

El desarrollo científico-tecnológico y su impacto en las auditorías y el control de la gestión empresarial

Scientific and Technological Development and its Impact on Auditing and Control of Management

Dra.C. Maricela Arias-Madrazo, marias@uo.edu.cu; MSc. Rafael Domingos-Sapilinha, raulm@uo.edu.cu

Universidad de Oriente, Santiago de Cuba, Cuba

Resumen

La ciencia y la tecnología han sido elementos esenciales en el desarrollo de la sociedad; evidencia de ello es la Informática convertida en factor determinante del progreso en todas las ramas del conocimiento. La relación entre Informática y auditoría es significativa, dada su funcionalidad para supervisar y controlar sistemas y activos, y su empleo como herramienta de trabajo. Por tanto, el objetivo de esta investigación es analizar el papel que juegan los sistemas informáticos en la auditoría, utilizando el método de análisis-síntesis y el histórico lógico, concluyendo que se trata no solo del uso de medios informáticos en auditoría, sino que la Auditoría Informática es factible y posibilita la reducción de costos, mejora la calidad en la información, la prevención de fraudes y la satisfacción social.

Palabras clave: procesos informáticos, auditoría, control, prevención.

Abstract

Science and technology have been essential elements in the development of society; evidence of this is the Computing converted determinant of progress in all branches of knowledge. The relationship between computers and auditing is significant, given its role to monitor and control their systems and assets, and its use as a tool. Therefore, the objective of this research is to analyze the role of information systems in the audit, using the method of analysis-synthesis and logical historical, concluding that it is not only the use of information technology in audit, but the computer audit is feasible and possible to reduce costs, improve quality of information, fraud prevention and social satisfaction.

Keywords: computer processes, audit, control, prevention.

Introducción

El desarrollo de la sociedad está marcado por el uso de las tecnologías de la información, caracterizadas por su constante cambio e inserción en todos los campos de la investigación científica. Su influencia ha trascendido al mundo de los negocios de forma acelerada y amplia, al punto de constituir un eslabón básico de la cadena empresarial. En tal sentido, la Informática no es ajena al campo de la Auditoría, posibilitándole a los auditores encargados de revisar y evaluar los controles contables, activos y patrimonio de la organización, no solo rapidez y eficacia, sino también que al aplicar las tecnologías de la información en las auditorías, se ha obligado a esta a responder con alternativas, a las críticas y cuestionamientos realizados por autoridades e inversionistas, sobre la necesidad y conveniencia de investigar si los principios y normas para la revisión de los sistemas computarizados empleados por los auditores, aún conservan toda su validez y responden a los objetivos de esta ciencia.

Jorge Núñez Jover (1999) alertaba:

El desarrollo científico y tecnológico es una de los factores más influyentes sobre la sociedad contemporánea. La globalización mundial, polarizadora de la riqueza y el poder, sería impensable sin el avance de las fuerzas productivas que la ciencia y la tecnología han hecho posibles. Los poderes políticos y militares, la gestión empresarial, los medios de comunicación masiva, descansan sobre pilares científicos y tecnológicos. También la vida del ciudadano común está notablemente influida por los avances tecnocientíficos (p.3).

El presente trabajo es un acercamiento a la importancia que para la actividad contable y de auditoría tiene la actualización y aplicación de sistemas informáticos, con el objetivo de analizar el papel que juegan estos en la auditoría de las empresas, considerando que el adecuado uso de la Informática mejoraría sustancialmente el proceso contable, aportando entre sus ventajas fundamentales: evitar fraudes contables, aumentar la seguridad y la calidad en la información, disminuir o evitar la fuga de información, preservar los sistemas informáticos, por tanto, evitar pérdidas monetarias en las instituciones, mejorando la satisfacción y la calidad en los servicios, que finalmente se reflejarán en el cliente.

Fundamentación teórica

La Auditoría, según se contempla en la Ley de la Contraloría de la República de Cuba (2009), es el proceso sistemático, realizado de conformidad con normas y procedimientos técnicos establecidos, consistente en obtener y evaluar objetivamente las

evidencias sobre las afirmaciones contenidas en actos jurídicos o de carácter técnico, económico, administrativo u otros, con el fin de determinar el grado de correspondencia entre esas afirmaciones, las disposiciones legales vigentes y los criterios establecidos.

