INFORMACIÓN FINANCIERA Y ADMINISTRATIVA. UN PARADIGMA DESDE LA UNIVERSIDAD

AUTORES: Miriam Patricia Cárdenas Zea[1]
Milton Peralta Fonseca[2]
Ricardo Aguirre Pérez[3]
Alexandra Elizabeth Haro Chong[4]
Darwin Javier Zamora Mayorga[5]

DIRECCIÓN PARA CORRESPONDENCIA: mcardenas@uteq.edu.ec

Fecha de recepción: 10 - 11 - 2015 Fecha de aceptación: 23 - 12 - 2015

RESUMEN

La información recurso determinante para la toma de decisiones en las organizaciones financieras inmersas en la globalización, promueven la competitividad con variadas estrategias para la captación de mercado, los mismos que se vuelven vulnerables con la falta de aplicación de normativas de seguridad a la información. Por lo tanto en el presente trabajo se analizara el nivel de conocimiento y aplicabilidad de las normativas de seguridad de la información que garantizan la integridad y confiabilidad de la misma en las entidades financieras del sector. Los resultados evidencian la falta de conocimiento de la norma ISO 27001, y una clara omisión en la aplicabilidad.

PALABRAS CLAVE: seguridad información; normativa de seguridad de información; sistema financiero.

FINANCIAL AND MANAGEMENT INFORMATION. A PARADIGM FROM THE UNIVERSITY

ABSTRACT

Determining resource information for decision-making in financial organizations immersed in globalization, promote competitiveness with various strategies for capturing market, they become vulnerable to the lack of enforcement of safety regulations to information. Therefore in this study the level of knowledge and applicability of the rules of information security to ensure the integrity and reliability of the same in the financial institutions sector is analyzed. The results show a lack of knowledge of the ISO 27001 standard and a clear omission in the applicability.

[1] Docente. Universidad Técnica Estatal de Quevedo. Quevedo, Los Ríos, Ecuador.
[2] Docente. Universidad Técnica Estatal de Quevedo. Quevedo, Los Ríos, Ecuador.
[3] Docente. Universidad Técnica Estatal de Quevedo. Quevedo, Los Ríos, Ecuador.
[4] Docente. Universidad Técnica Estatal de Quevedo. Quevedo, Los Ríos, Ecuador.
[5] Docente. Universidad Técnica Estatal de Quevedo. Quevedo, Los Ríos, Ecuador.

KEYWORDS: information security; information security policy; financial system.

INTRODUCCIÓN

La principal barrera en la aplicación de la tecnología en el sector financiero es la seguridad del significativo volumen de datos sensibles que se manejan. Los bancos obligados a utilizar aplicaciones basadas en normativas y rigurosos marcos de referencia son los que enfrentan las mayores restricciones para su utilización. Hay quienes consideran este riesgo como uno de los principales obstáculos para su utilización debido a que las complicaciones sobre la protección y confidencialidad de los datos preocupan al mercado. (López; Albanese; Sánchez; 2012).

La falta de experiencia de los gerentes en relación con la gestión de proyectos de implementación de tecnologías de la información, más aún de cloud computing — dado su reciente desarrollo, puede ser una fuente de riesgos significativa si no se realiza una adecuada capacitación de la dirección. (López; Albanese; Sánchez; 2012)

En Ecuador existen miles de conexiones de banda ancha, lo que quiere decir que muchas de estas redes se conectan a internet por estos accesos y ahora es muy necesario ser conscientes de la necesidad de fortalecer la seguridad de los sistemas actuales para mantener la integridad de la información.

Desde hace varios años organizaciones como AUDISEC (Seguridad de la Información) y el Consejo Superior de Administración Electrónica preocupados por la seguridad de la información, han establecido normas que garanticen la seguridad de la información generada por los sistemas informáticos; basándose en el análisis de riesgo, la política de seguridad, la de seguridad física, la de seguridad del recurso humano, la gestión de activos, de comunicaciones y operaciones, control de acceso, mantenimiento de sistemas y gestión de incidentes de seguridad.

A partir de este antecedente, la Universidad Técnica Estatal de Quevedo, realizó un diagnóstico de la situación actual de la problemática, con la finalidad de contribuir a la mitigación de un problema social con el cumplimiento de las políticas y normativas establecidas para garantizar la seguridad de la información de los usuarios del sistema financiero, por lo que se propone programas de transferencias de tecnología vinculando a la Universidad con las instituciones financias.

La información es un activo para las empresas, su construcción conglomeran diferentes factores que están regulados por normas que se aplican escuetamente y se desconocen, por tal razón no solo se ve amenazada la información, han sido vulnerados los productos que ofertan las entidades financieras. Por lo anteriormente expuesto el objetivo de este trabajo es analizar el nivel de conocimiento y aplicabilidad de las normativas de seguridad de la información que garantizan la integridad y confiabilidad en las entidades financieras del sector.

