UN SGSI COMO CONTRIBUCIÓN A LA CALIDAD DE LA INFORMACIÓN DE LOS SERVICIOS DE CONSULTORÍA.

Generalidades

En el presente capítulo se expone el procedimiento propuesto basada en la integración de varios modelos, normas, herramientas y buenas prácticas para la implementación de un SGSI, que se alinee con la NC ISO/IEC 27001:2016. Permite la retroalimentación y mejora del diseño e implementación. Se basa en un avance progresivo y con un enfoque sistémico que considere las necesidades de la organización y la estructura organizacional. Con este tipo de investigación se pretende dar solución a la necesidad que actualmente presenta el objeto de estudio, en cuanto al manejo y protección de la información tanto de los clientes como de la misma organización.

La correcta implementación del procedimiento asegurará que la seguridad de información en la organización deje de ser una actividad poco organizada para ser un conjunto de actividades metódicas y controladas, siendo todos los trabajadores protagonistas y responsables de su cumplimiento. Además se aspira a incrementar la conciencia en seguridad. El procedimiento propuesto, comprende 6 etapas básicas que se despliegan a través de 14 pasos (Figura 3). El objetivo que se persigue en este capítulo es argumentar cada una de las etapas, con el fin de poder alcanzar un correcto entendimiento del objetivo que se traza con el desarrollo del mismo.

Figura 3. Procedimiento para implementar un SGSI como contribución a la calidad de la información de los servicios de consultoría.

Etapa 1: Compromiso y Preparación

Objetivo: Asegurar el compromiso de la alta dirección y el involucramiento de los trabajadores para desarrollar las actividades planificadas según el alcance propuesto; sentar las bases para el desarrollo del procedimiento mediante la creación del equipo gestor.

Técnicas y/o herramientas de trabajo: - Observación directa y análisis documental - Revisión bibliográfica - Tormenta de ideas - Trabajo en grupo
Entradas: - Principales dificultades y deficiencias en la gestión de la seguridad de la información, obtenidas de los resultados de controles internos, auditorías y revisiones por la dirección efectuadas hasta la fecha. - No conformidades en la práctica de la prestación de servicios, vinculadas con la seguridad de la información. - Ventajas de la gestión de la seguridad de la información; beneficios esperados. - Propuesta preliminar del alcance del proyecto.
Contextos de desarrollo: Reuniones del CD Capacitaciones
Salidas: - Acta de compromiso de la dirección. - Cronograma de aplicación del proyecto según alcance preliminar propuesto, aprobado en acuerdo por el CD; debe quedar evidencia documental. - Motivación de los trabajadores. - Grupo gestor conformado.

Paso 1: Compromiso de la dirección e involucramiento de los trabajadores

El primer paso del procedimiento está encaminado en contar con la intención de cambio. En el mismo se analizan las oportunidades de implementar el sistema.

Se efectúa una reunión inicial con las partes interesadas para comunicar de forma general el procedimiento y los objetivos que el mismo persigue.

El compromisos de la dirección debe estar orientada en el establecimiento y/o mejoramiento de políticas, objetivos, funciones y responsabilidades de seguridad de la información, comunicar a la organización la importancia del cumplimiento de lo que se establece, brindar los recursos necesarios, decidir criterios y niveles para aceptación de riesgo, asegurar que los

procedimientos de seguridad de la información brindan apoyo a los requisitos de la organización. Identificar y atender los requisitos legales y reglamentarios y mantener la seguridad suficiente mediante la aplicación correcta de todos los controles que se implementen y asegurar que se realicen las auditorías internas y efectuar las revisiones cuando sea necesario.

En el desarrollo de la actividad se hace necesaria la creación de un acta en el que se notifique el compromiso de la dirección de la organización.

Se establecerá una capacitación para el consejo de dirección, de los principales conceptos teóricos y prácticos que serán abordados, para lograr familiaridad con los términos y herramientas.

Puede ser de objeto de ayuda la búsqueda de información actualizada en materia de seguridad de la información y el análisis del contexto que posibilite establecer los principios de implementación.

En reuniones sindicales se notificarán a los trabajadores las actividades propuestas, las intenciones de implementación, así como los objetivos que se persiguen. Se pedirá el compromiso de los trabajadores para que el desarrollo de las actividades puedan ser ejecutadas de forma correcta.

Paso 2: Creación del grupo gestor

En reunión efectuada con el consejo de dirección (CD), se conformará el equipo de trabajo que se encargue de gestionar las actividades planificadas, así como un responsable general, quien debe responder ante la dirección sobre la ejecución del cronograma propuesto.

Para la confección del mismo se propone la existencia de una persona perteneciente al CD, para que de esta manera las decisiones que se requieran tomar puedan estar respaldadas por la dirección.

Se ejecutarán las capacitaciones necesarias para lograr que el grupo gestor, esté capacitado para iniciar con la ejecución de las actividades propuestas.

Las mismas estarán desplegadas en las competencias de los trabajadores, siendo el departamento de recursos humanos (RRHH) responsable de su resguardo.

Etapa 2: Diagnóstico

Objetivo: Proporcionar una revisión de la realidad interna y externa de la organización en materia de seguridad de la información, identificando las brechas existentes que pueden afectar las actividades planificadas.

Técnicas y/o herramientas de trabajo:

- Entrevistas
- Listas de chequeo

- Observación directa y análisis documental - Síntesis y elaboración de informe
Entradas: Marco Legal normativo de la seguridad de la información Informe de resultados de la gestión de riesgos de seguridad informática. Principales dificultades y deficiencias en la gestión de la seguridad de la información en los servicios científicos-técnicos en la organización, obtenidas de los resultados de controles internos, auditorías y revisiones por la dirección efectuadas hasta la fecha. No conformidades en la práctica de la prestación de servicios, vinculadas con la seguridad de la información. ANEXO 1: Guía de diagnóstico de ciberseguridad Guía Autocontrol Plan de desarrollo y uso de las TIC NC ISO/IEC 27001:2016. Anexo A
Contextos de desarrollo: - Todas las áreas de la organización
Salidas: - Plan de medidas diagnóstico de ciberseguridad - Informe de diagnóstico aprobado por el consejo técnico asesor. - Plan de acción.

Paso 3: Comprender la organización y su contexto

Se analiza el contexto en que se desenvuelve la organización. Con vista de a identificar debilidades, amenazas, fortalezas y oportunidades de la organización, el diagnóstico se realizará por áreas para abarcar todos los procesos de la organización. En el mismo se recogerán los datos a través de las herramientas o técnicas seleccionadas, que luego serán procesadas por el grupo gestor seleccionado. Aquellos incidencias detectadas, luego de su análisis, se recogerán en el registro de no conformidades, la estructura de la misma se muestra en el anexo 9.

Se aplicarán encuestas por cada proceso existente en la organización. Se aplicará obligatoriamente a todos los jefes de procesos, o sus equivalentes por áreas. Aleatoriamente, se aplicarán a los especialistas y personal de apoyo. No deben faltar por encuestar a: secretaria, responsable de gestión archivística, comunicadora, responsable del control interno, administrador de la red y director(a) de la organización.

Se deben realizar al menos 5 entrevistas a clientes, que permitan obtener una visión de cómo se define a la organización en los servicios prestados con respecto a la seguridad de la información.

Se aplicará la guía de ciberseguridad, unido a la guía de autocontrol. Todos los criterios que responden a la seguridad de la información se recogerán en un documento excel para determinar el estado de cumplimiento de los mismos.

Para determinar al cumplimiento de los requisitos que establece la NC ISO/IEC 27001:2016, se utilizará igualmente el Microsoft excel en el que se agruparán los 114 controles de los anexos de dicha norma. La evaluación del estado actual de madurez por cada uno de los dominios se empleará la escala referida a: Inexistente, Parcialmente Implementado e Implementado. Por cada control se analizará si el mismo es aplicable, en caso afirmativo, establecer el estado de los mismos dentro de la organización.

Para brindar elementos más explicativos sobre el estado de la seguridad de la información en la organización se desarrollará un informe en el que se incluya un análisis en:

Objetivos y política de la gestión de la información: se identifica la existencia de objetivos y políticas que agrupen los preceptos para asegurar toda la información y su adecua manipulación.

Organigrama organizacional: se analiza relación con las políticas de la organización a la cual se subordina; cómo inciden y en qué grado son vinculantes y obligatorias. Este aspecto proporciona una visión general de las diferentes actividades y funciones que se desarrollan.

Procesos: se identifica el mapa de procesos de la organización, con el objetivo de ofrecer una representación gráfica que ayuda a visualizar y estudiar su interrelación con los flujos de información. Ofrecer información detallada de la organización, identificar su misión, visión y objetivos estratégicos.

Inventario de la información relevante: se debe identificar si la organización posee un inventario de todas las fuentes que contengan información relevante para la organización.

Control de Riesgos: se evalúa la existencia de metodologías para la apreciación de los riesgos de seguridad de la información, análisis y tratamiento de los mismos.

Regla de acceso y uso: se determina si la organización ha definido los permisos, privilegios y las reglas de acceso a la información del sistema, así como identificar si se han asignado los perfiles de usuario (roles) y si se han establecido su relación con las responsabilidades funcionales en la organización.

Catálogos de normas: se realiza una revisión de la presencia y empleo de estándares, normativas, leyes o recomendaciones para la gestión de la información de la organización que deben tenerse en cuenta a lo largo de todo el proceso de desarrollo.

*Controles**:*** se revisa la existencia de controles operativos y técnicos, y si los mismos se encuentran documentados.

Control interno: se evalúa la existencia del plan de control interno y la inclusión de procesos de gestión de la seguridad de la información. Se debe tener en cuenta lo que se establece en la Resolución 60/11 Normas del Sistema de control interno de la Contraloría General de la República.

Capacitación: identificar los niveles de competencias de los trabajadores en el manejo y uso de la información y las fuentes contenedoras, los compromisos organizacionales para la capacitación de los trabajadores, la existencia de un programa de formación del personal en el que se contemplen las necesidades y requerimientos necesarios de superación.

Modelo de actuación: reconocer si se han definido y asignado responsabilidades asociadas a la gestión de la seguridad de la información, conocer el personal que está involucrado en este proceso y determinar la participación y compromiso de la alta dirección con estos proyectos.

Inventario de tecnología: evaluar la infraestructura existente en la organización y la seguridad que los mismos contienen. Enfatizar en: soporte tecnológico, proyectos de digitalización, bases de datos, repositorios de información, software de gestión, documentos en formato digital y procedencia.

Tabla de retención de documentos: determinar las características, tipología documental y define los períodos de conservación y las acciones de disposición sobre los documentos. Es un instrumento archivístico que identifica, de acuerdo con sus funciones y procedimientos, los documentos que produce, recibe y se debe conservar. Permite normalizar la producción documental, garantizando la organización de la información activa de la empresa.

Regla de acceso y uso: determinar si la organización ha definido los permisos, privilegios y las reglas uso aceptable de los activos y los medios que la soportan, así como si se han asignado los perfiles de usuario (roles), accesos y relación con las responsabilidades funcionales en la organización.

Organización de la información: evaluar la forma en que la información se despliega en la organización, así como los niveles de encriptación y que acciones se establecen para asegurar su confidencialidad, integridad y disponibilidad de la misma.

Soporte documental: se deben identificar el soporte documental existente, que permite aligerar las etapas que deben cumplirse para la documentación.

Identificación y trazabilidad del producto: conocer si se garantiza la identificación y trazabilidad del producto “información” desde que se conforma hasta que se culmina, definiéndose en qué direcciones se debe trabajar en caso de no garantizarlo.

Bienes del cliente: precisar la información que son propiedad del cliente para la realización del servicio solicitado por él, los medios y recursos que permiten controlar y preservar la propiedad del cliente por quienes hacen uso de estos.

Preservación del producto: verificar si se tiene establecida la forma de preservar el producto durante el proceso de realización y su entrega para mantener la conformidad con los requisitos. La preservación debe incluir la identificación, almacenamiento y protección.

Producto no conforme: analizar si se identifica y controla el servicio no conforme con los requisitos establecidos para prevenir su uso o entrega no intencionados, si el CTA cumple sus funciones con respecto al seguimiento de los servicios para identificar cualquier deficiencia y si están definidos los criterios de aceptación y rechazo. Se debe precisar la forma más adecuada para identificar y proceder con los servicios no conformes.

De acuerdo a las técnicas de captación de información existentes, la autora sugiere que deben utilizarse: análisis documental, entrevistas, listas de chequeo y observación directa.

Paso 4: Elaboración y aprobación del informe de diagnóstico

Se analizará los documentos identificados, así como el resultado de las entrevistas, listas de chequeo y encuestas ejecutadas. Como resultado final del diagnóstico se elaborará un informe final que en el mismo debe quedar reflejado las deficiencias detectadas de acuerdo a los requisitos de la norma, se moldearán por cada epígrafe de la NC ISO/IEC 27001:2016, las observaciones que a partir del diagnóstico pudieron determinarse en relación a los mismo, así como el conjunto de actividades que se llevarán a cabo para darle cumplimiento.

El informe de resultados puede contener toda la información que la dirección del centro y el grupo gestor de la seguridad de la información estimen convenientes, con el fin de que el diagnóstico sea lo más completo posible. El mismo debe sintetizar los resultados para un mejor entendimiento del mismo.

Quienes deberían participar:

- Grupo gestor designado para la seguridad de la información.
- Jefes de Procesos.
- Trabajadores seleccionados para el desarrollo de las entrevistas.

Etapa 3: Diseño y documentación

Objetivo: Corregir las brechas existentes en la organización con respecto a los requisitos establecidos en la NC ISO/IEC 27001:2016 y proporcionar un marco de trabajo que permita la comprensión del SGSI, alineado al sistema de gestión de la calidad (SGC) implementado.

Técnicas y/o herramientas de trabajo:
- Diagramación de procesos y flujos

- Síntesis y elaboración del informe - Tormentas de ideas - Juicio de expertos
Entradas: - Informe final del diagnóstico en términos de gestión de la información. - Plan de medidas diagnóstico de ciberseguridad - Plan de desarrollo y uso de las TIC
Contextos de desarrollo: - Reuniones del grupo gestor - Reuniones del CD
Salidas: - Inventario de activos de información - Procedimiento de apreciación y tratamiento de los riesgos. - Informe sobre evaluación y tratamiento de riesgos - Plan de tratamiento del riesgo - Objetivos y política de integración del SGSI y SGC - Objetivos y política operacionales de seguridad de la información - Declaración de aplicabilidad - Procedimientos de gestión de la seguridad de la información - Instrucciones técnicas - Listado de registros - Listado actualizado de normativas, legislación y/o regulaciones sobre seguridad de la información - Plan de Contingencia

Paso 5: Inventario de activos de información

En esta etapa se debe realizar un estudio de todos los activos de información independiente del formato en que este se encuentre. Se pretende centralizar la seguridad de la información digital e impresa, con el fin de que puedan ser medibles en un único sistema.

El inventario de activo se realizará por procesos, áreas o grupos de trabajo quedando de manera agrupada, todos los activos que intervengan en los procesos de producción, emisión, almacenamiento, comunicación, visualización y recuperación de la información.

Se consideran activos de información todo aquello que presente un valor y para la organización, sean Datos o Información, Software, Hardware, Servicios, Personas o Conocimiento

En el inventario de activos de seguridad se incluirá la información necesaria que permita identificarlo, describirlo, clasificarlo y ubicarlo, la cual se realizará para cada proceso de la organización. Se recomienda para su confección la tabla que se muestra en el anexo 2.

Esta información se incluirán en la herramienta de gestión de activos, y se prestará especial cuidado en distinguir los activos críticos para la organización.

Los activos de información se clasificarán y etiquetarán de acuerdos a los criterios que se establecen por la organización.

Al menos anualmente o cuando se produzcan cambios significativos, se revisará el inventario de activos con el fin de mantenerlo actualizado.

El encargado de sentar las bases de clasificación de la información será la dirección que, una vez realizada esta clasificación e incluida en los procedimientos, deberá de informar al responsable del SGSI implementado para su aplicación a nivel de medidas de seguridad en los activos de información identificados en el sistema.

Posteriormente, se deben notificar a todo el personal la clasificación de la información indicada.