Su origen se remonta (Miranda, 1982) al año 254 a.n.e., cuando se inspeccionaban y comprobaban las cuentas, primeras manifestaciones de auditoría. Su evolución estuvo aparejada a la Contabilidad y al desarrollo de la gran empresa; sin embargo, su progreso tecnológico quedó rezagado.

Ese rezago se manifestó en su limitación a la verificación física de los equipos informáticos y, en alguna medida, a los sistemas, como consecuencia del desconocimiento del profesional de auditoría de estas técnicas, para evaluar evidencias necesarias, relevantes y suficientes, así como dictaminar el uso adecuado de la tecnología en la preservación de la información, los recursos, la gestión y la prevención de fraudes o delitos económicos. Este es un campo pendiente para la Auditoría.

Métodos utilizados

La investigación ha sido posible por la aplicación de los métodos y categorías científicas del conocimiento, en particular el método histórico-lógico y el análisis-síntesis, ambos considerando el contexto histórico de surgimiento y desarrollo de las tecnologías de la información y el papel protagónico de la Informática, por su aplicación en todas las ramas de la ciencia y la técnica; su avance creciente desde los albores de su surgimiento y, en particular, en los sistemas de gestión empresariales. Asimismo se establece la relación entre la Auditoría Informática y la necesidad de implicación de esta ciencia en la prevención de los fraudes y delitos informáticos.

El análisis ha permitido descomponer, por un lado, los conceptos de Informática, delitos informáticos y Auditoría como ciencia en general y, por otro el papel e importancia de la Auditoría Informática para el logro de los objetivos de desarrollo de la Auditoría.

Resultados y discusión

Una necesaria reflexión sobre el vínculo de la ciencia y la tecnología indica lo conveniente que resulta referirse a la ciencia y la tecnología como procesos sociales (Núñez, 1999), que no puede olvidar la educación científica.

En su obra (Núñez, 1999) aborda dos tesis importantes: la primera se refiere a las revoluciones industriales y los profundos cambios tecnológicos que las acompañan,

cambios que conducen a una aproximación creciente con la ciencia, hasta confundirse ambos, en la segunda mitad del siglo XX, por medio de la revolución científica y tecnológica. En este sentido, fundamenta que el paradigma tecnológico que se desenvuelve en las tres últimas décadas ha sido, especialmente, intensivo en el consumo de conocimientos e impactante en términos de su alcance social.

La segunda tesis hace referencia al ascenso del capitalismo y su dominio planetario, afirmado luego de la crisis del socialismo europeo. En este caso, refiere que la consolidación de la ciencia moderna y del capitalismo son dos procesos históricamente paralelos e interconectados. La llamada “mundialización del capitalismo” es un proceso asociado no solo a las fuerzas productivas y a las relaciones de producción que le proporcionan su fundamento, sino también a las pautas de consumo que él promueve y a los modelos de desarrollo que preconiza, a los cuales atribuye una universalidad que sus apologetas consideran imposible de contestar.

A partir del análisis realizado en estas dos tesis y otros elementos desarrollados desde la interioridad de la consolidación de la ciencia moderna y del capitalismo, aclara (Núñez, 1999) que el fenómeno, esencialmente nuevo en la segunda mitad del siglo, es la industrialización de la ciencia, colocando dentro de ella el desarrollo tecnológico.

En los años 40 y 50 del pasado siglo se gestan las bases de la llamada III Revolución Industrial (Fajnzylber, 1983), proceso vinculado a la crisis económica capitalista de fines de los sesenta, caracterizada por el estancamiento económico y la inflación. En esas bases o fundamentos se encuentra el desarrollo de la computación (ya con resultados alcanzados en los Estados Unidos con sistemas de apoyos para estrategias militares), de la energía nuclear y de los descubrimientos básicos sobre el código genético. Esos conocimientos y sus potencialidades productivas, serían movilizados en el contexto de la crisis, buscando potenciar la industrialización.

Hacia finales de los años sesenta se produce la caída del sector industrial expresada en el decrecimiento de la productividad. Se buscan nuevas vías para potenciar el desarrollo dinámico de la misma a partir de la innovación tecnológica, y comienzan los países capitalistas a invertir en innovación y desarrollo (I+D); Estados Unidos de América representó un rol predominante al duplicar los gastos de innovación con respecto al resto de los países desarrollados. Es a partir de este periodo que se consolidó un nuevo paradigma tecnológico cuyas áreas principales son la Biotecnología, los nuevos materiales, la nueva base energética y las ramas de la electrónica, computación y

telecomunicaciones; el liderazgo dentro de estas correspondió al sector electrónico, provocando un avance desconocido hasta la fecha en las tecnologías de la información.

