UNA MIRADA HACIA EL FORTALECIMIENTO DE LA SEGURIDAD CONTABLE

Maria Isabel Pinzón-Ariza [a]

[a] *Facultad de Contaduría Pública, Universidad Santo Tomas, Tunja, Colombia. maria.pinzona@usantoto.edu.co*

Resumen— En la actualidad, los distintos dispositivos electrónicos junto con las redes de información y la web han llevado a cabo un mejor almacenamiento y transmisión de datos relacionados con el gobierno y las empresas, en la actualidad las organizaciones ante estos cambios responden a la continua evolución de las tecnologías de la información contando con diversas herramientas que proporcionan innegables ventajas y a su vez amenazas y riesgos en los diferentes escenarios utilizados para el manejo de la información.. El presente artículo tiene por objetivo identificar y exponer hallazgos originales de investigaciones vinculadas a delitos cibernéticos en el ámbito contable, con el objetivo de fomentar el uso adecuado y la gestión de la información mediante diversas estrategias que contribuyan a proteger los activos intangibles de las organizaciones. Se implementa la metodología de exploración sistemática de literatura teniendo en cuenta palabras claves que fueron buscadas en bases de datos académicas donde se escogieron 60 estudios que plasmaron en su contenido los criterios de búsqueda y se escogieron 30 artículos de investigaciones teóricas y empíricas que abordaron el tema central de investigación. Se concluye que son diversos los estudios realizados alrededor de la problemática, pero falta profundizar aún más en los diversos métodos que se usan para cometer delitos informáticos en la parte contable, para que las empresas estén totalmente informadas de cómo cuidar su información y que esta no sea vulnerable ante los delincuentes, así mismo se resalta el papel que tienen los revisores fiscales al permitir la identificación de errores en los distintos departamentos de las empresas y/o deficiencias en el control interno.

Palabras Clave— ciberataques, información contable, nuevas tecnologías,

Abstract— Currently, different electronic devices along with information networks and the web have carried out better storage and transmission of data related to government and companies, currently organizations respond to these changes to the continuous evolution of information technologies with various tools that provide undeniable advantages and at the same time threats and risks in the different scenarios used for information management. This article aims to identify and present original findings of research related to cybercrimes in the accounting field, with the aim of promoting the proper use and management of information through various strategies that contribute to protecting the intangible assets of organizations. The methodology of systematic exploration of literature is implemented taking into account keywords that were searched in academic databases where 60 studies were chosen that reflected the search criteria in their content and 30 articles of theoretical and empirical research that addressed the central research topic were chosen. It is concluded that there are various studies conducted around the issue, but there is a need to delve deeper into the various methods used to commit cybercrimes in the accounting field, so that companies are fully informed about how to protect their information and ensure it is not vulnerable to criminals. It also highlights the role of statutory auditors in enabling the identification of errors in different departments of companies and/or deficiencies in internal control.

Una visión Inicial

Los avances tecnológicos a nivel global han creado importantes desafíos para la protección de la información; por lo tanto, las organizaciones deben adquirir habilidades para gestionar de manera segura las transformaciones y así minimizar las vulnerabilidades en la administración de datos. De esta forma, en Latinoamérica se presentan estrategias que las empresas aplican para proteger sus activos más preciados; ya que es importante destacar que numerosas compañías en Colombia utilizan modelos de seguridad orientados a mantener a distancia a los ciberdelincuentes.

Por lo tanto, la diversidad que presentan los sistemas de información de las organizaciones actuales, a lo que se suma un cambio constante en las TIC, ha originado, sin duda, para los individuos y entidades beneficiarias, riesgos, peligros y fluctuaciones relacionadas con los contextos de Internet, Intranet, evolución tecnológica, administración de la información en general, y en particular en lo que concierne a la contabilidad. (Álvarez y Pérez, 2004).

Con base a lo anterior, Gamba (2010) citado por Ojeda y otros (2010) exponen lo siguiente:

> "El desarrollo de la tecnología informática y su impacto en casi todos los niveles empresariales ha dado lugar a actividades ilegales comúnmente tituladas delitos informáticos. Estos delitos, efectuados a través de las Tecnologías de la Información y la Comunicación (TIC), exteriorizan un rasgo particular: se destacan por su alto grado de transnacionalidad, ya que las estructuras de estos crímenes suelen llegar a muchos países (p.12)"

Es así como con el pasar del tiempo han ido evolucionando conjuntamente técnicas de seguridad de datos informáticos y contables con las diversas formas de cometer delitos en contra de estos bienes inmateriales de la empresa. Una prueba de esto es el caso citado por Mora y Ramírez (2016) citando a el periódico el Tiempo donde se menciona:

> "Un hito relevante en la cronología de los delitos informáticos en Colombia se remonta al 11 de mayo de 1983, cuando se produjo el robo de 13.5 millones de dólares. La investigación reveló que Roberto Soto interfirió en las líneas del Banco de la República, envió un mensaje al Chase Manhattan Bank en Londres y ordenó que los fondos fueran transferidos a su cuenta. Luego, realizó transferencias a un banco de Zúrich y a cuentas cifradas en Panamá; finalmente, los recursos fueron llevados a las Islas Azores y a las Islas Caimán, donde se evaporaron" (p.3).