Paso 6: Selección e implantación de metodología de gestión de riesgos

El primer paso para llevar a cabo el proceso de gestión del riesgo en la organización es definir la metodología que se va a seguir. El objetivo de este primer paso es hacer que todas las partes conozcan la metodología y la gestión del riesgo se haga de manera homogénea en todas las áreas.

En el capítulo 1 se analizó la NC ISO 31000:2018, como una metodología para gestionar los riesgos. Como parte de la visión organizacional de implementar sistemas que adopten dicha metodología para todos sus procesos de gestión, esta investigación asumirá sus criterios. Tomando como referencia esta norma se expone el esquema de trabajo para la gestión de los riesgos

Evaluación de los riesgos

Objetivo: Identificar, análisis y evaluación del riesgo.

- ✓ Actividad: Identificación del riesgo

El proceso de la identificación del riesgo debe ser permanente e interactivo basado en el resultado del análisis del contexto estratégico y debe partir de la claridad de los objetivos estratégicos de la entidad para la obtención de resultados, identificando los factores internos o externos a la entidad, que pueden ocasionar riesgos que afecten el logro de los objetivos. Es la base del análisis de riesgos que permite avanzar hacia una adecuada implementación de políticas que conduzcan a su control.

Para la identificación de los riesgos se hará un inventario de los mismos, definiendo en primera instancia las causas o factores de riesgo, tanto internos como externos, los riesgos, presentando una descripción de cada uno de estos y finalmente definiendo los posibles efectos. Los riesgos

más significativos para la entidad relacionados con el desarrollo de los procesos y los objetivos organizacionales quedarán en los primeros niveles del inventario.

No.	Riesgo	Causas (factores internos o externos)	Descripción	Efectos (consecuencias)

No.: consecutivo que identifica el riesgo

Riesgo: representa la posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la entidad y afectar el logro de sus objetivos.

Causas (factores internos o externos): son los medios, las circunstancias y agentes generadores de riesgo. Los agentes generadores que se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo; se pueden clasificar en cinco categorías: personas, materiales, comités, instalaciones y/o entorno.

Descripción: se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.

Efectos (consecuencias): constituyen las consecuencias de la ocurrencia del riesgo sobre los objetivos de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como: daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Técnicas y/o herramientas sugeridas son: Tormenta de ideas a partir de la integración del comité de control interno formado por expertos de las áreas críticas para identificar los riesgos, Entrevistas semi-estructuradas, Listas de verificación, Observación directa

- ✓ Actividad: Análisis del riesgo

Se establece la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.

Es importante tener en cuenta los controles existentes en la organización para reducir los riesgos, ya que esto puede variar la valoración del impacto y las consecuencias sobre un activo de información.

Para establecer los criterios de analizar el riesgo se ha seleccionado un método semi-cuantitativo, donde se utiliza una escala de valoración numérica para el impacto y la probabilidad, donde se combinan para determinar un nivel de riesgo. Esta investigación ha tomado como referencia la postulada por los autores Santofimio & Manrique (2015), y que a su

vez a modificado para que la misma sea apropiada a las especificaciones del objeto de estudio investigado.

Se define la clasificación de la probabilidad de ocurrencia del riesgo de la siguiente forma:

Tabla 1. Calificación de la probabilidad de ocurrencia del riesgo

Calificación de la Probabilidad					
Concepto	**Muy Baja**	**Baja**	**Moderada**	**Alta**	**Muy Alta**
Calificación	0,1	0,3	0,5	0,7	0,9
Definición	Probabilidad de ocurrencia muy baja, prácticamente nula.	Probabilidad baja, menor que 1%, eventos posibles, pero poco probables.	1%<Probabilidad<5%, eventos que pueden ocurrir.	5%<=Probabilidad<10%, la experiencia indica que ocurren con alguna frecuencia.	Probabilidad >=10%, se presentan en forma relativamente frecuente.

Para evaluar el impacto de acuerdo al efecto final, se establece es importante que se tengan en cuenta los principales factores que inciden en el éxito de la organización y las incidencias de estos en materia de seguridad de la información, por ejemplo pueden ser:

- El costo económico de materializarse el riesgo.
- Los tiempos de desarrollo de las actividades de la organización.
- La calidad de los servicios y productos internos y externos.

En la siguiente tabla se ejemplifica el modo de proceder para estimar el valor cualitativo del impacto para determinar su evaluación.

Tabla 2. Evaluación del Impacto

Evaluación del Impacto					
	0,05	**0,1**	**0,2**	**0,4**	**0,8**
Costo	Incremento insignificante del costo	Incremento en el costo <5%	5%<=Incremento en el costo<10%	10%<=Incremento en el costo<20%	Incremento en costo>=20%
Tiempo	Atraso insignificante de tiempo	Atraso en tiempo <5%	5%<=Atraso general <10%	10%<=Atraso general <20%	Atraso general >=20%
Calidad	Disminución de la calidad apenas apreciable	Sólo aplicaciones muy exigentes son afectadas.	La reducción de la calidad requiere aprobación del cliente.	La reducción de la calidad es inaceptable para el cliente.	El producto final del proyecto es totalmente inutilizable.

Con los valores anteriores se procede a cuantificar el riesgo para cada amenaza identificada a través de la Matriz de Análisis Cuantitativo de Riesgos.

Tabla 3. Matriz de Análisis Cuantitativo de Riesgos

Riesgo	Probabilidad	Estimación de Probabilidad(P)	Objetivo Afectado	Impacto	Estimación de Impacto (I)	Tipo de riesgo	Valor Riesgo (P*I)
			Tiempo				
			Costo				
			Calidad				

Cálculo del riesgo: Este se realiza a partir de la probabilidad de ocurrencia del riesgo y el impacto que este tiene sobre la organización (Riesgo = Estimación de Probabilidad de la amenaza x Estimación de Impacto).

Con este procedimiento se determinan los riesgos que se deben controlar, con la prioridad establecida.

Al finalizar el cálculo los riesgos se ubican en rangos y se clasifican de acuerdo a los niveles: Muy Alto, Alto, Moderado, Bajo y Muy Bajo, luego se ordenan de mayor a menor y se aborda cada uno de acuerdo a su prioridad.

En la Tabla 3 se clasifica el tipo de riesgo, esto se hace después de obtener los resultados de la estimación del riesgo de acuerdo a: costo, tiempo y calidad.

Tabla 4. Niveles de riesgos

Nivel de Riesgo	Probabilidad x Impacto	Tipo de riesgos
Muy Alto	**Mayor a 0.50**	No tolerable o No aceptable
Alto	**Menor a 0.50**	
Moderado	**Menor a 0.30**	Intermedio
Bajo	**Menor a 0.10**	Tolerable o aceptable
Muy Bajo	**Menor a 0.05**	

Riesgo no tolerable o No aceptable: El tratamiento es esencial, se deben realizar todas las acciones que ameriten su corrección, en caso de que el mismo amerite recursos para su mitigación y que la organización no disponga de los mismos, este se documentará y analizará con las instancias superiores, declarándose como un elemento de alto impacto para la organización.

Riesgo Intermedio: Se toman en cuenta costos y beneficios contra las consecuencias probables para decidir.

Riesgo tolerable o aceptable: No son necesarias medidas de tratamiento

- ✓ Actividad: Valoración del riesgo

El propósito de la valoración del riesgo es apoyar a la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis de riesgo, con los criterios del riesgo que se definen para determinar cuándo se requiere una acción adicional. Esto puede conducir a una decisión de: no hacer nada más; considerar opciones para el tratamiento del riesgo; realizar un análisis adicional para comprender mejor el riesgo; mantener los controles existentes; reconsiderar los objetivos.

Es necesario el entendimiento del riesgo durante el análisis, para tomar decisiones de las acciones futuras. Consideraciones éticas legales, financieras, entre otras, son elementos de entrada para la decisión. Las decisiones pueden incluir: si un riesgo necesita tratamiento, prioridades para el tratamiento, si una actividad debería emprenderse y/o cuál de los diferentes caminos debería seguirse.

El proceso de valoración del riesgo debe documentarse junto con los resultados de la valoración. La extensión del informe dependerá de los objetivos y el alcance. No puede faltar en el reporte los siguientes criterios:

- Apreciación del riesgo de seguridad de la información
- Criterios de aceptación y apreciación del riesgo
- Lista de riesgo, identificación de dueños
- Probabilidad de ocurrencia y niveles de riesgos, consecuencias de materializarse el riesgo
- Resultados de la identificación del riesgo
- Resultado del análisis de riesgos y su evaluación

Tratamiento del riesgo

Luego de evaluar el riesgo, se hace necesario establecer el tratamiento que deben tener los mismos. Una vez que se procese el riesgo, es posible que el mismo introduzcan otros nuevos que es de necesidad gestionarlos. De acuerdo a la NC ISO 3100:2018, el tratamiento del riesgo implica un proceso iterativo y puede establecerse siguiendo las siguientes pautas:

- formular y seleccionar opciones para el tratamiento del riesgo;
- planificar e implementar el tratamiento del riesgo;
- evaluar la eficacia de ese tratamiento;
- decidir si el riesgo residual es aceptable;

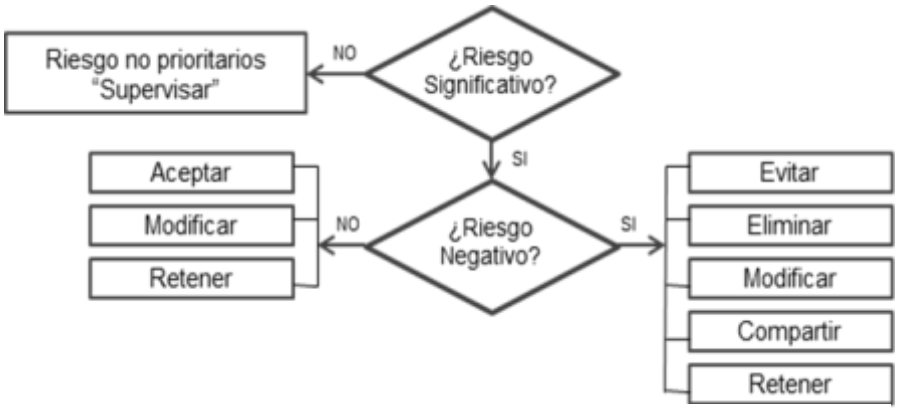


Figura 4. Estrategia de tratamiento del riesgo según NC ISO 3100:2018

- si no es aceptable, efectuar tratamiento adicional

La NC ISO 3100:2018, establece para tratar el riesgo una o más de las siguientes opciones:

- evitar el riesgo y decidir no iniciar o continuar con la actividad que genera el riesgo;
- aceptar o aumentar el riesgo en busca de una oportunidad;
- eliminar la fuente de riesgo;
- modificar la probabilidad de ocurrencia;
- modificar las consecuencias que atribuyen a la ocurrencia;
- compartir el riesgo
- retener el riesgo con base en una decisión informada.

La selección de las opciones para el tratamiento del riesgo se deberá realizar de acuerdo con los objetivos de la organización, los criterios del riesgo y los recursos disponibles. En figura 4 se muestran la estrategia a seguir.

Una vez analizado el riesgo, se realizará un nuevo análisis, de no existir opciones disponibles para el tratamiento o si las opciones no modifican suficientemente el riesgo, entonces los mismos se encontrarán dentro del nivel de riesgos aceptable, los que se incluirán en el listado de riesgos de la organización, los mismos se documentará y será objeto de seguimiento, revisión y, cuando sea apropiado, realizar un tratamiento adicional.

Aquellos riesgos que presenten un nivel de riesgo “muy alto”, y luego de su tratamiento se encuentre en las opciones de “aceptar”, estos irán a los riesgos generales de la organización.

Los riesgos que no tengan incidencia en toda la organización, serán monitoreados por los jefes de procesos de control interno y por el equipo gestor.

Si del resultado de la gestión del riesgo se desencadena alguna acción que tributa a la estrategia de informatización, esta será plasmara en el “Plan de desarrollo y uso de las TIC”.

La dirección de la organización y otras partes interesadas deberían ser conscientes de la naturaleza y el nivel del riesgo residual después de ejecutado esta actividad.

Técnicas y/o herramientas sugeridas: Juicio de Expertos

Seguimiento y revisión

El seguimiento y la revisión se incorporarán en todas las actividades, donde se establece una retroalimentación en todos los procesos de la gestión de la seguridad de la Información.

Debe darse un seguimiento continuo para que la valoración del riesgo pueda actualizarse cuando sea necesario.

Los riesgos asociados a los procesos serán auditados por los responsables de los procesos de control Interno de la organización, quedando plasmados en las actas de auto inspección.

Quienes deberían participar:

- Grupo gestor designado para la seguridad de la información.
- Trabajadores seleccionados para formar parte de los expertos en gestión de riesgos de seguridad de la información.

Resultado esperado

- Opciones de tratamiento de riesgo y controles de implementación
- Declaración de aplicabilidad
- Plan de tratamiento de riesgo

Paso 7: Gestión de la documentación de la NC ISO/IEC 27001:2016 para la contribución a elevar la calidad de la información de los servicios de consultoría.

Paso 7.1: Normas de seguridad aplicables a los servicios

El objetivo que se persigue es declarar punto de referencia para dirigir la organización y establecer y revisar los objetivos de seguridad en la prestación de servicios, los que a su vez contribuyen al cumplimiento de las políticas establecidas y elevar la calidad de los resultados finales.

Se definen por el equipo gestor de la organización los medios disponibles para el almacenamiento de la información. En el caso de la información digital los mismos deben contar con las condiciones tecnológicas adecuadas para su explotación. Se deberán implementar los instrumentos de seguridad.

El equipo gestor definirá por cada servicio el medio a almacenar. La información es brindada al responsable del sistema de gestión de la calidad, quien deberá por cada procedimiento de servicio incorporar la siguiente información:

Identificación: Se refiere al nombre o título con el que se identifica el documento o directorio - en caso que aplique se incluye el código del mismo. Por cada documento debe establecerse un código que permita homogenizar su recuperación.

Almacenamiento: Se trata del lugar físico y/o electrónico donde se almacena los datos.

Protección: Es la manera de cómo se preservan los datos para asegurar su integridad. (Carpetas, cuadernillos, medios electrónicos, etc.) También se refiere a las acciones que se toman para proteger el registro (accesos restringidos, contraseñas, etc.)

Recuperación: Es la forma a través de la cual se rescata el registro, tomando en cuenta su localización. (Título, Fechas, Número consecutivos, etc.)

Retención: Tiempo en que se debe mantener los datos, se determina en función de la normatividad de la organización y regulaciones que se aplican.

Disposición: Es la acción a tomar sobre los datos cuando se ha cumplido el tiempo de retención establecido, es decir, el destino final de los mismos, ejemplo: eliminación, guarda permanente, reciclaje, entre otros.