Según Fajnzylber (1983) los objetivos propuestos por los países desarrollados en el plano económico y productivo se alcanzaron. El sector informático determinó cambios de estructura al generar nuevas formas de organización del trabajo, de gestión, de administración pública, de la cultura, y en las interrelaciones humanas. Sin embargo, la Informática no estuvo al alcance de todos los países, incluso inaccesible para algunos sectores dentro de las potencias capitalistas. Se produce una brecha entre los países informatizados y aquellos que no podían acceder a esta, por la calificación de su fuerza laboral y el pobre o escaso poder económico.

Comienza el surgimiento acelerado de un nuevo modelo en las esferas electrónicas, la computación, la Informática y la Biotecnología, como expresión de todo el desarrollo de I+D, al tiempo que se producen cambios en los medios de comunicación, en la cultura, en la conciencia y valores de los grupos sociales en los diferentes países, sin excluir los impactos negativos al medio ambiente, consecuencia del desarrollo de la nueva tecnología.

Por otra parte, en la esfera económica, la globalización de los mercados, el paradigma tecnológico dominante, la competencia entre los grandes bloques económicos y la propia ideología neoliberal, han convertido el tema de la competitividad en el núcleo de las estrategias de empresas, gobiernos e instituciones de investigación. Ser o no ser competitivo resume las opciones de sobrevivencia y triunfo, o fracaso y anulación. La competitividad a su vez descansa en la innovación, es decir, en la “introducción de una técnica, producto o proceso de producción o de distribución de nuevos procesos que con frecuencia puede ser seguido de un proceso de difusión” (Martínez, 1997, p. 516).

Efectivamente, se hizo necesaria para el mundo la introducción de esa nueva técnica; llegó el momento en que el “proceso de difusión” desbordó los límites y barreras existentes hasta entonces y se expandió por cualquiera de las opciones de competitividad. Este desarrollo tecnológico y su introducción cimentada en esa gran competitividad, exigió del control de toda la tecnología de la información, la comprobación de su efectividad y eficacia y el uso racional de los cuantiosos recursos destinados a este fin.

Al margen de este desarrollo, en consonancia con lo antes expresado, referido a la necesidad del control, es inevitable un paréntesis histórico relacionado con la Auditoría,

pues desde su surgimiento hasta la fecha se ha encargado de comprobar el uso racional y destino adecuado de los recursos, la razonabilidad de los estados financieros para emitir una opinión autorizada sobre la eficiencia y eficacia de las actividades de carácter económico, administrativo y productivo de una organización, de la custodia y utilización de sus activos.

Sin embargo, independientemente del desarrollo alcanzado en las tecnologías de la información a nivel de organización y a nivel de la administración pública, en los albores de los años 90 la Auditoría es casi ajena al mundo de la tecnología, tanto en su empleo por los auditores, como en su función fiscalizadora, incluso con los ya impactantes resultados del desarrollo de las llamadas Nuevas Tecnologías de la Información y las Comunicaciones (NTIC), la creciente lucha por el mercado, y las millonarias inversiones en innovación, desarrollo y talento humano y los progresivos fraudes informáticos.

Ese avanzado desarrollo de las NTIC obligó el comienzo de la comprobación de estos sistemas, sobre todo, de aquellos que se diseñaron específicamente para la gestión empresarial, si bien limitado a la verificación y custodia física de los equipos, el acceso a su uso y a los reportes de salida de los sistemas.

Uno de los primeros sistemas de información, inclinados a apoyar la gestión de los negocios, fue el Sistema de planeación de Recursos de la Empresa, (*Enterprise Resource Planning*, ERP) en la década de los 90, sistema que fue inicialmente aceptado como la solución para satisfacer las necesidades de información en todos los niveles de gestión, aunque en la realidad no se demostró, al margen del mérito que representó la integración de sistemas aislados, profesionales, e información de una organización.

La utilidad esperada del ERP no se materializó en la práctica debido, en gran medida, a la resistencia al cambio de las direcciones empresariales; al hecho de que cada cual trabajara en la captación de información desde diferentes plataformas para iguales destinos, pero de forma costosa, inoperante, rígidas y limitadas.

