Delitos informáticos y entorno jurídico vigente en Colombia*

Jorge Eliécer Ojeda-Pérez

Economista, Universidad La Gran Colombia, Bogotá, Colombia. Ingeniero de sistemas, Universidad Antonio Nariño, Bogotá, Colombia. Especialista en sistemas de información, Universidad de los Andes, Bogotá, Colombia. Magíster en ingeniería industrial, Universidad de los Andes, Bogotá, Colombia. Profesor de medio tiempo, Universidad Santo Tomás de Aquino, USTA, Bogotá, Colombia. Investigador principal del grupo de investigación en Seguridad Informática y Delitos Informáticos de la especialización en Auditoría de Sistemas, Universidad Santo Tomás de Aquino, USTA.
Correo electrónico: jojeda16@gmail.com

Fernando Rincón-Rodríguez

Abogado, Universidad Libre de Colombia, Bogotá, Colombia. Director Especialización en Auditoría y Administración de la Información Tributaria, Universidad Santo Tomás de Aquino, USTA, Bogotá, Colombia. Consultor jurídico del grupo de investigación en Seguridad Informática y Delitos Informáticos de la especialización en Auditoría de Sistemas de Universidad Santo Tomás de Aquino, USTA.
Correo electrónico: fernandorincon@usantotomas.edu.co

Miguel Eugenio Arias-Flórez

Ingeniero de telecomunicaciones, Universidad Santo Tomás de Aquino, USTA, Bogotá, Colombia. Ingeniero superior de telecomunicación, Ministerio de Educación, Madrid, España. Especialista en gerencia de proyectos de telecomunicaciones, Universidad Santo Tomás de Aquino, USTA, Bogotá, Colombia. Máster en administración de negocios, MBA, Escuela Europea de Negocios, Salamanca, España. Profesor de tiempo completo, Universidad Santo Tomás de Aquino, USTA, Bogotá, Colombia. Coinvestigador del grupo de investigación en Seguridad Informática y Delitos Informáticos de la especialización en Auditoría de Sistemas de la Universidad Santo Tomás de Aquino, USTA.
Correo electrónico: miguelarias@usantotomas.edu.co.

Libardo Alberto Daza-Martínez

Economista, Pontificia Universidad Javeriana. Magíster en ciencias económicas, Universidad Santo Tomás de Aquino, USTA. Especialista en pedagogía para el desarrollo del aprendizaje autónomo de la Universidad Nacional Abierta y a Distancia, UNAD. Director de las especializaciones: Auditoría de Sistemas y Gerencia de Negocios Internacionales. Líder del grupo de investigación en Seguridad Informática y Delitos Informáticos de la especialización en Auditoría de Sistemas de la Universidad Santo Tomás de Aquino, USTA.
Correo electrónico: libardodaza@usantotomas.edu.co.

* El presente artículo es producto del trabajo de investigación desarrollado por el grupo de investigación Seguridad y Delitos Informáticos, SEGUDELIN, de la especialización en Auditoría de Sistemas de la Universidad Santo Tomás de Aquino, USTA. El artículo fue preparado de marzo a mayo de 2010.

Resumen El documento describe y analiza la evolución y el marco conceptual de los delitos informáticos planteados por diferentes autores nacionales e internacionales, y establece la relación con la reciente Ley 1273 de 2009, mediante la cual la legislación colombiana se equipara con la de otros países en cuanto a la normatividad sobre el cibercrimen, que ha venido vulnerando distintos campos de las relaciones y comunicaciones personales, empresariales e institucionales. El ciberdelito, como tendencia que incide no sólo en el campo tecnológico sino también en el económico, político y social, debe ser conocido, evaluado y enfrentado, por lo cual el análisis de la norma, su aporte y alcance puede dar otros elementos de juicio para entender la realidad de nuestras organizaciones y visualizar sus políticas y estrategias, a la luz de la misma norma y de los estándares mundiales sobre seguridad informática.

Palabras claves autor Seguridad informática, delitos informáticos, cibercrimen, sistemas de información, entorno jurídico.

Palabras claves descriptor Seguridad informática, delitos por computador, sistemas de información.

Computer crime and current legislation in Colombia

Abstract This article describes and analyses the evolution and conceptual framework of computer crime raised by different national and international writers, and establishes the connection with the recent Law 1273/2009, whereby Colombian law is equated with that of other countries in terms of the legislation on cybercrime, which has been violating various fields of personal, business and institutional relationships and communications. Cyber-crime, as a trend that affects not only technology but also economics, politics and society, must be acknowledged, evaluated and faced. That is the reason why the analysis of the norm, its contribution and extent can grant additional elements of judgment to understand the reality of our organizations and view their policies and strategies in light of the same rules and global standards on computer security.

Key words author Computer security, computer crime, cybercrime, information systems, legal environment.

Key words plus Computer Science Security, Computer Crimes, Information Systems.

Crimes informáticos e o ambiente jurídico vigente na Colômbia

Resumo O documento descreve e analisa a evolução do quadro conceitual dos crimes informáticos proposto por diferentes autores nacionais e internacionais, e estabelece a relação com a recente Lei 1273 de 2009, mediante a qual a legislação colombiana se equipara com a de outros países no que diz respeito à normatividade contra o cibercrime, que tem penetrado diferentes âmbitos das relações e comunicações pessoais, empresariais e institucionais. O cibercrime, como tendência que incide não só no campo tecnológico, mas também no econômico, político e social, deve ser conhecido, avaliado e enfrentado, por isso a análise da norma, sua contribuição e alcance pode dar outros elementos de juízo para entender a realidade de nossas organizações e visualizar suas políticas e estratégias, com base na norma e nos padrões mundiais sobre segurança informática.

Palavras-chave autor segurança informática, crimes informáticos, cibercrime, sistemas de informação, ambiente jurídico.

Introducción

La variedad, amplitud y complejidad de los sistemas de información que adquieren, requieren o encuentran disponibles las organizaciones actuales, junto a la dinámica del permanente

cambio observado en las tecnologías de la información y las comunicaciones, han impulsado de múltiples formas y, al mismo tiempo, condicionado las grandes transformaciones de las organizaciones, los mercados y el mundo de la modernidad y de la posmodernidad. Son cambios que, además de sus innegables ventajas, han traído simultáneamente para las personas y las organizaciones, amenazas, riesgos y espectros de incertidumbre en los escenarios de internet, intranet, desarrollo tecnológico, gestión de la información, la comunicación y los sistemas (Álvarez-Marañón & Pérez-García, 2004, pp. 30-40).

Con cada vez mayor frecuencia y mayor impacto, los dispositivos de almacenamiento y procesamiento de información –llámense servidores, estaciones de trabajo o simplemente PC– son vulnerados en sus elementos más sensibles, dejando expuestos no sólo múltiples y significativos datos de distinto valor (financiero, crediticio, estratégico, productivo…), sino los mismos patrimonios reales de personas y organizaciones y, aún más, su dignidad, su honra y su vida.

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.

En este documento se describen los antecedentes y el origen del fenómeno en su dimensión delictiva, junto con el concepto de diversos autores y autoridades nacionales e internacionales que han estudiado y enfrentado el tema y que hoy sirven de apoyo para contextualizar su impacto en el ámbito informático y jurídico y, por supuesto, en el social y económico.

A partir del acelerado incremento en las posibilidades de interrelación global por el uso de la comunicación satelital (la internet, el correo electrónico, los teléfonos celulares, las redes sociales…), las personas y las organizaciones privadas y públicas han quedado expuestas, por las vulnerabilidades de los sistemas de intercomunicación y manejo de la información y por la falta de preparación y de cuidado en su uso, al progresivo y peligroso impacto de la *ciberdelincuencia*.

De ahí la importancia de conocer el contexto y las consecuencias de los delitos informáticos y la normatividad aplicable en nuestro medio, para orientar posibles respuestas o formas de prevención y tratamiento. Ése es el sentido de la Ley 1273 de 2009, expedida en Colombia sobre delitos informáticos. En ella se hace una revisión de los delitos que atentan contra las principales características de calidad, de la información que, en últimas, son condiciones de seguridad (confidencialidad, integridad, disponibilidad) y lo que legalmente puede esperar el cliente de las organizaciones en las cuales ha depositado su confianza.

También se referencian guías, procedimientos y estándares internacionales sobre auditoría de sistemas, sistemas de seguridad informática, evaluación y seguimiento recomendados por las organizaciones más reconocidas en el ámbito internacional, como la Asociación para la Auditoría y Control de Sistemas de Información, ISACA (Information Systems Audit and

Control Association) y su IT Governance Institute, ITGI, que desarrollaron los Objetivos de Control para la Información y Tecnologías relacionadas, CObIT (Control Objectives for Information and related Technology) y varias de las certificaciones internacionales más difundidas. De la misma manera, se estudiaron las bases jurídicas para el tratamiento de los delitos informáticos en Colombia, como la Ley 599 del 24 de julio de 2000 y la Ley 1273 del 5 de enero de 2009. Con base en los referentes jurídicos y los estándares internacionales, se analizaron las condiciones de seguridad informática de una muestra de entidades financieras.