La organización para el control de la seguridad y la gestión de los servicios debe considerar los aspectos siguientes:

- Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información en condiciones de seguridad y calidad.
- Toda información que entra a la organización procedente de clientes a razón de la prestación de un servicio, que tributará al resultado final del mismo, debe estar registrada. Para el mismo se hará uso de registro declarado en el anexo 4.
- Disponer acciones para que el envío de información confidencial y de los instrumentos para la realización de operaciones a sus clientes, se haga en condiciones de seguridad. Cuando dicha información se envíe o adjunta a un correo electrónico, ésta deberá estar cifrada.
- Dotar de seguridad, la información confidencial de los clientes que se maneja en los equipos, redes y locales de la organización, para ello se establecerá un destino final de la información para ser almacenada. En el caso de la información digital se establecerán accesos de “solo lectura” y permisos específicos para acceder a diferentes niveles. Para el caso de la información impresa, se establecerá los permisos de acceso restringido.
- Toda información de resultados de servicios debe almacenarse en un almacén central cumpliendo con los aspectos técnicos y operativos que garanticen su seguridad, y que permita la retroalimentación para trabajos futuros.
- Por cada proceso o servicio se debe llevar un control de versiones. En el mismo se establece el identificador del documento o directorio, fecha de la última versión y responsable. Este se confecciona sobre la base de un registro, que se almacena en formato digital.
- El resultado final de un servicio, cuando la entrega en sobre los medios digitales debe ser entregada en formato pdf, así como definir en las propiedades de los documentos: título, elaborado por, organización que realizó el servicio, categoría del servicio prestado y palabras claves de los mismos.
- Cada trabajador debe velar porque la información enviada a los clientes esté libre de software malicioso.
- Proteger las claves de acceso a los sistemas de información. En desarrollo de esta obligación, la organización evitará el uso de claves compartidas, genéricas o para grupos. La

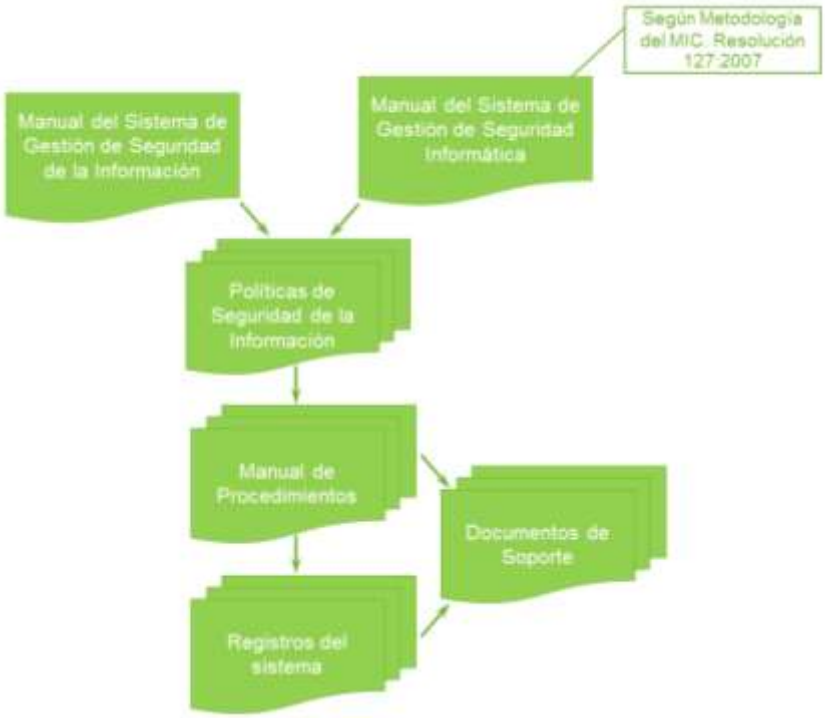
identificación y autenticación en los dispositivos y sistemas de computarizados en de la organización será única y personalizada.

- Se establecerán políticas en los sistemas de cómputos que eviten la instalación de programas o dispositivos que capturen la información de los clientes y de sus operaciones.
- Se debe establecer los mecanismos para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en sistemas de cómputo sólo pueda ser realizado por personal debidamente autorizadas.
- Es obligatorio que todo el personal de nueva incorporación a la organización, reciba notificación con las obligaciones con respecto del cumplimiento de la política de seguridad de la información y declarar los compromisos de confidencialidad. El mismo recibirá una formación inicial, por parte del personal de la organización.
- El responsable jurídico participa en la confección del compromiso de confidencialidad a firmar por los trabajadores y terceros que desarrollen funciones en la organización, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de las políticas de seguridad y el tratamiento de incidentes de seguridad que requieran de su intervención.

Paso 7.2: Documentación requerida por la NC ISO/IEC 27001:2016

La NC ISO/IEC 27001:2016 define diferentes tipos de información de obligatorio cumplimiento; sin embargo, no toda la información necesita ser documentada como un documento independiente. Es flexible para que la organización decida sobre el tamaño de la documentación y el nivel de detalle que se documenta.

El diseño de la documentación del SGSI, debe centrarse en establecer una estructura sencilla y de fácil manipulación, aplicable a la organización y que proporcione evidencias para el logro de los objetivos y las metas. Además que el mismo permita adaptarse a las particularidades declaradas en la metodología del ministerio de informática y las comunicaciones de Cuba.



Para el desarrollo de la misma,

se propone una estructura documental representada por cinco niveles: Manual de sistemas, Políticas, Procedimientos, Registros, Documentos de soporte.

Manual de SGSI: Constituirá el principal documento que mostrará la constancia escrita del sistema, y que lo describe adecuadamente. Sirve de referencia permanente durante su aplicación y mantenimiento. Con el fin de cumplir con los parámetros exigidos se desarrollará 2 manuales, uno con la estructura propuesta por la resolución 127 y otro que recoja las particularidades del SGSI. En el mismo se declarará los objetivos que se persigue con la implementación.

Políticas: Se declararán los criterios operativos a ser ejecutados que complementan el logro de los objetivo trazados y constituirá la guía para indica cuál las reglas o normas a seguir para hacer lo correcto en cada caso. Será material de referencia para los manuales que estarán vigentes.

Manual de procedimientos: Será un documento de nivel operativo, que especifica las instrucciones para llevar a cabo las actividades del sistema. Su elaboración, permitirá agrupar los procedimientos de los dos manuales establecidos. Será material de referencia para los manuales que estarán vigentes.

Registros del sistema: serán los documentos que proporcionen la evidencia del cumplimiento y conformidad con las precisiones del SGSI establecidas. Será material de referencia para los manuales que estarán vigentes.

Documentos de Soporte: Serán aquellos documentos complementarios, con el fin de formalizar la actividades y tareas requeridas sobre la gestión de la seguridad de la información.

En el epígrafe 1.3.1 del capítulo 1 se abordó la lista de documentos y registros que requiere la NC ISO/IEC 27001:2016, la que constituyen el pilar para el desarrollo de los procedimientos para la organización. Para dar cumplimiento con lo que recoge la resolución 127 en materia de seguridad de las tecnologías de la Información, se continuará con la estructura documental que exige la metodología que se implementa en Cuba.

Actividad: Revisión, actualización y/o definición de las políticas, objetivos y declaración de la aplicabilidad de seguridad.

Se pretende desarrollar los objetivos y políticas de seguridad que defina la correcta gestión de la seguridad de la información integral en la organización.

Para definir la política y objetivos de seguridad debe estar sobre la base de los resultados del diagnóstico y alinearlos con los objetivos generales del centro en todas las funciones y niveles pertinentes.

Actividad: “Desarrollo de los objetivos de integración al SGC y objetivos operativos de seguridad de la información”

Los objetivos y el alcance deberán estar alineados con la realidad de la organización y las prioridades existentes. Se deben tener en cuenta las condicionantes y recursos que disponga la organización.

Se elaborarán objetivos de integración entre el sistema de gestión de la calidad y seguridad de la información, de los mismos se despliegan en una serie de objetivos operativos de calidad y de seguridad de la información.

El equipo gestor de SI y los asesores de calidad elaborarán la propuesta a ser llevada al consejo de dirección. Los responsables de cada sistema serán los responsable de su seguimiento y medición.

Por cada objetivo propuesto se tendrá en cuenta: la persona responsable, los recursos necesarios, la planificación de las tareas a realizar y la evaluación de los resultados.

El responsable del sistema de calidad tiene la misión de comprobar que los objetivos permanentes son conocidos, comprendidos y aplicados por todo el personal de la organización.

Anualmente, la dirección de la organización, unido al responsable de la seguridad de la información y calidad definirán nuevos objetivos, que se llevarán a cabo en el transcurso del siguiente período, con el fin de mantener el compromiso de mejora continua del SGSI.

A la hora de determinar los nuevos objetivos se valorará, el grado de cumplimiento para el período anterior, y el grado de cumplimiento de la política de seguridad de la información.

Se tendrán en cuenta, los resultados de las auditorías, la legislación que sea aplicable, el compromiso de mejora continua y operacional de la organización, las opciones tecnológicas existentes y las quejas y comentarios tramitados.

Actividad: “Desarrollo de las políticas de integración al SGC y políticas operativas de seguridad de la información”

En el caso de existir una política de seguridad de la información y calidad ya definida; se debe realizar un análisis profundo de la misma para evaluar si es necesario hacer una actualización, donde se debe tener en cuenta puntos como por ejemplo, activos que no se midieron y las incidencias sobre este, evaluación de controles que no sean operativos y sostenibles en el tiempo.

La política de la calidad y seguridad de la información pretende integrar dentro de las actividades de la organización la gestión de la calidad bajo la NC ISO 9001: 2015 y la gestión de la seguridad de la Información bajo la NC ISO/IEC 27001: 2016, como forma y cultura de evolucionar hacia la satisfacción de las partes interesadas, la gestión de los riesgos, la gestión

integral de la seguridad de la información en todas sus fases de tratamiento y la mejora de los procesos, productos y servicios de la organización.

Así mismo se establecerán políticas operativas que proporcionarán como deberá definirse, mantenerse y actualizarse el SGSI, así como establecer y revisar los objetivos del mismo, la cual debe ser comunicarse a toda la organización y se publicará en los diferentes medios comunicativos existentes. La misma debe revisarse anualmente para su adecuación y extraordinariamente cuando ocurran situaciones especiales y/o cambios sustanciales en el SGSI.

Se desarrollará un documento que debe firmarse por la dirección del centro en el que se establecerán las políticas operativas de uso de los activos, los deberes de los usuarios con relación al SGSI, usos prohibidos e ilegales y consecuencias derivadas por el incumplimiento de las políticas y normas establecidas en dicho documento.

Actividad: Desarrollo del documento “Declaración de la aplicabilidad”.

La declaración de la aplicabilidad constituirá un documento en el que se debe recoger los controles que se aplicarán en la organización y cuáles no. Para aquellos que se apliquen, se deben incluir los objetivos del control, una breve descripción del mismo, la razón para su selección y la referencia del documento que establece las pautas para su implantación. En el caso de los controles no seleccionados, se deben indicar las razones de su exclusión.

Formará parte de las herramientas de control de utilidad para el grupo gestor de seguridad de la información y responsables del sistema de control interno de la organización.

El formato a tener en cuenta es el que se expresa en el anexo 3, en el mismo se recogen las siguientes informaciones:

- Sección: Se declara la sección y apartado de la norma que pertenece el control.
- Controles NC ISO/IEC 27001:2016: Se recoge cada uno de los controles declarados en el anexo A de la norma, y mostrando para cada uno una pequeña descripción de lo que constituyen cada uno.
- Exclusión(S/N): Se determina si el control será implementado o no en la organización.
- Justificación: Las razones para discernir si el control es aplicable o no, determinado los procesos, tecnologías y/o personas en donde se aplica.
- # de Acciones de control x año: Se declara el número de acciones de comprobación que se ejecutarán por año.
- Evidencia o registro de implementación: Describe el modo de implementar cada control; por ejemplo, haciendo referencia a un documento (política, procedimiento, instrucciones de trabajos, etc.) o detallando brevemente el procedimiento vigente o el equipo que se utiliza.

- Observaciones: Se detalla información adicional al control, en caso de que se requiera mejorar la comprensión del mismo.

Actividad: Desarrollo del “Plan de contingencias”

Se elabora el plan a través de procedimientos que indica una solución alternativa que permite renovar el funcionamiento de los servicios críticos de la organización ante la eventualidad que lo afecte de forma parcial o total

Para la elaboración del mismo se tendrá en cuenta: los nombres de los responsables de la contingencia y sus responsabilidades y el plan de recuperación de desastres. Las acciones a ser considerada serán antes, durante y después del desastre.

Quienes deberían participar:

- Grupo gestor designado para la seguridad de la información.
- Director(a) de la organización.

Resultado esperado:

- Documentos con las políticas de la seguridad de la información, objetivos, declaración de la aplicabilidad y plan de contingencias

Gestión de Documentos

La disponibilidad de toda esta documentación y registros es necesaria, para las personas autorizadas. Es conveniente, contar con un repositorio adecuado para preservar esta documentación, con un sistema de consulta y acceso, que permita gestionar roles, usuarios, permisos de acceso, tipos de acceso, auditoría, etc.

Etapa 4: Operación

Objetivo: Alcanzar personal capacitado en las técnicas y herramientas para la aplicación del sistema, así como implementar las particulares técnicas y operativas del diseño que se ha establecido.

Técnicas y/o herramientas de trabajo: - Mapas mentales y conceptuales - Trabajo en equipo
Entradas: - Estructura final del Sistema de gestión de seguridad de la información aplicando la NC ISO/IEC 27001:2016 - Objetivos y política, Procedimientos, Instrucciones técnicas, Registros y documentación del sistema de seguridad de la Información
Contextos de desarrollo: - Capacitaciones - Reuniones del grupo gestor

- Todas las áreas de la organización
Salidas: - Registro de capacitación en las técnicas y herramientas para la aplicación del sistema. - Personal capacitado. - Sistema implementado en la organización. - Registro de solicitud de cambios

Paso 8: Entrenamiento del cliente interno

Se debe comunicar a los trabajadores y autoridades competentes los resultados obtenidos a través de diferentes canales de comunicación. Debe comunicarse la política de seguridad de la información y los objetivos que se persiguen, el programa de entrenamiento del cliente interno y los resultados que se persiguen con su aplicación en el nuevo ciclo de implantación.

El segundo objetivo es la necesidad de educar e informar al personal desde su ingreso y de forma continua, cualquiera que sea la situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de sus expectativas depositadas en los materiales de seguridad y asuntos de confidencialidad. Es necesario reducir los riesgos que generan los errores humanos, la comisión de actos ilícitos, utilización inadecuada de instalaciones y recursos y manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

Es responsabilidad del área de recursos humanos, unido al responsable de la seguridad de la información, establecer las necesidades formativas relativas a la seguridad de la información.

Anualmente, deben verificarse las carencias que se observan en el personal o áreas o demandadas del propio personal y ser incluidas en el plan anual de capacitación de la organización.

La planificación de la formación quedará plasmada en el acta de revisión por la dirección, por parte del responsable del SGSI y que se aprobará por el CD, quien además dota de los recursos necesarios para su impartición.

Adicionalmente, el personal de la organización podrá recibir otras capacitaciones no planificadas durante la revisión por la dirección, por no ser necesarias en el momento de realización de la planificación.

El registro de capacitación debe incluir: objetivos de la capacitación para cada caso, recursos necesarios, el cronograma de ejecución y los roles y responsabilidades necesarios para la ejecución del plan.

<u>Quienes deberían participar:</u>

- Responsable del plan de capacitación. (Dpto.RRHH).

- Responsable de la seguridad de la información.
- Totalidad de los trabajadores.

Resultado esperado:

- Personal capacitado
- Registro de capacitación.

Paso 9: Implementación y monitoreo del sistema

El objetivo de esta etapa consiste en implementar las particulares técnicas y operativas del diseño que se ha establecido, de manera que se pueda identificar y aplicar de forma sistemática el plan global que se ha definido.

Es aquí donde se integran todos los elementos del diseño realizado, donde se ponen de manifiesto las virtudes y surgen las necesidades de cambio.

Es importante tener en cuenta las opiniones y comentarios de los trabajadores. En caso de detectar no conformidades, el grupo gestor debe de coordinar las acciones necesarias para revisar y aprobar los cambios que realmente son necesarios.

Los cambios generados deben notificarse a los trabajadores.

Se necesita realizar los ajustes necesarios y analizar las brechas para cumplir los objetivos trazados por el equipo y valorar la factibilidad del sistema. Se deben controlar los cambios para formalizarlos (registro de solicitud de cambios).

Etapa 5: Control

Objetivo: Realizar seguimiento para detectar acontecimientos que pongan en peligro la seguridad de la información en la organización y gestionar las incidencias registradas para determinar las acciones correctivas y preventivas necesarias.

Técnicas y/o herramientas de trabajo: - Técnicas establecidas en la declaración de la aplicabilidad - Trabajo en grupo
Entradas: - Plan de tratamiento del riesgo - Declaración de la aplicabilidad - Requisitos del SGSI - Requisitos legales de aplicación al SGSI - Requisitos de la NCISO 27001:2016. - Requisitos de los clientes documentados en contratos. - Gestión de No Conformidades, Acciones Correctivas y Preventivas. - Preliminar acta de revisión del sistema por la dirección. - Informe de auditorías internas

- Informe de no conformidad, acción correctiva y preventiva.
Contextos de desarrollo: - Todas las áreas de la organización - Sistema de control Interno de la organización
Salidas: - Informes de control - Informes de auditorías - Informe de gestión de no conformidades - Registro de acciones correctivas

Paso 10: Controles periódicos

Los responsables de los activos establecerán verificaciones periodicidad, para comprobar el estado del activo. Por su parte el responsable de la administración de la SI, deberá de monitorear con regularidad los activos, para conocer si el funcionamiento de los controles es el correcto, para ello, hará uso de cronogramas planificados. De acuerdo a los niveles que se alcanzaron en la evaluación del riesgo, se definirán la periodicidad de estos.