DESARROLLO

Se realizó el diseño de dos instrumentos que fueron aplicados en las entidades financieras de la zona 5 y sus sectores de influencia, para determinar el grado de conocimiento acerca de la seguridad de la información, que debe tener un funcionario de las mencionadas instituciones.

Las encuestas constaron de 25 y 12 interrogantes, dirigida a jefes, administradores, supervisores y empleados en general de las entidades bancarias, los instrumentos se aplicaron a 52 personas de diferentes instituciones financieras como Bancos, el muestreo desarrollado durante los meses de noviembre, diciembre de 2014 y enero del 2015, fue de conveniencia, debido a la dificultad que presentaba la realización de un muestreo probabilístico entre los funcionarios por sus diferentes cargos.

Se realizó un análisis descriptivo (univariante), con el fin de proporcionar medidas resumidas de las mismas. Para las preguntas continuas se calcularon las medias y para las discretas, frecuencias y porcentajes, en los distintos niveles de cada variable.

En el análisis exploratorio unidimensional de las variables, cada bloque de preguntas, que consta de 25 variables que constituyen la matriz inicial correspondientes, a las diferentes preguntas incluidas en la encuesta, 9 fueron de tipo nominal y 16 de tipo ordinal. Mientras que el segundo instrumento tres fueron de tipo nominal y 9 de tipo ordinal.

A continuación se presentan los bloques:

Bloque I: Datos de identificación en las instituciones.

Bloque II: Cumplimiento de normativa

Bloque III: Estrategias de seguridad.

Bloque IV: Toma de decisiones

Bloque V: Presupuesto para la seguridad.

La seguridad de la información conlleva todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad e integridad de la misma. La seguridad de la información conlleva los riesgos de los negocios incluyendo no solo las vulnerabilidades y un aspecto de las amenazas, sino el conjunto de los factores que determinan tales riesgos: activos, vulnerabilidades y amenazas.

Las instituciones financieras deben estar siempre en constante evolución y sometida a distintas exigencias que evidencien una permanente actualización y difusión de las estrategias de seguridad para el adecuado desarrollo de los objetivos planteados que garantizan la confianza de los usuarios en la institución financiera como medidas para la protección, uso y conservación de

los recursos financieros, materiales, técnicos y cualquier otro recurso de propiedad de la entidad.

Los pilares son la confidencialidad: solo personas autorizadas tienen acceso a la información; la integridad: la información y sus métodos de proceso son exactos y completos; la disponibilidad: los usuarios autorizados tienen acceso a la información y a sus activos asociados requeridos.

El objeto o propósito consiste en mantener la continuidad de los procesos organizacionales que soportan los activos a resguardar, así mismo se intenta minimizar el costo global de la ejecución de dichos procesos como las pérdidas de los recursos asignados a su funcionamiento.

Las instituciones generalmente no establecen presupuesto para las herramientas de software como sistema de seguridad de la información, lo que conlleva no brindar un servicio de calidad a sus usuarios.

A partir de esto se plantean que los procesos de cotidianidad están regulados por principios, normas, leyes que conducen a un sistema ordenado de calidad en los diferentes campos. Es así que para la seguridad de la información en la actualidad está en vigencia la norma ISO, normas que rigen la seguridad informática, la seguridad del software.),

Por otra parte las entidades bancarias expresan un nivel bajo en técnicas, dinámicas de aprendizaje para asegurar y comprender la norma ISO/IEC 27001. La información es un activo valioso que puede impulsar o destruir su empresa. Además si se gestiona de forma adecuada, le permite trabajar con confianza. La gestión de la seguridad de la información le ofrece la libertad para crecer, innovar y ampliar su base de clientes sabiendo que toda su información confidencial seguirá siéndolo.

Las normas específicas de Información Financiera para el Sistema Bancario y Financiero Nacional se armonizaron coherentemente con el contenido de los estados financieros emitidos por los bancos e instituciones financieras no bancarias, con las Normas Internacionales de Información Financiera (NIIF); garantizando a que los auditores y supervisores comprueben y evalúen que los estados financieros cumplían con los elementos relevantes.

Las Normas Específicas de Información Financiera para el sistema bancario y financiero internacional, recogen características cualitativas que deben poseer los estados financieros, las que son comunes a cualquier sector económico del país, a saber:

- Comprensibilidad: La información suministrada en los estados financieros debe ser fácilmente comprensible por los usuarios.
- Relevancia: Para que sea útil, la información debe ser relevante, ejercer influencia sobre las decisiones económicas de los que la utilizan, ayudándoles a evaluar sucesos pasados, presentes o futuros, o bien a confirmar o corregir evaluaciones realizadas anteriormente.