Objetivo

El objetivo fundamental del trabajo es tener elementos de juicio claros sobre los delitos informáticos y su contexto, su evolución y tendencias, tanto como de la normatividad aplicable a este fenómeno delictivo, a la luz de la Ley 1273 de 2009, para entender, por contraste, la vulnerabilidad de los sistemas de información de las organizaciones financieras y, como consecuencia, señalar algunas formas de prevención y tratamiento de los riesgos que afectan la infraestructura tecnológica y la integridad, confiabilidad y disponibilidad de la información de esas entidades.

1. Contexto de los delitos informáticos

Recordando un poco la historia, al ser humano actual le ha sucedido lo mismo que a nuestros antepasados prehistóricos cuando fabricaron el primer cuchillo. Tuvo un gran alivio en sus labores diarias, se sintió feliz, porque ya contaba con una herramienta que le ayudaría en sus tareas cotidianas de supervivencia. Pero no faltó quien usara esta herramienta con otras intenciones en contra de sus congéneres y terminara cometiendo delitos que, seguramente, en su momento no se llamaron así, aunque sí se entendían como actos en contra de la supervivencia de los demás.

Con los sistemas informáticos ha ocurrido algo similar a lo observado en la historia. El hombre vive cada vez más interesado y condicionado por la informática, debido a su vertiginoso desarrollo y a la enorme influencia que ha alcanzado en muchas de las actividades diarias de las personas y las organizaciones. Pocas personas, en la actualidad, pueden abstraerse del contacto directo o indirecto con un sistema de cómputo, lo cual muestra de distintas maneras el poder y alcance de la tecnología informática en las sociedades del mundo.

Así como la tecnología y su desarrollo han incidido en prácticamente todas las actividades del ser humano a lo largo de su historia, en la actualidad, la dependencia tecnológica ha venido concentrándose cada vez más en el fenómeno de la tecnología informática, la información y la comunicación. Con efecto retardado, se descubrió luego que ese desarrollo venía acompañado de distintos y también novedosos riesgos.

En 1980, la ArpaNet (Advanced Research Projects Agency Network) del Departamento de Defensa de Estados Unidos, creadora de la internet, documentó que en su red se emitieron extraños mensajes que aparecían y desaparecían en forma aleatoria, y que algunos códigos

ejecutables de los programas usados sufrían una mutación; en ese momento, los hechos inesperados no pudieron comprenderse pero se les buscó solución. Los técnicos altamente calificados en seguridad informática del Pentágono desarrollaron un *antivirus* para contrarrestar el riesgo y atender la urgencia del caso, a los tres días de ocurrido el evento (Trend Micro, 2008).

A medida que el uso de internet se ha extendido, ha aumentado el riesgo de su uso inadecuado. Los *delincuentes cibernéticos* viajan por el mundo virtual y realizan incursiones fraudulentas cada vez más frecuentes y variadas, como el acceso sin autorización a sistemas de información, piratería informática, fraude financiero, sabotaje informático y pornografía infantil, entre otros. Para enfrentarlos, no obstante la dificultad para descubrirlos, varios países han dispuesto un sistema judicial especializado que permite procesarlos y castigarlos. A ese grupo de países se unió Colombia en 2009.

Las herramientas de los *ciberdelincuentes* han evolucionando si no más rápido, por lo menos paralelamente al desarrollo tecnológico, como ha venido sucediendo con los virus informáticos. En un comienzo, los *ciberdelincuentes* infectaban los equipos de sus víctimas al transportar mano a mano los virus desarrollados, en los medios de almacenamiento de información disponibles en ese momento: los disquetes. Más tarde, utilizaron las redes de datos al aprovechar la internet, pero encontraron la barrera de las restricciones de acceso para evitar contagios. De nuevo, regresaron a la difusión contaminante mano a mano al emplear las memorias móviles con puerto USB y arreciaron los bombardeos de *malware*[1] en la internet. De igual manera, los ciberdelincuentes han utilizado el correo electrónico y los *chat rooms* o salas de conversación virtual de internet para buscar presas vulnerables.

Pero además de los delincuentes informáticos propiamente tales, otros tipos de delincuentes han encontrado espacios propicios en los distintos medios de comunicación electrónica, para desarrollar sus crímenes, como los pedófilos que buscan generar relaciones de confianza *on line* con niños inocentes, para luego aprovecharse de ellos y hasta secuestrarlos o asesinarlos. Estafadores, falsificadores, defraudadores, secuestradores, proxenetas, traficantes de armas, de drogas, de personas, de pornografía, de información, sicarios y terroristas se agregan a esta tenebrosa lista que utiliza el ciberespacio y la red para multiplicar sus negocios, sus ilícitas ganancias y sus manifestaciones criminales.

Con ese antecedente, las entidades que desarrollaban o trabajaban en los escenarios informáticos del mundo, comenzaron a generar instrumentos de control y sanción a quienes en forma inescrupulosa utilizaban la informática para delinquir. Sin embargo, se encontró que los entes encargados de sancionar a quienes hacían uso ilegal y delictivo de las herramientas informáticas, no tenían cómo judicializar a los nuevos delincuentes. La ley inglesa sirvió para que otros países –en especial aquellos donde la internet

1 *Malware*, *malicious software* o código malicioso. Se trata de cualquier software, mensaje o documento con capacidad de producir daños en los sistemas informáticos y en las redes. En este grupo de programas peligrosos, se encuentran las bombas lógicas, los gusanos, los virus y los troyanos, entre otros. Álvaro Gómez-Vieites (2006). *Enciclopedia de la seguridad informática*, 144. Madrid: Alfaomega.

tenía más desarrollo– se sumaran al esfuerzo de discutir y promulgar leyes orientadas a proteger y sancionar la violación de la información.

Sin embargo, en el caso colombiano, la reacción fue lenta y tardía, de acuerdo con los estudios realizados por Cisco en 2008, según los cuales el país registraba una de las calificaciones más bajas en seguridad informática (62 puntos de 100 posibles), en comparación con otros seis países de Latinoamérica. Esa situación, que obedece a distintos factores, según concepto de algunos ejecutivos de firmas relacionadas con la informática y la auditoría (Etek, Cisco, Trend Micro), se explica en factores como:

- Falta de información, falta de claridad o debilidad en la gestión gerencial, referidos particularmente a la implementación de la seguridad informática.
- Abuso en el empleo de los sistemas y sus aplicativos.
- Ausencia de políticas claras sobre seguridad informática.
- Falta de reconocimiento estratégico al área de Auditoría de Sistemas.
- Falta de conciencia en el desempeño de los sistemas de información.
- Baja gestión y poco uso de herramientas de análisis y control.
- Falta de evaluación con relaciones beneficio/costo y criterios de continuidad del negocio, sobre uso y seguridad de la información y los recursos informáticos.

Según Manuel Bustos, director de la multinacional de seguridad de la información Etek: "La industria en general, el sector gobierno y las pyme son los menos preocupados por la seguridad de la información, porque requiere inversiones y normalmente no le dedican lo suficiente para lograr un nivel adecuado de seguridad" (Cisco, 2008).

Para José Battat, ejecutivo de Trend Micro: "En el país, las pyme viven un proceso más lento en cuanto a la implementación de estrategias de seguridad; sin embargo, poco a poco, tanto los proveedores como esas empresas han buscado los mecanismos para solventar esta falta" (Cisco, 2008).

De acuerdo con las conclusiones del mencionado estudio realizado por Cisco, líder mundial en redes, las tres principales formas de ataque informático a las organizaciones son, en su orden: virus informático (45% del total), los abusos por parte de los empleados (42%) y luego la penetración a los sistemas por parte de fuentes externas (13%).

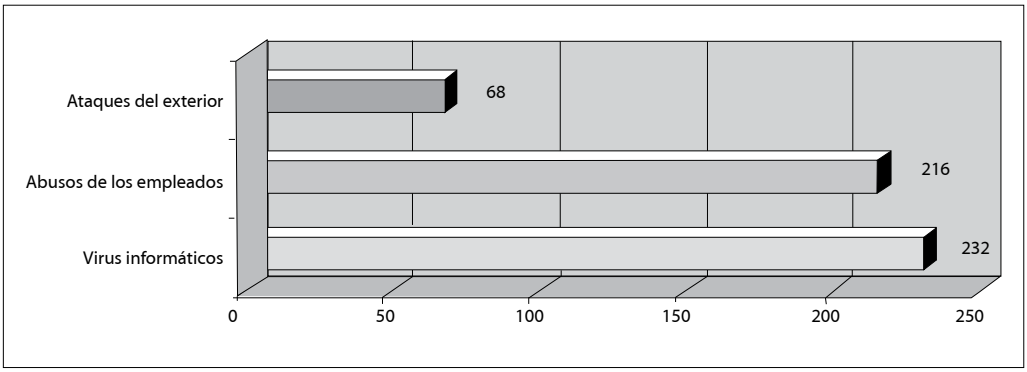

Figura 1. Frecuencia de ataques informáticos a las organizaciones.
Fuente: Cisco, 2008.