La no generalización de los ERP fue complementado con *Enterprise Performance Management* (EPM), es decir un sistema de gestión de rendimiento empresarial que, ofrecía un conjunto de soluciones especializadas para las funciones de planificación y control de las empresas, aportando herramientas de alertas, análisis, información y, sobre todo, la posibilidad de brindar a los decisores de la organización toda esta información desde la esencia (integración) de la misma. Las bondades que

proporcionaban las soluciones EPM estaban centradas en el desarrollo y control del presupuesto, la contabilidad estratégica, simulaciones financieras con apoyo de modelos estadísticos, indicadores y cuadro de mando integral, control de costos, gestión del proceso de cierre contable, entre otros.

No obstante, estos sistemas se utilizaron en paralelo con otros creados como consecuencia de la competitividad; se introducían nuevos y disímiles sistemas que pretendían, desde la visión de sus creadores, aportar mejoras a la gestión empresarial, y elevar la rapidez, eficiencia, eficacia, calidad y seguridad de los mismos. Sin dejar de reconocer que estos objetivos se alcanzaron por muchos de estos sistemas, la seguridad y vulnerabilidad de los mismos propició el crecimiento de su impacto negativo. Según avanzó la Informática y su aplicación en el campo económico, se desencadenaron los aspectos nocivos, relacionados con el delito informático.

En consecuencia, muchas organizaciones internacionales, de gestión, cibernéticas, de derecho y la propia Organización de Naciones Unidas (ONU) empezaron a tomar en cuenta estos delitos y comenzaron a alertar, registrar, medir, prevenir y a clasificar estos. Dada la variedad de estas clasificaciones, solo se hará referencia a la emitida por las Naciones Unidas.

La ONU clasifica los delitos informáticos en tres tipos fundamentales (Estrada Garavilla, 2008):

1. Fraudes cometidos mediante manipulación de computadoras.
2. Falsificaciones informáticas.
3. Daños o modificaciones de programas o datos computarizados.

Si bien todos estos fraudes representan afectaciones cuantiosas a la economía y a las organizaciones, los fraudes realizados mediante la manipulación de los datos de entrada –los que se manifiestan de dos formas, como alteración de los documentos digitales y mediante el uso de las computadoras para falsificar documentos de uso comercial–, son de los que más impactan en los estados financieros a partir de falsearse la realidad contable.

Es obvio que si se reconoce el impacto y la existencia de los delitos informáticos, debían crearse los mecanismos de control, prevención y el de sanción correspondiente, encaminándose específicamente a la prevención y seguridad, al establecimiento de conceptos, clasificaciones, personal adecuado, objetivos y normativas para este nuevo y necesario tipo de auditoría, no prevista hasta entonces, en las normas y legislación

vigente en cada país, respecto a la actividad fiscalizadora de los recursos informáticos y de tecnología de las comunicaciones de un gobierno e institución. De no concebirse, se estaba limitando la interrelación entre ciencia y técnica y su impacto en el desarrollo social.

Unido a lo anterior, se reconocieron e identificaron otros factores que reclamaron de la un aplicación de la Auditoría Informática, que se rubrican en la medida en que los gobiernos, las leyes, organizaciones empresariales toman conciencia de su importancia. Dentro de los factores que propician la Auditoría Informática se encuentran las políticas internas de la empresa, los altos costos debido a errores, pérdida de información y de capacidades de procesamiento de datos, los que aumentaban la posibilidad de toma de decisiones incorrectas; el valor del hardware, software y personal y, algo relevante como elemento de prevención de riesgos de fraudes: la necesidad de mantener la privacidad y confidencialidad de las transacciones de la organización (Hernández, 2011).

Los conceptos de auditoría, desde los más antiguos hasta los más contemporáneos, están indicando que para la informática e informatización de la sociedad y la propia ciencia, se requiere no solo de la aceptación e inclusión de este tipo de auditoría entre los términos y conceptos asumidos por esta ciencia, sino también sus objetivos y alcance, áreas de aplicación, programas y procedimientos.

No obstante, aun reconociendo este tipo de auditoría, se han mantenido definiciones que limitan el concepto de Auditoría Informática solo al lado tangible aun en las normativas de muchos países. Esta reflexión se fundamenta en las primeras definiciones de Auditoría Informática y en algunas denominaciones que todavía se emplean.