Consecuentemente, diversos países han estado modificando sus códigos penales con el fin de sancionar este tipo de delitos y otros que afectan de manera evidente a las empresas mediante sus registros contables. Entre tanto, las distintas formas de delitos informáticos están catalogadas en el Código Penal Colombiano, e incluyen: el acceso abusivo a sistemas informáticos, la interrupción ilegítima de sistemas o redes de comunicación, la interceptación de datos, el daño informático, el uso de programas informáticos maliciosos, la infracción de datos personales, la sustitución de sitios web para recolectar información personal, el hurto mediante medios informáticos y otros delitos afines, así como la transferencia no autorizada de bienes, todos ellos tipificados como delitos protegidos." (Manjarrés y Jiménez, 2012).

En este sentido, la contabilidad como área de estudio incorpora aspectos de otras disciplinas, donde la seguridad informática debería ser considerada como una de ellas al establecer los requerimientos de la información contable. Al considerar los principios básicos de la información, tales como la integridad, la confidencialidad y la disponibilidad, se puede identificar su impacto en la optimización de los requerimientos de la información presentes en los sistemas de contabilidad.

Por otra parte, el término "delitos contables o económicos" generalmente, se refiere a cualquier infracción no violenta que resulta en una merma económica. Así, estos delitos abarcan un amplio espectro de actividades ilegales, que van desde la estafa hasta la evasión de impuestos y el lavado de activos. La definición de "delincuencia económica" es difícil de establecer y su interpretación precisa sigue siendo aún difícil. Esta labor se ha complicado aún más por el rápido desarrollo de las tecnologías, que facilitan nuevas formas de perpetrar dichos delitos (Naciones Unidas, 2005).

Por lo anterior, es fundamental reunir y difundir ciertos hallazgos derivados de los estudios efectuados en el medio de los delitos contables, con el fin de implementar estrategias que han sido producto de estudio y que se deben adoptar para evitar estos comportamientos ilícitos y así aumentar la seguridad en el manejo de los bienes intangibles de una organización y que hacen parte de los recursos vitales de la misma, si bien se han realizado estudios que han dado resultados a través de la utilización de las mismas herramientas que tenemos a disposición se requiere publicar y concientizar a los lectores sobre como resguardar y cuidar de los bines patrimoniales para poder enfrentar los retos en la globalización de la información.

Igualmente, se pretende ilustrar como ha sido el desarrollo tecnológico y, a su vez, la transformación en los métodos de conservación de datos, así como la necesidad de acrecentar de modo progresivo la protección de las bases de datos que engloban prácticamente toda la información relacionada. Se estudian diferentes contextos de riesgo que afectan la información y las medidas adoptadas para neutralizar, reducir y gestionar estos escenarios, basándose en las mejores prácticas en la implementación de la seguridad informática en los sistemas contables.

Con base en lo anterior, se enfatiza el rol de la contabilidad desde una perspectiva ética, que debe orientarse a la lucha contra la corrupción, el fraude y una variedad de prácticas inadecuadas que se presentan hoy en día para adulterar la información en las empresas (Muñoz y Silva, 2019). Lo anterior como base para el ejercicio de su profesión y para tranquilidad de la organización.

Metodología

El presente artículo implementa como metodología la revisión de literatura con base en palabras claves que fueron buscadas en repositorios de estudios académicos donde se eligieron 60 artículos que compilaran los criterios de búsqueda y se escogieron 30 artículos de investigaciones teóricas y empíricas que abordaron el tema central de investigación entre los años 2002 a 2022, este proceso se realizó en tres etapas; primeramente se identificaron los estudios más importantes, luego se realizó un análisis crítico de los enfoques metodológicos y de los resultados presentados y finalmente se realizó la síntesis de los hallazgos para evaluar la perspectiva que se tiene del estudio. El resultado de este proceso se refleja en el apartado de los resultados y son los más importantes asociados al tema exponiendo teorías y perspectivas que sostienen la investigación del tema central de investigación.

Resultados

La administración de la información contable

Melchor, Lavín y Pedraza (2012) en la investigación que realizaron, encontraron que la información se presenta como un elemento crucial para las empresas en la creación y mantenimiento de ventajas competitivas; no obstante, en recientes tiempos, ha sido amenazada por los elevados grados de incertidumbre en su gestión. Así mismo se examina el nivel de impacto que la calidad de los datos y su gestión segura tienen en los sistemas de información contable (SIC) y su repercusión en el desempeño de las pymes.

