Análisis de la Importancia de los Delitos Informáticos en Latinoamérica

David Leonardo Robles Alvarado

Universidad Santo Tomás

Facultad de Contaduría Pública

Especialización en Auditoría y Aseguramiento de la Información

Tunja

2024

Contenido

pág.

Lista de Tablas

pág.

Resumen

El análisis de la importancia de los delitos informáticos en Latinoamérica, se desarrolla a partir de la problemática existente en materia contable y donde se definen situaciones que han puesto en tela de juicio la seriedad, privacidad y confidencialidad de los sistemas de información contable en la región evaluada, tomando en cuenta la legislación existe, los delitos frecuentes y la necesidad de definir controles a los diferentes procesos organizacionales, evitando la vulneración de los sistemas como de pérdida de la confidencialidad y de los datos de las cuentas y los clientes.

El estudio resalta además la importancia de las Tecnologías de la Información y las Comunicaciones en los procesos organizacionales, permitiéndoles ser muchos más productivos, competitivos y rentables, entendiendo que a través de ellas se mejora el nivel de organización, se llega a nuevos mercados y clientes, se agilizan y optimizan las actividades operativas, brindando respuestas eficaces, atendiendo las exigencias de los entornos, pero sobre, permite agilidad en el desarrollo de análisis y determinación del comportamiento financiero de las empresas y mercados.

Palabras clave: Tecnologías de la Información y las Comunicaciones, delitos informáticos, sistemas de información contable, confidencialidad, vulneración de los sistemas informáticos, malware

Abstract

The analysis of the importance of computer crime in Latin America is based on the existing problems in accounting and where situations are defined that have called into question the seriousness, privacy and confidentiality of accounting information systems in the region assessed, taking into account existing legislation, frequent crimes and the need to define controls to the different organizational processes, avoiding systems breach such as loss of confidentiality and account and customer data.

The study also highlights the importance of Information and Communication Technologies in organizational processes, allowing them to be many more productive, competitive and profitable, understanding.

Keywords: Information and Communications Technologies, computer crimes, accounting information systems, confidentiality, computer systems infringement, malware

Introducción

A partir del surgimiento y desarrollo tecnológico[1] en el mundo como en Colombia, han sido más los ataques cibernéticos[2] bajo la comisión de delitos, que los mismos avances observados, generando alertas a las diferentes organizaciones y empresas a fin de establecer medidas de ajuste, detectando los factores de riesgo, así como acciones de tipo jurídico como administrativo que permitan contrarrestar los efectos y su impacto social.

> "El auge de las tecnologías del último siglo ha traído consigo innumerables avances para la humanidad, pero también otra serie de retos para las autoridades, legisladores e investigadores en las Américas, quienes han tenido que centrarse cada vez más en la persecución y sanción de los delitos cibernéticos, como la pornografía infantil, robo de identidad, acoso cibernético o "hacking". Según estimaciones de LACNIC, el organismo que maneja el Registro de Direcciones de Internet para América Latina y Caribe, el cibercrimen le cuesta a nuestra región alrededor de 90.000 millones de dólares al año". (Organización de los Estados Americanos [OEA], 2016)

Muchos de los países latinoamericanos se han ido concientizando frente al tema, al punto de revolucionar e involucrar sistemas de seguridad avanzados que lleven a una disminución de los ciberataques en diferentes entornos, máxime cuando sectores como el bancario, las comunicaciones, de servicios e incluso los de inversiones, han sido víctimas de estos delitos, lo que les genera pérdidas de información y de vulneración a la seguridad.

> "La tendencia de crecimiento en ciberataques también se refleja en todos los países, con la excepción de Costa Rica, que registró un leve aumento del 2%. La lista de países la lidera Ecuador (+75%), seguido por Perú (+71%), Panamá (+60%), Guatemala (+43%) y Venezuela (+29%). En total, solo el Top20 de malware en la región genera un promedio de 35 ataques por segundo. En este contexto, Brasil lidera la región con más de 1,390 intentos de infección por minuto, seguido de México (299 por minuto); Perú (96 por minuto), Ecuador (89 por minuto) y **Colombia** (87 por minuto)". (Diazgranados, 2021)

---

[1] "Consiste en la utilización de los conocimientos científicos existentes para la producción de nuevos materiales, dispositivos, productos, procedimientos, sistemas o servicios o para su mejora sustancial, incluyendo la realización de prototipos y de instalaciones piloto" (Instituto Vasco de Estadística, s.f.).

[2] "Cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital" (IBM, s,f,).

De ahí que se haya masificado el uso de la seguridad informática[3] como un mecanismo que involucra tanto la tecnología[4] como la mano de obra, todo en función de definir acciones, políticas, mecanismos y controles, apoyados en una infraestructura de software[5] y hardware[6], que permita a la vez una disminución de los riesgos mediante la revisión constante y la auditoria permanente de los procesos.

> "El sector financiero es uno de los que más invierte en materia de protección de los datos y de los sistemas de información. Ha venido incorporando, además, prácticas internas de ciberseguridad y seguridad de la información. No obstante, es pertinente seguir fortaleciendo las capacidades empresariales para anticiparse a estos riesgos". (Pardo et al., 2018, p. 1)

Es evidente que las organizaciones del nuevo siglo, prefieren una mayor inversión en seguridad antes que en herramientas y mecanismos de tipo operativo, de inversión e incluso comercial, dado que el impacto generado por las acciones delictivas es mayor en comparación con aquellos relacionados con el desarrollo de las actividades propiamente dichas.

> "Las tecnologías clave de la 4ta revolución industrial como el Internet de las cosas (IOT), la automatización, el blockchain, el big data y el cloud computing, están conduciendo la logística a nivel global, hacia la logística 4.0, lo que demanda la solución de temas como la alfabetización digital, el costo y la velocidad de acceso a Internet, así como la ciberseguridad". (Mariano, 2021, p. 7)

En materia contable la situación no es diferente, en tanto los datos existentes son relevantes para el desarrollo organizacional, permitiéndole la toma de decisiones oportuna y ajustada a la realidad y a las normas. Sin embargo, la seguridad informática debería ser una prioridad en la medida que les fortalece institucionalmente gracias a los controles y la misma detección de los riesgos a los cuales se expone el sistema existente.

---

[3] "Conjunto de medidas multidisciplinares de protección para evitar que una red informática y sus datos sufran algún tipo de vulneración, filtración, publicación de información privada o ataque" (Hewlett Packard Enterprise Development LP, 2024).

[4] "Conjunto de nociones y conocimientos científicos que el ser humano utiliza para lograr un objetivo preciso, que puede ser la solución de un problema específico del individuo o la satisfacción de alguna de sus necesidades" (Equipo editorial, Etecé, 2022).

[5] "Conjunto de reglas o programas que dan instrucciones a un ordenador para que realice tareas específicas. También se conoce como aplicaciones de software, paquetes de software, herramientas de software y programas de software. El software puede utilizarse para gestionar datos, automatizar procesos y crear aplicaciones o productos informáticos" (Arimetrics, 2022).

[6] "Conjunto de componentes y dispositivos físicos que la integran. Corresponde a todas las partes tangibles de un sistema informático. Sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Hardware es una palabra inglesa (literalmente: partes duras)" (Universidad Nacional del Sur, s.f., p. 15).

Se hace necesario en este caso que el sistema contable en general, defina acciones a favor de la seguridad informática a fin de disminuir la acción delictiva de quienes muestren algún interés frente a los datos de las organizaciones y entidades.

1. Generalidades

Desde hace tiempo, el tema de los delitos informáticos[7] en Colombia como en el mundo, se ha constituido en un contexto de análisis y de intervención permanente por parte de quienes administran la seguridad como de los entes jurídicos como empresariales, dada la importancia que tiene la preservación de los datos, así como el desarrollo continuo de mecanismos de mitigación.

No se debe olvidar que la actualización digital se desarrolla en función de las expectativas y necesidades sociales y donde, tanto software como hardware son determinantes en los procesos tecnológicos electrónicos, brindando respuesta a las plataformas en los diferentes campos del conocimiento.

Es de tener en cuenta que, a la par con el desarrollo de nuevas plataformas y herramientas informáticas[8] que buscan la protección de la seguridad de los datos, surgen los delitos informáticos afectando entornos como el contable donde se limita el acceso a la información para darle paso a la comisión de delitos y la posterior afectación de la seguridad.

Tabla 1

Estadísticas que indican el porcentaje de los países que aún no tienen sanción penal según cada delito informático.

Delito informático	%
Acceso ilícito	19%
Interceptación ilícita	33%
Atentado contra la integridad de los datos	14%
Atentado contra la integridad del sistema	33%
Abuso de los dispositivos	71%
Falsedad informática	57%
Fraude o estafa informática	48%
Pornografía infantil	19%

Fuente: Temperini, 2014, p. 10.

[7] "Acto humano culpable ejecutado con empleo de herramientas informáticas, que lesiona bienes jurídicamente protegidos, y que se encuentra tipificado y sancionado en la norma jurídica" (Narváez, 2015, p. 159).

[8] "Durante el 2022, las denuncias en Colombia por ciberdelitos crecieron un 26%, registrándose cada 8 minutos una nueva denuncia en nuestro país, siendo el hurto por medios informáticos el delito con mayor número de registros". (Tanque de Análisis y Creatividad de las TIC [TicTac], 2023)

Lo más preocupante en este caso, es que no sólo son personas sino organizaciones bien estructuradas que, a través de mecanismos especializados, atentan contra la seguridad de los datos y de la información que reposa en las diferentes dependencias de empresas, organismos e instituciones, y donde desafortunadamente y en muchas ocasiones, no se puede mitigar el impacto.

Así, el riesgo de pérdida de la información contable en este caso, llama ampliamente la atención de los expertos en seguridad, toda vez que es tomada como una oportunidad por la ciber delincuencia en la medida que sustrae datos confidenciales, los cuales usa posteriormente para continuar con la actividad delictiva, generando un detrimento patrimonial para los tenedores de la información.

El mundo por lo mismo, se ha venido preocupando por definir procedimientos y mecanismos a través de los cuales se logre aumentar la seguridad de los datos e informes en las organizaciones a través de la estandarización de las normas ISO[9] en la medida que le aportan valor a los beneficios organizacionales como una manera de evitar el robo de información y a través de ella la comisión de los delitos.