Una de las primeras definiciones de Auditoría Informática la enmarca solo en la revisión práctica (Aguirre, 1987) que se realiza sobre los recursos informáticos con que cuenta la entidad con el fin de emitir un informe o dictamen sobre la situación en que se desarrollan y se utilizan los recursos. En este periodo es frecuente la denominación por Aguirre, Bautista y otros catedráticos de México, de “Auditoría en Informática”.

En Cuba, el Reglamento de la Ley 107 de la Auditoria, la denomina Auditoría de tecnologías de la información y las comunicaciones que consiste:

En el examen de las políticas y procedimientos y utilización de los recursos informáticos, así como de la confiabilidad y validez de la información, la

efectividad de los controles, aplicaciones, sistemas de redes y otros vinculados a la actividad informática (p.166).

Criterios más exactos a lo que debe ser la Auditoría Informática aparecen acuñados por diferentes firmas de asesores, auditores, informáticos, asociaciones y universidades, que ya conciben a la Auditoría Informática más allá de las prácticas primeras, y la asumen no solo como el proceso de recoger, agrupar y evaluar evidencias (Santana, 2013) para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

A partir de ese concepto se está definiendo a la Auditoría Informática como el proceso de recoger, agrupar evidencias que sustentan y confirman los objetivos de protección de activos e integridad de datos y la eficiencia y eficacia de su gestión.

Actualmente, uno de los conceptos más abarcadores de Auditoría Informática sin limitaciones, según criterio de los autores, es el que incorpora a conceptualizaciones como la anterior, aspectos que recogidos por separados la limitan, pero integrados definen adecuadamente su alcance. De tal modo, se le adiciona su capacidad de detectar, de forma sistemática, el uso de los recursos y los flujos de información dentro de una organización y determinar la información crítica para el cumplimiento de su misión y objetivos, identificando las necesidades, costos, valor y los obstáculos del flujo de información eficiente

La existencia de conceptos y definiciones precisas de la Auditoría Informática, evidencia que aún deben precisarse los propósitos, objetivos, técnicas y procedimientos propios, teniendo en cuenta la universalidad de su aplicación. Objetivos y propósitos que todavía transitan desde una visión estrecha hasta una más amplia, sin corresponderse plenamente al impacto de esta tecnología.

La Auditoría Informática está llamada a detectar evidencias de riesgos y/o problemas en el apoyo informático a todos los procesos de negocios originados generalmente por un mal uso informático y/o del control, y a proponer mejoras continuas.

Si se tienen en cuenta los fraudes informáticos, el *hacker* de información contable, financiera, y tecnológica, la Auditoría Informática debe desempeñar un papel dirigido no solo a los sistemas, sino a las personas, a la información, a la preservación de la información de todo tipo, lo cual constituye la base de la gestión de la organización; de lo contrario no es posible concebir a la Auditoría como ciencia, sino se es capaz de

confirmar sus resultados en la técnica. Vale recordar a Engels (1894) cuando expresó que cuando en la sociedad surge una necesidad técnica, esta hace progresar la ciencia a mayor escala y a mayor velocidad que diez universidades, por lo que afirma que en la técnica encuentran su expresión los resultados de la ciencia.

Entonces, ¿cuál debe ser el objetivo y alcance de la Auditoría Informática si debe respaldar el desarrollo social a partir de los adelantos técnicos?

A esta interrogante se puede responder con datos de publicaciones españolas que contemplan anualmente los delitos económicos y fraude empresarial en Europa que más del 50 % de los delitos económicos están relacionados con la apropiación indebida de activos, el soborno y corrupción y la manipulación contable, seguidos de las transacciones no autorizadas y financiación fraudulenta obtenida ambas con un 8 % del total de los delitos clasificados y cometidos en el año. Según los datos aportados por el informe de delitos económicos de España, estos delitos representaron afectaciones en el orden de un millón de euros aproximadamente en un año (López Andreo, 2010).