2. ¿Qué es un delito informático?

En el proceso de evolución de las ciencias, como parte de la dinámica del cambio natural, social o tecnológico, entre muchos otros, cuando se conocen nuevos fenómenos, su interpretación o su tratamiento generan controversias que resultan de su confrontación con los paradigmas vigentes, las formas de pensamiento o los sistemas reconocidos, para que puedan ser aceptados dentro del cuerpo de los saberes convencionales, o de las normas o tradiciones colectivas.

Desde las primeras manifestaciones del comportamiento social del hombre, la prescripción y aplicación de las normas definitorias de la conducta de los asociados estuvo mediada por los intereses de los más fuertes o de los más capaces, según el reconocimiento colectivo. En esas condiciones, el hecho de que alguno de los miembros de la sociedad transgrediera las normas, prohibiciones o restricciones establecidas, necesariamente conducía a la sanción pública, proporcional al significado o dimensión de la transgresión en el entendimiento colectivo o normativo.

Las penas, desde entonces, se manifestaron en restricción o eliminación de las libertades, de las relaciones o capacidades, o de la vida misma; o en afectación de sus bienes, patrimonio o capacidad productiva. Surgieron, entre ellas, el forzamiento a trabajos, el destierro, la expropiación, las penas pecuniarias, el castigo físico, la desmembración y, en muchas ocasiones, la muerte. Con el cambio de época y más recientemente, en referencia a Estados Unidos, Kenneth C. Laudon y Carol Guercio-Traver (2009), señalan: "Antes de los automóviles había muy pocos crímenes entre estados y muy poca jurisdicción federal sobre el crimen. Lo mismo pasa con internet; antes de internet, había muy poco cibercrimen".

El Derecho como ciencia social reconoce sus orígenes en el nacimiento de las sociedades y, en su proyección, no puede estar alejado del influjo proveniente del cambio en las ciencias y la tecnología y en el desarrollo de la civiliza-

ción. En la evolución de paradigmas, el derecho a la vida y otros directamente relacionados –hasta incluir el medio ambiente– han tomado fuerza suficiente como para convertirse en los nuevos paradigmas de los derechos del ser humano, hasta el punto de ser reconocidos por el concierto mundial de las naciones. Con las nuevas concepciones, ha venido desapareciendo progresivamente la pena de muerte, incluso como castigo último de delitos execrables. Esa tendencia se ha venido manifestando en las distintas expresiones jurídicas y, en especial, en el Derecho Penal, lo cual indica la necesaria correspondencia entre la interpretación jurídica y la realidad histórica de cada pueblo.

El desarrollo y el impacto de las Tecnologías de la Información y las Comunicaciones (TIC) han generado la concomitante necesidad de ajuste de muchas de las formas de operación y de gestión de las organizaciones, tanto de los procedimientos y estándares de las ciencias y otras tecnologías, como de la interpretación del mundo, sus culturas y paradigmas; y de esa tendencia no se excluye el Derecho.

La información hace parte del proceso de bienes que llegan a ser universalmente reconocidos y como tales deben ser jurídicamente protegidos, junto a las herramientas que facilitan su manejo, lo cual se integra en el concepto de *informática*. Este concepto empezó a configurarse como tal a mediados del siglo XX en Rusia (*informatika*, de Alexander Mikhailov), en Alemania (*informatik*, de Karl Steinbuch, 1957), en Inglaterra (*informatics*, de Walter Bauer, 1962), pero básicamente del francés *informatique* como acrónimo de *information* y *automatique* (Philippe Dreyfus, 1962), luego extendido al español como: "Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores" (Diccionario de la Real Academia Española, DRAE).

Esta definición, con sus elementos constitutivos, es importante en cuanto permite identificar algunas premisas necesarias para la adecuada comprensión del fenómeno de los delitos informáticos y su manejo organizacional e institucional.

Nótese que al concebir la informática como el manejo de información por medios automatizados, no se hace discriminación alguna ni se da significación especial a la naturaleza de la información, ni tampoco a los medios o mecanismos que se utilizan o requieren para su manejo, más allá de lo que se puede entender por automatización. De tal manera, que siempre que se haga referencia a lo informático, deberá considerarse que, en sí mismo, no se trata de un tema que pueda derivar en algo distinto a las condiciones de su naturaleza tecnológica, pero aclarando, por supuesto, que el objetivo principal de esta mirada corresponde más que todo a una posición analítica y complementaria de lo informático.

En ese mismo sentido, conviene considerar el planteamiento de Mario Gerardo Piattini-Velthuis y Emilio del Peso-Navarro (2001) en relación con el Derecho Penal: "Muchos estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo…". De aquí la importancia

de buscar una aproximación que permita relacionar la normatividad jurídica con la realidad y con las tendencias de la tecnología y los delitos informáticos.

Dentro de la normatividad colombiana, la Escuela Positiva del Derecho Penal tuvo gran influencia y uno de sus grandes discípulos fue Jorge Eliécer Gaitán y, recientemente, el inmolado profesor Alfonso Reyes-Echandía. Desde allí se ha entendido el delito como: "…el comportamiento humano, atípico, antijurídico y culpable, conminado con una sanción penal". Y en referencia específica al delito informático, se han venido incorporando conceptos de distintos autores:

Julio Téllez-Valdés (2007), en su libro *Derecho Informático*, enfoca el delito informático desde el punto de vista típico y atípico y lo define como "actitud contraria a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)".

Alberto Suárez-Sánchez (2009), por su parte, señala: "En conclusión, el delito informático está vinculado no sólo a la realización de una conducta delictiva a través de medios o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información *per se* como bien jurídico tutelado, diferente de los intereses jurídicos tradicionales".

Luis Camacho-Losa (1987), de otro lado, había dicho: "Toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, o que, por el contrario, produce un beneficio ilícito a su autor aun cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas".[2]

Otras concepciones sobre delito informático, complementarias todas, referidas por Suárez-Sánchez (2009), señalan un foco común con elementos distintos en su formalidad, mas no en su esencia:

> La especificidad del delito informático le viene dada por dos factores fundamentales: las acciones se vinculan al funcionamiento de una máquina y, en buena parte de los supuestos, recae sobre un objeto intangible o inmaterial (Choclán-Montalvo, 1997).
>
> La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnere los derechos del titular de un elemento informático, ya sea hardware o software (Davara-Rodríguez, 2007).
>
> Podría ser *delito informático* todo comportamiento criminal en el que aparezca involucrado un ordenador; de este modo, casi cualquier delito con esta peculiaridad podría ser, eventualmente *delito informático* (Aldama-Baquedano, 1993).
>
> Conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de

2 Tomado de Alberto Suárez-Sánchez (2009), *La estafa informática*, 45-46. Bogotá: Grupo Ibáñez.

> técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos (Gómez-Perals, 1994).

Mario Gerardo Piattini-Velthuis y Emilio del Peso-Navarro (2001) recuerdan el elemento sancionatorio: "Se podría definir el *delito informático* como toda acción (acción u omisión) culpable realizada por un ser humano, que cause perjuicio a persona sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor, aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la Ley, que se realiza en el entorno informático y está sancionado con una pena".

La Constitución de España define el delito informático como "la realización de una acción que reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos".

Guillermo Beltramone, Rodolfo Herrera-Bravo y Ezequiel Zabale (1998) añaden el concepto de soporte: "Toda conducta que revista características delictivas, es decir, sea típica, antijurídica y culpable y atente contra el soporte lógico de un sistema de procesamiento de información, y la cual se distingue de los delitos computacionales o tradicionales informatizados".

En Colombia, entre quienes han tratado el tema, podemos referir a Henry William Torres-Torres, ya que amplía el concepto a lo internacional en su definición de delito informático: "Toda conducta punible en la que el sujeto activo utilice método o técnica de carácter informático en su ejecución que tenga como medio o instrumento elementos integrantes de un sistema informático o telemático o intereses jurídicos tutelados por el derecho a la intimidad, a la propiedad intelectual y el software a que sin estar reconocida por nuestro legislador es aceptada por tratadistas internacionales como Infracción Informática".

Entre las anteriores concepciones, hay dos enfoques complementarios, para entender el fenómeno informático: por una parte, la identificación de conductas que utilizan las herramientas informáticas en la acción delictiva y por la otra, las conductas que atacan o vulneran los bienes informáticos y sus componentes, ya cobijados por la protección jurídica del país.

También se advierte que, en el esfuerzo de llegar a una definición comprensiva pero simple, como lo hace la mayoría de tratadistas, se procura sintetizar las conductas tipificables como delito, lo cual conlleva el riesgo de confundir, eventualmente, la definición de delito informático, como género, con el objeto del delito mismo. A esto se agrega otra circunstancia que incide claramente en la definición de delito informático, como es la efectiva falta de '*madurez*' en el tratamiento normativo penal de aquellas conductas que, no obstante ser antijurídicas y culpables, no han tenido la debida tipificación en algunos países, lo cual mantiene el riesgo en el sentido de la globalidad de las relaciones, de las comunicaciones, de los negocios.