> "El estándar ISO 27010 aporta una guía sobre los métodos, modelos, procesos, controles y demás mecanismos para realizar el intercambio de información de una manera segura, garantizando la confianza y el entendimiento, respetando los principios de seguridad de la información". (ISOTools Excellence, 2014)

Es un secreto a voces que, las nuevas tecnologías han venido a revolucionar el sistema humano desde diferentes contextos, facilitando el desarrollo de procesos y la disminución del tiempo de respuesta. Sin embargo, surge una limitación mayor asociada con la falta de capacitación y formación en materia de bioseguridad: la ciber delincuencia, un flagelo de alto impacto dadas las implicaciones en materia económica, financiera, jurídica e incluso en lo que auditoria y aseguramiento de la información se refiere.

Implica ello, la necesidad de desarrollar el análisis pormenorizado de la importancia de los delitos informáticos en materia contable en Latinoamérica a la luz de los crecientes datos de

[9] "ISO (Organización Internacional para la Normalización) es una red mundial que identifica cuáles normas internacionales son requeridas por el comercio, los gobiernos y la sociedad; las desarrolla conjuntamente con los sectores que las van a utilizar; las adopta por medio de procedimientos transparentes basados en contribuciones nacionales proveniente de múltiples partes interesadas; y las ofrece para ser utilizadas a nivel mundial" (Organización Internacional de Normalización, s.f., p. 1).

ciber delincuencia, resaltando el papel que cumple el contador público frente al tema de la administración de la Tecnología de la Información[10], de manera que se conozcan en profundidad los diferentes delitos informáticos en materia contable, definiendo la legislación existente a nivel internacional y así dar a conocer las sanciones jurídicas como administrativas aplicables al tema de la ciber delincuencia en la región de estudio.

[10] "Las Tecnologías de la Información y la Comunicación (TIC) es un término que contempla toda forma de tecnología usada para: crear, almacenar, intercambiar y procesar información en sus varias formas, tales como: datos, conversaciones de voz, imágenes fijas o en movimiento, presentaciones multimedia y otras formas, incluyendo aquéllas aún no concebidas. Su objetivo principal es la mejora y el soporte a los procesos de operación y negocios para incrementar la competitividad y productividad de las personas y organizaciones en el tratamiento de cualquier tipo de información" (Ayala y Gonzales, 2015, p. 28).

2. Objetivos

2.1 Objetivo General

Analizar la importancia de los delitos informáticos en materia contable en Latinoamérica a la luz de los crecientes datos de ciber delincuencia.

2.2 Objetivos Específicos

- Determinar el papel que cumple el contador público frente al tema de la administración de la Tecnología de la Información en los países latinoamericanos.
- Identificar los diferentes delitos informáticos en América Latina en materia contable.
- Señalar la legislación contable aplicable al tema de los delitos informáticos a nivel internacional.
- Definir el impacto de los sistemas de información contable Vs. los delitos informáticos en los países latinoamericanos.

3. El Contador Público Frente al Tema de la Administración de la Tecnología de la Información en los Países Latinoamericanos

Es de conocimiento general, que el contador público cumple una de las funciones más importantes en las organizaciones, destacándose la garantía de las condiciones de transparencia, ética, moralidad, honestidad, claridad en los datos, exactitud en las cifras y precisión en los resultados, demostrando su compromiso para con el crecimiento y fortalecimiento empresarial.

Ello implica básicamente, el involucrar mecanismos y acciones que faciliten el control y auditoria[11] de todas las operaciones contables y financieras, de tal manera que la gestión organizacional, demuestre la confianza y fiabilidad hacia los grupos de interés, entendiendo la importancia de la disciplina contable, la integración con los sistemas de información, la tecnología y la transformación digital.

La función contable cumple un papel esencial en los procesos económicos, productivos y de desarrollo en las organizaciones, lo que genera la necesidad de hacer suya la información suministrada por las nuevas tecnologías, logrando procesos transparentes, eficaces, confiables y ágiles en comunión con las necesidades sociales y administrativas.

> "En los últimos años, la contabilidad ha experimentado transformaciones significativas debido a diversos factores como la globalización, la evolución de los medios digitales y el enfoque hacia la cientificidad. Estos cambios han planteado numerosos desafíos para los profesionales contables en términos de medición, valoración, registro, divulgación, control e integración de la información. Se reconoce especialmente que el avance económico a nivel global conlleva implicaciones que afectan la disciplina contable. En este contexto, la contabilidad desempeña un papel crucial en respaldar el proceso de transición y convergencia mundial hacia la estandarización de normas para la presentación de estados financieros. Este panorama, a su vez, plantea nuevos desafíos económicos que los contadores deben abordar". (González et al., 2021, p. 32)

Las ventajas generadas por las nuevas tecnologías digitales hacia las organizaciones son tan amplias y diversas, que ha exigido de las directivas y de quienes orientan las actividades

[11] "La auditoría constituye una herramienta de control y supervisión que contribuye a la creación de una cultura de la disciplina de la organización y permite descubrir fallas en las estructuras o vulnerabilidades existentes en la organización" (Villardefrancos y Rivera, 2006, p. 54).

productivas, comerciales y de servicios, el integrar mecanismos, plataformas y recursos que optimicen los procesos de gestión, pudiendo así controlar y verificar con mayor precisión, agilidad y pertinencia la información contable y financiera, cuya responsabilidad recae en el contador público.

No es un secreto que las nuevas tecnologías de la información y las comunicaciones, han demandado una mayor atención en materia empresarial y administrativa, toda vez que a través de ellas se responde con mayor facilidad y agilidad a las exigencias contables y financieras, pudiendo de esta manera, hacer frente a los nuevos parámetros determinados por las normas, lo que se constituye en un reto para los profesionales de la contaduría pública, especialmente de quienes no demuestran un mayor compromiso con las actividades.

> "Los hallazgos precedentes revelan una problemática importante en la profesión contable, puesto que durante los últimos años se ha venido evidenciando la falta de apropiación ética y social que deben asumir los profesionales contables, en relación con los diferentes retos económicos, digitales y científicos que impactan en la disciplina y, a su vez, en el ejercicio profesional (Pérez, 2015; 2019)". (González et al., 2021, p. 32-33)

Esa estandarización de las normas, exige día a día una mayor preparación y actualización en materia tecnológica, del personal que cumple funciones de orden contable y financiero, buscando una mayor respuesta a los requerimientos y lineamientos definidos en el entorno, además de facilitar la organización, análisis y presentación de estados financieros, permitiendo una mejor toma de decisiones.

Aquí, el contador público tiene una gran responsabilidad frente al cumplimiento de los objetivos organizacionales, por cuanto está en la obligación de generar una información contable y financiera acorde con la situación empresarial, mejorando la exactitud de los resultados, disminuyendo los tiempos de formalización de los datos, reconociendo además la importancia y utilización de los sistemas tecnológicos, la transparencia de los procesos y l a diligencia en la presentación de los informes y solicitudes.

> "La función del contador público ha evolucionado en paralelo con los avances tecnológicos. A lo largo del tiempo, se ha mantenido una interacción constante entre las demandas de las empresas y los progresos en tecnología, lo que ha conducido al desarrollo de estrategias efectivas. Estas estrategias no solo generan nuevas oportunidades para el crecimiento y la mejora de las organizaciones, sino que también incrementan la complejidad del entorno

empresarial y presentan desafíos adicionales para la profesión contable". (González et al., 2021, p. 45-46)

Dentro del conjunto de exigencias organizacionales, quizá sea la búsqueda de adaptación a las nuevas tecnologías, la que enaltece la labor de los profesionales contables, pues de una parte la sugiere la necesidad de adecuar los procedimientos a las plataformas y estructuras globalizadoras[12], de otra el generar confianza en los grupos de interés al mejorar la agilidad en el desarrollo de las tareas y requerimientos.

Las TIC en el contexto contable, demuestra no sólo la incidencia de los nuevos procedimientos en el desarrollo administrativo, sino que le apuesta a lograr una mayor actualización profesional donde se genere confianza, agilidad, precisión y análisis de los datos, lo que eleva la credibilidad de las empresas, su productividad y competitividad.

"[Las TIC] han evolucionado la manera de hacer las cosas, ya que se han desarrollado en diferentes áreas, en las cuales con ayudas de este tipo de herramientas se ha facilitado la manera de hacer las cosas esto conlleva a que las empresas se tengan que adaptar a estas nuevas herramientas tecnológicas las TIC's, como nos describe Parrales (2017)". (Chan et al., 2021, p. 2)

No obstante, la realidad demuestra que en no todos los casos se acepta el reto de adecuar cada proceso a las estructuras tecnológicas por parte de la fuerza laboral, pues de cierta manera se desplaza fácilmente la mano de obra, a cambio de optimizar los procesos empresariales desde lo contable, lo financiero, lo productivo y lo comercial, generando mayor incertidumbre y negación.

Las TIC en este caso, sugieren la socialización organizacional, definiendo las ventajas y oportunidades frente a criterios como el crecimiento, la productividad[13], la rentabilidad y la competitividad, entendiendo que no se puede lograr un real desplazamiento de la mano de obra, sino que, por el contrario, requiere de una integración entre opciones novedosas que brindan mayor agilidad al desarrollo de las actividades, frente a la necesidad de tomar decisiones basadas en los resultados.

---

[12] "Proceso que integra a nivel mundial el conocimiento, tiene su referente histórico en los cambios de las formas como se abordan procesos, métodos e información; su inicio se documenta al final del siglo XX, Castells, M. (2001) más allá de la discrepancia sobre si es un producto del desarrollo tecnológico o una evolución inevitable del capitalismo" (Flores, 2016, p. 26).

[13] "Relación insumo - producto que se lleve a cabo en cualquier entidad y actividad organizacional, es decir, la productividad está dada por un 'cociente' que indica qué tantas unidades se produjeron en virtud de los insumos utilizados con una visión totalmente enfocada y permeada por la eficiencia o, en otras palabras, 'el proceso de hacer más con menos'" (Montes, 2003, citado por Aguirre, 2022, p. 26).

> "Las TIC apoyan los procesos de mejoramiento de la productividad y la competitividad. Contribuyen a fortalecer la capacidad empresarial y de posicionamiento del producto o servicio en el mercado, además de la reducción de costos e incremento de la eficiencia en el empleo de los recursos (humanos, materiales y financieros)". (Berrones, 2020, p. 23)

Se toma en cuenta en este caso que, la capacidad empresarial se mide por los resultados obtenidos en cada una de las áreas organizacionales y la integración que se pueda hacer de ello con la tecnología, con la adopción de mecanismos, plataformas y programas, en función de brindar mayor seguridad a los datos y la información, evitando la presencia de acciones delictivas que afecten la rentabilidad, la confidencialidad de las cuentas y de los mismos usuarios de los servicios financieros.