- Fiabilidad: Para que sea útil, la información debe ser también fiable, estar libre de error material y de sesgo o prejuicio, y los usuarios pueden confiar en que es la imagen fiel de lo que pretende representar, o de lo que puede esperarse razonablemente que represente.
- Comparabilidad: Los usuarios deben ser capaces de comparar los estados financieros de un banco o institución financiera no bancaria a lo largo del tiempo, con el fin de identificar las tendencias de la situación financiera y del desempeño. También deben ser capaces de comparar los dichos estados de instituciones diferentes, con el fin de evaluar su situación financiera, desempeño y cambios en la posición financiera en términos relativos.

La determinación de políticas de seguridad, demanda primero el planteamiento de objetivos de la seguridad. Una vez creada la política de seguridad, el siguiente paso es poner en práctica las normas que contiene. Este paso incluye la formación de empleados y la mejora necesaria de software y hardware para implementar normas. Asimismo, cuando se realizan cambios en el entorno informático, se debe actualizar la política de seguridad. De esta forma se cubren los posibles riesgos que puedan implicar estos.

La función de las universidades es la producción de conocimiento científico y tecnológico; es por eso que a través de las alianzas se busca ocupar el lugar de prominencia que les corresponde, no sólo como centros de estudio y saber, sino también como centros que producen resultados que responden a las demandas del sector productivo (administrativo y financiero) para hacerse partícipes en el desarrollo de políticas de seguridad en este ámbito, con la aplicación e innovación de nuevas tecnologías, sin olvidar la participación y regulación del Estado para el fomento de esta relación.

Posteriormente tabulada la información, se realizó un análisis exploratorio unidimensional sobre las variables para cada bloque de preguntas del cuestionario, el instrumento se enfocó en la aplicación de la seguridad de la información para medir el nivel de cumplimiento de políticas y normativas que rigen la seguridad de la información, se examinaron también los elementos, normativas y estrategias de seguridad que los involucrados de las instituciones financieras aplican y difunden para garantizar la integridad de la información de los usuarios.

La seguridad e integridad de la información es de suma importancia para el desarrollo y crecimiento de las entidades bancarias.

En la figura 1, el 54% que representa el mayor porcentaje de encuestados; hace referencia a las políticas de seguridad integral y física del personal que tienen implementadas las entidades bancarias, un 27% hace referencia a las políticas de respaldo de la información, el 13% hace referencia a las políticas de seguridad a los perfiles del personal, el 4% sobre las políticas de seguridad del software y el 2% a políticas para la adquisición de equipos, estos resultados evidencian el desconocimiento de los factores que comprende la seguridad de la

información, debido a la desarticulación que existe entre la universidad y las instituciones financieras.

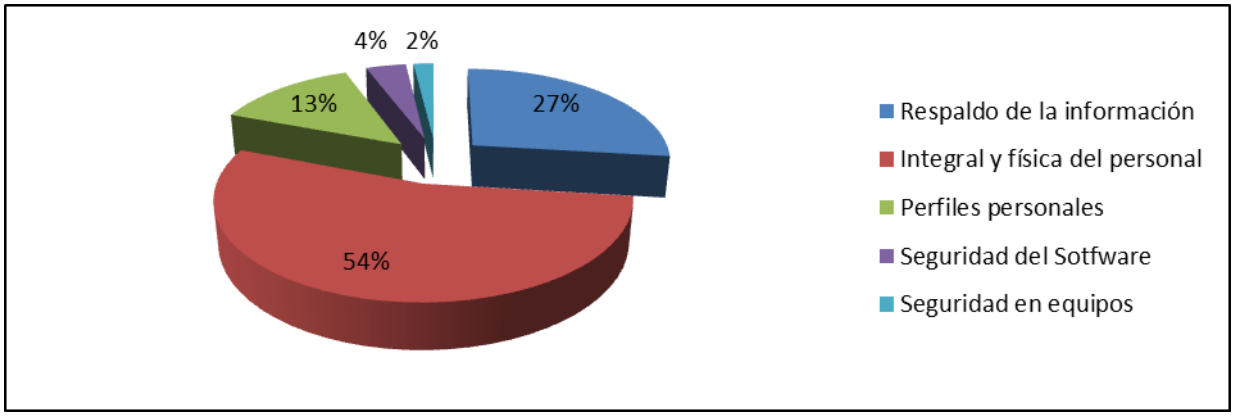

Figura 1. Política de mayor importancia para la institución.

(Dussan y Ciro, 2006), plantean la importancia de las políticas, dentro de las empresas, pues el establecimiento de una política de seguridad, integra un conjunto de directrices, normas, procedimientos e instrucciones que guía las actuaciones de trabajo y define los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como en el tecnológico. También a partir de sus principios, es posible hacer de la seguridad de la información, en tanto que todos puedan contar con un arsenal informativo documentado y normalizado, dedicado a la estandarización del método de operación de cada uno de los individuos involucrados en la gestión de la seguridad de la información.