Las revisiones establecidas por el responsable de SI, tributarán a un informe de control, que al finalizar el mes, se entregará a la dirección, donde se plasmarán las acciones de control llevadas a cabo y los resultados de las mismas.

Recomendaciones para los controles:

- Mantenerse actualizado en materia de vulnerabilidad, a partir de la subscripción a boletines empresariales de seguridad.
- Mantener control de las actualizaciones de las protecciones implementadas.
- De existir modificaciones en los activos de información, hay que reevaluar el sistema.
- Establecer controles sorpresivos en las áreas de la organización, para evaluar comportamiento de los responsables de los activos.
- Desarrollar preguntas sorpresivas al personal de la organización, para medir el nivel de conocimiento en material de la seguridad de la información.

Paso 11: Auditorías Internas

Las auditorías permiten determinar si el sistema está adecuadamente implantado y se mantiene de acuerdo a los requisitos de las NC/IEC 27001:2016. A continuación se despliega el procedimiento para planificar y llevar a cabo las auditorías internas del SGSI que da solución a la gestión eficaz de auditoría en seguridad.

Selección de auditores

El personal que realice actividades de auditoría interna, sea de origen interno o externo, deberá tener conocimiento sobre la auditoria, no pertenecer al área auditada, conocimiento específico de la organización y delos servicios que se ofrecen (como mínimo, tres meses en un puesto de trabajo en la organización), conocimiento y experiencia en la aplicación e interpretación de la NC ISO/IEC 27001:2016 (mínimo 20 horas), tener formación, bien por experiencia bien por asistencia a capacitaciones, sobre el desarrollo de técnicas de auditoría (mínimo 20 horas), y haber participado en al menos tres auditorías como observador.

En el caso de que se contrate a un auditor externo para la realización de una auditoría interna, se solicitará los documentos acreditativos que evidencien el cumplimiento de los requisitos que se definieron con anterioridad.

Planificación de las auditorías internas

El responsable de la seguridad de la información dejará constancia del plan previsto de auditorías internas en el acta de revisión por la dirección, que se revisará y aprobará por el CD. En dicho plan deberá recogerse la realización de al menos una auditoria al año.

Para la realización de la planificación de auditorías se seguirán los siguientes criterios:

- Importancia de la actividad auditada.
- Resultados de auditorías internas o externas anteriores.

Estos criterios permiten realizar una planificación de auditorías, definir el alcance y la frecuencia, acordes a las necesidades de mejora del sistema.

Preparación de auditorías internas

Cuando se acerque la fecha aproximada de realización de la auditoria, el responsable de la seguridad de la información debe informar a las áreas afectadas de la realización de la auditoria con al menos una semana de antelación.

Si el auditor es externo a la organización podrá utilizar sus propios formatos pero deberá seguir esta metodología.

Ejecución de las auditorías internas

La ejecución de la auditoria se desarrolla con el fin de verificar el cumplimiento de lo que se establece en el alcance de la auditoria de manera que asegure que las distintas áreas cumplen con lo que se determina en el SGSI.

Para realizar las auditorias se tendrán en cuenta los requisitos del SGSI, requisitos legales de aplicación al SGSI, requisitos de ISO 27001, requisitos de los clientes documentados en contratos, gestión de no conformidades, acciones correctivas y preventivas, acta de revisión del sistema por la dirección, informe de auditorías internas, informe de no conformidad, acción correctiva y preventiva.

Durante la realización de la auditoria, los auditores dejan constancia de los todas las observaciones y desviaciones detectadas en el funcionamiento del SGSI, y reflejan la perfecta trazabilidad de las mismas a través de las distintas evidencias objetivas que las sustentan.
Los auditores realizan la auditoria a través de entrevistas, examinan documentos y observan actividades y situaciones en las áreas.

Informe de auditorías internas y seguimiento de las acciones correctivas

A partir de todas las desviaciones detectadas en la ejecución de la auditoria, el auditor elaborará el informe de auditoría interna, donde dejará constancia de las observaciones y comentarios de los hallazgos que se encuentren (anexo 8).
El responsable de SGSI, conjuntamente con los responsables de las áreas, analiza los hallazgos y plantean soluciones a los mismos.
De cada desviación que requiera la apertura de una acción correctiva el responsable de la SI se abrirá un registro de no conformidad, acción correctiva y preventiva (anexo 9), y actúa de acuerdo con lo que establece el procedimiento “Gestión de no conformidades, acciones correctivas y preventivas”.
El responsable de la SI se responsabiliza del seguimiento y cierre de las acciones correctivas abiertas como consecuencia de la auditoría interna.
Tanto el informe de auditoría interna como los informes de acción correctiva son entradas de la reunión de revisión por la dirección del SGSI. En la anexo 7 se presenta el diagrama de flujo a tener en cuenta.

Paso 12: Gestión de no conformidades, Acciones correctivas necesarias

La detección de no conformidades, y ejecución de acciones correctivas puede surgir como resultado de: la prestación de un servicio, quejas y reclamaciones de clientes, desviaciones relativas al sistema de seguridad, detectadas durante su aplicación, incidentes de seguridad, auditorías internas o externa, supervisiones o controles que fueron realizados, etc.

Gestión de apertura de un informe de no conformidad y acción correctiva

Cualquier trabajador de la organización que detecte no conformidades que se produzcan durante el desarrollo de las actividades debe informar al responsable del SGSI, de tal circunstancia.
Asociado a la apertura de una no conformidad, siempre irá la gestión de una acción correctiva, es decir, la solución a implantar para resolver una no conformidad, estará compuesta de dos partes:

- Resolución del problema, solución inmediata y aplicación de acciones para evitar que dicho problema vuelva a repetirse, acción correctiva.

Las no conformidades se evaluarán como “leves” o “graves”:

Se consideran “leves” aquellas no conformidades que cumplan cualquiera de estos dos requisitos:

- Sean detectadas por el equipo gestor del SGSI o personal de la organización y se puedan solucionar a través de disposiciones inmediatas que eliminen el problema puntual.
- Sea detectada por un auditor interno, bien como observaciones.

Se consideran “graves” aquellas no conformidades que cumplan cualquiera de estos dos requisitos:

- Aquellas que, para su resolución, necesiten la apertura de la acción correctiva correspondiente.
- Detectadas por un auditor interno o externo y que se presenten en el informe de auditoría como incidencias. El responsable designado en cada caso para la ejecución de la disposición inmediata o de la acción correctiva, realizará las actividades definidas, quienes entregan el impreso No conformidad / Reclamación / Acción correctiva al responsable del SGSI (Anexo 9)

El responsable del SGSI, registra las no conformidades que se produzcan en el informe de No conformidad / Reclamación / Acción correctiva. (anexo 9)

Seguimiento y cierre de un informe de no conformidad y acción correctiva.

Los implicados asignados por el responsable del SGSI, para implementar las decisiones adoptadas para solucionar una no conformidad, una vez implantadas dichas acciones se comunican el resultado al equipo gestor.

El responsable del SGSI se encarga de realizar el seguimiento de la eficacia de dicha implementación, y verificará: la no conformidad fue solucionada eficazmente, la implementación de las acciones correctiva para evitar que dicha situación vuelva a repetirse, y las no conformidad detectadas, luego de un tiempo, no han vuelto a reproducirse.

Para ello, en la casilla de “Evaluación de la eficacia de las acciones correctivas y/o preventivas tomadas y cierre de las no conformidades”, del informe de no conformidad, y acción correctiva, el responsable del SGSI registrará cualquier observación que considere oportuna.

Una vez implementada la solución y comprobada su eficacia, de acuerdo a lo descrito anteriormente, el responsable del SGSI cierra el informe de no conformidad, y acción correctiva firmándolo y anotará la fecha de cierre.

El responsable del SGSI recopilará todas las no conformidades abiertas, reclamaciones recibidas, y acciones correctivas que estén cerradas o continúen abiertas (anexo 10), lo que constituirá un elemento de entrada para la revisión por la dirección.

Etapa 6: Mejora

Objetivo: Seguimiento del SGSI a través de a la revisión por la dirección de la organización e implementar acciones que permitan asegurar el perfeccionamiento continuo del sistema.

Técnicas y/o herramientas de trabajo: - Trabajo en grupo
Entradas: - Informe de controles periódicos - Informe de auditorías - Informes de gestión de no conformidades
Contextos de desarrollo: - Reuniones del CD
Salidas: - Informe de revisión por la dirección - Acciones de mejora

Paso 13: Revisiones por la dirección

La dirección tiene que revisar el SGSI de la organización, establecer una planificación ordenada de las mismas. Para su correcto funcionamiento, deben de realizarse al menos una vez al año y siempre después de que todas las áreas y procesos de la organización hayan sido auditadas.

La dirección, para llevar a cabo la revisión del sistema, recopila toda la información necesaria que le facilita el responsable de seguridad de la información. El informe debe presentar una escritura clara y concisa. Se recomienda el uso de gráficos para mejorar la comprensión del mismo.

Los puntos a tener en cuenta en el informe son:

1. Resultados de acuerdos tomados en revisiones realizadas por la dirección en años anteriores.
2. Resultados de las auditorías.
   2.1 Auditorías Internas.
   2.2 Auditorías Externas.
   2.3 Controles periódicos.
3. Incidencias detectadas por clientes.
   3.1 Satisfacción a nivel institucional.
   3.2 Peticiones, quejas, reclamos, sugerencias y felicitaciones.
4. Cumplimiento de los requisitos legales y otros requisitos.
5. El estado de las acciones correctivas, acciones preventivas y notas de mejora.
6. Las acciones de seguimiento de revisiones previas efectuadas por la dirección.

7. Resultados de la gestión realizada sobre los riesgos identificados, los cuales deben estar actualizados.
8. Oportunidades de mejora.

A partir de los datos anteriores, la dirección verifica que el sistema es eficaz y que se obtienen los resultados que confirman el cumplimiento de la política y objetivos que se plantearon. Así mismo, se determina si el mismo está de acuerdo con los requisitos de la NC ISO/IEC 27001:2016.

Durante la revisión por la dirección, se analiza el estado de ejecución de las auditorías planificadas para el año en curso y se planifica el programa para el siguiente año y se dejará evidencia de ello.

En el caso de que se produzcan cambios importantes en la organización, los procesos o en la política, se realizarán revisiones del sistema extraordinarias.

Los resultados que se obtienen en la revisión por la dirección deben incluir las decisiones tomadas referidas a la mejora de la eficacia del sistema de gestión y de los controles y procesos de seguridad de la información, las oportunidades de mejora continua, las necesidades de cambio en la gestión del SGSI.

Estos resultados se reflejan en el registro acta de revisión por la dirección (anexo 11), y si procede, éstos se comunicarán por el responsable de seguridad de la información, al resto del personal de la organización.

Los asistentes a estas revisiones por la dirección son:

- Dirección.
- Equipo gestor de la seguridad de la información.
- Personal de otras áreas que la dirección estime oportuno.

Paso 14: Acciones de mejora

Las mejoras deben estar determinadas en consecuencia de la implementación de la política de seguridad de la información, los objetivos de la seguridad de la información, los resultados que se obtuvieron tras la realización de la auditoría, análisis de los eventos monitorizados, las acciones correctivas o preventivas, la gestión de revisiones o sugerencias emitidas (internas o externas) para el mismo se hará uso del formulario de sugerencias de mejora (anexo 12).

El responsable de seguridad de la información, unido a todo el equipo formula las propuestas de mejora que se conciliarán con la dirección de la organización. El plan debe compilar la totalidad de las acciones implicadas en la mejora continua (acción preventiva o correctiva, sugerencias), además otros datos que puedan ser de interés (ej. información sobre la descripción de la mejora,

responsables de ejecución, acciones de seguimiento). Debe permitir el control y seguimiento de las diferentes acciones a desarrollar.

Conclusiones del capítulo

Se logra diseñar un procedimiento para la implementación de un sistema de seguridad de la información como contribución a la gestión de la calidad de la información de los servicios de consultoría.

La propuesta del procedimiento tiene como objetivo encausar una adecuada gestión de la seguridad de la información a partir de la integración de modelos, normas, herramientas y buenas prácticas en la implementación de un SGSI, que se alinee con la NC ISO/IEC 27001:2016.

El procedimiento transcurre por 14 pasos, que se despliegan en 6 etapas: Compromiso y Preparación, Diagnóstico, Diseño y Documentación, Operación, Control y Mejora.

Las características del procedimiento permiten que sea aplicable a organizaciones de cualquier sector empresarial.

CAPITULO III. APLICACIÓN PARCIAL DEL PROCEDIMIENTO PARA IMPLEMENTAR UN SGSI COMO CONTRIBUCIÓN A LA CALIDAD DE LA INFORMACIÓN DE LOS SERVICIOS DE CONSULTORÍA

En el capítulo se recoge el resultado de la aplicación parcial del procedimiento propuesto en la organización objeto de estudio.

Etapa 1: Compromiso y Preparación

Paso 1: Compromiso de la dirección e involucramiento de los trabajadores

El primer paso en esta etapa fue la búsqueda de referencias bibliográficas que permitió la actualización de la información en relación a la seguridad de la información. Para ello se consultaron artículos de bases de datos Redalyc, Google Scholar, Dialnet, ScienceDirect y Elsevier, así como metodologías afines al objeto de investigación.

En reunión con el consejo de dirección se presentó el material didáctico con los resultados obtenidos de la investigación, donde se emitieron las principales conceptualizaciones para mejor entendimiento de la actividad. Se comunicó a los presentes el procedimiento y los objetivos que el mismo persigue. En la misma aprobó los pasos a seguir a través de la creación de un plan de actividades.

Se formuló el compromiso de seguridad de la información y se manifestó a través de la firma del acta la voluntad del consejo de dirección en el cumplimiento de sus funciones y responsabilidades sobre la seguridad de la información

Para lograr el involucramiento de los trabajadores, se efectuaron 2 encuentros. El primero fue auspiciado por el consejo de dirección, quién brindó las intenciones de implementación del sistema. Se efectúo una capacitación con los conceptos y virtudes de implementar el SGSI en la organización. En el segundo encuentro se dio a conocer el cronograma planificado, y las responsabilidades de cada trabajador para el desarrollo del mismo. Se desarrolló una tormenta de ideas, sobre las mejores prácticas para alcanzar una eficaz implementación. En el debate se recogieron no conformidades que tributaron al diagnóstico de la organización.

Paso 2: Creación del grupo gestor

En reunión efectuada en el consejo de dirección se formularon las propuestas para la conformación del grupo gestor. El mismo quedó presidido por la responsable de la seguridad informática. La integraron además el administrador de la red, como encargado de los servicios técnicos, el responsable del proceso de gestión de las TIC, el especialista de capacitación, especialista del control interno y especialista principal de operaciones, siendo la misma integrante del consejo de dirección.

Una vez seleccionados los integrantes se les impartió un taller sobre técnicas y herramientas útiles para que puedan ejecutar el diagnóstico, además se les instruyó en diferentes técnicas de trabajo en grupo para la solución de problemas.

Etapa 2: Diagnóstico

Paso 3: Comprender la organización y su contexto

Para la realización de este paso se recogieron evidencias documentales, se realizaron entrevistas y se examinaron los documentos establecidos para la realización de los procesos, y se comprobaron las actividades y condiciones en las áreas de interés. Además se revisaron los resultados de las auditorías e inspecciones anteriores, prestando especial atención a las deficiencias detectadas. A continuación se realiza un compendio del diagnóstico realizado.

El Ciget de Holguín perteneciente al Instituto de Información científica y tecnológica (IDICT) del Ministerio de Ciencia Tecnología y Medio Ambiente tiene como Misión: Ofrecer productos y servicios de información científico-tecnológica, desarrollo profesional y consultorías integrales orientados a satisfacer las necesidades de nuestros clientes y en apoyo a la toma de decisión y la innovación, con profesionales competentes y comprometidos y como Visión: Somos en Cuba la organización de Ciencia Tecnología e Innovación, líder en productos y servicios de información integrales, que facilitan el desempeño productivo y competitivo de los clientes.