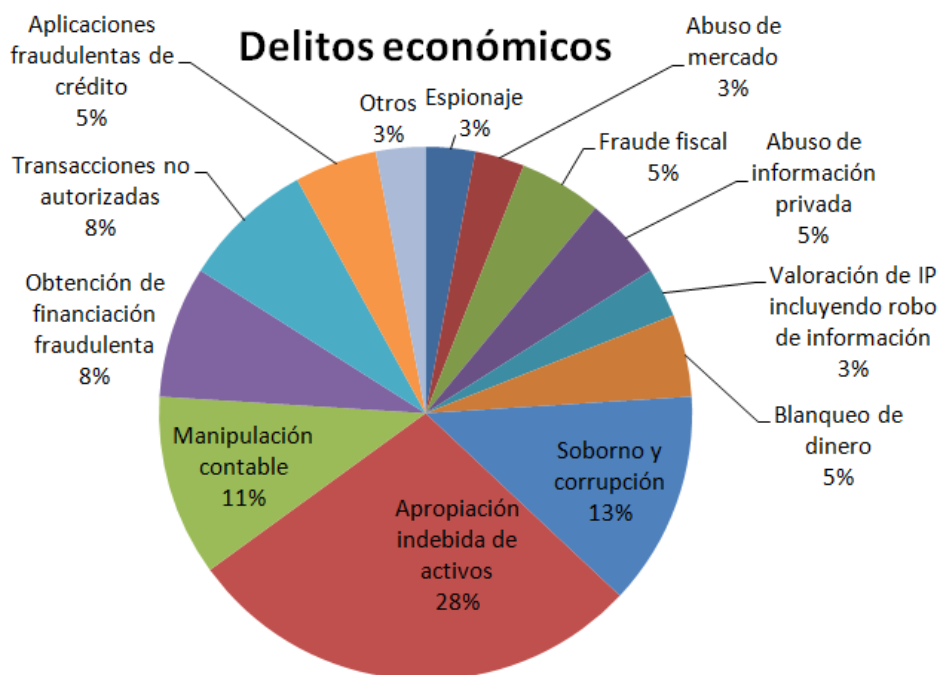


Gráfico 1 Tipos de fraude más experimentados en España según encuestados
Fuente: López Andreo (2010).

El desarrollo de la Informática y de los profesionales de esta, y un no despreciable número de personas “adictas a la computación”, están indicando que los sistemas de auditoría, normas y procedimientos, si se procura prevenir el riesgo por robo de

información, falsificación, e incluso hasta la extinción de una empresa, debe evolucionar a la par que el desarrollo de la Informática o de los efectos que esta ocasiona desde su lado negativo a la economía. No se puede olvidar de que existen sujetos que cometen los delitos informáticos, denominados sujetos activos (Gallegos, 2012), los que se diferencian principalmente por la naturaleza de los delitos cometidos.

Así pues, en la calificación de sujetos activos pueden entrar desde usuarios que acceden a sistemas informáticos de forma ilegítima pero sin intenciones delictivas, hasta empleados que roban información sensible de su propia empresa para sacar un beneficio económico (Gallegos, 2012).

Inicialmente están los llamados *hacker* (Gallegos, 2012), persona que muestra un elevado interés en el funcionamiento de los sistemas operativos y nuevas tecnologías, cometiendo las infracciones denominadas como *hacking*, en las que, por lo general, investigan las nuevas herramientas tecnológicas y su desarrollo, teniendo como objetivo final conocer el funcionamiento de cualquier sistema informático.

Surge después un tipo activo denominado *crackers* dedicados a romper las protecciones y otros elementos de seguridad de los programas comerciales, en su mayoría con el fin confeso de sacar provecho de los mismos en el mercado negro. El *cracker* conoce las dos caras de la tecnología: la programación y la parte física de la electrónica, lo que les posibilita crear códigos para utilizarlos en la copia de archivos. Sus acciones (Gallego, 2012) pueden ir desde la destrucción de información (ya sea a través de virus u otros medios) hasta el robo de datos y posterior venta.

El último sujeto activo al que se va a hacer referencia es al *phreaker*; sujeto con amplios conocimientos en el ámbito de los sistemas telefónicos, (tanto terrestres como móviles) y amplios conocimientos sobre Informática. Su objetivo es la eliminación de la protección en redes públicas y corporativas de telefonía, evitando así pagar por el servicio usado y, en algunos casos, obtener un beneficio económico mediante la falsificación de las tarjetas de prepago para llamadas telefónicas, cuyos códigos obtienen al lograr el acceso mediante técnicas de “*hacking*” a sus servidores.

Cualquiera de estos tipos de sujetos activos informáticos (y otros no mencionados y citados por Gallegos como los llamados *lammers* y los gurús) aun cuando su móvil sea un reto intelectual, los resultados de sus acciones delictivas, afectan considerablemente la economía de la empresa y la de un país.