El desarrollo organizacional[14] varía en función de los resultados obtenidos en cada una de las áreas funcionales. Un aspecto que demanda no sólo certeza en las cifras, sino innovación, seguridad, agilidad en el desarrollo de las operaciones contables, financieras, comerciales y productivas, sin perder de vista desde luego, la importancia que tienen las nuevas tecnologías y los procesos en el blindaje a través de estrategias y programas, en los resultados obtenidos por periodo de evaluación y análisis.

> "El conocimiento del grado de dominio de las competencias de TI requeridas por un profesional contable se convierte en un elemento fundamental para gestionar la información y el saber dentro de una organización. Las empresas actuales, requieren profesionales de la contabilidad capaces de potencializar los beneficios de las TIC con la finalidad de generar ventajas competitivas". (Chan et al., 2021, p. 9)

El tema de las comunicaciones y las nuevas tecnologías, dejan entrever la importancia y la necesidad planteada por muchas organizaciones, frente al quehacer empresarial y donde lo contable y lo financiero, demanda mayor preparación y formación frente al buen uso de la información, al delito generado en las redes, a la inclusión de procedimientos y acciones que le garantice a los clientes y usuarios, la seguridad en el manejo de sus datos y cuentas.

Implica esto que, la dirección administrativa debe enfocar y definir el uso responsable de las redes tecnológicas y de los procedimientos, enfocados desde fuego a optimizar la misma operatividad empresarial, pudiendo ser ello una ventaja competitiva que llame la atención de

[14] "Proceso de conocer y cambiar la salud, la cultura y el desempeño de la organización. Está diseñado para mejorar las habilidades, el conocimiento y la efectividad individual de una empresa en términos de todos sus objetivos" (Inzua, 2020, p. 1).

quienes ser convierten en clientes y/o usuarios, y de esta manera aportar al crecimiento y fortalecimiento institucional, a mejorar su credibilidad, confianza en los profesionales que apoyan la labor contable como financiera, pero ante todo a renovar la imagen y confianza lograda gracias a la buena gestión, a su compromiso con el buen manejo de los recursos, pero sobre todo a mantener un buen panorama de reciprocidad entre los grupos de interés.

> "Las tecnologías de la información y la comunicación representan para el profesional contable una oportunidad de crecimiento y de competitividad en este mundo globalizado. La influencia de estas en los procesos financieros de las organizaciones ha generado que las empresas, las universidades, el Estado y demás organismos que regulan la profesión contable requieran de personas empoderadas de todas las actividades que se realizan en las entidades de negocios, con una visión estratégica, innovadoras, con capacidad de análisis, liderazgo en procesos y en costos, comunicación asertiva y habilidades en el manejo de un lenguaje jurídico". (Carmona y Muñoz, 2020, p. 6)

Hoy en día, han ido en aumento las empresas y organizaciones que ven en el uso de las tecnologías, una oportunidad para no sólo generar bienes y servicios de calidad, basados en las necesidades y expectativas del entorno, sino a buscar un mayor acercamiento con el cliente y/o usuario, encontrando en esta analogía, respuestas a posibles falencias e inconvenientes en el ejercicio empresarial, especialmente en el plano financiero y contable dada su vulnerabilidad y representatividad en las finanzas organizacionales como empresariales.

Sin embargo, en la actualidad existe cierta renuencia de algunas empresas y entornos frente a la adopción de mecanismos y estructuras tecnológicas, por cuanto son cada vez más los delitos y fraudes generados desde las redes, que afectan la credibilidad, confianza y seguridad, especialmente de las pequeñas y medianas empresas, lo que sugiere una reevaluación de los procedimientos, así como la toma de decisiones desde lo contable y lo financiero.

> "En el contexto de la administración en la era digital, las Tecnologías de la Información y la Comunicación (TIC) se presentan como un respaldo fundamental para llevar a cabo diversas tareas en los diferentes departamentos empresariales. En el ámbito de las Pequeñas y Medianas Empresas (pymes), la generación, conservación y transmisión de la información desempeñan un papel esencial en el funcionamiento de la entidad, destacando su importancia, sobre todo, en el ámbito financiero". (Fernández y Urbiola, 2018, citados por Bermeo-Giraldo et al., 2020, p. 26-27)

América Latina no ha sido la excepción, pues día a día se conoce el impacto traído desde las nuevas tecnologías hacia los procesos de información contable como financiera, demandando mayor interés, responsabilidad, compromiso y confidencialidad de los directivos hacia la información de sus clientes, buscando mitigar el daño generado desde las nuevas plataformas, dado el crecimiento de suplantaciones, fraudes[15], desvío de recursos, afectación y alteración de las cuentas, saqueo de las mismas, entre otras más acciones perpetradas por delincuentes que conocen del uso de dichos sistemas.

Permite esto entender, que no basta sólo con actualizar y tecnificar a las organizaciones, la tarea va mucho más allá, es decir, el anticiparse a los eventos y resultados generados que pidieran afectar la estabilidad organizacional, lo que indica que las nuevas tecnologías traen consigo un sinnúmero de ventajas y oportunidades, aunque a la vez crea incertidumbre respecto a las acciones fraudulentas que pudieran derivarse por un uso indebido, especialmente en el contexto financiero y contable donde su uso se ha masificado.

> "Según Ontiveros, Álvaro, Navarro y Rodríguez (2012), las Tecnologías de la Información y la Comunicación (TIC) representan el principio esencial para la automatización de tareas, brindando respaldo a las funciones del ámbito financiero. La integración de las TIC con este sector es tan profunda que resulta difícil observarlos de forma independiente. La aplicación de las TIC en este entorno ha transformado la manera en que se registran y ejecutan las tareas operativas, utilizando instrumentos y programas que se caracterizan por ser sistemas de información donde la disponibilidad de datos es puntual y precisa para la toma de decisiones (Díez, 2008). Además, la interacción directa con diversos actores a través de las TIC, como proveedores, clientes, administraciones públicas y entes reguladores, posibilita mantener actualizada la información financiera (Acosta y Navarrete, 2013)". (Bermeo-Giraldo et al., 2020, p. 30)

Las alertas respecto al uso indebido de las nuevas tecnologías, están a la orden del día, pues más allá de facilitar el desarrollo de las operaciones financieras para las empresas, entidades y los mismos clientes por su misma interacción, facilita la comisión de todo tipo de delitos, afectando desde luego las finanzas organizacionales, la imagen y la credibilidad de ellas en el entorno.

---

[15] "La palabra fraude viene del latín FRAUD, que consiste en una acción que resulta contraria a la verdad y a la rectitud, el fraude se comete en perjuicio de una persona u organización, también es considerado como la utilización de una conducta deshonesta o engañosa con el fin de obtener alguna injusta ventaja sobre otra persona u organización" (Linares, 2011, p. 3).

Por ello, funciones como el control y la auditoría[16] se han convertido en herramientas valiosas para muchas empresas, toda vez que a través de ellas se logra la detección oportuna de errores y eventuales afectaciones y daños a los sistemas, así como la vulneración de las redes de información, la obtención de claves, datos y recursos, donde se cuestiona la seguridad como factor preventivo.

> "En el ámbito del control y gestión de la información financiera, destaca la facturación electrónica como un método destinado a eliminar la labor manual en la emisión y recepción de facturas. Su objetivo es minimizar errores en el proceso, garantizar la seguridad e integridad en el acceso a los datos, así como agilizar y automatizar la generación de informes para facilitar un análisis y control más efectivos". (Díaz-Córdova et al., 2016, citados por Bermeo-Giraldo et al., 2020, p. 34)

No obstante, el desarrollo de estas tecnologías, abre la posibilidad para muchos delincuentes, de ingresar a datos e información confidencial en muchas de las empresas, poniendo en evidencia la vulnerabilidad y la falta de controles a los procesos a nivel interno, creando incertidumbre y duda a la hora de acceder a estas plataformas.

Ante ello, Latinoamérica y muchos países en el mundo, han definido convenios para afrontar esta realidad y problemática a la vez, buscando acciones, alternativas y mecanismos que les permita disminuir los daños y afectaciones como limitar el acceso de los delincuentes a muchos sistemas de información y de datos de las empresas, por cuanto ello afecta su imagen, credibilidad y seguridad, y por ende su permanencia y crecimiento en el mercado.

> "De acuerdo con la información en el sitio web de la ONU, a junio 2021, 66 Estados ya forman parte del Convenio (países europeos, Argentina, Australia, Canadá, Cabo Verde, Chile, Colombia, Costa Rica, Estados Unidos de América (EUA), Filipinas, Ghana, Israel, Japón, Mauricio, Marruecos, Panamá, Paraguay, Perú, República Dominicana, Sri Lanka, Senegal y Tonga, otros 2 países ya lo firmaron (Irlanda y Sudáfrica) y 9 países han sido invitados a adherirse (Benín, Brasil, Burkina Faso, Guatemala, México, Nueva Zelanda, Níger, Nigeria y Túnez)". (Departamento Contra la Delincuencia Organizada Transnacional [DDOT], 2022, p. 6)

[16] "La Auditoría de Gestión se define como el mecanismo dispuesto por los organismos de control externo, para examinar y evaluar las actividades realizadas, en un sector, entidad, programa, proyecto u operación, con el fin y dentro del marco legal respectivo, de determinar su grado de eficiencia, eficacia y economía, y por conducto de las recomendaciones que al efecto se formulen, promover la correcta administración del patrimonio público o privado" (Maldonado, 2015, citado por Intriago, 2022, p. 8).

Afortunadamente, se ha ido creando conciencia respecto a la necesidad que tienen las organizaciones de establecer controles y mecanismos que imiten la acción de delincuentes que buscan una oportunidad a través de las redes informáticas[17] para acceder a la información confidencial de las organizaciones y llevar a cabo todo tipo de delitos como los fraudes, las suplantaciones, la desviación de recursos, incluso superando fronteras, convirtiendo el hecho en algo de carácter trasnacional.