La figura 2, se muestran que el 80% de la población encuestada en las instituciones bancarias manifiestan que la información financiera es la que en mayor medida se manipula, no así el 12% determina la información administrativa y el 8% manipula la información contable. De acuerdo con los resultados, este tipo de empresas manejan información financiera, son entidades legalmente autorizadas y constituidas para actuar con operaciones de dinero, su realidad influyen en las decisiones económicas de sus usuarios.

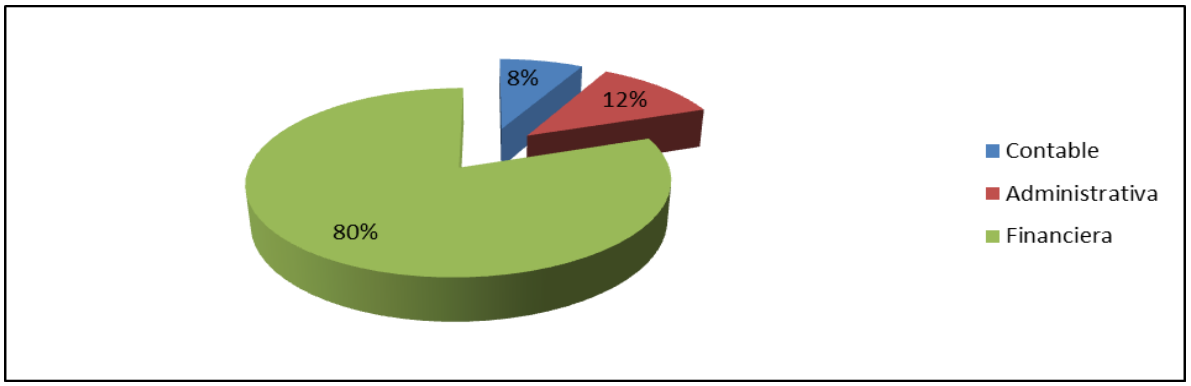

Figura 2. Información que maneja la institución.

(Morales y Baudillo, 2013), manifiesta que "El objetivo de la contabilidad financiera es proporcionar un sistema de información y comunicación externas, al recopilar, dar forma compacta, interpretar y diseminar datos económicos, que den una representación financiera de los derechos económicos y el interés relativo de los segmentos de la economía, a fin de facilitar a esos segmentos la formulación de juicios y la toma de medidas". La comunicación externa de esta información debe ser útil y confiable. Útil porque debe proporcionar la información que el usuario requiere y confiable porque las cifras en ella reflejadas deben ser fiel reflejo de la situación financiera y de la gestión administrativa de la empresa, lo cual permitirá al usuario la toma de decisiones acertadas como elemento de predicción del desempeño futuro de la entidad. La importancia de la información contable que se generan dentro de las empresas influye en la toma de decisiones y crecimiento de las mismas.

Aplicando el cuestionamiento sobre las normas de seguridad que se deben aplicar en las empresas financieras, la figura 3 revela que el 58% de los funcionarios manifiestan que la norma ISO 9001 la aplican para la seguridad; norma internacional que regula los sistemas de gestión de calidad. Un 13% manifiesta que es la ISO 19011, la que aplican para la seguridad de la información; norma que regula los procesos para las auditorías internas de los sistemas de gestión de la calidad y gestión ambiental y otro 13% indican que se utiliza la norma ISO 27001 norma que si regula la seguridad de la información, quedando un 16% que manifiestan la aplicación de la norma OSHA; norma que regula la Administración de Seguridad y Salud Ocupacional. Los resultados reflejan la poca importancia debido a la falta de asesoramiento técnico, inversión en tecnologías, y sistemas de seguridad de la información que las instituciones financieras le adjudican a la seguridad de la información según los datos obtenidos.

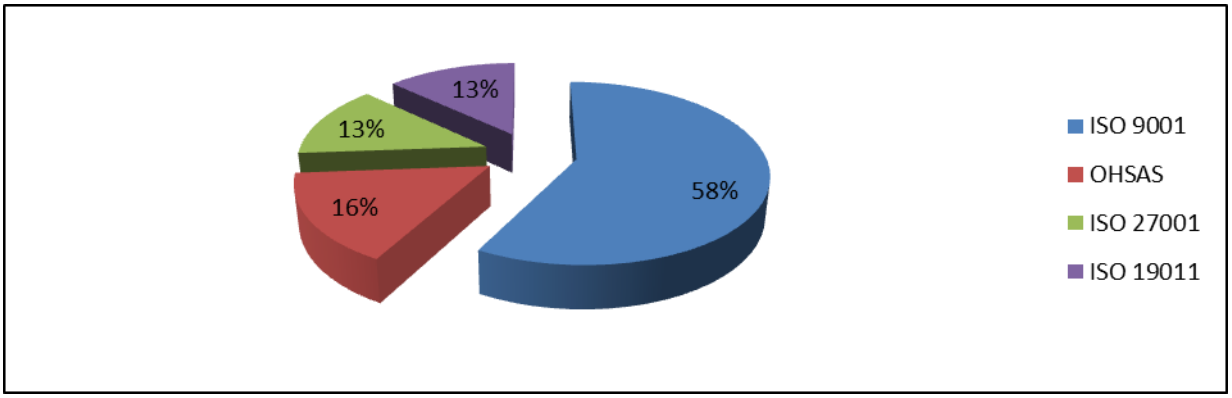

Figura 3. Normas de seguridad para la información.