Entonces, la Auditoría Informática debe desarrollarse a la par de su contexto y las tecnologías, partiendo siempre del concepto de que ante todo la auditoría debe ser una herramienta para la prevención. En este caso de los delitos informáticos que como se observa de la propia clasificación de la ONU, laceran grandemente la economía de las organizaciones y del país.

Conclusiones

- 1. El análisis efectuado del desarrollo científico-tecnológico y su impacto en las auditorías y el control de la gestión empresarial está indicando que existe aún un reto y una exigencia pendiente para la Auditoría de renovar, actualizar y atemperar al desarrollo tecnológico sus conceptos, normas y procedimientos, evitando que crezcan más rápido los impactos negativos para la economía derivados del constante cambio y desarrollo de la Informática, frente a un lento accionar de las técnicas y normas de Auditoría.*
- 2. La Auditoría, apoyada en la informatización y utilización de los equipos de cómputo, eleva la calidad de la misma al ampliar significativamente su implicación en la planificación, control y seguimiento de la gestión empresarial. Este mejoramiento trae consigo mayor cobertura en atención y satisfacción social en el servicio prestado, generando nuevas y mayores oportunidades, aumento del bienestar y sentido de pertenencia por parte de la sociedad.*
- 3. El uso de sistemas informáticos en Auditoría debe entre otros aspectos centrarse en la preparación del talento humano, lo que permitirá alcanzar los objetivos de prevención, reducción de fraudes, pérdidas y consecuentemente lograr que los recursos invertidos propicien el incremento del desarrollo económico y social.*

4. *El crecimiento de los delitos económicos, en desproporción a las medidas de control y prevención indican que se debe poner a disposición de todos los usuarios de las tecnologías de la información y las comunicaciones, las diferentes técnicas de manipulación, vulneración y de agresión que pueden amenazar sus sistemas informáticos.*

Referencias bibliográficas

1. Aguirre Bautista, J. J. (1987). *Programa de Auditoría en Informática*. México: UNAM.
2. Engels, F. (1894). Carta a Borgius. en *Obras Escogidas*. (tomo único). Editorial Progreso, Moscú.
3. Estrada Garavilla, M. (2008). Delitos informáticos. Recuperado de https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf
4. Fajnzylber, F. (1983). *La industrialización trunca de América Latina*. México: Editora Nueva Imagen.
5. Gaceta Oficial de la República de Cuba (2009), Ley 107/09 de la Contraloría General de la República de Cuba.
6. Gallego Yuste, A. (2012). Delitos informáticos: malware, fraudes y estafas a través de la red y cómo prevenirlos. Proyecto final de grado, Universidad Carlos III de Madrid, España. Recuperado de http://e-archivo.uc3m.es/bitstream/handle/10016/16868/pfc_alberto_gallego_yuste.pdf?sequence=1
7. Hernández Hernández, E. (2002) *Auditoría en Informática*. (segunda edición). CECSA, México.
8. López Andreo, J. (2010). *Informe sobre delitos económicos y fraude empresarial en España*. Recuperado de <https://www.pwc.es/en/servicios/forensic-services/assets/informe-delitos.pdf>

-
9. Martínez, E. (1997). *Ciencia, tecnología y Estado en América Latina: el fin del siglo XX. Democracia para una nueva sociedad*. Caracas, Venezuela: Editorial Nueva Sociedad.
 10. Meigs, W. B. (1981). *Principios de Auditoría*. (décima impresión). México: Editorial Diana.
 11. Miranda A. Torras, O. y González, J. (1982). *Auditoría de las empresas socialistas*. (tomo I). La Habana: Combinado Poligráfico Juan Marinello.
 12. Núñez Jover, J. (1999). *La ciencia y la tecnología como procesos sociales: algo que la educación científica no debería olvidar*. La Habana: Editorial Félix Varela.
 13. Santana Roldán, C. (2013). ¿Qué es una auditoría informática? Recuperado de <https://www.codejobs.biz/es/blog/2013/02/25/que-es-una-auditoria-informatica>
 14. Schlosser, R. E. (2002). *Auditoria*. España: Océano.
 15. Sotomayor Alfonso, A. (2008). *Auditoria Administrativa*. México: McGraw Hill Interamericana.