El delito informático también se conoce con la denominación anglosajona de *computer crime* y se sabe que quienes cometen estos delitos son expertos conocedores de la tecnología, con fundamento científico e investigativo

de los sistemas y también del comportamiento humano y organizacional. Otra característica importante es que el atractivo del delito no siempre es el botín económico, sino que puede obedecer a intereses de diverso orden, como los personales, psicológicos, sociales, laborales, políticos o de simple *curiosidad* tecnológica. Paradójicamente, sus acechanzas están *cubiertas* o protegidas por la misma *seguridad* que ofrece la tecnología informática.

No obstante la atención que el tema ha recibido en los últimos años, en particular por los críticos y costosos impactos recibidos, aún falta claridad interpretativa para orientar y dirigir mejor los recursos y las acciones en su contra. Eso se observa en la actualidad cuando con frecuencia se confunde el delito con la técnica utilizada para cometerlo. Para citar un ejemplo: es común oír decir que alguien ha sido víctima del *delito* de *clonación de tarjeta* (*carding*), por el cual, de manera subrepticia, alguien copia los datos personales del titular genuino de la tarjeta. Si bien la conducta de copiar fraudulentamente los datos de alguien produce un *clon* de la tarjeta original, no se puede decir que ése sea el delito, sino que, al tenor de lo establecido en la Ley 1273 de 2009, sería violación de datos personales (Artículo 269 F del Código Penal). Situaciones como ésta han contribuido de alguna manera, a dificultar no sólo la definición de delito informático, sino su interpretación para un adecuado tratamiento jurídico e institucional.

En la interpretación analítica presentada en este documento, los autores concuerdan con la siguiente definición de delito informático: toda conducta ilícita que puede ser sancionada a la luz del Derecho Penal, por hacer uso indebido de la información y de cualquier medio informático empleado para su manejo, o de la tecnología electrónica o computarizada, como método, como medio o como fin, en perjuicio de la libertad de las personas y organizaciones, o de su patrimonio, o propiedad (activos), o de su derecho a la vida, a la intimidad, al crédito y buen nombre.

Dicho de otra manera, en este contexto, se puede colegir que el delito informático es toda conducta ilícita, ya sea por acción u omisión, que realiza una persona mediante el uso de cualquier recurso informático y que, como consecuencia, afecta un bien informático jurídico y/o material que se encuentra legalmente protegido, haciéndose penalmente responsable por tal hecho.

3. Legislación penal colombiana sobre delitos informáticos

La Ley 1273 del 5 de enero de 2009, reconocida en Colombia como la *Ley de Delitos Informáticos*, tuvo sus propios antecedentes jurídicos, además de las condiciones de contexto analizadas en el numeral anterior. El primero de ellos se remite veinte años atrás, cuando mediante el Decreto 1360 de 1989 se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de software. A partir de esa fecha, se comenzó a tener asidero jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas.

En este mismo sentido y en el entendido de que el soporte lógico o software es un elemento informático, las conductas delictivas descritas en los Artículos 51 y 52 del Capítulo IV de la Ley 44 de 1993 sobre Derechos de Autor, y el mismo Decreto 1360 de 1989, Reglamentario de la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor, se constituyeron en las primeras normas penalmente sancionatorias de las violaciones a los citados Derechos de Autor. Al mismo tiempo, se tomaron como base para la reforma del año 2000 al Código Penal Colombiano:

> Capítulo Único del Título VII que determina los Delitos contra los Derechos de Autor: Artículo 270: Violación a los derechos morales de autor. Artículo 271: Defraudación a los derechos patrimoniales de autor. Artículo 272: Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones.

El Código Penal colombiano (Ley 599 de 2000) en su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones:

> Artículo 192: Violación ilícita de comunicaciones. Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Artículo 194: Divulgación y empleo de documentos reservados. Artículo 195: Acceso abusivo a un sistema informático. Artículo 196: Violación ilícita de comunicaciones o correspondencia de carácter oficial. Artículo 197: Utilización ilícita de equipos transmisores o receptores. Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles.

Una norma posterior relacionada fue la Ley 679 de 2001, que estableció el Estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con niños menores de edad. De igual manera, consagra prohibiciones para los proveedores o servidores, administradores o usuarios de redes globales de información, respecto a alojar imágenes, textos, documentos o archivos audiovisuales que exploten a los menores en actitudes sexuales o pornográficas. Sin embargo, la norma no contiene sanciones penales, sino administrativas (Artículo 10), pues siendo simple prohibición, deja un vacío que quita eficacia a la Ley, cuando se trata de verdaderos delitos informáticos.

Para subsanar lo anterior, el 21 de julio de 2009, se sancionó la Ley 1336, "por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual, con niños, niñas y adolescentes". En forma específica, en su Capítulo VI, sanciona los "Tipos penales de turismo sexual y almacenamiento e intercambio de pornografía infantil" con penas de prisión de diez (10) a veinte (20) años y multas de ciento cincuenta (150) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes (SMLMV).

La Ley 1273 de 2009 complementa el Código Penal y crea un nuevo bien jurídico tute-

lado a partir del concepto de la *protección de la información y de los datos*, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones. El primer capítulo de los dos en que está dividida la Ley, trata de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. El segundo Capítulo se refiere a los atentados informáticos y otras infracciones.

A partir de la Ley 1273 de 2009, se tipificaron los delitos informáticos en Colombia en los siguientes términos: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios *web* para capturar datos personales y transferencia no consentida de activos.

Este marco jurídico se ha convertido en una importante contribución y un instrumento efectivo para que las entidades públicas y privadas puedan enfrentar los "delitos informáticos", con definiciones de procedimientos y políticas de seguridad de la información; y, en consecuencia, con las acciones penales que pueden adelantar contra las personas que incurran en las conductas tipificadas en la norma. Con ella, Colombia se ubica al mismo nivel de los países miembros de la Comunidad Económica Europea (CEE), los cuales ampliaron al nivel internacional los acuerdos jurídicos relacionados con la protección de la información y los recursos informáticos de los países, mediante el Convenio 'Cibercriminalidad', suscrito en Budapest, Hungría, en 2001 y vigente desde julio de 2004.

Con los desarrollos jurídicos hasta ahora logrados acerca de "la protección de la información y de los datos y la preservación integral de los sistemas que utilicen las tecnologías de información y comunicaciones", las organizaciones pueden amparar gran parte de sus sistemas integrados de información: datos, procesos, políticas, personal, entradas, salidas, estrategias, cultura corporativa, recursos de las TIC y el entorno externo (Davenport, 1999), de manera que, además de contribuir a asegurar las características de calidad de la información, se incorpora la administración y el control, en el concepto de protección integral.

Retomando la estructura de la Ley 1273 de 2009, el capítulo I está orientado especialmente a apoyar la labor de los grupos de Auditoría de Sistemas, al apuntar al propósito de aseguramiento de las condiciones de calidad y seguridad de la información en la organización, cuando se refiere a los "atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos". Corrobora la importancia de la información como activo de valor para las organizaciones (ISO/IEC 17799/2005), que es necesario proteger adecuadamente para garantizar la continuidad del negocio, la maximización del retorno de la inversión y el aprovechamiento de las oportunidades del entorno, así como para disminuir y contrarrestar los riesgos y delitos que la amenazan.

La gestión confiable de la seguridad de la información en las organizaciones parte del establecimiento de políticas, estándares, proce-

dimiento y controles eficientes, en natural concordancia con las características del negocio y, en ese sentido, el capítulo I de la Ley 1273 de 2009 contribuye a tal propósito, de la misma manera que los estándares nacionales e internacionales sobre administración eficiente de la información.

En las siguientes figuras se presenta un detalle del contenido de la Ley y sus características aplicables a este análisis. La figura 2 identifica las actuaciones con las cuales se tipifica el delito y la punibilidad aplicable (en su mayoría, penas de prisión entre 48 y 96 meses y multas de 100 a 1.000 SMLMV).

El artículo 1 de la Ley 1273 de 2009 incorpora al Código Penal el Artículo 269A y complementa el tema relacionado con el "acceso abusivo a un sistema informático", que se manifiesta cuando el pirata informático o *hacker* aprovecha la vulnerabilidad en el acceso a los sistemas de información, o las deficiencias en los procedimientos de seguridad informática establecidos por las organizaciones, para extraer beneficios económicos o para indagar o demostrar la capacidad y recursos que ofrece la tecnología de la información. Cuando se presenta este abuso, en muchos casos, se observa que proviene de los mismos usuarios del sistema, tal como se evidencia en los informes anuales de la PricewaterhouseCoopers, *The global state information security* y en estudios realizados por Cisco (2008), en los cuales se señala que el 42% de los tres casos de abuso más frecuentes corresponde a los detectados entre los empleados.