Wilson y Macevi (2002) definieron la Administración de la Información (AI) como la aplicación de principios administrativos para la obtención, conformación, seguimiento, distribución y uso de la información que se necesita para decidir de manera oportuna y eficaz con el fin de cumplir los objetivos de la empresa. Por ende, la AI está relacionada con el valor, la calidad, la propiedad, la aplicación y la protección de la información en el marco de la función de la organización.. igualmente, Druker (1988) manifiesta que el concepto de organismo cimentado en la información es un paso más avanzado en el desarrollo de las instituciones que utilizan la información de forma eficaz.

Entretanto, el Instituto Americano de Contadores Públicos Certificados en Estados Unidos señala que es esencial que los peritos de la contabilidad obtengan conocimientos, destrezas y habilidades en tecnologías de información (TI), circunscribiendo la comisión eficaz de datos (Dillon y Kruck, 2004). Esto tiene como propósito que dichas capacidades se empleen para optimar la utilidad organizacional, dado que se concibe que la información no se agota con su uso, sino que su dirección se optimiza a través de su manejo y trasmisión. Por lo tanto, es esencial que el departamento de contabilidad en las organizaciones reconozca la importancia de estas habilidades, ya que frecuentemente los datos e información financiera se convierten en un recurso poco aprovechado.

La administración adecuada de la información y la calidad se contemplan como cuestiones que aún están pendientes de consideración para todos los actores involucrados en los técnicas de gestión, tales como directivos, gerentes, personal de sistematización y cualquier beneficiario que dependa regularmente de la información formada por los sistemas contables digitales (Melchor, Lavin & Pedraza, 2012). En este sentido, las entidades deben aunar esfuerzos para la adquisición de un software que registre las operaciones financieras que engloben, por ejemplo, operaciones en los sectores de compras, ventas y otros procedimientos comerciales, con el objetivo primordial de suministrar información apropiada para la que la gerencia atine en sus decisiones.

La adquisición de softwares que apoyen las actividades de la empresa representa un impacto beneficioso en la productividad y el desempeño de la organización al elevar las ventas, facilitar el acceso a un número mayor de clientes y mejorar la relación con ellos, así como al incrementar la eficiencia en los procesos comerciales y reducir costos, entre otros factores. Aunque se pueden reconocer beneficios en el uso de métodos de información y en los progresos tecnológicos, también se ha desarrollado la vulnerabilidad de dichos sistemas.

Según, Beard y Wen (2007), los sistemas de informacion actualmente tienden a presentar amenzas y problemas durante su procesamiento o ejercicio. Ejemplos de esto incluyen la generación de software ilegal, el acceso o eliminación de archivos, y la destrucción o corrupción de la lógica de un software a través de virus, entre otros riesgos. Así, el problema de la inseguridad informática continúa siendo relevante a pesar de que se han implementado acciones correctivas y se han creado programas para la seguridad de la información, estos esfuerzos no han dado los frutos que se esperan en materia de mitigación de la vulnerabilidad porque cada día los ataques informáticos cobran más fuerza y son más agresivos.

En realidad, recientemente los dirigentes, comités de auditoría, especialistas en contabilidad y auditores están articulando esfuerzos para perfeccionar el control interno y defender la amparo de la información financiera, con el objetivo de frenar que los delincuentes informáticos puedan acceder a ella. y proteger a toda costa los datos contables de las organizaciones. Sin embargo, es fundamental que todos estos esfuerzos sean respaldados por la organización a través de la educación y capacitación que se proporciona a sus colaboradores, de manera que estén al tanto de cómo salvaguardar esta información.

Con base a los anterior Abu-Musa (2006) señala que usualmente los trabajadores son honestos y con buenas intenciones; no obstante, la fatiga, la falta de capacitación adecuada o la desatención pueden ocasionar errores en la información, lo que repercute negativamente en la empresa. En este sentido, es necesario contar con controles en los sistemas de información, incluyendo tanto el hardware como el software, así como en cualquier Sistema de Información (SIC), para advertir e identificar fallos y evitar el detrimento accidental o intencionada de bienes informativos. (Henry, 1997).

Luego de describir de forma amplia el estado actual en lo que atañe a la seguridad de la información y las vulnerabilidades que enfrenta, es indispensable puntualizar que acciones se generan de los delitos informáticos en el área contable a fin de promover el buen uso y manejo de la información a través de las diferentes estrategias que permiten salvaguardar los bienes inmateriales de las organizaciones.