Es así como muchos de los países a nivel latinoamericano como europeo, han ido tomando conciencia a través de convenios y acuerdos con respecto a la necesidad de plantear soluciones y tomar acciones de tipo administrativo, legal y procedimental, que lleven a una disminución de los delitos de orden informático en cuanto desvirtúa la importancia de las nuevas tecnologías de la información y las comunicaciones en los procesos empresariales y en su manejo financiero y contable

En el convenio se establecen las medidas que deberán adoptar los países con relación a los delitos cibernéticos, categorizados de la siguiente forma:

> "1. *Delitos contra la confidencialidad, la integridad y la accesibilidad (Triada CIA) de los datos y sistemas informáticos*: acceso ilícito a sistemas informáticos, interceptación ilícita de datos informáticos, interferencia en el funcionamiento de un sistema informático y abuso de dispositivos que faciliten la comisión de delitos.
>
> 2. *Delitos informáticos*: Falsificación informática mediante la introducción, borrado o supresión de datos informáticos, fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
>
> 3. *Delitos relacionados con el contenido*: Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.
>
> 4. *Delitos relacionados con infracciones de la propiedad intelectual y derechos afines* (copia y distribución de programas informáticos, o la piratería informática)". (DDOT, 2022, p. 6-7)

En materia financiera, la adopción de medidas de ajuste, ha permitido enfrentar de manera diligente las acciones por ciberdelitos[18] donde se desparece la información de los clientes, se

[17] "Una red informática está constituida por un conjunto de ordenadores y otros dispositivos, conectados con o sin cable, con el objetivo de compartir unos determinados recursos. Éstos pueden ser aparatos como impresoras, escáner, etc., o programas que incluyen archivos, carpetas, etc." (Xunta de Galicia, s.f., p. 1).

[18] "Son conductas ilegales realizadas por ciberdelincuentes en el ciberespacio a través de dispositivos electrónicos

interfieren los datos, se suplanta a los tenedores de las cuentas, se generan fraudes, se alteran cifras o se desvían recursos, afectando la credibilidad en las operaciones contables como e las mismas entidades administradoras de los recursos.

Las redes informáticas en este caso, se constituyen en medios de carácter tecnológico que facilitan la operatividad de las organizaciones y entidades, disminuyen tiempos de respuesta a las necesidades y expectativas de clientes y/o usuarios, facilitan la actualización de los datos y por ende, emiten informes en tiempo real y con la absoluta veracidad de las cifras y de la información en general.

> "La Organización de Estados Americanos (OEA) a través Departamento de Cooperación Jurídica Internacional (DCJI) promueve la cooperación jurídica internacional en materia de justicia y lucha contra la corrupción y el fortalecimiento de la cooperación entre los Estados en materia de asistencia mutua penal y combate de los delitos cibernéticos en el marco de la Reunión de ministros de Justicia u otros ministros, Procuradores o fiscales generales de las Américas (REMJA). Adicionalmente, REMJA junto con socios estratégicos procura y coordina capacitaciones para oficiales de gobierno para el enjuiciamiento exitosos de los delitos cibernéticos, talleres legislativos para actualizar las leyes en materia de delito cibernético y para promover mejores prácticas contra los delitos cibernéticos". (DDOT, 2022, p. 7-8)

América Latina ha tenido mayor conciencia respecto a la necesidad de plantear acciones para diminuir el ciberdelito, apoyados en los convenios establecidos entre los países y a través de los cuales se busca diminuir los fraudes perpetrados por las redes y con ayuda de las nuevas tecnologías, de manera que se garantices desde todos los contextos, el buen uso de los servicios financieros[19], impidiendo de alguna manera, la carrera de la delincuencia trasnacional[20].

---

y redes informáticas. Consiste en estafas, robos de datos personales, de información comercial estratégica, suplantación de identidad, fraudes informáticos, ataques como cyberbulling, grooming, phishing cometidos por ciberdelincuentes que actúan en grupos o trabajan solos" (Ministerio de Justicia Argentino, 2023).

[19] "Los servicios financieros son servicios de intermediación mediante los cuales se genera valor a través del dinero. Estos servicios los prestan los bancos y otras entidades financieras, las compañías de seguros, las sociedades gestoras de fondos y los mercados de valores" (Díaz y López, s.f., p. 5).

[20] "La delincuencia organizada transnacional abarca prácticamente todos los actos delictivos graves de carácter internacional perpetrados con fines de lucro y relacionados con más de un país. Hay muchas actividades que pueden calificarse de delincuencia organizada transnacional, entre ellas el tráfico de drogas, el tráfico ilícito de migrantes, la trata de personas, el blanqueo de capitales, el tráfico de armas de fuego, productos adulterados, flora y fauna silvestres y bienes culturales, e incluso algunos aspectos de la delincuencia cibernética" (Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], s.f., p. 1).

En este caso, se hace necesario y prudente a la vez, el estudio de la legislación existente, conociendo las acciones frente a los delitos generados en las redes de información tecnológica, validando permanentemente el segmento contable como financiero, aportando así a la seguridad y cooperación demandada entre las naciones afectadas, redoblando los esfuerzos frente al seguimiento de las actividades mediante la inclusión de nuevos mecanismos de detección fraudulenta.

4. Delitos Informáticos en América Latina en Materia Contable

El desarrollo tecnológico en el mundo en los últimos años, ha incidido ampliamente en los entornos empresariales como un recurso de interacción social, financiera y comercial, permitiendo que exista mayor reciprocidad entre los grupos de interés, facilitando el conocimiento sobre las necesidades y expectativas, abordando responsablemente el uso de las redes de información, formando a los colaboradores de manera que se logre una sustitución manual por una tecnificada que agiliza el desarrollo de las actividades y por lo mismo, concientizando a la sociedad en general para que haga uso de ellas.

Sin embargo, la misma crisis social y económica generada en el mundo producto de la pandemia por la presencia del Covid 19, puso en evidencia la necesidad de hacer uso de la tecnología como recursos informativos, de atención, establecimiento de relaciones comerciales, gestiones y pagos, transferencias, entre un sinnúmero de opciones que le permitieron al mundo entero, enfrentar el desafío del confinamiento con la mayor tranquilidad y agilidad.

> "El empleo de la informática a nivel global ha experimentado un aumento notable y ha adquirido una importancia significativa en la sociedad. La simple oferta de servicios que facilitan la vida de los usuarios, especialmente en términos de comunicación e información, convierte a la informática en una herramienta útil y, en muchos casos, indispensable". (Márquez y Mousalli, 2016, citados por Acosta et al., 2020, p. 354)

Esa simplificación de tareas como lo menciona el autor, ha sido objeto de cuestionamientos desde las mismas organizaciones y la sociedad en general, dada la vulnerabilidad a la cual se exponen y que ha llevado a que muchos de ellos desistan de la tecnología y la virtualidad[21] como opción de intercambio de información.

Sin embargo, muchas entidades y empresas, han mantenido la idea de hacer parte fundamental de las relaciones existentes, la tecnología como recurso valioso, ágil y oportuno, en la medida que favorece las transferencias y la información de productos y servicios, pero a la vez cuestionan el hecho de perder la privacidad por la ciber delincuencia y todo lo que ello implica.

[21] "La palabra Virtualidad proviene desde los orígenes de Platón cuando comenta que el conocimiento se genera por medio de las ideas y de imágenes que el hombre capta de su contexto. Sí el hombre tiene la capacidad de imaginar y de contextualizar la realidad; entonces la palabra virtualidad significa que por medio del proceso imaginario permite al hombre entrar en otro proceso que es el de aprendizaje; por medio de él podemos transformar la realidad y a su vez 7 entenderla" (Martínez et al., 2014, p. 6).

> "Cuando la gerencia aborda la gestión de riesgos, es crucial dirigir su atención hacia el ámbito informático. Es necesario que estén conscientes del riesgo tecnológico, las amenazas cibernéticas y las deficiencias en los sistemas, ya que estos factores también representan una amenaza para el logro de los objetivos organizacionales y, en consecuencia, para la continuidad del negocio". (Peralta y Aguilar, 2021, p. 103)

No cabe duda que la revolución informática[22] ha creado una nueva realidad en la forma de establecer las relaciones empresariales, pero a la vez plantea una serie de cuestionamientos sobre la facilidad con la cual los delincuentes, acceden a datos e información sin autorización alguna, poniendo en riesgo la tranquilidad, seguridad y estabilidad emocional de las personas.

Pero quizá lo más preocupante en este caso, es que sean las organizaciones, las llamadas a definir mecanismos y acciones para garantizar la confidencialidad de los datos y la información, pues quienes han desarrollado las plataformas, se eximen de la responsabilidad frente a su manejo y buen uso de los recursos informáticos proporcionados para el mejoramiento de la calidad, en las diferentes operaciones llevadas a cabo por las organizaciones.

> "En la medida que las nuevas tecnologías de la información y las comunicaciones involucran innumerables recursos tecnológicos y humanos, los delitos que atentan contra los sistemas y datos informáticos pueden ser cometidos por cualquier persona, que no solo lo haría sin el consentimiento del titular de los datos o violando las medidas de seguridad adoptadas por el operador de la información, sino también sobre los elementos de seguridad internos del software o hardware". (Garzón y Cuero, 2022, p. 207)

Es evidente que el tratamiento de datos al que hacen referencia muchas organizaciones que ven en las redes la mejor oportunidad para comercializar bienes y servicios, suele estar expuesto a fallos y vulneraciones, que demandan día a día mayor atención por parte de las empresas y entidades, so pena de incurrir en sanciones por parte de las mismas superintendencias y de la sociedad en general.

Implica esto que, se requiere de controles y seguimientos a los diferentes procesos donde se comparte datos e información de las personas y de las mismas organizaciones, pero además de

[22] "La revolución tecnológica de los últimos 50 años ha sido un elemento determinante en el nivel de globalización al que estamos asistiendo hoy en día. En especial, el desarrollo de la informática ha revolucionado las formas de comunicación al grado que, prácticamente, ha impactado en todos los órdenes de la vida individual y social. Así, la informática se ha convertido en un factor democratizador de primer orden al poner al alcance de millones de personas un instrumento formidable de comunicación, de información y de acceso al conocimiento que hasta hace apenas unas décadas era impensable que se desarrollara de la forma en que lo ha hecho" (Arce, s.f., p. 1).

ello, realizar seguimientos a quienes hacen parte de las mismas organizaciones y a quienes se les comparte información como un recurso de control y verificación continua y evitar así que existan delitos informáticos.

> "Los incidentes de actividades ilícitas en el ámbito informático están experimentando un aumento constante, representando una amenaza para la privacidad de la información de individuos o entidades. En muchas ocasiones, esto se debe a la falta de precaución en cuanto a la protección de los datos. Por tanto, es de suma importancia implementar sistemas de seguridad efectivos para salvaguardar la información. En última instancia, el análisis de las legislaciones en diversos países revela que, a pesar de contar con leyes al respecto, persisten lagunas legales que impiden atribuir responsabilidades judiciales directas a los perpetradores de delitos cibernéticos". (Acosta et al., 2020, citados por Peralta y Aguilar, 2021, p. 104)

El Estado además de regular la actividad ilícita de los ciberdelincuentes, está en la obligación de generar mecanismos para controlar el uso de los medios informáticos y de las comunicaciones, de manera tal que no se afecten las finanzas en este caso, y la rentabilidad de las organizaciones donde usualmente se producen robos, desvíos de recursos, suplantaciones de identidad con fines criminales, entre otros aspectos.