Por otra parte (Caldera y Freire, 2015), plantean que las políticas y normativas existentes en los departamentos de documentación de las cadenas de televisión marcan y definen la posterior labor del personal de estas instituciones. Por otra parte es menester destacar que es fundamental contar con estas herramientas no sólo para que faciliten la tarea sino para que determinen y delimiten cómo

se debe realizar la labor documental, la conservación de los soportes documentales y de la información contenida en ellos, la ética y deontología profesional, etc. Dichas políticas deben quedar claramente reflejadas y conocidas por el profesional de estos servicios, tanto por medio de la realización de cursos de formación, previo a realizar labores documentales.

La figura 4, evidencia que el 89% de los funcionarios encuestados manifiestan que en la gran mayoría de bancos se aplican las normas ISO para la seguridad de la información, un 9% determina que se trabaja bajo la norma COBI y solo un 2% de la población manifiesta que se aplican las normas de ITIL que hacen referencia a las normas de las buenas prácticas que se basa en la gestión de servicios para el negocio y la tecnología. Los resultados evidencian que la mayoría de las empresas aplican las normas ISO para la seguridad de la información física y tangible debido a que son reconocidas internacionalmente para estandarizar, desarrollar, implementar y mantener procesos y sistemas de gestión. La seguridad informática es el área de la computación que se enfoca en la protección y la privatización de sus sistemas y en esta se pueden encontrar dos tipos: La seguridad lógica que se enfoca en la protección de los contenidos y su información y la seguridad física aplicada a los equipos como tal, ya que el ataque no es estrictamente al software del computador como tal sino también al hardware.

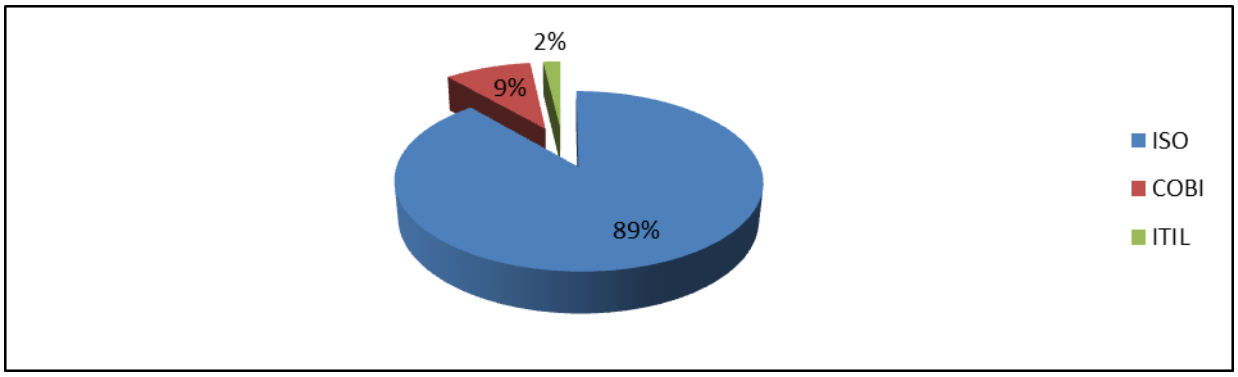

Figura 4. Normas que aplica la empresa para la seguridad de la información física y tangible.

(Ojeda, Jorge; Rincón, Fernando; Arias, Miguel; Daza, Libardo, 2010), manifiestan que en el contexto mundial, las tendencias del cambio caracterizadas y aceleradas por las tecnologías de la información y la comunicación han venido aparejadas con las tendencias delictivas, ahora caracterizadas como ciberdelito entre cuyos gestores y dinamizadores en el mundo, se encuentra gente preparada, estudiosa, investigativa y con gran poder de mimetización en el ciberespacio. Frente a eso, los países afectados han desarrollado distintos mecanismos tecnológicos y también jurídicos para actuar en los escenarios del cibercrimen, entre los cuales el sector financiero es uno de los más amenazados. Por esta misma razón, sus condiciones de vulnerabilidad y gestión del riesgo informático pueden señalar un derrotero para orientar las normas, políticas, estrategias y procedimientos que permitan enfrentar tal amenaza y velar por la seguridad de toda la sociedad, puesto que ella no sólo va

dirigida a un sector en particular, sino a todas las actividades del mundo en las que se muevan recursos financieros.