El fraude en la información y el rol del revisor fiscal

El rol del revisor fiscal al evidenciarse cualquier tipo de delito informático es fundamental para reconocer y dar a conocer a la organización lo que pasa cuando no se adoptan medidas de seguridad en casos que pueden ser previsibles, por ello el revisor fiscal cumple un papel fundamental para mitigar estas irregularidades y acciones corruptas.
Lo anterior lleva a reflexionar como la corrupción y el fraude resuenan con fuerza en cualquier rincón del planeta, la corrupción es una plaga que perjudica diversas áreas de la sociedad, presionando la credibilidad, estabilidad y transparencia de individuos, empresas e instituciones; circunstancia que a menudo afecta a los contadores públicos en el caso del fraude corporativo debido a su proximidad con la información financiera y contable, y su obligación de aportar pruebas ante entidades (García, Morelo y Serpa, 2022).

Pero no todo está perdido, los revisores disponen de normativas claras en su propio trabajo que les habilitan para formular conceptos fundamentados no solo en su criterio sino en fundamentos legales robustos. En el contexto colombiano, las Normas de Auditoría Generalmente Aceptadas (NAGA), establecidas por el Consejo Técnico de la Contaduría Pública, son las bases que los contadores públicos deben observar al realizar auditorías o revisiones fiscales y al formular juicios. Además, las Normas Internacionales de Auditoría (NIA) tienen un carácter global y se originaron del proceso de convergencia que comenzó con la Ley 1314 de 2009.

Ante esto cobra relevancia el ejercicio de una fiscalización constante, lo cual puede facilitar la detección de fallas en las diferentes áreas una organización y/o deficiencias en el control interno tanto en su diseño como en su aplicación y operatividad, permitiendo tomar acciones de mejora oportunamente. De igual forma, aunque la posibilidad parezca remota, esta labor permite detectar indicios de posibles fraudes o casos de corrupción y es tarea del revisor fiscal revelar estos hechos ante los altos mandos gerenciales de la organización, en casos extremos el profesional deberá dirigirse ante las autoridades competentes para denunciar la situación presentada (Guzmán, Palma y Morales, 2020).

Por consiguiente, resulta esencial que el revisor fiscal tenga competencias efectivas en comunicación, tanto oral como escrita y conozca los diferentes canales de comunicación dentro y fuera de la organización para transmitir de la manera más oportuna, clara, trasparente y objetiva sus hallazgos y recomendaciones a los diferentes órganos de las entidades de control. Para ello, el profesional puede apoyarse en la NIA 260 y 265, que hacen referencia al proceso de comunicación entre el Revisor fiscal y los diferentes agentes de la organización, brindando una "guía" de cuáles cuestiones deben comunicarse, de qué forma y a qué persona(s) en específico, es decir, al nivel adecuado.

Además, los empresarios exigen que el contador o revisor fiscal mantenga total reserva o confidencialidad al realizar su labor, lo cual es lógico. Sin embargo, el contador público que en el desempeño de sus tareas descubra señales de fraude, tiene la responsabilidad de comunicar a la entidad correspondiente, tales señales o anomalías detectadas. De igual forma, es su responsabilidad reportar los delitos de corrupción, especialmente cuando se vinculan con el artículo 26 de la Ley 43, 1990,la cual fue modificada por la Ley 2195 del 2022, que establece que es responsabilidad de los revisores fiscales reportar ante las autoridades penales, disciplinarias y administrativas los hechos de corrupción y la posible participación en delitos que transgredan hacia la administración pública, el ambiente, el mando económico y social, así como la financiación del terrorismo y de organizaciones criminales. También deben comunicar sobre la actividad de recursos concernientes con actividades terroristas y delictivas, conforme a lo estipulado en la Ley 1474 de 2011, así como cualquier otra conducta punible que afecte el patrimonio público económico que identifiquen en el ejercicio de su labor.

Del mismo modo, también se menciona en el Decreto 410 Código de Comercio en su artículo 211 expone que el revisor fiscal deberá asumir la responsabilidad por los perjuicios que genere a la sociedad, a sus asociados o a terceros, como resultado de negligencia o intencionalidad en el desempeño de sus deberes.

En este mismo sentido, en el ámbito internacional se encuentra la NIA 240 en la cual se presenta las funciones del auditor en relación con el fraude en las auditorías de estados financieros y explica la manera en que deben aplicarse las normas de auditoría 315 y 330 para gestionar los riesgos de errores significativos. También proporciona pautas al auditor sobre cómo obrar y qué instrucciones debe seguir al descubrir contextos que generen sospechas de un posible fraude.

Por consiguiente, se entiende que hay situaciones que ameritan que el revisor fiscal deba levantar el secreto profesional, pues de no hacerlo, se verá inmerso en la

situación presentada y deberá reconocer su conducta frente la organización y entidades de control y fiscalización por los perjuicios que pueda ocasionar. Así mismo debe ser cuando se presenten anomalías informáticas que conlleven a la filtración de datos de la empresa, los colaboradores deben dar parte inmediatamente se presente el suceso para no arriesgar aún más a la organización.