Es necesario entonces, que se blinde la información suministrada por los clientes dentro de las organizaciones por parte de los empleados y funcionarios, evitando el robo de datos, recordando a las personas, la necesidad de mantener la confidencialidad y privacidad en tanto se podría afectar la seguridad física como de los recursos de los clientes en este caso, permitiendo que se les amenace y vulnere sus derechos.

> "Cada día los delitos informáticos van tomando auge en todos los niveles cibernéticos. Los infractores crean y activan diferentes modalidades que les permitan delinquir tales como, el hurto, estafas, chantajes, entre otros, perjudicando de manera fehaciente la privacidad e identidad de cualquier persona o entidad. La necesidad de instaurar sistema de seguridad, que permita el resguardo de la información, cada día toma más relevancia, sobre toda cuando la información que se maneja es de primera línea". (Acosta et al., 2020, p. 365)

Es evidente que, en todo contexto normativo, suelen observarse vacíos respecto a la aplicabilidad de la legislación, llevando a que los casos de corrupción[23], suplantación, fraudes y

[23] "Se concibe mejor como una forma deficiente de hacer las cosas cuando se considera que las formas éticamente superiores no se encuentran disponibles, son defectuosas o demasiado costosas. De no colapsar, la corrupción puede

desvío de recursos en el plano financiero, aumente a la par con las afectaciones a empresas y personas.

Significa esto que, el Estado debe legislar frente al uso responsable de las redes, de los recursos tecnológicos, no sólo definiendo aspectos de orden administrativo sino aquellos factores donde se involucra el contexto contable y financiero, toda vez que es allí donde en mayor grado confluyen delitos que afectan tanto el orden productivo como rentable e incluso competitivo.

> "Cuando se habla de delito informático, Fuentes, Mazún y Cancino (2018) la definen como el conjunto de comportamientos que genera delito penal y, que debe ser tratado legalmente ya que el mismo tiene por objeto daños a terceras personas, ocasionando diferentes lesiones y, en algunos casos pérdidas de bienes jurídicos. Es necesario aclarar, que este tipo de delitos suceden en el ciberespacio (figura 1)". (Acosta et al., 2020, p. 355)

Existen en este caso, elementos suficientes para entender la necesidad que tiene el mercado latinoamericano de definir acciones que lleven a una disminución de los delitos informáticos, entendiendo que se trata de una situación trasnacional donde se evidencian afectaciones a las finanzas y al orden contable de las empresas, entidades y organizaciones, incluso de los clientes y usuarios, generando caos, incertidumbre y una marcada inseguridad.

---

conducir a un patrón tenaz de comportamiento no ético que se sostiene y repite durante muchos años" (UNODC, s.f., p. 9).

Figura 1

Tipos de delitos informáticos.

Fuente: Acosta et al., 2020, p. 357.

Aunque, a decir verdad, existen daños de mayor gravedad que debieran ser contextualizados y analizados por quienes administran el sistema financiero y tecnológico, y donde se involucra a los clientes y usuarios, lo que sugiere una mayor familiaridad con las ventajas, pero también con los riesgos al hacer uso de las plataformas digitales[24] y efectuar así sus operaciones contables basados en aplicaciones diversas de una manera mucho más ágil y aparentemente segura.

Dentro de este tipo se delitos que suelen presentarse en el contexto latinoamericano, se conocen entre otros los siguientes:

"- *El acceso no autorizado:* no se tiene acceso sin derecho a un sistema o a una red cualquiera, violándose todas las medidas de seguridad existentes. Generalmente son operadas por genios de la informática conocidos como **crackers.**

- *El daño a los datos o programas informáticos:* es la eliminación o barrado total, descomposición, deterioro o erradicación de los datos o de los programas informáticos, sin que la persona ejecutante tenga derecho o acceso a realizar esa acción.

- *El sabotaje informático:* va direccionado a la alteración y eliminación total de datos o programas. Producen una interferencia, para bloquear los sistemas informáticos con la finalidad de obstruir el funcionamiento de las redes en su totalidad.

[24] "Las plataformas digitales o virtuales son soluciones online que permiten y facilitan la realización de diversas tareas en un mismo lugar por medio de Internet, permitiendo la optimización de recursos y tiempo" (Arroyo, s.f., p. 4).

- *La interceptación no autorizada:* se refiere a la captación que se realiza sin autorización previa, tomando en consideración mecanismos tecnológicos tradicionales.
- *El espionaje informático:* es la adquisición, revelación y transferencia de información cibernética, de tipo confidencial, comercial; sin permiso o autorización del propietario de la información, con el propósito de causar pérdidas económicas o de obtener algún beneficio oneroso". (Lara et al., 2014, citados por Acosta et al., 2020, p. 356)

Basta con analizar cada una de estas características, para entender no sólo la realidad de muchos países en Latinoamérica frente al tema de los delitos informáticos, sino que ello crea una mayor preocupación e incertidumbre en materia contable y financiera, debido a los eventuales movimientos que se pueden generar desde las mismas plataformas y donde en reiteradas ocasiones, se presentan robos, fraudes, alteración de las cuentas y lo más grave: la usurpación de la identidad[25] y de la confidencialidad de los clientes y de sus manejos financieros.

Existe desde luego una llegislación contable aplicable al tema de los delitos informáticos a nivel internacional y en especial en los países latinoamericanos, que dan cuenta de la importancia dada al tema de los delitos informáticos y de los riesgos que corre el sistema contable y financiero, lo que ha llevado a que muchos de ellos, legislen frente al tema, buscando un blindaje frente a tales actuaciones y comportamientos, pudiendo detener su impacto, sancionar tales conductas y judicializar a quienes vulneran las redes para obtener la información.

Tabla 2

Legislación latinoamericana en materia de delitos informáticos.

País	Ley	Objetivo
Brasil	Código Penal (Decreto-Ley Nº 2.848, 7 de diciembre de 1940 y sus numerosos cambios a lo largo de los años).	Tipos penales que aplica en el campo de los delitos cibernéticos: 154-A y sus párrafos (piratería de dispositivos informáticos) - para varios casos de delitos de alta tecnología y algunos casos de fraude bancario electrónico; art. 155, §4, B y C (robo por fraude por dispositivo electrónico o informático) - especialmente para casos de fraude bancario electrónico, 158 (extorsión) - especialmente para ataques de ransomware, Art. 171, §2º A y §2º B (estafa/fraude electrónico).

[25] "La usurpación de la identidad, entendida como la suplantación del titular de un derecho o crédito por un impostor para obtener un beneficio injusto, recibe cada vez más atención en materia de fraudes cometidos con la ayuda de las tecnologías de la información. Las consecuencias de la suplantación rebasan en muchos casos la pérdida económica directa del titular del derecho afectado, para comprometer su historia crediticia, su prestigio y hasta su identidad social" (Gabaldón y Pereira, 2018, p. 164).

	Ley de Lavado de Activos (ley N° 9.613, 3 de marzo de 1998	
Chile	Ley N° 21.459, vigente desde el 20 de junio de 2022	Legislación sobre ciberdelitos
	Ley N° 20.009	
Costa Rica	Sección del Código Penal	Delitos Informáticos, así como en el Convenio de Budapest.
	Proyecto de ley para crear una ley especial	
Guatemala	Iniciativa de Ley Número 4055	Delitos Informáticos
Bolivia	*Nomen Iuris* (art. 363 Bis., art. 363 Ter.)	Manipulación informática y Alteración, acceso y uso indebido de datos informáticos
Argentina	Ley 25.930 y su Decreto Reglamentario PEN 1232/2004	Incorpora una disposición vinculada a la defraudación mediante el uso de tarjetas de compra, crédito o débito al Código Penal de la Nación.
	Resolución 234/2016 del Ministerio de Seguridad de la Nación	Protocolo general en la investigación y proceso de recolección de pruebas en ciberdelitos.
México	- Constitución Política de los Estados Unidos Mexicanos - Ley General del Sistema Nacional de Seguridad Pública - Ley General de Transparencia y Acceso a la Información Pública - Ley Orgánica de la Administración Pública Federal - Ley de Instituciones de Crédito (Capítulo IV, Art. 112 Quáter)	
Panamá	No cuenta con legislación sobre ciberdelitos	
Paraguay	Ley 4439/11	
Perú	Ley 30171, de 2014 (modifica la Ley 30096)	Ley de Delitos Informáticos
	Ley 30096	Toma en cuenta el Convenio sobre Ciberdelincuencia de Budapest, ratificado en marzo del 2019 y vigente desde el 01 de diciembre del mismo año
República Dominicana	Resolución del Congreso Nacional núm. 158-12, del 11 de junio de 2012.	Convenio sobre la Cibercriminalidad
	Ley núm. 53-07, del 23 de abril de 2007	Crímenes y Delitos de Alta Tecnología
	Ley núm. 126-02	Comercio Electrónico, Documentos y Firmas Digitales, del 4 de septiembre de 2002
	Decreto núm. 313-22, del 14 de junio de 2022	Establece y regula la Estrategia Nacional de Ciberseguridad 2021-2030
	Resolución de la Junta Monetaria núm. 181101-02, del 1 de noviembre de 2018	Establece el Reglamento de Seguridad Cibernética y de la Información
Uruguay	Ley N° 18600 del 21 de setiembre de 2009	Documento Electrónico y Firma Electrónica

Fuente: DDOT, 2022, p. 9-15.

Tabla 3

Legislación colombiana en materia de delitos informáticos.

Ley	Objetivo
Ley 527 de 1999	Comercio Electrónico. Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones
Ley 1341 de 2009	Define principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones - TIC
Ley 1237 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Circular 052 de 2007 (Superintendencia Financiera de Colombia)	Fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios

Fuente: Elaboración propia.

5. Impacto de los Sistemas de Información Contable vs. los Delitos Informáticos en los Países Latinoamericanos

Las buenas prácticas en la búsqueda de la seguridad informática de la información, se ha venid asumiendo como un mecanismos de protección de los datos por parte de las organizaciones que han involucrado novedosos procedimientos y recursos, buscando mayor agilidad en el desarrollo de las actividades, respondiendo con eficacia a las inquietudes y necesidades de los grupos de interés, de tal forma que se optimicen las decisiones frente a la inversión, financiación, manejo de utilidades, rentabilidad y productividad.