Para dar cumplimiento a esta misión y visión, el centro se ha trazado como objetivos estratégicos a nivel vertical los siguientes:

1. Innovar como sistema.
2. Gestionar las competencias dinámicas de aprendizaje y compromiso de las personas.
3. Generar productos y servicios integrales, diversificados y diferenciados en función de las necesidades del cliente.
4. Perfeccionar la gestión de los procesos internos del sistema IDICT, según la 323.
5. Comercializar y exportar productos y servicios integrales.
6. Elevar los niveles de eficiencia para alcanzar un autofinanciamiento sostenible.

Económicamente es una organización que brinda servicios científicos técnicos de gestión de la información, gestión empresarial, propiedad intelectual e informática y su objeto social ha sido aprobado por Resolución No. 579/2013 del Ministerio de Economía y Planificación (MEP), de fecha 2013/10/22, que incluye los servicios tales como:

1. Brindar servicios de consultoría, asesoría, análisis y soluciones integrales en gestión de información, el conocimiento, la innovación, inteligencia empresarial y propiedad intelectual.
2. Prestar servicios de formación en temáticas asociadas a la gestión de información, del conocimiento, la innovación e inteligencia empresarial.

3. Ejecutar proyectos de investigación, desarrollo e innovación en materias afines a su actividad.
4. El centro cuenta con un mapa de procesos identificado por el sistema de gestión de la calidad y con el cual se ha logrado enfocar la integración de los sistemas a la gestión por procesos

Se cuenta con el 100% de las fichas de los procesos que responden al funcionamiento operacional de los mismos.

El Ciget se encuentra ubicado en un segundo piso, compartiendo área con centros productivos pertenecientes al CITMA.

Informáticamente cuenta con una estructura de estrella donde la conexión física existente entre los servidores, la red local y el proveedor de servicios de internet (CITMATEL) que se encarga de la parte de enlaces y conexiones hacia el exterior, dando soporte cuando existan problemas relacionados con redes. Se cuenta con una intranet corporativa, así como página web y cuenta en la red social facebook. Posee dominio .cu registrado y 3 sitios web con cara a internet.

Se encuentra vinculada a 3 proyectos institucionales que implican el trabajo en línea: Red CUBACIENCIA (Recolector y Directorio Nacional de Ciencia), administración y gestión editorial de la Enciclopedia Colaborativa Cubana en Red (EcuRed) y Observatorio Tecnológico.

Actualmente el Ciget cuenta con 34 máquinas, de las cuales 28 se encuentran en estado funcional, 5 estaciones de trabajo de las 28 existentes son utilizadas para prestar servicios en calidad de servidores no profesionales.

De una plantilla cubiertas de 40 trabajadores, se cuenta con acceso a internet y correo internacional 36 usuarios, 3 usuarios cuentan con acceso a internet desde sus locales de residencia a través del acceso conmutado previsto por el proveedor de servicios de red CITMATEL.

Se cuenta con personal capacitado para realizar las funciones y atribuciones que les corresponde según los cargos, entre ellos los especialistas en ciencias informáticas (4) específicamente son los que realizan un trabajo continuo en la implementación de nuevos servicios internos que contribuyen a mejorar el desempeño de los procesos así como el mejoramiento de servicios ya implementados y que requieren de modificaciones para un mejor uso y explotación. Por otro lado, se están realizando los procesos de capacitación y entrenamiento del personal, por medio de proveedores, principalmente la universidad de Holguín y se cuenta con 4 talleres planificados en el año para ser impartidos por los especialistas de informática de la organización.

Se cuenta con un plan de seguridad informática, el mismo presenta dificultades en relación a:

1. El PSI no se encuentra elaborado por la última metodología del Ministerio de Comunicaciones necesita por tanto la estructuración correcta.
2. El alcance del PSI es muy extenso incluyen temas innecesarios, como parte de la caracterización de la red; la metodología nueva establece que el alcance solo expresará el radio de acción que abarca el plan, de acuerdo al sistema informático objeto de protección, para el cual fueron determinados los riesgos y diseñado el SGSI.
3. La caracterización del sistema informático comienza por la ubicación del Ciget siendo esta información en realidad el alcance de dicho PSI.
4. Las políticas en sentido general deben ser reestructuras porque son normativas que establece las normas generales que debe cumplir el personal que labora en el sistema informático, estas políticas comprenden toda la organización y es obligatorio su cumplimiento, estas medidas serán los suficientemente generales y flexibles.
5. El acápite de las responsabilidades no delimita las mismas, carece del nombramiento del máximo responsable de seguridad informática de la institución que es el director general con su nombramiento y no refleja además los nombramientos del administrador de redes y del especialista de seguridad informática.
6. Contiene anexos innecesarios y no aparecen los usuarios con alcance a redes globales.

Se cuenta con una estructura documental vinculada con la actividad informática. Los procedimientos se encuentran internos en el manual, los cuales su estructura es a partir de que se debe hacer, pero no como, además de no contar con las operaciones técnicas, en el caso de los que lo requieren, siendo pocos explicativos.

Existe un sistema de gestión de archivos. La seguridad está deteriorada, al ser resguardado en un archivo central que incumple los parámetros de seguridad (tipo de archivo, localización, niveles de acceso, medios de protección ante desastres naturales)

Se planifica a nivel de institución un presupuesto anual destinado a la ejecución de los proyectos de I+D+I, y a la adquisición de equipamiento tecnológico, mantenimiento y reparaciones de los equipos existente, aunque resulta insuficiente debido al déficit existente en el centro y la obsolescencia de los mismos.

Presenta equipamiento tecnológico obsoleto, lo que impide la creación de nuevos servicios mejorados informáticamente para satisfacer las necesidades de los clientes.

Reducción considerable de estaciones de trabajo para los procesos productivos (PC e impresoras), estratégicos y de apoyo.

Lentitud en la conexión a internet, lo que afecta directamente la calidad y eficiencia de los resultados planificados por proyectos.

Uso de servidores no profesionales para la administración de la red del centro, lo que afecta en gran medida la calidad de los servicios internos y externos.

Las estaciones de trabajo funcionan bajo la distribución del sistema operativo Windows, siendo este de origen privativo, aunque ya se han realizado algunas acciones para la migración al software libre.

No existen procedimientos escritos para notificación y gestión de incidentes, en donde los problemas que ocurren son resueltos en el momento de ocurrir.

No existen documentos físicos o almacenados digitalmente de conocimiento general para los trabajadores que detallen normas y/o estándares de seguridad, la información es solo conocida por un número reducido de personas que inciden directamente en el control de la seguridad.

Los activos informáticos no cuentan con las condiciones adecuadas para su explotación

En las encuestas realizadas se logró alcanzar el 90 % de una plantilla cubierta de 40 trabajadores, en la figura 6 muestra representada gráficamente el comportamiento de las revelaciones encontradas:

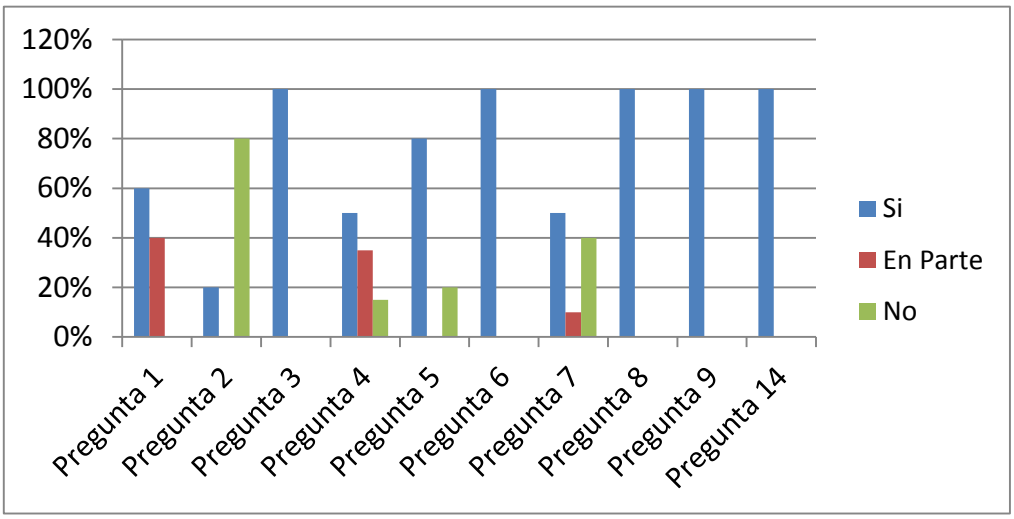


Figura 6. Representación del resultado de las encuestas diagnóstica sobre seguridad de la información a trabajadores de la organización

Con relación a la pregunta 1 el 58% de los trabajadores dieron si al conocimiento de las normas de seguridad de la información que tiene la organización. Siendo de importancia para el diagnóstico de la organización y alcanzar la validez de la misma, a través de la pregunta -¿Podría enunciar algunas de las normas de seguridad de la información que conoce?- se entrevistaron de forma aleatoria a 10 trabajadores, quienes centraron sus respuestas a los siguientes criterios:

- Las máquinas deben poseer antivirus
- Las contraseñas son personales

- No se puede acceder a los locales de los servidores de datos
- Debe existir un respaldo de información.
- La información que se comparte debe de ser confiable
- No se puede acceder a sitios que atenten contra la integridad y principios éticos de la organización.

Las respuestas expuestas denotan carencia de cultura en seguridad de la información presentando pocas formulaciones en relación a la fiabilidad, autenticidad e integridad de la información.

Solo el 22% creen que son suficientes las normas de seguridad de la información, queda evidente que los trabajadores abogan por la nueva incorporación de normas, donde en las recomendaciones que permita mejorar la seguridad de la información patentizaron que se hace necesario declarar otras en relación a la entrega de la información al clientes, que permita la seguridad de los datos; establecer un repositorio central de información para centralizar los materiales complementarios de los servicios, que permita mejorar el respaldo de la información y contar con materiales de consultas para futuros proyectos; desarrollar un directorio de normas y regulaciones para su consulta en cualquier momento.

A pesar de que el 100% de los trabajadores enuncian haber recibido capacitaciones, se cree que deban desarrollarse nuevas acciones que garanticen que los trabajadores conozcan conceptualizaciones sobre seguridad de la información.

Las preguntas 4 y 5 fueron validadas a partir de las recomendaciones efectuadas por los trabajadores.

Los incidentes relacionados con la seguridad de la información según los trabajadores están relacionados con: escasos recursos tecnológicos, duplicidad de la información en la red, poco espacio para el respaldo de los documentos o dificultad para la retroalimentación de los trabajos realizados.

En entrevista con el personal del área comercial, se evidenció que existe dificultad para el resguardo de los documentos. Presenta poca seguridad los contratos y fichas de clientes. En recomendaciones formuladas, se plantean la informatización del proceso comercial, unido a la gestión de proyectos, que permita la retroalimentación y disponibilidad de la información para todos los trabajadores implicados en la prestación de servicios, unido a la mejora de la confidencialidad de los mismos.

Un área de vital importancia y que maneja información sensible en la organización es el de propiedad intelectual, relacionado con la solicitud de búsqueda de patentes, búsqueda de interferencia, registro de invenciones, marcas, signos distintivos, derecho de autor. En entrevista

realizada se determinó que la información es manejada únicamente desde una pc, la seguridad de la misma no es suficiente según los datos que se manipulan, así como las salvas de información son realizados con una periodicidad anual. Tras recomendaciones de los integrantes del área se enunció, la creación de un sistema automatizado que permita agilizar la gestión de la información, que cuente con mecanismos para monitorear los datos, calendario de eventos, centralizar los datos en un servidor de mejor prestación y que permita el respaldo con periodicidad semanal.

En entrevistas a la directora de la organización la misma resaltó la importancia de informatizar los procesos de la organización, como medio para alcanzar mejor disponibilidad e integridad de los datos, así como mejorar los mecanismos de control existentes. A partir de las nuevas disponibilidad de acceso a internet, a través de la incorporación de una red wifi dentro de las instalaciones, se hace necesario crear los mecanismos para el correcto uso de la misma, además de contar con un procedimiento para proveer acceso a través de los datos móviles a trabajadores cuyo vinculación con la información amerite su uso; para ello se deben aplicar políticas de seguridad.

Es notable enunciar que el 100% de los trabajadores comparten el criterio de que es importante que la organización deba implementar un SGSI.

Para el caso de las encuestas formuladas a clientes externos, se alcanzó a realizar 6 intervenciones, de las mismas todos los resultados fueron positivos;. A pesar de no poseer elementos desfavorables, se debe de continuar en la ejecución de las actividades para la mejora de la seguridad, si se conoce que las acciones están encaminadas a mejorar la percepción del cliente.

Se aplicó la guía de ciberseguridad, emitida por el Ministerio de Comunicación

Del total de los controles evaluados por la NC ISO/IEC 27001:2016, 110 aplican a la organización, 37 controles están sin implementar (33,6%), 26 controles están parcialmente implementados (23,6 %) y 47 controles están siendo ejecutados (42,7%). En la figura 7 se evidencia el nivel de cumplimiento en que se encuentra cada uno de los controles.

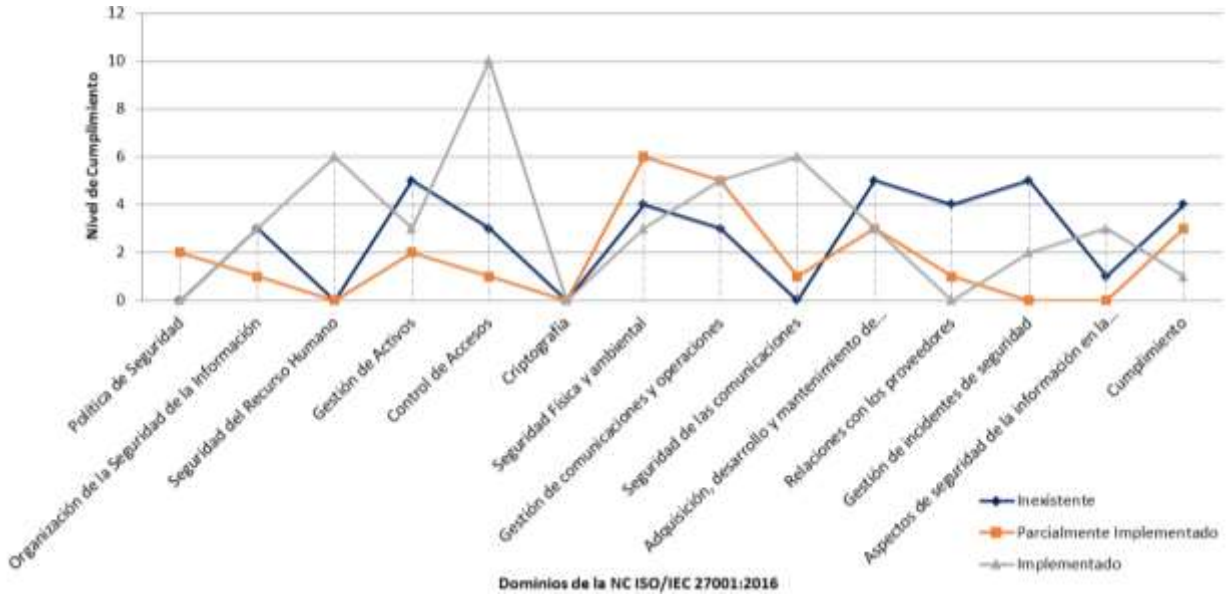


Figura 7. Nivel de cumplimiento según los dominios de la NC ISO/IEC 27001:2016 según los estados de Implementado, Parcialmente Implementado e Inexistente

En la figura 8, se encuentra el por ciento (%) de cumplimiento en que se encuentra cada uno de los controles que especifica la norma. Podemos ver que existen dominios sin ningún avance como el número diez, (10) que hace referencia a la criptografía y el quince (15) Relaciones con los proveedores.

También podemos observar los dominios que más % de cumplimiento poseen son el diez (10) Control de acceso, el siete (7) Seguridad de los recursos humanos, y el trece (13) Seguridad de las comunicaciones.

Finalmente, la gráfica de telaraña muestra una nueva visión del nivel de cumplimiento para cada uno de los dominios evaluados.