Modalidades de fraude informático contable

Hoy en día, existen varios sistemas de información, entre los cuales se hallan los contables, que acopian datos privados. Si no se toman las precauciones de seguridad imprescindibles, estos procedimientos pueden ser vulnerables. En la mayoría de las empresas, la seguridad de los sistemas de información es una prioridad, ya que el uso ilícito de la información puede implicar en consecuencias graves, circunscribiendo la pérdida de datos, errores en la introducción de información o el manejo inapropiado de información sensible.

Esteves (2011) con su investigación sostiene que, a pesar de su tamaño, las organizaciones enfrentan riesgos en sus sistemas de información, independientemente de los controles que tengan implementados. Lo crucial es el seguimiento constante que se realice a estos controles. A todos los colaboradores, independientemente de si son empleados o no, se les deben proporcionar los manuales de las tareas relacionadas con su labor. Uno de los límites que deben especificarse en los manuales correspondientes es la prohibición de instalar software no autorizado.

Entre tanto, Muñoz y otros (2019) exponen en su estudio que las amenazas y vulnerabilidades informáticas componen riesgos que perturban a todos los aspectos de la empresa, y las consecuencias pueden ser considerablemente serias en relación con la información que se maneja. Igualmente, Álvarez y Pérez (2004) consideran que las compañías poseen un conjunto de elementos que sirven para proteger y conservar la información, conocidos como activos. Estos activos se encuentran habitualmente expuestos a riesgos coligados con amenazas y vulnerabilidades.

Con relación a los riesgos Acosta, Benavides y García (2020) exponen que estos se originan de combinaciones de circunstancias y usualmente se denominan ataques o amenazas a los sistemas de información. Los tipos de riesgos que han sido más reconocidos incluyen: riesgos de integridad, riesgos de correspondencia, riesgos de acceso, riesgos de utilidad, riesgos en la infraestructura, riesgos de seguridad general, la concentración en la gestión de aplicaciones más grandes y complejas, la dependencia del personal esencial y el nulo control sobre estos mismos. Por lo cual se deben enfocar acciones para desempeñar funciones dependiendo del tipo de anormalidad que se perpetra.

De igual forma en el estudio realizado por Caraguay (2020) se deduce que los delitos informáticos son acciones ilícitas llevadas a cabo con dolo o negligencia, a través de dispositivos electrónicos, con el propósito de revelar, interceptar, eliminar, trasladar, atacar, manipular, divulgar o violar datos e información de sistemas informáticos, comprometiendo su privacidad, seguridad, integridad y disponibilidad. Esto genera una responsabilidad penal, siempre que estas acciones sean clasificadas y puedan atribuirse a los administradores de los fondos públicos.

Por lo tanto, la relevancia de identificar los distintos tipos de delitos informáticos presentes, facilita la adquisición de un instrumento innovador en el ámbito de la ciberseguridad, lo cual es fundamental para abordar de manera efectiva las consecuencias personales, económicas y sociales que enfrentan quienes son víctimas de este delito. (Escobar, 2017).

Al abordar el tema del delito informático, Fuentes y otros (2018) lo describen como un conjunto de conductas que constituyen un delito penal y que requieren un tratamiento legal, dado que su objetivo es causar daños a terceros, lo que puede resultar en diversas lesiones y, en ciertos casos, en la pérdida de bienes jurídicos. Es fundamental destacar que este tipo de delitos se producen en el ciberespacio

. En esta misma línea, Ruiz (1996) propone una tesis alineada con la de la Organización para la Cooperación y el Desarrollo Económico (OCDE, 2014), revelando que el delito informático se refiere a conductas ilegales que son contrarias a la ética y cuya divulgación y transmisión de datos en la red no están autorizadas.

Pero implementar estrategias para contrarrestar el fraude y diferentes delitos conexos conllevan a que se presenten a menudo varios problemas, incluyendo el elevado consumo de recursos por parte de los programas, lo que ocasiona lentitud en los computadores. También se presentan dificultades en el almacenamiento de bases de datos, la falta de mecanismos de protección para el acceso a la información en los servidores, y la interrupción de procesos, entre otros. Además, se ha advertido la ausencia de herramientas para detectar malware y una falta de conciencia sobre la seguridad informática entre los empleados, que es una de las principales causas de incidentes informáticos que impactan negativamente en los procesos de la organización. Si no se vigilan apropiadamente, estos problemas conducen al robo o la pérdida de información.

La gestión de las copias de seguridad en los sistemas

contables es crucial para la protección de la información y para asegurar la prolongación del servicio. Contar con procedimientos eficaces para el almacenamiento de estas copias asegura que la empresa esté preparada para enfrentar incidentes informáticos relacionados con el robo o la eliminación de datos segun Muñoz y otros (2019).