Un hecho que ha marcado a las empresas del nuevo milenio, gracias a que se han ido concientizando respecto a la importancia de generar planes alternativos basados en la innovación, maximización de los recursos y disponibilidades financieras, dando cumplimiento a los objetivos empresariales y competitivos que les permite aumentar su credibilidad y posicionamiento en el mercado.

Tendencias como la globalización, han facilitado de alguna manera el desarrollo organizacional, mejorando los procesos y procedimientos en desarrollo de todas las actividades humanas y empresariales, pudiendo tener mayor certeza con respecto al manejo de las finanzas, al control de las funciones contables, al crecimiento basado en la tecnología, a fortalecer los sistemas de información y las comunicaciones, a engrandecer las profesiones y sobre todo, a fortalecer las relaciones en la sociedad.

Pero, así como llega a tener muchas ventajas, despierta el interés de quienes buscan la vulneración de los sistemas de información de las organizaciones a través de la comisión de delitos informativos donde se pone en riesgo la confidencialidad de los datos y de las identidades con todo lo que ello implica.

Supone ello, la tarea para los estados, de legislar y de crear a través de los grupos de expertos, estrategias y herramientas para salvaguardar tanto la lealtad y credibilidad de la sociedad en las organizaciones, como para sancionar conductas contrarias a las normas, bajo una mayor funcionalidad de los sistemas tecnológicos, anteponiendo la confidencialidad e integridad de las personas, evitando todas las manifestaciones propias del ciberdelito en materia financiera.

“La globalización, las tecnologías de la información y la comunicación (TIC), el Internet y las redes sociales son fenómenos significativos que influyen actualmente en las relaciones

económicas entre países, organizaciones y la sociedad civil en general. A pesar de los avances tecnológicos, la comunicación continua a través de medios informáticos, el aumento de la productividad empresarial gracias a la innovación tecnológica, y el fortalecimiento de las relaciones comerciales, económicas, políticas y culturales entre naciones, también existe una amenaza constante por parte del crimen organizado transnacional (COT), expresada a través de diversas formas de ciberdelito en todos sus aspectos". (Barrios, 2018, citado por Gamba, 2019, p. 5)

En ese creamiento de las organizaciones, el uso de estas herramientas tecnológicas, debe exigir de las organizaciones, el refuerzo de todos sus mecanismos y procedimientos, anteponiendo la seguridad sobre cada recurso informático, blindando la información que reposa en sus bases de datos y sobre la cual, muchos delincuentes saquean cuentas, ingresan a las plataformas y desvían recursos, conocen la realidad financiera, generando todo un caos que pone en tela de juicio la las políticas de seguridad de los recursos y las personas.

A todo ello suele denominársele, delitos informáticos, donde la digitalización[26] de los datos, antes que convertirse en una ventaja para el desarrollo de las actividades dada la facilidad de acceso y de análisis, se advierte como un inconveniente dada la exposición de los datos y de la información.

"Internet está ganando una presencia cada vez más significativa en el ámbito económico, comercial y financiero mundial. En este entorno, las transacciones, acuerdos y flujos de capitales, bienes y servicios se realizan a una velocidad vertiginosa, transformándose en datos digitales que circulan de manera instantánea. Al mismo tiempo, la Red está absorbiendo rápidamente los canales de información, las telecomunicaciones, las comunicaciones entre individuos, la oferta de entretenimiento, cultura y arte, la actividad científica, la difusión de ideas y los medios de comunicación". (Flores, 2015, p. 4-5)

Como se puede observar, la Internet, siendo bien empleada, genera infinidad de ventajas y oportunidades para el crecimiento institucional, mejorando su nivel de competitividad y aceptación, aporta al aumento de la rentabilidad, abre nuevos espacios para la comercialización

[26] "Conjunto de resultados derivados del uso de este formato que cambia tanto la forma de llevar a cabo tareas, la comunicación y el acceso al conocimiento. Estamos ante una tecnología de propósito general cuyo desarrollo con otras ramas aporta conocimientos y técnicas que impactan en los distintos sectores económicos, el empleo, los hábitos de les personas y la propia geopolítica, como estamos viendo en el devenir de las decisiones de EEUU, China y Europa" (Martín, 2019, p. 1).

de los bienes y servicios, acerca al cliente a los bienes y servicios, crea lazos comerciales, facilita la transacción de operaciones, entre otras muchas motivaciones.

El sistema de información[27] contable, por ejemplo, se fortalece aún más al definir mecanismos y procedimientos ágiles, confidenciales, con herramientas eficientes que elevan la calidad de las operaciones. A pesar de ello, se ha ido convirtiendo en un problema para muchos países latinoamericanos, donde los casos de corrupción, desaparición de soportes financieros, blanqueo de capitales, desvío de recursos, afectación de las cuentas, deja en evidencia la vulneración de las bases de datos por la escasa seguridad informática como de capacitación de las personas frente a este tipo de situaciones.

> "Con el avance de la tecnología informática y su influencia en casi todas las áreas de la vida social y empresarial, han surgido comportamientos ilícitos llamados de manera genérica *delitos informáticos*, que han abierto un amplio campo de riesgos y también de estudio e investigación, en disciplinas jurídicas y técnicas, pero especialmente en aquellas asociadas con auditoría de sistemas o auditoría informática". (Ojeda-Pérez et al., 2010, p. 43)

La comisión de delitos es más común de lo que pudiera pensarse en los países latinoamericanos, acciones como las dobles contabilidades, los fraudes, el lavado de activos[28], entre otros más, sobresalen en el entorno, cuestionando las acciones emprendidas por las directivas de las organizaciones y entidades, donde no se prevén los daños y vulneraciones a los sistemas de información.

Países como Ecuador, por ejemplo, han ido definiendo mecanismos jurídicos a través de los cuales se indaga, sanciona y determina responsabilidades a quienes llevan a cabo delitos informáticos, lo que permite entender el compromiso para hacerle frente a la corrupción, la criminalidad, aun cuando no se quiera asegurar que, todos los procesos sean transparentes como se pudiera pensar.

"En Ecuador, los delitos informáticos más comunes incluyen el Pharming y el Phishing,

---

[27] "Conjunto de componentes interrelacionados que recolectan, procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control de una organización. Además de apoyar la toma de decisiones, la coordinación y el control, los sistemas de información también pueden ayudar a los gerentes y trabajadores a analizar problemas, visualizar asuntos completos y crear productos nuevos" (Laudon y Laudon, 2004, p. 8, citados por Murillo y Ospina, 2021, p. 7).

[28] "El lavado de activos es una actividad criminal que busca ocultar el verdadero origen ilícito de los recursos que obtienen los criminales mediante operaciones financieras y no financieras, en las que usan a sectores de la economía de los países -incluido el comercio exterior y el mercado de capitales- para hacerlos parecer lícitos, lo que vuelve a esta una actividad transnacional en la que se involucra a varios países y sus economías" (Ministerio de Justicia y del Derecho, s.f.).

> ambos tipificados y sancionados por la legislación del país. El Pharming implica la suplantación de páginas web oficiales para obtener información, mientras que el Phishing utiliza correos electrónicos para solicitar información personal o bancaria de manera fraudulenta. Estos delitos informáticos comenzaron a ser penalizados en Ecuador a partir de 2009. Sin embargo, desde entonces no ha habido actualizaciones en las leyes, lo que ha generado lagunas normativas y ha contribuido a que algunos delitos queden impunes debido a la falta de regulación". (Villón et al., 2018, citado por Peralta y Aguilar, 2021, p. 112)

Colombia a su vez no ha sido ajena a esta realidad latinoamericana, pues llama la atención, las cifras reportadas frente a las denuncias elevadas a las autoridades con respecto a los delitos de corte informático presentados en diferentes contextos y a los cuales se les hace el seguimiento y el tratamiento correspondiente y en comunión con las disposiciones emanadas en materia penal.

> "Con relación a los delitos registrados en el SIEDCO de la Policía Nacional, para los períodos correspondientes a la vigencia del 2019 al 2021 se registraron 109.503 casos de denuncias bajo los delitos de protección de la información y datos enmarcados en el Código Penal, respetivamente". (Garzón y Cuero, 2022, p. 207)

Tabla 4

Registro estadístico de delitos informáticos.

Año	Cantidad
2019	21.984
2020	46.549
2021	40.970
Total	**109.503**

Fuente: Garzón y Cuero, 2022, p. 207.

En la mayoría de los casos, los países latinoamericanos, recurren a la aplicación juiciosa de la normatividad existente, como un mecanismo para hacerle frente a las diversas situaciones generadas desde la ilegalidad y que demuestran tanto el compromiso como la seriedad con la cual se asumen los retos por la transparencia, la moralidad[29], la ética, la legitimidad de las

[29] "Mientras que algunos principios morales parecen ser transcendentes en cuanto al tiempo y la historia, como la equidad, en términos generales la moralidad no es estática. La moralidad describe los valores que comparten un grupo o sociedad en un punto específico de la historia" (Ethics Unwrapped, 2024).

actividades, la imparcialidad en los procesos de toma de decisiones, pero sobre todo para brindarle mayor seguridad y protección a las finanzas.

El derecho penal en este caso, es el llamado a definir procedimientos y sanciones drásticas que, desde la legalidad, sancionen tales conductas delictivas, definiendo a la vez mecanismos de aplicación y fortalecimiento de la seguridad informática, donde los sistemas de información contable lleguen a ser inquebrantables, definiendo de manera conjunta, planes de mitigación entre los países como una forma de hacerle frente a la problemática.

> "El desafío para los países en el ámbito de su marco jurídico, especialmente en el contexto del Derecho Penal Moderno, no se limita únicamente a perseguir y sancionar las formas tradicionales de delitos, sino que implica abordar más allá de la afectación a bienes jurídicos. Esto se debe a la necesidad de integrar criterios dogmáticos para imputar responsabilidad, implementar medidas de política criminal, establecer mecanismos procesales y utilizar técnicas de investigación que proporcionen garantías, pero que al mismo tiempo sean efectivas frente al intrincado entorno del delito informático y la criminalidad organizada. Estas últimas han generado modalidades sofisticadas de ataques a bienes jurídicos, como es el caso de la transferencia no autorizada de activos". (De Luarca y Saavedra, 2007, citados por Guerrero y Castillo, 2017, p. 30)

Habría que analizarse en este caso, si los procedimientos contables como de salvaguarda de la información, resultan ser eficientes y oportunos a la luz de los reiterados casos delictivos, donde se pone en tela de juicio la aplicación diligente de la norma, de tal forma que se realicen las adecuaciones pertinentes y se disminuyan las afectaciones a los sistemas de información contable a nivel global dentro del cual se hace mención al **Acuerdo de Budapest**[30].