El avance de la ciencia y la tecnología ha generado la creación de normas para la seguridad de equipos informáticos; en la figura 5 se evidencia que un 70% de los encuestados manifiestan que aplican la norma ISO 9001, un 13 % indica que aplican la norma ISO 27007, el 10% determina que aplican la norma 27004 a la seguridad de los equipos y un 7% aplica la norma 27005 para la seguridad de los equipos informáticos. En una coyuntura con la figura anterior se aprecia en porcentajes reales la aplicación de la norma ISO 9001 en concordancia con que ésta es una norma que se aplica desde el diseño de procesos para la gestión eficiente en las empresas.

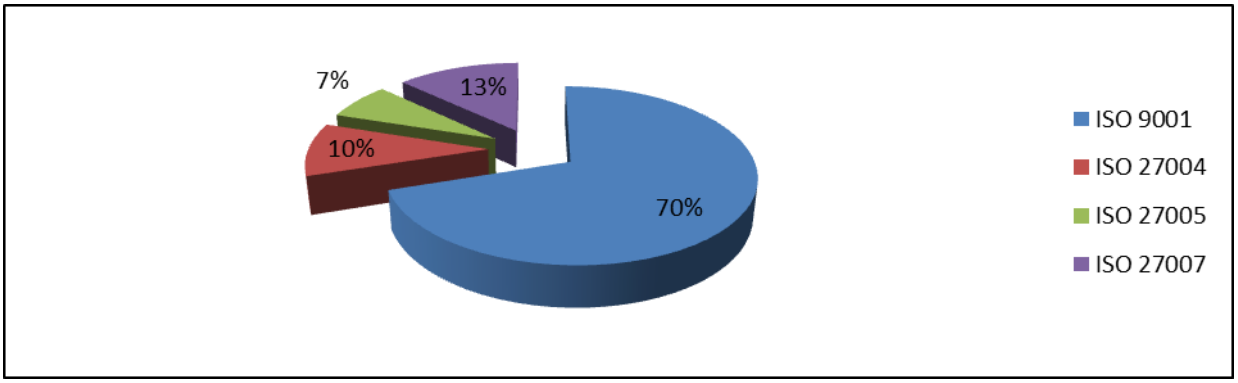

Figura 5. Seguridad para los equipos informáticos.

Por otra parte (Mesquida, Antoni Lluís; Mas, Antònia; Amengual, Esperança; Cabestrero, Ignacio, 2010) manifiestan que numerosas organizaciones del sector TI han optado por la implantación de sistemas de gestión con el objetivo de garantizar la eficacia y fiabilidad de sus procesos de negocio. Todas estas organizaciones normalmente han implantado sus sistemas de gestión de calidad, gestión de servicios y seguridad de la información, entre otros, de forma independiente o escasamente integrada. Sin embargo, en todos los sistemas de gestión existen ciertos elementos comunes que pueden ser gestionados de un modo integrado a través de la norma ISO 9001.

En la figura 6 se observa que dentro de las estrategias la para seguridad de los equipos, el 28% manifiesta que la más utilizada es la restricción de la Internet, el 27% manifiesta que consiste en evitar el uso de dispositivos de almacenamiento externo, luego el 24% hace referencia a la estrategia del mantenimiento preventivo correctivo de los equipos que se utilizan en la institución y el 21% impide el acceso a la información a personal no autorizado. Estos mecanismos y estrategias son de excelente aplicación para mantener una adecuada seguridad informática y así evitar los delitos informáticos, y como se aprecia en los resultados las entidades financieras involucradas en el estudio están divididas en la utilización de los mismos; por tal razón además a estas estrategias las instituciones financieras deben considerar aplicar ciertos principios fundamentales como el del mínimo privilegio, dinamismo y

participación universal de la información.