Si bien en diversas ocasiones se busca instaurar un sistema de seguridad para la información contable y financiera, muchos de estos sistemas no logran ser completamente eficaces. Esto se debe a que las empresas tienden a pasar por alto un elemento fundamental: la capacitación de sus empleados. La responsabilidad de manejar estas situaciones se asigna casi en su totalidad a los profesionales que se contratan para este propósito (Muñoz y otros, 2019). Así, en el contexto organizacional, la concientización está coligada al nivel de información que se brinda durante el adiestramiento, a diferencia de la formación, que se basa en el conocimiento, y la educación, que se enfoca en la percepción y la habilidad para descifrar ese conocimiento. como afirma Escobar (2022).

En consecuencia, Castro (2019), sostiene que las organizaciones no tienen la capacidad de mitigar los efectos de los delitos informáticos sin el soporte correcto, dado que una gran parte de las comunicaciones y procesos en el mundo son digitales. En este sentido, la ciberseguridad no es una opción, sino una obligación. Los riesgos cibernéticos que perturban al sector público, al sector privado y a las personas tienen distintas repercusiones y problemáticas. A pesar de ello, cada uno debe apadrinar medidas de seguridad que se acomoden a su naturaleza y contexto particular. (p.13).

En consecuencia los delitos informáticos hacen sensible todo tipo de información que se tiene en la empresa especialmente la contable, ante esto Espinet (2012) expone en su estudio que el delito informático es aquel que llevan a cabo los administradores, tanto de derecho como de hecho, de una sociedad ya determinada o en proceso de formación, quienes maniobran las cuentas anuales u otros documentos que habrían de reflejar de manera precisa el escenario jurídico o económico de la entidad, con la intención de no ocasionar un perjuicio económico a la misma, a alguno de sus socios. Por lo tanto, el delito financiero contable incluye cualquier conducta punible o no que se realice mediante las tecnologías de la información y la comunicación (TIC) con el objetivo de defraudar a un tercero, ya sea una persona física, jurídica o el Estado (p.24).

De acuerdo con la investigación realizada por Roa (2013), las empresas resultan ser un objetivo más atractivo para actividades delictivas, lo que ha llevado al surgimiento de auditorías de seguridad. Estas auditorías facilitan la contratación de empresas externas con experiencia en seguridad informática para que evalúen los equipos y los procesos. Basándonos en este concepto, se puede destacar que existen instrumentales que han surgido en la actualidad con el objeto de avalar la seguridad y el amparo de la información teniendo en cuenta que es el recurso más preciado que la organización tiene.

Ante esto, Acosta, Benavides y García (2020) En su investigación, sostienen que la prudencia, el escepticismo y la prevención son factores esenciales para que los propietarios de la información puedan protegerla adecuadamente. Esto es aún más crítico en el caso de datos que puedan causar daño directo a una entidad o a una organización.

Medidas de seguridad de la información

Actualmente, todas las empresas están sujetas a riesgos en la seguridad de sus datos, conocidos como vulnerabilidades. Estas vulnerabilidades se refieren a la susceptibilidad a ataques cibernéticos que consiguen dificultar la seguridad de un sistema, poniendo en peligro la integridad, disponibilidad o reserva de la información. Por ello, es decisivo implementar mecanismos que consoliden la identificación y eliminación eficaz de estas amenazas (INCIBE, 2020).

Según Martínez (2015), en Colombia, las equivocaciones más frecuentes que se relacionan en las empresas en el campo de la seguridad informática son, entre otros, la subestimación de la información, la idea errónea de que la seguridad se reduce a un antivirus y la confianza en tecnologías inapropiadas. Al mismo tiempo, Roa y Sanabria (2020) subrayan la importancia de los mecanismos de ciberseguridad para todas las organizaciones que llevan a cabo sus funciones mediante el tratamiento de datos.

En consecuencia, la gestión deficiente de los riesgos cibernéticos en las organizaciones a menudo resulta en repercusiones económicas significativas. Por ende, se necesita un trabajo sistemático, constante y completo, más de naturaleza preventiva que correctiva, que posibilite valorar la susceptibilidad a los riesgos cibernéticos e iniciar acciones para su control (Zuña, 2019).

Según la Escuela Internacional de Gestión Gerencial (2021) existen ciertas acciones que pueden mitigar dicha vulnerabilidad, estas se conocen como controles de seguridad, que pueden evitar la concretización de los delitos informáticos en la empresa o identificar un inconveniente cuando ya se haya producido. Para salvaguardar los sistemas, primero se deben detectar los peligros, por lo cual se deben implementar acciones como las que se mencionan a continuación:

Se debe implementar un cambio frecuente de las contraseñas de acceso a los sistemas, garantizando que estas sean complejas al incluir mayúsculas, minúsculas, números y caracteres especiales. Asimismo, es esencial cifrar la información para prevenir que terceros puedan descifrar la comunicación entre el emisor y el receptor. Es recomendable realizar auditorías y revisiones periódicas de los informes contables y otros documentos relevantes para el negocio. Finalmente, se sugiere resguardar la información de respaldo en lugares alternativos para aumentar las probabilidades de recuperación (Escuela Internacional de Gestión Gerencial, 2021, p.2)

Es crucial que cada usuario asuma la responsabilidad y conciencia de mantener buenas prácticas en la utilización de los sistemas. Muchos consideran que solo el departamento de sistemas tiene la obligación de asegurar el funcionamiento adecuado de los recursos de información. Sin embargo, es esencial que las buenas prácticas comiencen con el usuario mismo, quien debe resguardar sus contraseñas, acceder solo a aplicaciones autorizadas, evitar abrir archivos de fuentes desconocidas y salvaguardar el acceso físico a los sistemas.