El artículo 269B contempla como delito la "obstaculización ilegítima del sistema informático o red de telecomunicación", y se origina cuando el *hacker* informático bloquea en forma ilegal un sistema o impide su ingreso por un tiempo, hasta cuando obtiene un beneficio por lo general económico. Aquí también se enmarca el acceso a cuentas de correo electrónico sin el debido consentimiento de sus propietarios y el manejo o bloqueo de las claves obtenidas de distinta forma.

El artículo 269C plantea la infracción relacionada con la "interceptación ilícita de datos informáticos", también considerada en el Artículo 3 del Título 1 de la Convención de Budapest de 2001. Se presenta cuando una persona, valiéndose de los recursos tecnológicos, obstruye datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático, o de emisiones electromagnéticas de un sistema electromagnético que los transporte.

El delito relacionado con los "daños informáticos" está contemplado en el Artículo 269D y se comete cuando una persona que sin estar autorizada, modifica, altera, daña, borra, destruye o suprime datos del programa o de documentos electrónicos, en los recursos de las TIC.

El artículo 269E contempla el delito vinculado con el "uso de software malicioso" técnicamente denominado *malware*, ya generalizado en internet. Se presenta cuando se producen, adquieren, venden, distribuyen, envían, introducen o extraen del país software o programas de computador que producen daños en los recursos de las TIC.

El delito sobre "violación de datos personales" (*hacking*) lo trata el artículo 269F y está orientado a proteger los derechos fundamen-

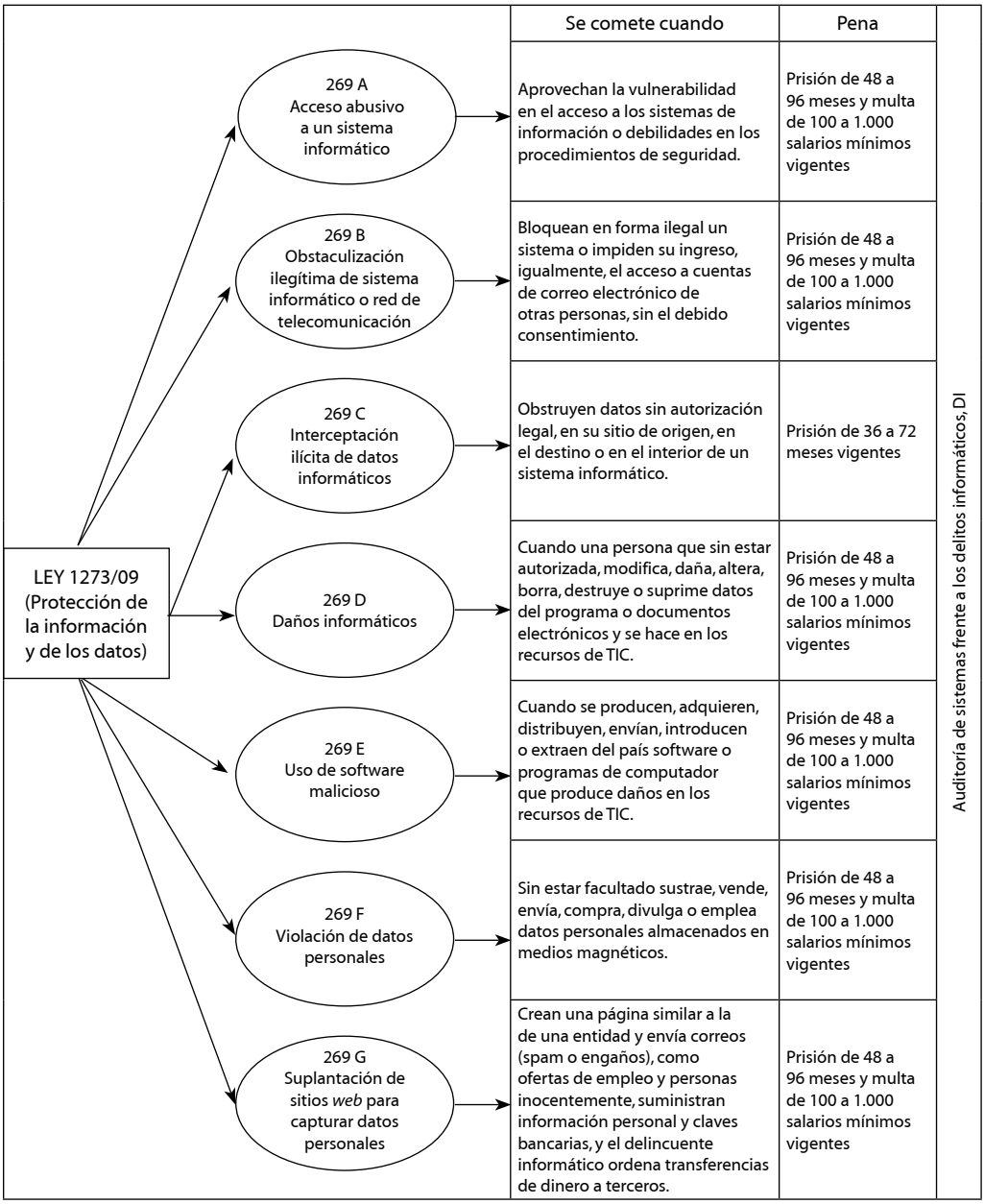

Figura 2. Legislación penal colombiana frente a los delitos informáticos (artículo 1 de la Ley 1273 de 2009).
Fuente: Elaboración de los autores, con base en la Ley 1273 de 2009. Congreso de la República (2009).

tales de la persona (como dignidad humana y libertad ideológica). Se da cuando un individuo sin estar facultado, sustrae, vende, envía, compra, divulga o emplea datos personales almacenados en ficheros, archivos, bases de datos o medios similares con el fin de lograr utilidad personal o para otros.

El artículo 269G trata de la "suplantación de sitios *web* para capturar datos personales". Sucede cuando el suplantador (*phisher*) o delincuente informático crea una página y un dominio similar al de la entidad a la cual desea abordar, lo ubica en un *hosting* (espacio en un servidor) desde donde envía correos *spam* o engañosos (por ejemplo, empleos). Al no distinguir la página original de la falsa, las personas inocentemente suministran información personal y claves bancarias que el suplantador almacena en una base de datos y luego ordena la transferencia del dinero de la víctima a cuentas de terceros quienes prestan sus cuentas o servicios (testaferros), que luego reclama o distribuye.

La Figura 3 muestra las "Circunstancias de agravación punitiva", o aquellas situaciones que por agravantes aumentan la pena del delito (Artículo 269H/Ley 1273 de 2009).

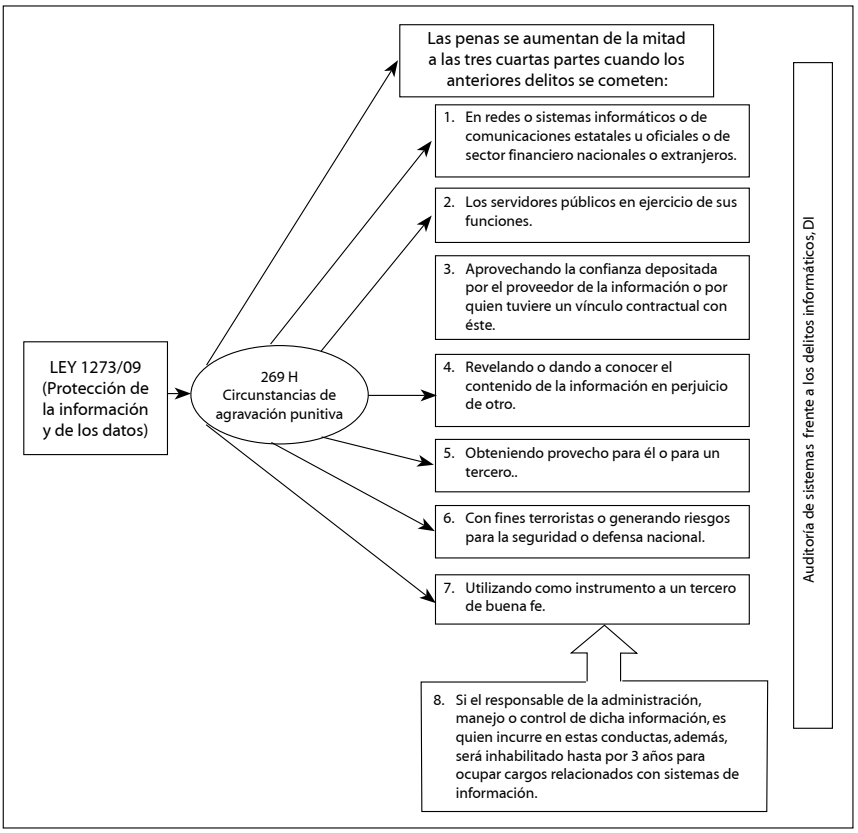

Figura 3. Legislación penal colombiana frente a los delitos informáticos (artículo 1 de la Ley 1273 de 2009).
Fuente: Elaboración de los autores, con base en la Ley 1273 de 2009. Congreso de la República (2009).