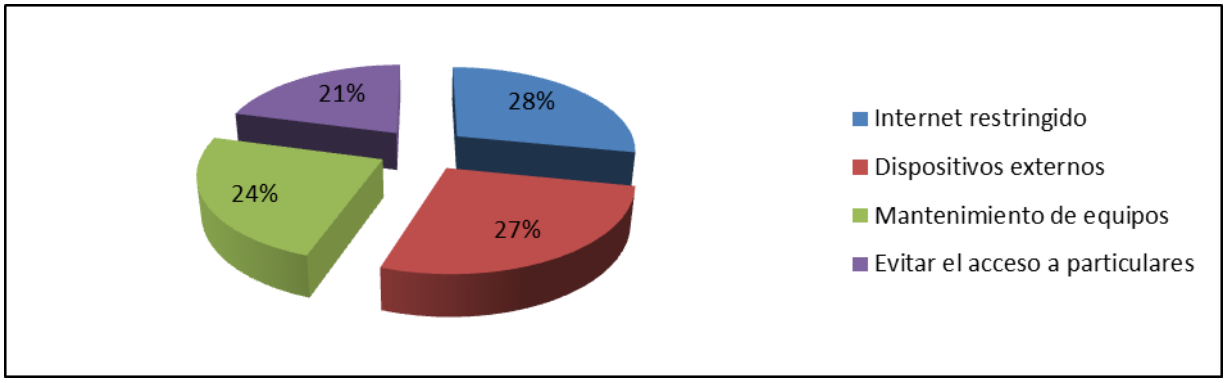

Figura 6. Estrategias para la seguridad de equipos informáticos.

Desde hace décadas a nivel internacional se difunden las normas de seguridad para garantizar integridad de la información, es así que en la figura 7 se citan estrategias para la seguridad de la información. El 41% de manifiesta que la capacitación constante al personal es la principal estrategia para brindad un buen servicio a los usuarios, el 29% indica que la implementación de software, 26% evidencian que la actualización de software es otra estrategia muy aplicada que da buenos resultados solo el cuatro por ciento manifiesta que la información impresa es una estrategia válida para garantizar la seguridad de la información. El boom de internet y los avances de la tecnología han fomentado una acelerada globalización, en la que intervienen procesos de envíos de información, recepción e investigación, etc. Procesos que deben tener establecidas estrategias que garanticen la seguridad de la Información.

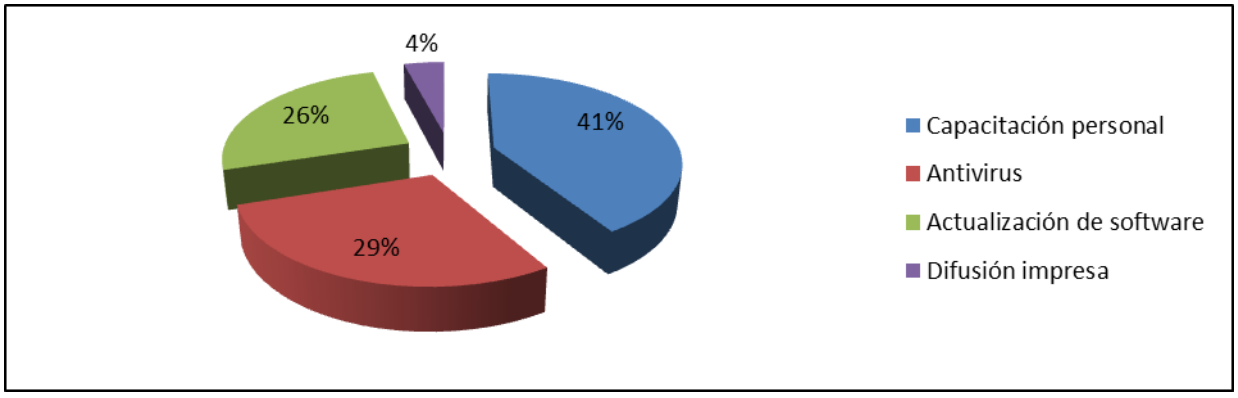

Figura 7. Estrategias para la seguridad de la información.

También (Díaz et al., 2014), manifiestan Los trascendentales cambios operados en el mundo moderno, caracterizado por su incesante desarrollo; la acelerada globalización de la economía, la acentuada dependencia que incorpora un alto volumen de información y los sistemas que la proveen; el aumento de la vulnerabilidad y el amplio espectro de amenazas, imponen nuevos retos a la práctica de la profesión de auditoría, en particular a la auditoría de seguridad Informática.

La elaboración de software esta sujeta a ciertas normativas para la seguridad de la información ya que no toda la información lo pueden reformular, se les diseña con ciertas restricciones y accesos de acuerdo a la actividad en la que nos desarrollamos; es así que, la figura 8 presenta que el 89% de los encuestados manifiestan no tener un software que garantice la seguridad de la información y solo un 11% de manifiesta tener un software que sí garantiza la seguridad e integridad de la información. Estos resultados demuestran la importancia de que se elaboren softwares que garanticen y esten alineados a la protección de la información en las entidades financieras, además de que la calidad de un software se entiende como el grado con el que un sistema o proceso debe cumplir con las exigencias especificadas y las necesidades de protección y seguridad de la información financiera.