En ese orden de ideas, el unir esfuerzos frente al uso responsable de los sistemas informáticos, demanda mayor atención de los países latinoamericanos para definir reglas de juego consistentes, apoyadas en el ordenamiento jurídico y de esta manera, enfrentar la ciber

[30] "El Convenio sobre la Ciberdelincuencia ("Convenio de Budapest") se considera la norma internacional más completa hasta la fecha, ya que proporciona un marco integral y coherente en contra del ciberdelito y la evidencia electrónica. Sirve como una guía para cualquier país que desea desarrollar una legislación nacional integral sobre ciberdelitos y como un marco para la cooperación internacional entre los Estados Parte de este tratado.

El Convenio de Budapest prevé: (i) la criminalización de la conducta, que va desde el acceso ilícito, ataques a la integridad del sistema y de los datos hasta el fraude informático y los delitos relacionados con la pornografía infantil; (ii) herramientas de derecho procesal para hacer más efectiva la investigación relacionada con ciberdelitos y la obtención de evidencias electrónicas; y (iii) una cooperación internacional más ágil y eficiente. El tratado está abierto para la adhesión de cualquier país" (Consejo de Europa, 2021).

delincuencia, especialmente cuando se altera la estabilidad contable de las organizaciones y entidades.

> "Mediante esta técnica [cooperación internacional] es posible lograr una armonización del Derecho sustantivo, así como en el ámbito procesal, que redunda definitivamente en un alivio de la singular incertidumbre que rodea los tipos ciberdelictuales. Para lograrlo, la cooperación internacional, que se materializa principalmente a través de convenios internacionales, deberá reunir unos requisitos mínimos cualitativos. **El Convenio sobre la Cibercriminalidad del Consejo de Europa** se presenta como la única solución internacional existente para el tratamiento de la cuestión ciberdelictual. A pesar de sus deficiencias, se convierte en una adecuada herramienta para la armonización legislativa interestatal y la lucha contra el ciberdelito". (Díaz, 2010, p. 169)

Colombia a diferencia de países como Panamá, cuenta afortunadamente con una regulación frente al comercio electrónico[31] y el uso de lineamientos frente a la digitalización de la información, pues define tanto el acceso como el uso de la información de los datos[32], de las TIC, determinando los elementos mínimos para garantizar la calidad y seguridad de la información que se establece en las redes.

Gracias a esto, se han tomado decisiones respecto a la formación en temas específicos como los delitos informáticos, su control, auditoría, garantizando la confidencialidad de los datos presentes en los sistemas de información contable que han sido digitalizados y de esta manera, disminuir el riesgo, efectivizando planes de mitigación del impacto generado como recursos de prevención

> "En el contexto colombiano y en comparación con otros países de la subregión, los progresos notables en términos de acceso a internet y tecnologías de la información y comunicación (TIC) han tenido un impacto significativo en el aumento de la participación en redes sociales, el comercio electrónico y diversas transacciones en línea, especialmente en el ámbito

[31] "El Comercio Electrónico se puede definir como cualquier forma de transacción comercial en la que un suministrador provee de bienes y servicios a un cliente a cambio de un pago, donde ambas partes acceden a través de Internet en lugar de hacerlo por un intercambio físico directo. En definitiva, el Comercio Electrónico supone comprar y/o vender productos y servicios a través de Internet" (Diputación Foral de Bizkaia, 2001, p. 3).

[32] "*Artículo 269A: Acceso abusivo a un sistema informático.* El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes" (Ley 1237 de 2009).

> financiero. Este desarrollo ha propiciado un aumento en la incidencia de delitos informáticos en todas sus formas, requiriendo que el Estado y las autoridades establezcan normativas y bases sólidas para la persecución de actividades delictivas y la imposición de sanciones ejemplares a los infractores (González, 2011, p. 481-511). No obstante, en la práctica, el ciberdelito, en particular la transferencia no autorizada de activos en el caso colombiano, enfrenta un problema significativo de impunidad". (Guerrero y Castillo, 2017, p. 37)

No con esto se quiera establecer que las nuevas tecnologías de la información y la comunicación, sean perjudiciales para el desarrollo y crecimiento de las economías, por el contrario, amplían las posibilidades para su desarrollo y fortalecimiento de las organizaciones en el mercado, manteniendo su estabilidad y ampliando todo un mundo de posibilidades de acuerdo a las necesidades y expectativas sociales.

Pese a ello, es fundamental que exista una mayor orientación con respecto a su uso responsable, a la prudencia con la cual se digitalizan los datos, a la veracidad de la información, pero sobre todo a la responsabilidad de las empresas y entidades para con la confidencialidad y privacidad de los datos.

> "Las variedades de fraudes que impactan al ámbito bancario y a sus usuarios abarcan desde métodos tradicionales como el fleteo y el taquillazo hasta complejas formas de delitos informáticos. Dentro de esta última categoría, se incluyen prácticas como el phishing (suplantación de sitios web), la instalación de troyanos o software espía para el robo de información, el acceso indebido a sistemas informáticos y la duplicación de tarjetas débito y crédito.
>
> El creciente uso de canales electrónicos para realizar operaciones bancarias y los progresos tecnológicos que facilitan a los delincuentes adquirir herramientas y establecer conexiones con organizaciones ilegales en diferentes territorios son factores que contribuyen a la tendencia en aumento de los ataques tecnológicos o informáticos dirigidos a las instituciones financieras". (Castellanos, 2012, p. 2)

6. Conclusiones

El análisis de la importancia de los delitos informáticos en Latinoamérica, sugiere una serie de conclusiones dentro de las cuales se destaca la necesidad de formular planes de acción y de mitigación que les permita a las empresas, mantener en absoluta reserva y confidencialidad los datos de sus clientes.

Existen riesgos frente a la privacidad de los clientes dentro de las organizaciones, un aspecto característico dentro de las economías latinoamericanas, quienes han ido adoptando para su misma operatividad, mecanismos basados en las nuevas tecnologías de la información y las comunicaciones, pero que, por un manejo inadecuado, podrían estar exponiéndolos a amenazas y riesgos por la misma vulnerabilidad de los sistemas de información contable que reposa en las redes.

Es de conocimiento público que las empresas y organizaciones latinoamericanas, cuentan con un sinnúmero de elementos de información que respaldan la credibilidad de los clientes, aunque, a decir verdad, diariamente se exponen a riesgos por pérdida de los datos, uso ilícito para desviar recursos, comisión de fraudes, entre otros aspectos dada la vulnerabilidad para su obtención.

La Contaduría Pública cumple en este caso un papel fundamental, en la medida que le aporta elementos de valor para organizar y elaborar sistemas de información contable acorde con las exigencias organizacionales como de carácter público, pero donde se requiere de un mayor blindaje para evitar su vulneración como accesos no autorizados a la información y los datos.

La cooperación internacional resulta ser una estrategia de un alto valor dentro de la búsqueda de alternativas para mitigar los riesgos por vulneraciones a los sistemas de información contable de las organizaciones, lo que sugiere la definición de nuevos parámetros que garanticen la privacidad de los datos de los clientes y de quienes administran los recursos financieros.

Es válido encontrar que en la mayoría de los pauses latinoamericanos, se han establecido sistemas penales y sancionatorios respecto al tema de los delitos informáticos, permitiendo la detección de eventuales vulneraciones al sistema y una posterior comisión de delitos, que requiere desde luego de un mayor seguimiento a los procesos, retroalimentaciones y adecuación de nuevos dispositivos de seguridad de manera conjunta.

Las actualizaciones del sistema operativo y de los antivirus dentro de las empresas, logran de

manera temporal, limitar el acceso fraudulento a las cuentas de las empresas, aun cuando en muchos de los casos, los infractores de la ley, logra desarrollar programas malware con los cuales, logran traspasar la protección de los sistemas de información contable, llegando a planillas donde efectúan desvíos de dineros, pagos, transferencias, sustrayendo contraseñas, pagando compras en línea y otras de manera presencial, incluso recurren a los cajeros electrónicos para efectuar retiros programados, tan solo por mencionar los de mayor afectación para los clientes.

Los controles y las auditorías dentro de las organizaciones, juegan un papel determinante en los procesos de blindaje de la seguridad y confidencialidad de los datos e información de los clientes y de las cuentas empresariales, donde normalmente se definen los procesos organizacionales, buscando la detección de malware a fin de evitar la pérdida de información.

Los sistemas de información contable, se establecen como una medida de organización y control de las operaciones financieras de las organizaciones, de ahí la importancia de administrar y gestionar de manera responsable las cuentas, asignando mecanismos seguros que mantengan la confidencialidad de los datos, de tal manera que no sólo se garantice un servicio con los clientes, sino que además se evite el robo de los datos a través de copias de seguridad como de almacenamiento de la información en la nube, pero administrada por una empresa con trayectoria, seriedad y confidencialidad.

Referencias Bibliográficas

Acosta, M. G., Benavides, M. M., y García, N. P. (2020, enero-marzo). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia (RVG), 25*(89), 351-368.

Aguirre Aguirre, J. C. (2022). *Los procesos y la productividad en la empresa L&M de Seguridad Privada Cía. Ltda. de la ciudad de Riobamba* (Trabajo de Grado). Universidad Nacional de Chimborazo. Ecuador.

Arce Islas, R. (s.f.). *La revolución informática, la cultura de la legalidad, México y Palermo*. Congreso de la Ciudad de México. Recuperado el 26 de enero de 2023 de http://www.ordenjuridico.gob.mx/Congreso/pdf/170.pdf

Arimetrics. (2022). *Qué es Software*. https://www.arimetrics.com/glosario-digital/software

Arroyo Vargas, R. M. (s.f.). *Mundos digitales*. Universidad Autónoma del Estado de Hidalgo. Recuperado el 28 de enero de 2023 de https://repository.uaeh.edu.mx/bitstream/bitstream/handle/123456789/20184/plataformas-digitales.pdf?sequence=1&isAllowed=y

Ayala Ñiquen, E.E. y Gonzales Sánchez, S. R. (2015). *Tecnologías de la información y la comunicación*. Lima: Universidad Inca Garcilaso de la Vega. http://tinyurl.com/mz8sz6mh

Bermeo-Giraldo, M. C., Montoya-Restrepo, L. A., Valencia-Arias, A., y Mejía-Cardona, M. A. (2020, enero-junio). Incursión de las TIC en la gestión de la información financiera en las empresas pyme comerciales: Estudio de caso. *NOVUM, Revista de Ciencias Sociales Aplicadas, 1*(10), 25-41.