Figura 8. % de Cumplimiento general de los dominios de la NC ISO/IEC 27001:2016

Al revisar detalladamente el estado de cada dominio, se encuentra lo siguiente:

A.5. Política de Seguridad

El Ciget dispone de una política de seguridad pero solo sustenta los preceptos para las tecnología de la información y las comunicaciones, además no se presentan políticas para el soporte y gestión de riesgos introducidos por el uso de dispositivos móviles, teletrabajo, reglas para el uso aceptable de información, transferencia de medios físicos, criptografía, escritorio limpio y pantalla limpia, transferencia de información, desarrollo seguro y relaciones con proveedores. Además pero no tener definido los intervalos de tiempo para realizan revisiones periódicas de la misma.

A.6. Organización de la seguridad de la Información

Se evidencia el interés compromiso de la dirección de la organización a implantar el sistema de seguridad de la información alineadas a la NC ISO/IEC 27001:2016. Se debe ganar en establecer relaciones con grupos de interés especial y asociaciones profesionales especializadas en seguridad dentro y fuera del país. Se deben implementar acciones relacionados con los dispositivos móviles y teletrabajo.

A.7. Seguridad de Recurso Humano.

Se evidencia un nivel de implementación para los controles de este dominio, pero se debe continuar en el abordaje de la formación y ganar en conciencia sobre seguridad de la información.

A.8. Gestión de Activos

No existen evidencias documentales que corrobore una correcta gestión de los activos de información. No se encontró el inventario de los activos de información.

A.9. Control de Acceso

Se evidencia importantes avances en el cumplimiento de este dominio

A.10. Criptografía

No se presentan aspectos hasta la fecha que relacionen a la organización a hacer uso de este dominio.

A.11. Seguridad Física y Ambiental

La mayor cantidad de controles en este dominio se encuentran parcialmente implementados, se deben realizar las acciones que permitan lograr una implementación total de los mismos.

A.12. Seguridad de las Operaciones

En este dominio se detectó ausencia de documentación o falta de instrucción técnica que evidencie la implementación de la gestión de capacidades, separación de los ambientes de desarrollo, pruebas, y operación, gestión de cambios y controles para la instalación de software en sistemas operativos.

A.13. Seguridad de las Comunicaciones

En este dominio no se encontró evidencia documental sobre políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.

A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información

En entrevistas efectuadas se justificó que las actividades ejecutadas en la organización que guardan relación con algunos controles de este dominio, se realizaban empíricamente, sin hacer uso de métodos documentados para su desarrollo. Se hace necesario establecer y aplicar reglas para la seguridad en los procesos de desarrollo y soporte.

A.15. Relaciones con los Proveedores

En cuanto a este dominio, los controles se hallan de forma inexistente, se deben desarrollar acciones que permitan erradicar las deficiencias de este.

A.16. Gestión de Incidentes de la Seguridad de la Información

En cuanto a este dominio, los controles se encuentran de una forma inexistente y es en el que la entidad debe trabajar más fuerte para cumplir con el objetivo planteado.

A.17. Gestión de la Continuidad de Negocio

La implementación de una instalaciones de procesamiento de información, sustentada en una gestión eficaz de la seguridad que en este se maneja, garantizará la continuidad del negocio, aumentará la disponibilidad de la información y mitigará cuantiosos riesgos que se pueden presentar.

A.18 Cumplimiento

Se debe de trabajar en el cumplimiento de requisitos legales y contractuales y las revisiones de seguridad de la información cuando el sistema se encuentre implementado.

Paso 4: Elaboración y aprobación del informe de diagnóstico

Como resultado de esta fase se analizó toda la información recopilada en el diagnóstico realizado y se elaboró un informe final por parte del representante del equipo gestor. Fue analizado y presentado a los miembros del consejo de dirección, donde se trazaron las pautas a seguir, para la planificación del SGSI.

Etapa 3: Diseño y documentación

Paso 5: Inventario de activos de información

Se realizó un inventario de activos de todos los grupos de trabajo de la organización que están implicados en el alcance. Haciendo uso de la tabla representada en el anexo 2.

El número de activos de información para la organización fue de 144, los que fueron tomados en cuenta para el análisis de riesgos. Según la estructura organizativa por cada grupo de trabajo estos fueron de:

Grupo	**# de activos de información**
Dirección	25
Grupo Económico	18
Grupo Administrativo	17
Grupo de Recursos Humanos	20
Grupo de Operaciones	18
Grupo de Gestión del Conocimiento	13
Grupo de Servicios de Información	21
Grupo de Propiedad Intelectual	12

CONCLUSIONES GENERALES

Como resultado de la presente investigación pudo arribarse a las conclusiones generales siguientes:

El estudio del marco teórico práctico referencial, permitió comprender los enfoques de la seguridad de la información y su implicación con la calidad de los servicios, especificando el control de la misma, a través de un SGSI vinculado a la NC ISO/IEC 27001:2016, aspecto de importancia y actualidad en los escenarios actuales.

Se diseñó un procedimiento para implementar un SGSI como contribución a la calidad de la información en los servicios de consultoría, según los requisitos de la norma NC ISO/IEC 27001:2016, integrado al marco legal cubano, el cual propone el desarrollo de seis etapas importantes; compromiso y preparación, diagnóstico, diseño y documentación, operación, control y mejora.

La aplicación parcial del procedimiento en el Ciget de Holguín demuestra su viabilidad y utilidad práctica como un instrumento metodológico, facilitó elevar la cultura de gestión de seguridad por parte de los trabajadores y determinar nuevas competencias de formación de los mismos; re-definir los roles y responsabilidades de seguridad; evaluar la organización con relación a los requisitos de la NC ISO/IEC 27001:2016 y del marco regulatorio asociado y obtener un inventario total de los activos de información de la organización.

RECOMENDACIONES

Derivadas de la investigación efectuada, así como de las conclusiones antes expuestas, se formularon las recomendaciones siguientes:

1. Continuar la aplicación del procedimiento para el diseño e implantación del sistema de gestión de seguridad de la información hasta su fase final, de manera que se complete el ciclo de gestión y se logre la mejora de los resultados en la organización.
2. Divulgar los resultados de esta investigación para su posible generalización en otros Centros de Información y Gestión Tecnológica.
3. Emplear la presente investigación como material de consulta para estudios posteriores y potenciales servicios de consultorías.

BIBLIOGRAFÍA

Aguirre, J. D., & Aristizabal, C. (2013). Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la Ofrenda. Universidad Tecnologica de Pereira. Tesis para optar por el título de máster

Arias, A. (23 de 08 de 2018). Obtenido de http://www.sesquile-cundinamarca.gov.co

Ávila, J. (25 de 04 de 2013). *Innsz.* Obtenido de http://www.innsz.mx/opencms/contenido/investigacion/comiteInvestigacion/confidencialidadInformacion.html

Baca Flore, V. M. (2016). Diseño de un Sistema de Gestión de la Seguridad de la Información para la Unidad de Gestión Educativa Local Chiclayo.

Baldecchi Q., R. (2014). Implementación efectiva de un SGSI ISO 27001.

Barbosa Martins, A., & Saibel Santos, C. (2005). Uma metodologia para implantação de um sistema de gestão de segurança da informação.

Bartnes, M. (2015). Understanding information security incident management practices. A case study in the electric power industry. Norwegian University of Science and Technology.

Bauer, S., Bernroider, E., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security, 26*(2017), 145–159.

Bermúdez Molina, K. G., & Bailón Sánchez, E. (2015). Análisis en seguridad informática y seguridad de la información basado en las normas ICO/IEC 2017 dirigido a una empres de servicio financieros. Guayaquil, Ecuador: Universidad Politécnica Salesiana. Tesis de grado

Biblioguías - Biblioteca de la CEPAL. (2019). Obtenido de https://biblioguias.cepal.org/c.php?g=495473&p=4398114

Bolivar, Y. A. (2015). Diseño de un sistema de gestión de seguridad de la información en la intranet del policlínico del sur Olaya Bogotá, bajo la norma ISO 27001. Bogotá D.C., Colombia: Universidad Nacional Abierta y a distancia UNAD.

Buesaquillo, M., Lopez, D. N., & Garcia, A. F. (2017). iseño del sistema de gestion de seguridad de la informacion para una agencia de viajes y turismo. Colombia: Instituición Universitaria Politécnico Gran Colombiano. Tesis de grado

Buitrago, Bonilla & Murillo. (2012). Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información - SGSI, en el sector de Laboratorios de análisis microbiológicos, basado en ISO 27001. Bogotá: Universidad EAN.

Bustamante, G., & Osorio, J. A. (2014). Metodología de la seguridad de la información como medida de protección en pequeñas empresas. Cuaderno Activa, 6, 71-77. Resultado de investigación

Bustamante, F., Fuertes, W., Diaz, P., & Toulqueridis, T. (2017). Methodology for Management of Information Security in Industrial Control Systems: A Proof of Concept aligned with Enterprise Objectives. Advances in Science, Technology and Engineering Systems Journal, 88-99.

Castillo, A. (2017). *Cronica de seguridad.* Obtenido de https://cronicaseguridad.com

Carazo, O. (2013). Elaboración de un Plan de Seguridad de la Información. Tesis para optar por el título de máster

Cely, R. (2018). Diseño del sistema de gestión de seguridad de la información (SGSI) con base al modelo de seguridad y privacidad de la información según lineamentos del Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la estrategia GEL. Colombia: Universidad Nacional Abierta y a Distancia (UNAD). Especialización en seguridad informática

Chaparro. (2016). Elaboración de un plan de implementación de la ISO/IEC 27001:2013 para la unidad de GST (Gerencia de Servicios Tecnológicos). Catalunya, España: Universitat Oberta de Catalunya. Tesis para optar por el título de máster

Clastornik. (2017). 77ª edición de Segurinfo - Congreso y Feria Iberoamericana de Seguridad de la Información. *Conferencia de Apertura.*

CubaDefensa. (2014). Sitio institucional de las fuerzas armadas revolucionarias de la república de Cuba. Obtenido de http://www.cubadefensa.cu/?q=glosario/S

Cuervo, S. (2017). mplementación ISO 270001. Empresa Ficticia S.A. Tesis para optar por el título de máster

Dávila, L. (2003). Evaluación de la Calidad en Sistemas de Información en Internet. México: Centro de Investigación y de Estudios Avanzados del IPN.

Decreto ley 221 de los archivos de la república de Cuba. (s.f.).

División consultoría de EvaluandoSoftware.com. (2016, 09 26). EvaluandoSoftware. com. Seguridad de la información empresarial. Obtenido de https://www.evaluandosoftware.com/seguridad-la-informacion-empresarial/

Espinosa, J. G., García, R. S., & Giraldo, A. (2016). Sistema De Gestión De Seguridad De La Información Para Los Tres Procesos Misionales De La Corporación Autónoma Regional de Risaralda (CARDER). Colombia: Universidad Autónoma de Manizales. Tesis para optar por el título de máster

Espona, M. (2015). Calidad de Información: una nueva herramienta para la investigación.

Gallegos, F. P., & Murillo, M. F. (2015). Metodología de gestión de la información enfocado a las Industrias de Telecomunicaciones en el Ecuador. Ecuador: Escuela Politécnica Nacional. Tesis para optar por el título de máster

García, F., & García, A. (2018). *Ingeniería de software. Sistemas de Información.* España: Universidad de Salamanca.

Garrido, N. (2016). *ASIS.* Obtenido de https://www.asis.org.pe

Gorriti, I. (2015). Plan de Implementación de la ISO/IEC27001:2013. España.

Guevara Huilcarema, T. d. (s.f.). Modelo de Gestión de Seguridad de la información para la corporación financiera nacional basado en gestión de riesgos. Quito, Ecuador: Escuela Politécnica Nacional. Tesis para optar por el título de máster

Guzmán, G. (2015). Metodologóa para la seguridad de tecnologías de información y comunicaciones en la clínica Ortega. Perú: Universidad Nacional del Centro del Perú.

Hernández, G. (2014). *Sistemas de Información: Manual de planificación energética OLADE.* Quito, Ecuador: OLADE.

Hussain, F. (2017). Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science, 124*(2017), 691–697.

Imbaquingo, D. E., Pusdá, M. R., & Jácome, J. G. (2017). *Fundamentos de Auditoría Informática basada en riesgos.* Ibarra, Ecuador: UTM.

INCIBE. (2015). *INCIBE.* Obtenido de Sitio Web del Instituto Nacional de Ciberseguridad de España, S.A. https://www.incibe.es

INCIBE. (2017). *INCIBE.* Obtenido de Sitio Web del Instituto Nacional de Ciberseguridad de España, S.A. https://www.incibe.es

INCIBE. (2018). *INCIBE.* Protección de la información. Obtenido de Sitio Web del Instituto Nacional de Ciberseguridad de España, S.A. https://www.incibe.es

Jauregui, A. (2014). *Lifeder.* Recursos Materiales de Empresas: Administración y Clasificación. Obtenido de https://www.lifeder.com

Landázuri, M. C. (2017). Formulación de una propuesta para un modelo de sistema de gestión de seguridad de la información para empresas de la industria bancaria en el sector privado. Tesis para optar por el título de máster

Londoño Forero, J. A. (2014). *Seguridad Informática.* Calameo.

Lugones, E. (2013). Obtenido de https://www.gestiopolis.com/sistemas-informacion-implicacion-cuba/

Lozano, M. (2017). Diseño de un plan estratégico de seguridad de información para una compañía del sector asegurador. Colombia: Institución Universitaria Politécnico Grancolombiano. Tesis de grado

Luis, A. A. (2009). Guía de aplicación de la Norma UNE- ISO/IEC 27001 sobre seguridad en sistemas de información para Pymes. Génova, Madrid: AENOREdiciones.

Macen, C. D. (2014). Políticas de seguridad de la información. Asuncion, Paraguay: Universidad Tecnológica Intercontinental. Tesis para optar por el título de máster

Maravilhas, S. (2015). Encyclopedia ofInformation Science and Technology, Third Edition. En I. Q. Value.

Margaret. (2016). Obtenido de https://searchsecurity.techtarget.com/definition/information-security-infosec

Martins, J., & dos Santos, H. (2010). Methods of Organizational Information Security. *Springer*.

Medina, A. (2017). Implementación de un repositorio digital para el entorno local de la Facultad de Comunicación de la Universidad de la Habana. *Anales de Investigación, 13*(2), 202-214.

Merino, J., & Torres Asencios, E. (s.f.). Implementación de un modelo de la seguridad de la información basados en ITIL v3 para una Pyme de TI. (http://hdl.handle.net/10757/614076, Recopilador) Perú: Universidad Peruana de Ciencias Aplicadas (UPC).

Moreno, J. (2015). *A un clic de las tic.* Obtenido de https://aunclicdelastic.blogthinkbig.com/la-seguridad-pasa-porque-nos-concienciemos-de-su-importancia/

Muñoz, J. (2016). Diseño de políticas de seguridad informática para la dirección de tecnologías de la información y comunicación (DTIC) de la universidad de Cuenca. Cuenca, Ecuador: Universidad de Cuenca. Tesis para optar por el título de máster

Nakrem, A. (2007). Managing I nformation Security in Organizations. A Case Study. Agder University College – Spring.

Navarro, A., & Amilcar, J. (2007). Metodología para la gestión de seguridad de información en Venezuela. Venezuela. Tesis de grado

NC ISO/IEC 27000:2016. (2016). *Tecnologías de la Información -Técnicas de Seguridad -Seguridad de Gestión de Seguridad de la Información (SGSI)- Visión de Conjunto y Vocabulario*. Cuba: Oficina Nacional de Normalización.

NC ISO/IEC 27001:2016. (2016). *Tecnologías de la Información -Técnicas de Seguridad -Seguridad de Gestión de Seguridad de la Información (SGSI)- Requisitos*. Cuba: Oficina Nacional de Normalización.

NC ISO 31000:2018. (2018). *Gestión de Riesgos - Directrices*. Cuba: Oficina Nacional de Normalización.

Nor, A., Zaidi, H., & Hussin, N. (2018). Information Quality in Organization for Better Decision-Making. *International Journal of Academic Research in Business and Social Sciences, 7*(12).

Oscar, G. (2006). La Gobernabilidad de la Seguridad de la Información en el proceso de Gobierno Corporativo. El Salvador: USAL universidad del Salvador. Tesis para optar por el título de máster

Paillacho, S. (2015). Modelo de un proceso de la gestión del riesgo de la seguridad de la información en entidades gubernamentales. Ecuador: Escuela Politécnica Nacional.