De igual forma, las empresas deben asesorarse y respaldar su información con entidades que acrediten el resguardo de la seguridad ya que aunque existen marcos de referencia enfocados a la seguridad informática contable no se especifican bien los pasos a seguir a la hora de implementar una política de seguridad en una la organización (Tovar y Amariles, 2014).

Conclusiones

Según la teoría de la revisión fiscal, es primordial que el revisor fiscal asegure la precisión de los datos contables y lleve a cabo un análisis de riesgos para identificar posibles errores u omisiones en la información suministrada por la dirección. Esto demuestra la importancia de que el revisor fiscal realice su trabajo de manera profesional y siguiendo los procedimientos legales contables.

En cuanto a la seguridad de la información, la ética y el compromiso con la organización no es posible dejarlas de lado porque estos son pilares fundamentales que necesitan del apoyo de los colaboradores y por ende estos deben capacitarse y bridárseles todas las herramientas necesarias para lograr proteger los datos contables y los sistemas de información.

Son numerosas las disciplinas que cobijan a la contabilidad, la seguridad informática es una de ellas y por lo tanto se hace incipiente que esta cubra todos los requerimientos de la organización, cumpliendo con su único fin que es proteger los datos e información primordial y privilegiada y prever las vulnerabilidades de los sistemas.

Como se expuso en el documento son diversos los mecanismos con los que se cuenta para evitar el fraude en los sistemas de procesamiento de datos y más específicamente en el área contable, pero estas necesitan del compromiso de los colaboradores de la organización para que cumplan su finalidad a cabalidad por lo cual se requiere que la empresa deje en claro desde un principio el manejo de dicha información y se establezca que debe ser de obligatorio cumplimiento.

La normativa colombiana es clara al indicar que cualquier anomalía en el área contable debe ser denunciada por los revisores fiscales, pero estos a su vez deben apoyarse con el personal encargado de seguridad informática para evitar este tipo de eventualidades o para descubrirlas tan pronto se presenten.

Referencias

[1] Abu-Musa, A. (2006). Perceived Security Threats of Computerized Accounting Information Systems in the Egyptian Banking Industry. Journal of Information Systems 20 (1): 187-203.

[2] Acosta, M., Benavides, M. y García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. Revista Venezolana de Gerencia. https://www.redalyc.org/journal/290/29062641023/html/

[3] Álvarez Marañón, G., & Pérez García, P. P. (2004), Seguridad informática para empresas y particulares. Madrid, SPAIN: McGraw-Hill.

[4] Álvarez, G. y Pérez, P. P. (2004). Seguridad informática para la empresa y particulares. Madrid: McGraw-Hill.

[5] Artaza Varela, Osvaldo. (2013). Sistemas de prevención de delitos o programas de cumplimiento: Breve descripción de las reglas técnicas de gestión del riesgo empresarial y su utilidad en sede jurídico penal. Política criminal, 8(16), 544- 573. ISSN 0718-3399.

[6] Beard, D.; H.J. Wen (2007). Reducing the Threat Levels for Accounting Information Systems. The CPA Journal 77 (5): 34-42.

[7] Caraguay Ramírez, S. (2020). Aplicación de informática forense en auditorías gubernamentales para la determinación de indicios de responsabilidad penal con delitos informáticos en Ecuador, México y Perú, 2007-2019. Estado & comunes, revista de políticas y problemas públicos , 2(11), 135-153. https://doi.org/10.37228/estado_comunes.v2.n11.2020.178

[8] Castro, S. (2019). Prólogo Asobancaria. En Organización de los Estados Americanos & Asociación Bancaria y de Entidades Financieras de Colombia (Eds.), Desafíos del riesgo cibernético en el sector financiero para Colombia y América. https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sectorfinanciero-para-Colombia-y-America-Latina.pdf

[9] Dillon T.W. y S.E. Kruck (2004). The Emergence of Accounting Information Systems Programs. Management Accounting Quarterly 5 (3): 29-36

[10] Drucker, P. (1988). The Coming of the New Organization. Harvard Business Review, enero-febrero: 1-19

[11] El Tiempo (1993). Doce secretos del robo de US$ 13.5 millones. [Artículo en línea] publicado el 20 de junio. Bogotá: Casa Editorial El Tiempo. http://www.eltiempo.com/archivo/documento/MAM-140569