Berrones Paguay, A. V. (2020). Influencia de las Tecnologías de Información en los procesos contables de las organizaciones. *Revista de Investigación Sigma, 07*(1), 22-28.

Carmona Henao, F. V. y Muñoz Ruiz, J. A. (2020, diciembre). Influencia de los avances tecnológicos en el ejercicio de la profesión de la Contaduría Pública. *RHS Revista Humanismo y Sociedad, 8*(2), 6-21. https://doi.org/10.22209/rhs.v8n2a01

Castellanos, D. (29 de octubre de 2012). Mitigar el riesgo de fraude es un desafío para las autoridades, la banca y los usuarios. *Semana Económica, 875*. https://marketing.asobancaria.com/hubfs/SemanasEconomicas-2014-2006/Sem_875.pdf

Chan Pereyra, M. A., Martínez Prats, G., y Tosca Magaña, S. A. (2021, julio-diciembre). El

Contador Público en la era digital. *Revista de Investigación Académica sin Frontera*, *14*(36). https://doi.org/10.46589/rdiasf.vi36.424

Consejo de Europa. (4 de junio de 2021). *Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: beneficios*. División de Ciberdelito. https://rm.coe.int/cyber-buda-benefits-junio2021a-es/1680a2e4de

Congreso de Colombia. (5 de enero de 2009). *Ley 1237 de 2009*. D. O. 47223.

Departamento Contra la Delincuencia Organizada Transnacional (DDOT). (16 de noviembre de 2022). *Diagnóstico regional del estado del combate al lavado de activos derivado de los delitos cibernéticos en los países miembros de la OEA*. Organización de los Estados Americanos (OEA). https://tinyurl.com/4p4wamc6

Díaz Ferro, Y. y López Picos, Y. (s.f.). *Estadísticas de servicios financieros*. Universidad de Santiago de Compostela. Recuperado el 27 de enero de 2023 de https://www.usc.es/export9/sites/webinstitucional/gl/institutos/crgi/descargas/ponencia/IEDP_YDIAZ_YOLANDALOPEZ.pdf

Díaz Gómez, A. (2010, diciembre). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *Revista Electrónica del Departamento de Derecho de la Universidad de La Rioja (REDUR)*, (8), 169-203. https://doi.org/10.18172/redur.num8

Diazgranados, H. (31 de agosto de 2021). *Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021*. Kaspersky Lab. https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

Diputación Foral de Bizkaia. (2001, septiembre). *Guía básica para la aplicación de las TICs en PYMES: Comercio electrónico*. http://tinyurl.com/5n7tmnyz

Equipo editorial, Etecé. (12 de agosto de 2022). *Tecnología*. https://concepto.de/tecnologia/#ixzz8Q2H9QVkH

Ethics Unwrapped. (2024). *Ética definida (glosario): Morales*. https://ethicsunwrapped.utexas.edu/glossary/morales?lang=es

Flores Prada, I. (2015). Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia. *Revista Electrónica de Ciencia Penal y Criminología*. RECPC 17-21 (2015).

Flores, M. V. (2016). La globalización como fenómeno político, económico y social. *Orbis, Revista Científica Ciencias Humanas*, 12(34), 26-41.

Gabaldón, L. G. y Pereira, W. (2008, junio-diciembre). Usurpación de identidad y certificación digital: Propuestas para el control del fraude electrónico. *Sociologías*, 10(20), 164-190.

Gamba Velandia, J. A. (2019*). El delito informático en el marco jurídico colombiano y el derecho comparado: Caso de la transferencia no consentida de activos* (Monografía de Investigación). Universidad Externado de Colombia. Bogotá D.C.

Garzón Pulgar, J. O. y Cuero Quiñones, K. S. (2022). Una mirada a la cibercriminalidad en Colombia y su asimilación con los delitos de impacto. *Revista Criminalidad*, *64*(3), 203-225. https://doi.org/10.47741/17943108.373

González Montoya, C., Puerta Castrillón, V., y Chamorro González, C. L. (2021, julio-diciembre). Principales retos de la profesión contable desde las perspectivas económica, digital y científica. *Revista Visión Contable*, (24), 31-57. https://doi.org/10.24142/rvc.n24a3

Guerrero Lozano, B. y Castillo Caicedo, D. P. (2017). *Desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario colombiano* (Tesis de Especialización). Universidad Nacional Abierta y a Distancia - UNAD. Bogotá D.C.

Hewlett Packard Enterprise Development LP. (2024). *¿Qué es la seguridad informática?* https://www.hpe.com/lamerica/es/what-is/it-security.html

IBM. (s.f.). *¿Qué es un ataque cibernético?* Recuperado el 26 de enero de 2023 de https://www.ibm.com/mx-es/topics/cyber-attack

Instituto Vasco de Estadística. (s.f.). *Investigación científica y desarrollo tecnológico (I+D)*. Eustat. Recuperado el 30 de enero de 2023 de http://tinyurl.com/2hkdrxwr

Intriago Alcivar, R. J. (2022). *Auditoría de gestión para mejorar los procesos administrativos en una empresa Agrícola del Cantón Quevedo 2021* (Tesis de Maestría). Universidad César Vallejo. Piura, Perú.

Inzua, F. (2020). *¿Qué es el desarrollo organizacional?* Colegio de Computación e Informática Ejecutivo. https://ccie.com.mx/wp-content/uploads/2020/05/DESARROLLO-ORGANIZACIONAL.pdf

ISOTools Excellence. (28 de febrero de 2014). *ISO / IEC 27010:2012: Gestión de seguridad de la información para las comunicaciones inter-sectoriales e inter-organizacionales*. Seguridad de la Información. https://www.pmg-ssi.com/2014/02/iso-iec-270102012-

gestion-de-seguridad-de-la-informacion-para-las-comunicaciones-inter-sectoriales-e-inter-organizacionales/

Linares Galván, J. E. (2011). *Control interno en la prevención y detección de fraude corporativo*. Universidad Javeriana. https://www.javeriana.edu.co/personales/hbermude/Audire/jelg2.pdf

Mariano Díaz, R. (2021). Estado de la ciberseguridad en la logística de América Latina y el Caribe. *Serie Desarrollo Productivo*, 228. Santiago: Comisión Económica para América Latina y el Caribe (CEPAL).

Martín Quetglas, G. (5 de junio de 2019). *¿Qué es la digitalización?* Real Instituto Elcano. https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/ari64-2019-martinquetglas-que-es-la-digitalizacion.pdf

Martínez Hernández, L. M., Ceceñas Torrero, P. E., y Ontiveros Hernández, V. C. (Coords.). (2014, julio). *Virtualidad, ciberespacio y comunidades virtuales*. Universidad Pedagógica de Durango. http://www.upd.edu.mx/PDF/Libros/Ciberespacio.pdf

Ministerio de Justicia Argentino. (2023, diciembre). *¿Qué es el ciberdelito?* https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito

Ministerio de Justicia y del Derecho. (s.f.). *Lavado activos*. Recuperado el 31 de enero de 2023 de https://www.minjusticia.gov.co/programas-co/ODC/Paginas/delitos-relacionados-lavado-activos.aspx

Murillo Abadía, E. y Ospina Ramírez, W. M. (2021). *Estudio de caso: Implementación de un sistema de información contable en Golcar S.A.* (Trabajo de Grado). Fundación Universitaria Los Libertadores. Bogotá D.C.

Narváez Montenegro, D. B. (2015, abril-junio). El delito informático y su clasificación. *Uniandes Episteme: Revista de Ciencia, Tecnología e Innovación*, *2*(2), 158-173.

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (s.f.). *Delincuencia organizada transnacional - La economía ilegal mundializada*. Recuperado el 29 de enero de 2023 de https://www.unodc.org/documents/toc/factsheets/TOC12_fs_general_ES_HIRES.pdf

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (s.f.). *Herramientas de conocimiento para académicos y profesionales. Módulo 1: ¿Qué es la corrupción y por qué nos atañe?* Recuperado el 30 de enero de 2023 de

https://grace.unodc.org/grace/uploads/documents/academics/Anti-Corruption_Module_1_What_Is_Corruption_and_Why_Should_We_Care_ESP.pdf

Ojeda-Pérez, J. E., Arias-Flórez, M. E., Rincón-Rodríguez, F., y Daza-Martínez, L. A. (2010, enero-junio). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad*, *11*(28), 41-66.

Organización de los Estados Americanos (OEA). (19 de mayo de 2016). *Ciberdelito: 90.000 millones de razones para perseguirlo*. https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/16

Organización Internacional de Normalización. (s.f.). *Progresar rápidamente*. Recuperado el 31 de enero de 2023 de https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/fast_forward-es.pdf

Pardo Moreno, G., Quijano Díaz, A., Felipe Ramírez, H., y Barrera Neira, C. (23 de abril de 2018). La gestión de la ciberseguridad: Un asunto de supervivencia para las organizaciones. *Semana Económica*, *1133*. https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf

Peralta Zúñiga, M. L. y Aguilar Valarezo, D. N. (2021, junio). La ciberseguridad y su concepción en las pymes de Cuenca, Ecuador. *Contabilidad y Auditoría*, *53*(27), 100-125.

Tanque de Análisis y Creatividad de las TIC (TicTac). (2023, abril). *Estudio anual de Ciberseguridad 2022-2023*. Cámara Colombiana de Informática y Telecomunicaciones. https://www.ccit.org.co/estudios/estudio-anual-de-ciberseguridad-2022-2023/

Temperini, M. G. I. (2014). Delitos informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. *En 2º Congreso Nacional de Ingeniería Informática / Sistemas de Información*, San Luis, Argentina. http://conaiisi.unsl.edu.ar/ingles/2013/82-553-1-DR.pdf

Universidad Nacional del Sur. (s.f.). *Introducción a la operación de computadoras personales*. Recuperado el 29 de enero de 2023 de https://cs.uns.edu.ar/materias/iocp/downloads/Apuntes/Unidad%201%20-%20Hardware.pdf

Villardefrancos Álvarez, M. del C. y Rivera, Z. (2006, mayo-diciembre). La auditoría como proceso de control: Concepto y tipología. *Ciencias de la Información*, 37(2-3), 53-59.

Xunta de Galicia. (s.f.). *Redes informáticas*. Recuperado el 28 de enero de 2023 de http://centros.edu.xunta.es/ieseduardopondal/ tecnoweb/temas_informatica/redes.pdf