Estas condiciones se dan cuando el delito se comete en redes, sistemas informáticos y de comunicaciones del Estado o del sector financiero nacional o extranjero; o cuando se origina o promueve por un funcionario público; o cuando se da a conocer información confidencial en perjuicio de otro para obtener provecho propio o de terceros; o cuando se actúa con fines terroristas para atentar contra la seguridad o defensa nacional, o cuando se usa como instrumento a un tercero de buena fe.

En la Figura 4 se trata de "Los atentados informáticos y otras infracciones"; referidos en los artículos 269I "Hurto por medios informáticos y semejantes" y 269J "Transferencia no consentida de activos", entendidos normalmente como delitos 'ordinarios' en cuya realización es importante el uso de recursos tecnológicos contemplados en el capítulo II de la Ley 1273 de 2009 analizada.

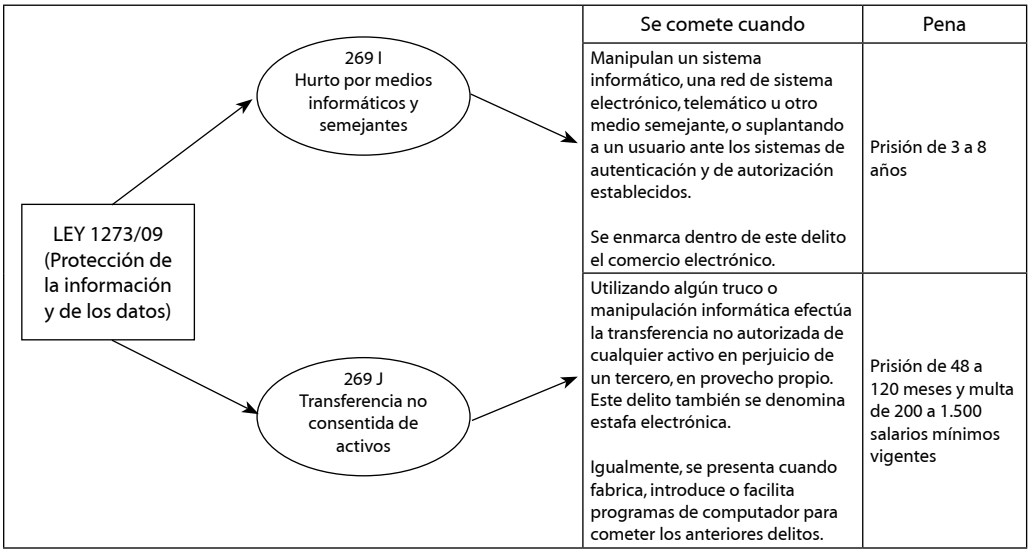

Figura 4. Legislación penal colombiana frente a los delitos informáticos (artículo 2 de la Ley 1273 de 2009).
Fuente: Elaboración de los autores, con base en la Ley 1273 de 2009. Congreso de la República (2009).

Las condiciones del contexto tecnológico de la información y las comunicaciones, sus tendencias y riesgos han generado la reacción del mundo, de sus instituciones y su justicia ante la aparición de los *delitos informáticos*. Frente a eso, ¿cómo están actuando las instituciones financieras colombianas?

4. La seguridad informática en las entidades financieras

Uno de los sectores económicos más amenazados y atacados por los delincuentes informáticos en todo el mundo, es el financiero, que tiene gran impacto, a su vez, en prácticamente

todas las transacciones económicas de la sociedad, de las personas, organizaciones y países. Sobre ese sector se hace el contraste analítico del contexto, tendencias, normatividad jurídica y estándares de seguridad informática con el cual se completa esta propuesta de estudio.

Para la observación del sector financiero se desarrollaron tres fases o momentos: un primero de diseño del instrumento (encuesta), para atender el enfoque general del estudio; el segundo, de aplicación del instrumento entre una población seleccionada de entidades financieras; y el tercero, de análisis de resultados cuyo primer avance aquí se presenta para luego llegar a una conclusión.

Con el instrumento se buscó detectar elementos claves de la realidad de las entidades financieras, en cuanto a la forma como determinan su propio enfoque de la seguridad informática y las estrategias con las cuales enfrentan los riesgos y las crecientes y peligrosas amenazas a la integridad, confiabilidad y disponibilidad de la información y de su infraestructura tecnológica. La encuesta se aplicó a los principales agentes y protagonistas especializados en la seguridad y la tecnología de la información y las comunicaciones de las entidades financieras (grupos de auditoría de sistemas y líderes del área de tecnología de información), por su responsabilidad en los procesos de gestión, operación, auditoría, seguridad y control de los sistemas de información.

La encuesta se estructuró sobre nueve ejes temáticos con los cuales se pretendía interpretar el concepto de seguridad integral de la organización:

1. Políticas y estrategias de seguridad de la información.
2. Conocimiento y aplicación de normas sobre seguridad y delitos informáticos.
3. Planes de seguridad y continuidad del negocio.
4. Gestión de riesgos y vulnerabilidades.
5. Procedimientos de seguimiento y control.
6. Técnicas y herramientas de auditoría.
7. Gestión del potencial humano en seguridad de la información.
8. Administración de los derechos digitales.
9. Inversiones en seguridad informática.

En la mayoría de los ejes temáticos, se plantearon afirmaciones para que el encuestado respondiera según el grado de aproximación o alejamiento que él pudiera observar en su organización acerca de cada afirmación. En otros, la respuesta trataba de verificar la existencia o no de un elemento del concepto integral de seguridad informática, o también el ordenamiento de temas para identificar prioridades de la organización sobre el mismo concepto.

Se identificaron 39 entidades objeto de estudio, con las cuales se buscó el contacto para la encuesta pero sólo 17 (44%) mostraron interés efectivo y disposición a responderla, como en efecto sucedió. La mayoría de quienes no respondieron, justificó su negativa en el explicable celo con el que las entidades financieras manejan y protegen su información, a pesar de que se garantizó la reserva y la confidencialidad de los datos suministrados.

Los primeros resultados de la encuesta aplicada a las 17 entidades durante el primer trimestre de 2010, se presentan en la Tabla 1:

Resultado general de los factores investigados, y a continuación se visualizan en forma comparativa entre los mismos factores en la Figura 5. De aquí resultan los elementos de juicio para un análisis preliminar.

No.	Factores	V	I
1	Políticas y estrategias de seguridad de la información	4,0	4
2	Conocimiento y aplicación de normas sobre seguridad y delitos informáticos	3,9	6
3	Planes de seguridad y continuidad del negocio	4,6	1
4	Gestión de riesgos y vulnerabilidades	4,3	2
5	Procedimientos de seguimiento y control	4,1	3
6	Técnicas y herramientas de auditoría	3,4	7
7	Gestión del potencial humano en seguridad de la información	3,3	8
8	Administración de derechos digitales	3,2	9
9	Inversiones en seguridad informática	4,0	4
Promedio general		3,9	

Tabla 1. Resultado general de los factores investigados.
Valoración (V) sobre 5, e Importancia (I) según prioridad.
Fuente: Encuesta a entidades financieras, 2010.

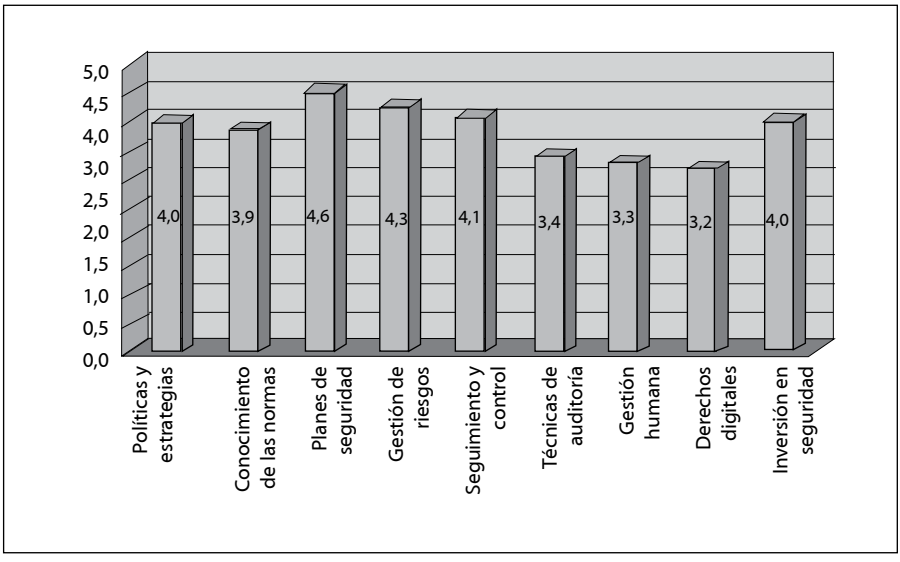

Figura 5. Valoración de la seguridad informática en las entidades financieras, 2009.
Fuente: Tabla 1. Resultado general de los factores investigados, entidades financieras, 2010.