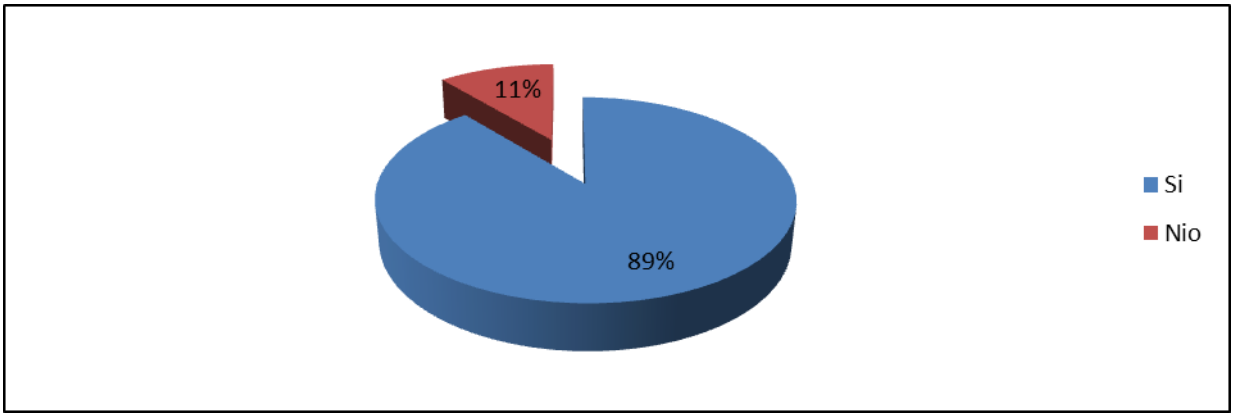

Figura 8. Normativas para la elaboración software que garantice la seguridad de la información.

(Díaz et al., 2014), manifiestan que la seguridad informática que contempla en la actualidad un importante número de disciplinas y especialidades distintas y complementarias, se ha convertido en una pieza fundamental en el entramado empresarial, industrial y administrativo de los países. Es por ello la necesidad imperante de crear la herramienta respectiva (software) para minimizar el riesgo al delito informático.

CONCLUSIONES

De acuerdo con el trabajo de campo realizado con dos instrumentos que fueron aplicados a funcionarios de instituciones financieras de la zona cinco, la información contable administrativa y financiera es considerada el activo más importante de las instituciones, especialmente aun si es información financiera como se demuestra en los resultados del trabajo de campo con el 80 %; es decir, que hacen caso omiso del cumplimiento de las normativas que rigen la seguridad de la información.

La revelación del desconocimiento de las normas para la seguridad de la información se evidencia en un 58% de las encuestas realizadas a los funcionarios de las instituciones financieras, lo que corroboramos con el artículo de la IV encuesta Latinoamericana de Seguridad de la información

2012, que indica que un 33,05% tienen poco entendimiento de la seguridad de la información.

Los avances de la ciencia y la tecnología han generado la creación de normas que regulan la seguridad de la información física y tangible, el desconocimiento de las mismas en pleno siglo XXI hace más vulnerable la información, las encuestas revelan que solo un dos por ciento aplican dichas normas y las difunden entre sus funcionarios, un 70% de la población encuestada aplica la norma ISO 9001, norma que rige la gestión de la calidad de los servicios, y solo un 7% aplica la ISO 27005, que rige la seguridad de los equipos informáticos. Este tipo de instituciones priorizan la política integral y física del personal en un 53%.

BIBLIOGRAFÍA

Caldera, J; Freire, R. (2015). Políticas de información en los servicios de documentación en las empresas televisivas. Revista Información, Cultura y Sociedad, 32: 113 – 128.

De Freitas, V. (2009). Análisis y evaluacion del riesgo de la información: caso de estudio Universidad Simón Bolívar. Revista Venezolana de Información, Tecnología y Conocimiento, 6 (1): 43 – 55.

Díaz, Yanet; Pérez del Cerro, Yunetsi; Proenza Pupo, Dayamí. (2014). Sistema para la gestión de la información de seguridad informática en la Universidad de Ciencias Médicas de Holguín. Revista Ciencias Holguín, 20 (2): 13 – 26.

Dussan, C; Ciro, A. (2006). Políticas se seguridad informática. Revista Entramando, 2 (1): 86 - 92

Ladino, Martha; Villa, Paula; López, Ana. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. Revista Scientia et Technica, XVI (47): 334 – 339.

López, María de los Ángeles; Albanese, Diana Ester; Sánchez, Marisa Analía. (2012). Gestión de riesgos para la adopción de la computación en nube en entidades financieras de la República Argentina. Revista Contaduría y Administración, 59 (3): 62-63.

Mesquida, Antoni Lluís; Mas, Antònia; Amengual, Esperança; Cabestrero, Ignacio (2010). Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. REICIS. Revista Española de Innovación, Calidad e Ingeniería del Software, 6 (3): 25 - 34

Morales, A; Baudillo, J. (2013). Utilidad de las normas internacionales de información financiera en la banca venezolana. Revista Centro de Investigación Universidad La Salle, 10 (39): 23 – 31.

Ojeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Revista Cuadernos de Contabilidad, 11 (28): 41 - 466