Pallas, G. (2009). Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Uruguay: Universidad de la República Montevideo.

Pavlov, G., & Karakaneva, J. (2011). Information security management system in organization. *Trakia Journal of Sciences, 9*(4), 20-25.

Pavlov, G., & Karakaneva, J. (2011). Information Security Management System in Organization. *Trakia Journal of Sciences, 9*(4), 20-25.

Pérez, J., & Gardey, A. (2013). *Definicion.* Obtenido de https://definicion.de/confidencialidad

Phillips, G. (25 de 3 de 2013). *DARKReading.* Obtenido de http://www.darkreading.com/risk/mission-impossible-4-reasons-compliance-is-impossible/d/d-id/1139416?

Pulido, A., & Mantilla, J. (2016). *Modelo para la implementación del sistema general de seguridad informática y protocolos de seguridad informática en la oficina TIC de la alcaldía municipal de Fusagasugá, basados en la gestión del riesgo informático.*

Rayme , R. (2007). Gestión de seguridad de la información y los servicios críticos de las universidades. Lima, Perú: Universidad Nacional Mayor de San Marcos.

Resolución 60/11. (2011). *Normas del sistema de control interno*. Cuba: Contraloría General de la República.

Robles, & Rodríguez. (2006). La gestión de la seguridad en la empresa.

Rowley. (1998). Towards a Framework for Information Management. *International Journal of Information Management, 5*, 359-369.

Ríos, J. (2014). Diseño de un sistema de gestión de seguridad de información para una central privada de información de riesgos. Perú: Pontificia Universidad Católica del Perú. Tesis de grado

Said, R., Abdullah, H., Uli, J., & Abidin, Z. (2014). Relationship between Organizational Characteristics and Information Security Knowledge Management Implementation. *Procedia - Social and Behavioral Sciences, 123*(2014), 433 – 443.

Santofimio, Y. L., & Manrique, C. T. (2015). Técnicas de evaluación del riesgo para determinar la viabilidad del proyecto en la etapa de formulación. Santiago de Cali, Colombia: Universidad San Buenaventura Cali.

Solarte, F., Enriquez, E., & Benavides Ruano, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Colombia: Universidad Nacional Abierta y a Distancia (UNAD).

Spanevello, F. (2012). IQ: Calidad de la Información. *Revista de Publicaciones Navales*.

Suhail, & Quadri. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security, 07*(03), 185-194.

Talavera, V. (2015). Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013. Pontificia Universidad Católica del Perú.

Universidad de Veracruzana (2019). Sitio web de la universidad de Veracruzana. Información segura...¡Es cultura!. Obtenido de https://www.uv.mx/

Vilalta, & Espinosa. (2008). Metodología para el diagnóstico de la calidad de los datos. *Revista Ingeniería Industria, XXIX*(2), 1-6.

Villena, M. A. (2006). Sistema de gestión de seguridad de información para una institución financiera. Lima, Perú: Pontífica Universidad Católica del Perú. Tesis de grado

Wallin, E., & Xu, Y. (2008). Managing Information Security in Healthcare: A Case Study in Region Skåne. Suecia: Lund University. Tesis para optar por el título de máster

Woodman. (1985). Information management in large organizations. En *Information management from strategies to action* (págs. 95-114). London: ASLIB.

Xiaoxia, H. (2012). Designing of the Information Security Examination System. *IERI Procedia, 2*(2012), 721-726.

Anexos

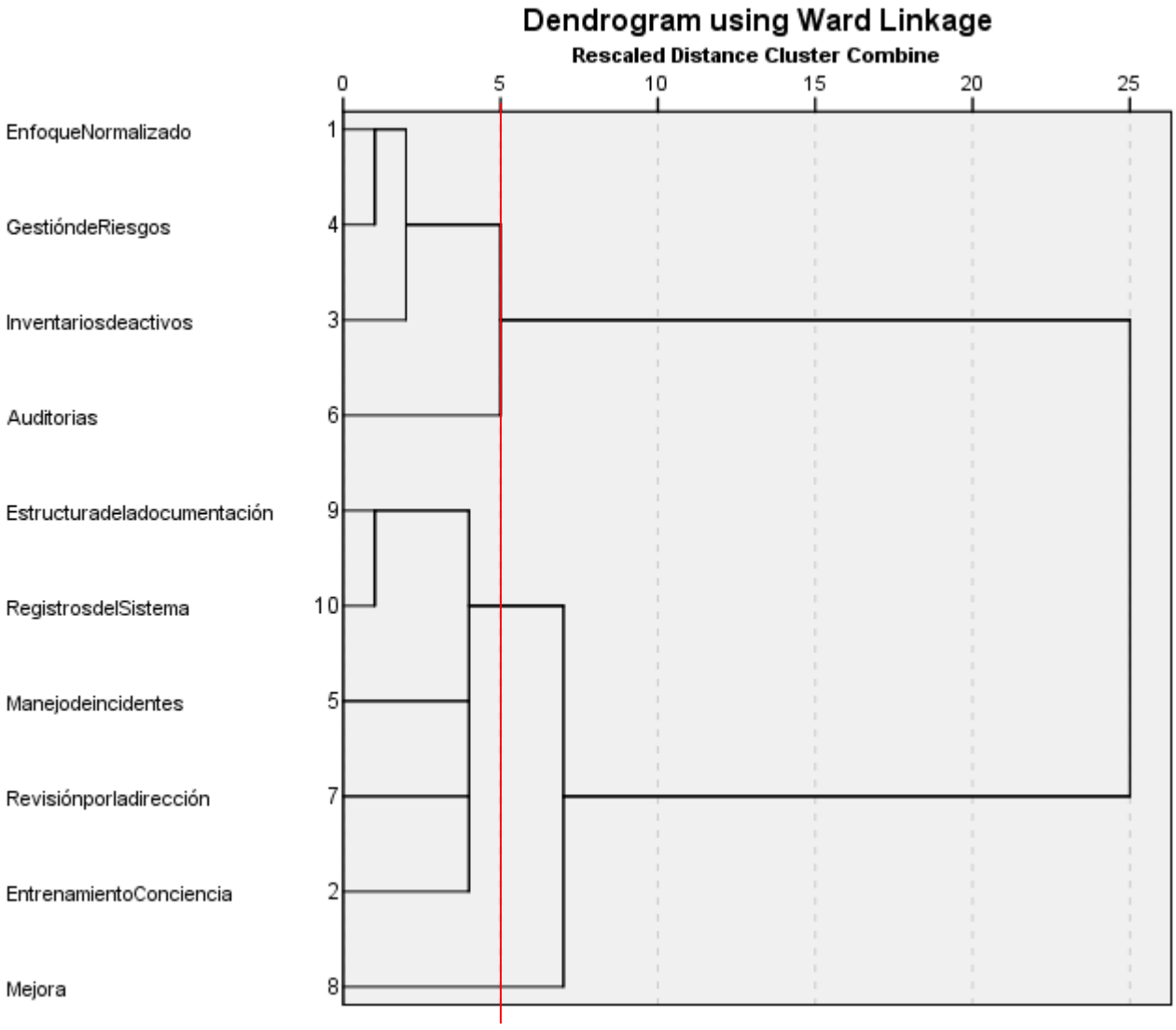
Anexo 1: Análisis de Investigaciones en relación variables estudiadas

No.	Autores(Año)	1	2	3	4	5	6	7	8	9	10
1	Barbosa(2005)	1	0	1	1	0	1	0	0	0	0
2	Cosachov(2006)	1	1	1	1	0	1	0	0	0	0
3	Villena(2006)	1	1	1	1	1	0	0	1	0	0
4	Nakrem(2007)	1	0	1	1	1	0	0	0	0	0
5	Navarro(2007)	1	0	1	1	0	0	0	0	0	0
6	Rayme(2007)	1	1	1	1	0	0	0	0	0	0
7	Andrés & Gómez(2009)	1	0	1	1	0	1	1	1	0	0
8	Pallas(2009)	1	1	1	1	1	1	1	1	1	1
9	Buitrago, Bonilla & Murillo(2012)	1	1	1	1	1	1	0	0	0	0
10	Aguirre & Aristizabal(2013)	1	0	1	1	0	1	0	0	0	0
11	Carazo(2013)	1	0	1	1	1	1	1	1	0	0
12	Guevara(2013)	1	1	1	1	1	1	1	0	1	1
13	Baldecchi(2014)	1	1	0	1	1	1	1	0	0	0
14	Bustamante & Osorio(2014)	1	0	0	1	0	1	1	0	0	0
15	Macen(2014)	1	1	1	1	0	0	0	0	0	0
16	Villena(2014)	1	0	1	1	0	0	0	0	0	0
17	Bermúdez & Bailón(2015)	1	0	1	1	0	1	0	1	0	0
18	Bolivar(2015)	1	0	1	1	0	1	0	1	0	0
19	Gorriti(2015)	1	0	0	1	0	1	0	0	1	0
20	Guzmán(2015)	1	1	1	1	1	1	1	1	0	0
21	Solarte, Enriquez & Benavides(2015)	1	0	1	1	0	1	1	1	0	0
22	Talavera(2015)	1	1	1	1	0	1	0	1	0	0
23	Baca(2016)	1	0	1	1	0	0	0	0	0	0
24	Chaparro(2016)	1	1	1	1	0	1	0	1	1	0
25	Espinosa, García & Giraldo(2016)	1	0	1	1	0	1	0	1	0	0
26	Merino & Torres(2017)	1	0	1	1	1	1	0	1	0	0
27	Muñoz(2017)	1	0	1	1	0	0	0	1	0	0
28	Buesaquillo, Lopez & Garcia (2017)	1	0	1	1	0	1	0	1	0	0
29	Bustamante, Fuertes, Diaz &Toulqueridis(2017)	1	0	1	1	0	1	0	0	0	0
30	Cuervo(2017)	1	0	1	1	0	1	1	0	1	0
31	Gallegos & Murillo(2017)	1	0	1	1	0	1	0	0	0	0
32	Landázuri(2017)	1	0	1	1	0	0	0	1	0	0
33	Lozano(2017)	1	1	1	1	0	1	1	1	0	0
34	Cely(2018)	1	0	0	0	1	1	0	0	0	0
35	Paillacho(2015)	0	0	1	1	0	1	1	1	1	0
36	Santofimio & Manrique(2015)	0	0	1	1	0	1	0	0	0	1
37	Tibaquira(2015)	0	0	1	1	0	0	0	0	0	0

38	Delvasto(2016)	0	0	1	1	1	0	0	1	0	1
39	Torres(2017)	0	0	1	1	1	1	0	0	0	0

Leyenda: 1-Enfoque Normalizado, 2-Entrenamiento/Conciencia, 3-Inventarios de activos, 4-Gestión de Riesgos,5-Manejo de incidentes, 6-Auditorias, 7-Revisión por la dirección, 8-Mejora, 9-Estructura de la documentación, 10-Registros del Sistema

Anexo1.1: Análisis clúster por variables relacionadas en los enfoques metodológicos



Anexo 2: Inventario de activos de información

INVENTARIO DE ACTIVOS DE INFORMACIÓN							
Id_ Activo (1)	Activo de Información (2)	Descripción (3)	Tipo(Digital o Físico) (4)	Contenedor (5)	Propietario (6)	Accesos (7)	Clasificación del Activo (8)

Leyenda:

(1) Consecutivo que identifica el activo de información que se asocia al proceso

(2) Nombre del activo de información que identifico el responsable del proceso

(3) Descripción del activo de información y su funcionalidad, dentro del proceso.

(4) Descripción del activo de información si es Digital o Físico

(5) Lugar(es), dispositivo(s) o medio(s), donde se encuentra la información

(6) Persona, encargada de controlar la creación, desarrollo, mantenimiento y uso de los activos, además de rendir cuentas.

(7) Área, persona, organización o proceso que hace uso de los activos de información.

(8) Clasificación de la información (Secreta, Confidencial, Uso interno, Pública) a la que corresponde el activo que se identificó.

Anexo 3: Declaración de aplicabilidad

La presente declaración describe los controles relevantes y aplicables al alcance del SGSI de la organización *para implementar las opciones de tratamiento de riesgos.* La misma se fundamenta en los controles de la ISO/IEC 27002 según la relación del Anexo A de la NC ISO/IEC 27001:2016.

Fecha de elaboración: Día / Mes / Año

Sección	Controles ISO 27001:2016		Exclusión (S/N)	Justificación	# de Acciones de control x año	Evidencia o registro de implementación	Observaciones
	Objetivo	Descripción					

Anexo 4: Control de documentos de origen externo

Nombre y/o identificación del documento	Procedencia	Formato	Fecha de Entrada	Responsable de control y distribución	Ubicación	Personal con acceso al documento

Anexo 5: Metodologías de análisis de riesgos

METODOLOGÍA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
OCTAVE	Pymes, organizaciones públicas y privadas	Se puede desarrollar por empleados de la misma organización, utilizando un equipo multidisciplinario. Involucra a todo el personal. Construcción de los perfiles de amenazas basados en activos. Identificación de la infraestructura de vulnerabilidades. Desarrollo de planes y estrategias de seguridad. Comprende las etapas de análisis y gestión de riesgos. Involucra procesos, activos, dependencias, recursos, vulnerabilidades, amenazas y salvaguardas. Relaciona amenazas y vulnerabilidades. Uso interno: gratuito. Posee tres métodos Octave, Octave-s y Octave allegro, adaptables a una organización.	No tiene en cuenta el principio de no repudio de la información. Utiliza muchos documentos en el proceso de análisis de riesgos. Se requiere de amplios conocimientos técnicos. No define claramente los activos de información. Uso externo: se debe comprar la licencia al SEI si se quiere implementar la metodología a un tercero.
MAGERIT	Gobierno, compañías grandes comerciales y no comerciales, Pymes.	Alcance completo en el análisis y gestión de riesgos. Está bien documentada en cuanto a recursos de información, amenazas y tipos de activos. Utiliza un completo análisis de riesgo cuantitativo y cualitativo. Es libre y no requiere autorización para su uso. Divide los activos de la organización en diferentes grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier riesgo. Se centra en tres objetivos: concientizar sobre la existencia de los riesgos y de la necesidad de atajarlos a tiempo, ofrecer un método sistemático para analizar tales riesgos, ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación. Permite que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión de riegos efectiva. Posee una buena base documental en tres libros: El método, Catálogo de elementos y Guía de técnicas, que son de acceso público. Posee herramientas para el análisis de riesgo como PILAR.	En su modelo no involucra los procesos, recursos, ni vulnerabilidades. Posee falencias en el inventario de políticas. Se considera una metodología costosa en su aplicación.
MEHARI	Gobierno, organismos, empresas grandes	Para su análisis de riesgos utiliza un modelo cuantitativo y cualitativo. Es un método capaz de evaluar y lograr la disminución de	Se enfoca solo en los principios de integridad,

	y medianas, compañías comerciales sin ánimo de lucro (educación, salud, servicios públicos, organizaciones privadas).	riesgos en función del tipo de organización. Posee bases de datos de conocimientos con manuales, guías y herramientas que permiten realizar el análisis de riesgos cuando sea necesario. Complementa y se acopla a las necesidades de la norma ISO 27001, 27002 y 27005 para definir los SGSI y la gestión de riesgos. Por medio de esta metodología se detectan vulnerabilidades mediante auditorías y se analizan las situaciones de riesgo. Combina análisis y evaluación de riesgos; particularmente, se especifica un módulo de evaluación rápida y uno de evaluación detallada.	confidencialidad y disponibilidad, olvidando el no repudio. La recomendación de los controles no se incluye dentro del análisis sino dentro de la gestión de los riesgos. El impacto de los riesgos se estima en el proceso de gestión y evaluación.
NIST SP 800 - 30	Utilizada por organizaciones gubernamentales y no gubernamentales.	Bajo costo relacionado con el riesgo analizado y solventado. Proporciona una guía para evaluación de riesgos de seguridad en las infraestructuras de TI. Presenta un resumen de los elementos clave de las pruebas de seguridad técnica y la evaluación con énfasis en técnicas específicas, sus beneficios, limitaciones y recomendaciones para su uso. La guía provee herramientas para la valoración y mitigación de riesgos. Asegura los sistemas informáticos que almacenan, procesan y transmiten información. Mejora la administración a partir de los resultados del análisis de riesgos. Se aplica en el análisis y la gestión de los riesgos.	En su modelo no tiene contemplados elementos como los procesos, los activos ni las dependencias.
CORAS	Utilizada por organizaciones gubernamentales y no gubernamentales.	Posee diferentes herramientas de apoyo para el análisis de riesgos, un editor gráfico para soportar la elaboración de los modelos basado en Microsoft Visio y utiliza lenguaje grafico basado en UML (Unified Modelling Language). Provee un repositorio de paquetes de experiencias reutilizables. Provee un reporte de las vulnerabilidades encontradas. Útil en el desarrollo y mantenimiento de nuevos sistemas. Basada en modelos de riesgos de sistemas de seguridad críticos.	No realiza análisis de riesgos cuantitativo. En su modelo no tiene contemplados elementos como los procesos y las dependencias.
CRAMM	Organizaciones públicas y privadas.	Aplica los conceptos de manera formal, estructurada y disciplinada protegiendo los principios de seguridad y sus activos. Realiza un análisis de riesgos cualitativo y cuantitativo. Es aplicable a todo tipo de sistemas y redes de información y se puede utilizar en todas las etapas del ciclo de vida del sistema de información desde la planificación y viabilidad, por medio del desarrollo e implementación del mismo. Se puede usar siempre que sea necesario para identificar la seguridad y/o requisitos de contingencia para un sistema de información o de la red. Identifica y clasifica los activos de TI. Evalúa el impacto empresarial. Identifica y evalúa amenazas y vulnerabilidades, evalúa	En su modelo no tiene con- templados elementos como los procesos y los recursos.