1. El primer eje temático de la encuesta sobre *Políticas y estrategias de seguridad de la información*, se indagó con seis (6) preguntas cuyo promedio entre las entidades investigadas llegó a 4 sobre 5, lo que indica que, en general, las entidades financieras encuestadas atienden en un 80% la definición y desarrollo de políticas y estrategias de seguridad informática. Sin embargo, el 94% de ellas dispone de *planes y políticas de seguridad de la información*, y sólo el 24% de ellas *tiene relación con instituciones internacionales de seguridad informática y delitos* informáticos. Hay preocupación general, aunque no suficiente todavía.
2. El segundo factor clave está relacionado con el *Conocimiento y aplicación de normas sobre seguridad y delitos informáticos* y, al respecto, en promedio, el 60% de los encuestados dijo conocer y aplicar el Código Penal Colombiano (Ley 599 de 2000). Un porcentaje más alto (82%) señaló su conocimiento sobre las normas de la Superintendencia Financiera de Colombia (en especial la Circular Externa 014 del 17 de abril de 2008 sobre *transacciones a través de los canales de distribución dispuestos por las entidades vigiladas*) y otro 76% dice estar aplicando la ley 1273 de 2009. Indica esto que el conocimiento de la Ley no es generalizado y que se da una importancia asimétrica a las disposiciones vigentes sobre delitos informáticos, a pesar de su importancia, no sólo para la organización sino para el cliente y la institucionalidad.
3. El tercer eje relacionado con *planes de Seguridad y Continuidad* también se analizó con seis (6) preguntas, sobre las cuales el 94% de las entidades manifestó el desarrollo de *planes documentados y aprobados de continuidad del negocio* (Business continuity planning, BCP), al identificar los procesos y las áreas clave que requieren mayores controles y seguridad. Se resalta la seguridad expresada en procedimientos para crear copias, cuya aplicación se da en el 100%.
4. En cuanto a la *gestion de riesgos y vulnerabilidades* se observa, como en el caso anterior, aunque sin llegar a ese nivel, una alta atención que en promedio llega al 86% de los encuestados. El punto de *revisión* periódica de antivirus informáticos y de los sistemas de prevención y detención de malware es el factor más atendido (cerca del 100% de los casos) y lo mismo sucede con el *desarrollo de mapas de riesgos actualizados*. La *detección específica de riesgos en el manejo de datos*, como fraudes, o *en el nivel del negocio*, o *financiero*, o de *cumplimiento de normas*, es identificada por las entidades, aunque en proporciones no mayores al 31%.
5. La *calificación promedio del factor clave* relacionada con los *procedimientos de seguimiento y control*, fue de 4,1, que corresponde al 82% de la percepción general, siendo uno de los tres aspectos más *reconocidos* entre los nueve factores analizados, lo cual indica el grado de importancia que las entidades han dado al establecimiento y consolidación de guías y medios de control de sus *sistemas de seguridad*, lo cual se corrobora con el 92% de atención al "*establecimiento de procedimientos de identificación y autenticación*", según *todos* los encuestados, mientras que, paradójicamente, esa atención baja (al 64%)

cuando se indaga sobre realización de *pruebas de seguridad* (*ethical hacking*, penetración, vulnerabilidad).

6. En el factor relacionado con las *técnicas y herramientas de auditoría*, se buscó identificar el empleo de distintas herramientas relacionadas con los procesos de auditoría y se encontró que, en promedio, el 68% de los encuestados le presta atención al empleo de diversos instrumentos, entre los que se destacan el *cifrado de paquetes* (88%), el *aprovechamiento de las herramientas específicas de auditoría* (58%) y la *aplicación del Balanced Scorecard* (48%). Sobre este último instrumento, en diversos estándares como el CObIT 4.1 (ISACA, 2007, pp. 162-164) se menciona y recomienda su aplicación en los distintos dominios, en especial cuando se trata del "Monitoreo y Evaluación", por cuanto permite evaluar el desempeño del sistema de seguridad informática con respecto a los objetivos estratégicos de la organización y el uso de los recursos, lo mismo que en la administración de riesgos y en el alineamiento del sistema de gobierno de seguridad de la información con los requerimientos impuestos por la estrategia corporativa. De igual manera, ofrece una visión del grado de desempeño de las TIC, desde las perspectivas financiera, de los clientes, de los procesos internos y del aprendizaje y el crecimiento.
7. La *gestión del potencial humano en seguridad de la información* de las organizaciones encuestadas, es importante como enfoque integral sólo en el 66% de las entidades. El énfasis es en los procesos periódicos de *capacitacion de los funcionarios encargados de la seguridad de la entidad* (76% de los casos), reconociendo que el personal encargado es suficiente, que la capacitación es la adecuada y que hay responsables del seguimiento a los incidentes de seguridad de la información.
8. En el eje *administración de los derechos digitales* se encuentra tal vez la mayor debilidad detectada entre los encuestados, pues la atención promedio dada a este aspecto cubre apenas el 64% de las entidades. Y aunque el 76% manifiesta que la *privacidad de la información en la entidad se encuentra en una etapa madura de desarrollo*, sólo el 58% afirma estar de acuerdo con el nivel de *legitimación de los derechos de autor* en la entidad, en cuanto hace a la autoría y desarrollo de herramientas de software.
9. En general, las *inversiones en seguridad informática* reciben un aceptable nivel de atención (80%), pero se observa asimetría en la atención, pues mientras los recursos asignados anualmente a *tecnología y procesos de seguridad en información* se reconocen en el 94% de los casos. No sucede lo mismo con los recursos para la *capacitación a los empleados en seguridad de la información* ya que en este punto la atención sólo se reconoce en el 70% de los encuestados.

Conclusiones

Los acelerados procesos de *globalización* con sus innumerables y cada vez más sorprendentes atractivos y posibilidades para la humanidad entera, impulsados todos por el avance tecno-

lógico de las comunicaciones y la *informática* se han convertido en el nuevo paradigma de las relaciones personales, organizacionales, locales e internacionales, del conocimiento y el desarrollo. Pero tan importante y dinámico cambio que ha condicionado los nuevos comportamientos sociales, económicos, políticos y éticos de las personas y los pueblos, ha venido acompañado de un no menos dinámico y, a la vez, peligroso proceso de una nueva delincuencia que, al utilizar o impactar los sistemas de información y comunicación de las organizaciones y el mundo, ha llegado a posicionarse como uno de los cada vez mayores peligros para la seguridad, la honra, vida y bienes de las personas y las organizaciones de todos los países.

Frente a esos dos fenómenos: el positivo o neutro de la globalización por la tecnología, la información y las comunicaciones, y el negativo de la *ciberdelincuencia*, las organizaciones[3] y algunos gobiernos del mundo[4] han venido tomando conciencia de la perspectiva de futuro y la subyacente amenaza, para actuar mancomunadamente y construir barreras no sólo tecnológicas, sino también jurídicas y sociales que permitan enfrentar con probabilidades de éxito ese gran mapa de riesgos generado por los delitos informáticos.

Como consecuencia, se han diseñado, divulgado y aplicado no sólo modelos, sistemas, herramientas y procedimientos de seguridad informática, sino también el necesario complemento legal para combatir el delito, además de la capacitación y preparación especializada para manejar estos componentes de seguridad, de manera integrada y cada vez más generalizada entre la sociedad.

En Colombia, con algunos antecedentes de carácter jurídico (sobre la base de los derechos de autor) y alguna normatividad complementaria (Código Penal y circulares de la Superintendencia Financiera), en 2009 se logró expedir la Ley 1273, con la cual pudo acceder al grupo de países que se han preparado con herramientas más eficaces para contrarrestar las acciones delictivas del cibercrimen, en sectores claves de la sociedad como el financiero, cuyas condiciones de vulnerabilidad son las más estudiadas e investigadas por los delincuentes informáticos.

En el contexto mundial observado, las tendencias del cambio caracterizadas y aceleradas por las tecnologías de la información y la comunicación han venido aparejadas con las tendencias delictivas, ahora caracterizadas como *ciberdelito* entre cuyos gestores y dinamizadores en el mundo, se encuentra gente preparada, estudiosa, investigativa y con gran poder de mimetización en el ciberespacio. Frente a eso, los países más afectados, en general, y Colombia, en particular, han desarrollado distintos mecanismos tecnológicos y también jurídicos para actuar en los escenarios del cibercrimen, entre los cuales el sector financiero es uno de los más amenazados. Por esta misma razón, sus condiciones de vulnerabilidad y gestión del riesgo informático pueden señalar un derrotero para orientar las normas, políticas, estrategias y pro-

3 En particular, las especializadas en productos de la tecnología informática (Cisco, por ejemplo), en sistemas de protección, seguridad y control informático (como ISACA) o en servicios relacionados (Etek).