[12] Escobar, D. (2022). Capacitación y concientización en seguridad de la información. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, (2-2), 1-6. https://www.aacademica.org/escobards/65

[13] Escuela Internacional de Gestión Gerencial (2021). Los riesgos del sistema contable y la importancia de la seguridad informática. http://igsglobal.org/2021/12/06/los-riesgos-del-sistema-contable-y-la-importancia-de-la-seguridad-informatica/

[14] Estevez, Y. (2011). El fraude en los sistemas de información. https://revistas.uexternado.edu.co/index.php/contad/article/view/3364/301

[15] Fuentes, Tomás; Mazún, Rodrigo y Cancino, Gianny (2018), Perspectiva sobre los delitos informáticos: Un punto de vista de estudiantes del Tecnológico Superior Progreso. Revista Advance in Engineering and Innovation [AEI].
[16] Gálvez Toro, A. (2001). Enfermería Basada en la Evidencia. Cómo incorporar la investigación a la práctica de los cuidados. Granada: Fundación Index.
[17] Gamba, J. (2010). Panorama del derecho informático en América Latina y el Caribe. Santiago de Chile: Comisión Económica para América Latina y el Caribe.
[18] García Barbosa, M. D. ., Mórelo Pinto , A. M. ., y Serpa Ávila , I. F. . (2022). La corrupción: relación con la ética contable y las NIIF. Panorama Económico, 30(2), 104–136. https://doi.org/10.32997/pe-2022-4213
[19] Guzmán, R., Palma, E., y Morales, R., (2020). (Eds.). El Revisor Fiscal y la evaluación del control interno. Edición 1. Editorial Instituto Tolimense de Formación Técnica Profesional ITFIP.
[20] Hart, C. (1998). Doing a literature review. London: Sage Publications. [Links]
[21] Henry, L. (1997). A Study of the Nature and Security of Accounting Information Systems: The Case of Hampton Roads, Virginia. The Mid-Atlantic Journal of Business 33 (3): 171-189
[22] Manjarrés, I y Jiménez, F. (2012). Caracterización de los delitos informáticos en Colombia. Pensamiento Americano, 5 (9); pp. 71-82. ISSN: 2027-2448.
[23] Martínez-Cortes, J.F., (2015) . Seguridad de la Información en pequeñas y medianas empresas (pymes). Universidad Piloto de Colombia.
[24] Melchor Medina, J., Lavín Verástegui, J., & Pedraza Melo, N. (2012). Seguridad en la administración y calidad de los datos de un sistema de información contable en el desempeño organizacional. ContaduríA Y AdministracióN, 57(4). doi:http://dx.doi.org/10.22201/fca.24488410e.2012.159
[25] Melchor Medina, José, Lavín Verástegui, Jesús, & Pedraza Melo, Norma Angélica. (2012). Seguridad en la administración y calidad de los datos de un sistema de información contable en el desempeño organizacional. Contaduría y administración, 57(4), 11-34. Recuperado en 14 de noviembre de 2024, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0186-10422012000400002&lng=es&tlng=es.
[26] Muñoz Quintero N. P. & Silvia Ruiz M. E. (2019), Articulo: La Auditoria Forense y La Lucha Contra los Delitos Financieros: Una Perspectiva General. Revista El Centuario No.13.
[27] Muñoz, H.; Zapata, L; Requena, Dina M. y Ricardo, L. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia Revista Venezolana de Gerencia, vol. 2, Universidad del Zulia. https://www.redalyc.org/articulo.oa?id=29063446029
[28] Ospina, M., y Sanabria, P.,(2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista Criminalidad, 62(2).
[29] Roa Buendía, J. F. (2013), Seguridad informática. Madrid, SPAIN: McGraw-Hill España. Semana. (2019), Así está Colombia en el ranking de ciberseguridad mundial. https://www.semana.com/nacion/articulo/asi-esta-colombia-en- el-ranking-de-ciberseguridad-mundial/601118
[30] Ruiz, Enrique (1996), Responsabilidad penal en materia de informática: Revista Informática y Derecho Año 9. No. 10 y 11, UNED, Centro Regional de Extremadura, Mérida, pp 25-36.
[31] Tovar Yepes C. F. & Amariles Bedoya K, (2014), Proyecto de Grado: Mitigación De Riesgo De Delitos Informáticos En El Contexto Empresarial, Facultad de Ingeniería de Sistemas. Universidad Pedagogía de Pereira.
[32] Wilson, T. y E. Macevi (2002). The Development of the Information Management Research Area. Information Research 7 (3): 17-27.
[33] Zuña, C., Arce, E., Romero, Á., y Soledispa, W., (2019). Análisis de la seguridad de la información en las pymes de la ciudad de Milagro. Revista Universidad y Sociedad, 9(2), 313-318