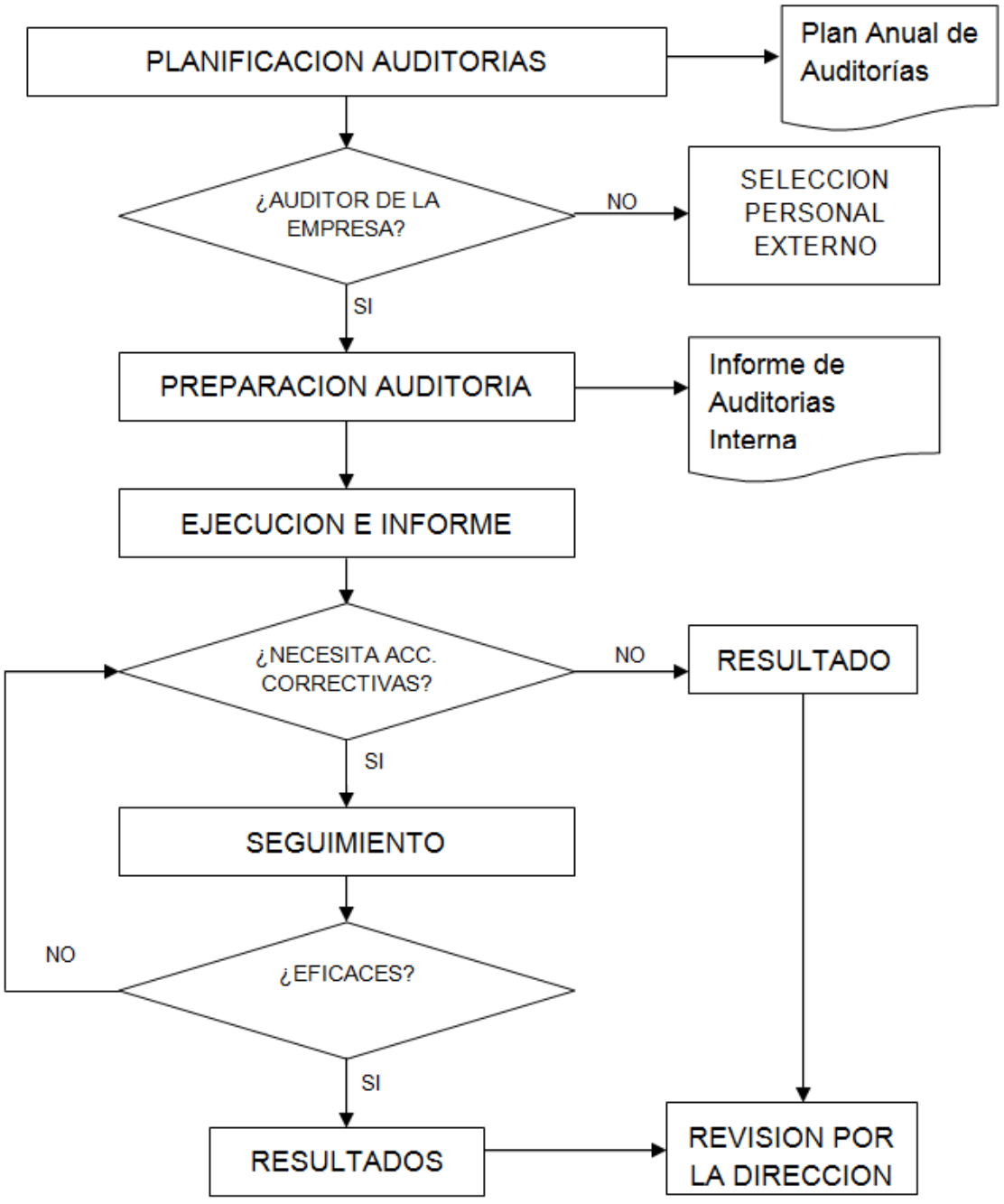
		niveles de riesgo e identifica los controles requeridos. Compuesta por más de 4.000 contramedidas reunidas en grupos y subgrupos con los mismos aspectos de seguridad, incluyendo activos de software, hardware y protecciones medioambientales. Combina análisis y evaluación de riesgos.	
NC-ISO 31000:2018 Gestión del riesgo. Directrices. NC-ISO /IEC 31010:2015 Gestión del riesgo. Técnicas de apreciación del riesgo.	Gobierno, organismos, empresas grandes y medianas, compañías comerciales sin ánimo de lucro (educación, salud, servicios públicos, organizaciones privadas).	Estructura las actividades para poner en marcha y mejorar continuamente los procesos de gestión de riesgos. Es parte de la organización y el liderazgo. Fundamental en la manera en que se gestiona la organización en todos sus niveles. Contribuye a la mejora de los sistemas de gestión. Es parte de todas las actividades de una organización e incluye la interacción con las partes interesadas. Considera el contexto externo e interno de una organización, incluido el comportamiento humano y los factores culturales. Se puede aplicar a cualquier tipo de riesgo, cualquiera que sea su naturaleza, y tanto si sus consecuencias son positivas o negativas.	

Fuente: Metodologías para el análisis de riesgos en los SGSI, Helena Alemán Novoa, Claudia Rodríguez Barrera, 22/06/2014, Revista especializada en Ingeniería

Anexo 6: Plan de tratamiento de riesgos

#	ACTIVIDADES	FECHA DE TERMINACIÓN PLANIFICADA	RECURSOS	RESPONSABLE	FECHA DE TERMINACIÓN	OBSERVACIONES

Anexo 7: Diagrama de flujo del proceso de auditoría interna



Anexo 8: Informe de auditoría

Auditoría No.:	**Fecha de ejecución:** *(inicio-final)*
Auditado:	
Auditor Líder:	
Equipo Auditor:	
Objetivo: *(Definición del objetivo de la auditoría)*	
Alcance: *(Definición de los procesos, áreas o actividades que serán auditados)*	

EVALUACIÓN DE LOS RESULTADOS

Fechas y los lugares donde se realizaron las actividades de auditoría

Criterios de auditoría

Hallazgos de la auditoría

Conclusiones (dar a conocer los resultados obtenidos en el proceso de auditoría, especificando cómo el auditado cumple con los criterios de auditoría previamente definidos (grado de cumplimiento) y cuántas no conformidades se detectaron por áreas o procesos).

Recomendaciones para la mejora (proponer acciones para mejorar el sistema de gestión auditado).

Propuesta de auditoría de seguimiento (de ser necesario la realización de auditorías de seguimiento especificar: fecha, áreas o procesos implicados, requisitos a reevaluar, responsables de eliminar las no conformidades detectadas y recursos necesarios para la r**MIC**ealización de la misma).

Elaborado por: (Nombre y apellidos del auditor líder)	**Firma:**	**Fecha:**
Aprobado por: (Nombre y apellidos del director general)	**Firma:**	**Fecha:**

Anexo 9: Registro de No conformidad / Reclamación / Acción correctiva

CIGET - Holguín IDICT INSTITUTO DE INFORMACIÓN CIENTÍFICA Y TECNOLÓGICA

NO CONFORMIDAD / RECLAMACIÓN / ACCIÓN CORRECTIVA

IDENTIFICACIÓN:								**FECHA**	**Nº**
ORIGEN	☐	Auditoría interna	☐	Auditoría externa	☐	Sugerencia	☐	Supervisiones	
	☐	Queja/Reclamación	☐	Proveedor	☐	Control calidad servicio	☐	Revisión por la dirección	
	☐	Satisfacción del cliente	☐	Revisión informe final.	☐	Seguimiento del SGC	☐	Otra causa (especificar)	

Descripción de la no conformidad

Requisito incumplido de norma y/ o documento de referencia

Evaluación de la no conformidad ☐ **LEVE** ☐ **GRAVE**	Documentada Por :

DISPOSICIÓN INMEDIATA (elimina la NC solucionando el problema puntual)

	Implantada por: Fecha Límite.

ACCION CORRECTIVA Y/O PREVENTIVAS A TOMAR

Acciones Correctivas: Si ____ No ____	**Acciones Preventivas: Si ____ No ____**

Análisis de causas:

	ACCIONES	RESPONSABLE	RECURSOS	FECHA LÍMITE	APROBACIÓN
1					
2					
3					

EVALUACIÓN DE LA EFICACIA DE LAS ACCIONES CORRECTIVAS Y/O PREVENTIVAS TOMADAS Y CIERRE DE LAS NO CONFORMIDADES

Resultados de las acciones correctivas y/o preventivas tomadas:

Se da por cerrada la no conformidad observada _____ **Observaciones:**	Responsable de Cerrar la No Conformidad: Firma: Fecha del cierre:

Anexo 10: Reporte de no conformidades a la dirección

NO.	**NO CONFORMIDAD** (1)	**ORIGEN** (2)	**DETECTADA POR** (3)	**FECHA** (4)	**CORRECCIÓN** (5)
1.					
2.					
3.					
4.					
5.					
6.					
Elaborado por: (6) **Firma:**			**Fecha del reporte:** (7)		

Leyenda:

(1) Breve descripción de la NC.

(2) Origen de la NC detectada (ej.: auditoría interna o externa, controles, supervisiones, etc).

(3) Nombre y apellidos de la persona que detectó la NC.

(4) Fecha en que fue detectada la no conformidad.

(5) Estado en que se encuentra ().

(6) Nombre y apellidos del jefe del proceso.

(7) Fecha en que se reporta la NC

Anexo 11: Acta de revisión del sistema por la dirección

ACTA DE REVISIÓN DEL SISTEMA POR LA DIRECCIÓN

Fecha:
Asistentes:

INFORMACIÓN DE ENTRADA.

- Lectura del acta anterior y análisis de tareas programadas.
- Política y objetivos de la seguridad vigentes.
- Resultados y seguimiento de las revisiones anteriores del sistema por la dirección.
- Informes de auditorías internas y externas.
- No conformidades, acciones correctivas, y preventivas del sistema.
- Incidentes de seguridad.
- Indicadores del sistema de gestión.
- Reclamaciones de los clientes.
- Recursos Humanos.
- Resultados de la apreciación al riesgo: análisis de riesgos, el plan de tratamiento de riesgos, y las métricas de seguridad.
- Inventario de activos
- Proveedores.
- Cambios internos y/o externos que afecten al SGSI
- Oportunidades de mejora
- Revisión del estado de la organización.
- Seguimiento del plan de tratamiento de riesgos y análisis de las métricas de seguridad
- Análisis del desempeño de los procesos no contemplados con indicador
- Otras tareas de evaluación de la eficacia de los controles implantados
- Verificación del cumplimiento de control y supervisión previstos en la aplicación Activos de Información con revisión expresa de: copias de seguridad, accesos e intrusiones, uso de la red y cumplimiento de políticas por parte de los trabajadores.
- Previsión de necesidades y objetivos futuros.
- Otros factores que puedan afectar al funcionamiento de la empresa y al SGSI.

RESULTADOS.

- La mejora de la eficacia del sistema de gestión y de los controles y procesos de seguridad de la información.

Responsable de Seguridad de la información Firma:	Aprobado por Dirección Firma:

Anexo 12: Formulario de sugerencias de mejora

CIGET - Holguín IDICT INSTITUTO DE INFORMACIÓN CIENTÍFICA Y TECNOLÓGICA	**SUGERENCIAS DE MEJORA**

Nº: /

FECHA:

SUGERENCIA DE MEJORA:

Nombre y Apellido: ……..

A completar por el responsable del SGSI:

Descripción de la Resolución:

Plazo de Implementación:

Aprobación por la Dirección:

SI ☐
NO ☐ **Motivo:**_____

Fecha:

Verificación de Cumplimiento:
Fecha:_____
Nombre de quien verificó: _____

Anexo 13: Encuesta diagnóstica sobre seguridad de la información a trabajadores de la organización

Con vista a trabajar en el perfeccionamiento de la seguridad de la información en la organización, le pedimos su colaboración en dar respuesta a las siguientes interrogantes. El objetivo de la misma es identificar a través de la opinión de los trabajadores Ciget de Holguín¸ las fortalezas y debilidades que se presentan actualmente dentro de la organización en cuanto a seguridad de la información. De antemano le agradecemos por la colaboración brindada.

No.	ENUNCIADO	SI	EN PARTE	NO
1	¿Conoce usted las normas de seguridad de la información que tiene la Organización?			
2	¿Considera suficientes las normas de seguridad de la información dentro de organización?			
3	¿Ha recibido capacitación y concientización sobre seguridad de la información dentro de la organización?			
4	¿Cree que el nivel de seguridad de la información dentro de la organización es el adecuado?			
5	¿Considera suficiente la seguridad de los activos de información dentro de la organización?			
6	¿Al momento de su vinculación le fue entregado el manual de funciones del cargo y las políticas se seguridad de la información establecidas por la organización?			
7	¿Realiza copia de seguridad de la información que maneja en sus labores diarias de acuerdo a lo establecido en la organización?			
8	¿Sabe a quién debe de reportar un incidente de seguridad de la información y de qué manera?			
9	¿Considera importante que el sistema de control interno y sistema de gestión de calidad de la organización deben incluir políticas de seguridad de la información?			

10. Como crees que incide la seguridad de la información en la ejecución de sus trabajo diario.

_____

_____

11. Ha tenido algún incidente de seguridad de la información que dificulte el desarrollo de su actividad diaria. *En caso afirmativo*. Enuncie en breves palabras.

_____

_____

12. Podría brindar alguna recomendación que permita mejorar la seguridad de la información en la organización

_____

_____

13. ¿Cree usted que la organización debería implementar un sistema de gestión de seguridad de la información?

SI _____ NO _____

Muchas gracias por su colaboración

Fuente: Adaptado de Pulido & Mantilla (2016)

Anexo 14: Encuesta diagnóstica sobre la seguridad de la información entregada al clientes externos

ENUNCIADO	SI	A VECES	NO
¿La información que se entrega se encuentra actualizada?			
¿La información presenta la totalidad de los datos solicitados?			
En caso de que sea necesaria la entrega de información ¿Ha recibido orientación que explica cómo, con quién y donde se encuentran las mismas?			
La información que se tramita entre consultor y clientes es tratada con discrepción y confidencialidad?			
Conoce de la existencia de cláusulas de confidencialidad, integridad y disponibilidad de la información en los contratos de servicios?			
¿La información que se tramita por medios electrónicos se encuentra exenta de virus?			
¿Puede encontrar rápidamente información del servicio prestado, aunque haya finalizado el mismo?			

¿Ha tenido algún incidente relacionado con la seguridad de la información en la prestación del servicio?

_____

_____

_____

Muchas gracias por su colaboración