4 Barack Obama, presidente de Estados Unidos, ha recomendado crear un grupo de coordinación de ciberseguridad, encargado de la estrategia de protección de redes gubernamentales y privadas.

cedimientos que permitan enfrentar tal amenaza y velar por la seguridad de toda la sociedad, puesto que ella no sólo va dirigida a un sector en particular, sino a todas las actividades del mundo en las que se muevan recursos financieros.

En una primera observación general, puede decirse que las condiciones de seguridad del sistema financiero, visto por los resultados de las 17 entidades encuestadas, presentan distintas condiciones de riesgo que llevan a concluir que la confiabilidad no está plenamente demostrada, bien porque no se ha generalizado una conciencia integral del fenómeno y su negativo impacto, o porque los riesgos y amenazas, por el medio en el cual se desarrollan, siguen sin estar identificados en todo su espectro, o porque ha faltado coherencia en el aparejamiento de los sistemas de seguridad a los riesgos previstos, o porque los instrumentos apropiados también permanecen desconocidos, o porque se mantiene la pobre noción de las herramientas técnicas, jurídicas y sociales para enfrentarlos, en fin, entre otras muchas razones, porque las estrategias diseñadas siguen limitadas o son insuficientes para generar cultura de la seguridad informática en las instituciones, en las organizaciones y en la sociedad.

Si bien el sector analizado reconoce la importancia de la planificación de la seguridad informática, tal reconocimiento no es suficientemente coherente con las técnicas, herramientas y procedimientos aplicados y menos con la preparación del talento humano para garantizarla, ni con la inversión destinada al efecto.

No basta con planear y nombrar responsables si en el direccionamiento no se incorpora el desarrollo integral del sistema de seguridad que genere una cultura apoyada desde las propias capacidades y fortalezas internas: las existentes y las que es necesario preparar y consolidar, junto con el conocimiento, la conciencia clara y el aprovechamiento efectivo del apoyo existente en las fuerzas externas del Estado, de la Ley y de la sociedad misma, además de las entidades que internacionalmente trabajan el tema.

Éste es un reto colectivo. No es solamente para las organizaciones o las personas que están en la mira permanente de los ciberdelincuentes. Es un desafío para la sociedad y el Estado, para los jueces y los administradores de justicia, que deben estar preparados no sólo en el conocimiento de la Ley y la jurisprudencia, sino en el apropiado conocimiento del contexto tecnológico, informático y de sus proyecciones delictivas.

No obstante las observaciones corresponden a una muestra de un sector específico, por las condiciones de ese sector y su impacto en toda la sociedad, no es exagerado destacar que el reto del cibercrimen, ante las condiciones para enfrentarlo (vistas en el sector tal vez más significativo para observarlo), implican un reto a las propias condiciones de supervivencia y desarrollo de las personas, las organizaciones y las instituciones del país y del mundo. No se puede subestimar su poder, complejidad y alcance que puede llegar no sólo a los recursos, propiedades y derechos, sino de las posibilidades de vida. No basta con formar grupos de defensa o ataque al cibercrimen, si no se construye la conciencia organizacional y ciudadana de la seguridad informática, como parte integral de la cultura de

mejoramiento de las condiciones de vida de la gente.

Referencias

Aldama-Baquedano, Concepción (1993). Los medios informáticos. *Poder Judicial* (30), 9-26.

Álvarez-Marañón, Gonzalo & Pérez-García, Pedro Pablo (2004). *Seguridad informática para la empresa y particulares*. Madrid: McGraw-Hill.

Asociación para la Auditoría y Control de Sistemas de Información, Information Systems Audit and Control Association, ISACA (2007). *Objetivos de control para la información y tecnologías relacionadas* (Control Objectives for Information and related Technology, CObIT). Disponible en: http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx.

Beltramone, Guillermo; Herrera-Bravo, Rodolfo & Zabale, Ezequiel (1998). *Nociones básicas sobre los delitos informáticos.* Disponible en: http://rodolfoherrera.galeon.com/delitos.pdf.

Camacho-Losa, Luis (1987). *Delito Informático*. Madrid: Gráficas Cóndor.

Choclán-Montalvo, José Antonio (1997). Estafa por computación y criminalidad económica vinculada a la informática. *Actualidad Penal* (47), 22-28.

Colombia, Congreso de la República (1993). Ley 44 de 1993, por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944. *Diario Oficial No. 40.740*, 5 de febrero de 1993. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley/1993/ley_0044_1993.html.

Colombia, Congreso de la República (2000). Ley 599 de 2000, por la cual se expide el Código Penal. *Diario Oficial No. 44.097*, 24 de julio de 2000. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley/2000/ley_0599_2000.html.

Colombia, Congreso de la República (2001). Ley 679 de 2001, por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. *Diario Oficial No. 44.509*, 4 de agosto de 2001. Disponible en: http://www.cntv.org.co/cntv_bop/basedoc/ley/2001/ley_0679_2001.html.

Colombia, Congreso de la República (2009). Ley 1273 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 conservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. *Diario Oficial No. 47.223*, 5 de enero de 2009. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html.

Colombia, Congreso de la República (2009). Ley 1336 de 2009, por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. *Diario Oficial No. 47.417*, 21 de julio de 2009. Disponible en: http://www.

icbf.gov.co/transparencia/derechobienestar/ley/2009/ley_1336_2009.html.

Colombia, Policía Nacional, Dirección de Investigación Criminal, DIJIN. http://www.dijin.gov.co.

Colombia, Presidencia de la República (1989). Decreto 1360 de 1989, por el cual se reglamenta la inscripción del soporte lógico (*software*) en el Registro Nacional del Derecho de Autor. 23 de junio de 1989. Disponible en: http://www.convenioantipirateria.org.co/index.php?option=com_content&view=article&id=98:decreto-1360-de-1989&catid=45:decretos-reglamentarios&Itemid=109.

Davara-Rodríguez, Miguel Ángel (2007). *Código de internet*. Madrid: Aranzadi.

Davenport, Thomas (1999). *Ecología de la información*. México: Oxford University Press.

Gómez-Perals, Miguel (1994). Los delitos informáticos en el derecho español. *Informática y Derecho: Revista Iberoamericana de Derecho Informático* (4), 481-496.

Gómez-Vieites, Álvaro (2006). *Enciclopedia de la seguridad informática*. Madrid: Alfaomega.

Huidobro-Moya, José Manuel (2005). *La tecnología e-business*. Madrid: Thompson.

International Organization for Standardization, ISO, International Electrotechnical Commission, IEC (2005). *ISO/IEC 17799/2005. Disponible en: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612*.

Laudon, Kenneth C. & Guercio-Traver, Carol (2009). *E-commerce*. México: Pearson Prentice Hall.

Office of Public Sector Information, OPSI (1990). *Computer Misuse Act*. Disponible en: http://www.opsi.gov.uk/revisedstatutes/uk-acts-1990a.

Peso-Navarro, Emilio del (2001). *Peritajes informáticos*. Madrid, Díaz de Santos.

Piattini-Velthuis, Mario Gerardo & Peso-Navarro, Emilio del (2001). *Auditoría informática*. Madrid: Alfaomega.

Suárez-Sánchez, Alberto (2009). *La estafa informática*. Bogotá: Grupo Ibáñez.

Superintendencia Financiera de Colombia (2008). Circular externa 014 de 2008. Información sobre transacciones efectuadas a través de los canales de distribución dispuestos por las entidades vigiladas. Disponible en: http://www.actualicese.com/normatividad/2008/04/17/circular-externa-014-de-17-04-2008/, http://www.superfinanciera.gov.co/NormativaFinanciera/Paginas/bolfinanciera2008_04.htm.

Téllez-Valdés, Julio (2007). *Derecho informático*. 3ª ed. México: McGraw Hill.

Torres-Torres, Henry William (2002). *Derecho informático*. Medellín: Ediciones Jurídicas.

Infografía

Cisco, Presentación de información diversas fuentes, 2008. http://www.dinero.com/negocios/telecomunicaciones/colombia-tiene-mejorar-seguridad-informatica_50693.aspx.

www.eltiempo.com/tecnologia/enter/actualidad_a/home/colombia-debil-en-seguridad-informatica_4393234.

PricewaterhouseCoopers, *The global state of information security*. http://www.pwc.com/be/

en/publications/the-global-state-of-infor-maiton-security.jhtml.

Trend Micro (2008). *Los 20 virus informáticos más importantes de la historia, sepa cuáles son*. http://www.elcomercio.com.pe/ediciononline/HTML/2009-01-22/los-20-virus-informaticos-mas-importantes-historia-sepa-cuales-son.html.

http://www.elguruinformatico.com/2009/01/25/los-peores-virus-informaticos-de-la-historia/.

http://www.delitosinformaticos.com/delitos/colombia3.shtml.

- Fecha de recepción: 1 de febrero de 2010
- Fecha de aceptación: 23 de mayo de 2010

Para citar este artículo

Ojeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad*, *11* (28), 41-66.