LA PRÁCTICA DE DELITOS INFORMÁTICOS EN COLOMBIA

EDISON RAUL SERRANO BUITRAGO

AUTOR

ASESOR TEMATICO

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE RELACIONES INTERNACIONALES

ESPECIALIZACIÓN EN ADMINISTRACIÓN DE LA SEGURIDAD

BOGOTÁ NOVIEMBRE 19 DE 2014

Resumen

La importancia de referir el origen, evolución, métodos y tipos de personas que intervienen en un hecho delictivo de carácter informático en Colombia, tiene como fin último reiterar la necesidad de proteger la información y los activos personales o de una empresa e institución, se estima que todo equipo de cómputo y medio informático es vulnerable de ser afectado. Se determina que el delito informático lo puede cometer una persona con conocimientos básicos de sistemas, que el internet facilita las actividades delictivas y para contrarrestar esta amenaza, se requieren controles adecuados y una cultura que motive la seguridad informática. Se requiere denunciar estos delitos oportunamente ante las autoridades competentes a fin de evitar la impunidad, solo de esa manera se podrán reducir fraudes, robos y en general los delitos informáticos.

Palabras clave:

Delictivo, Informático, Activos, Amenaza, Impunidad.

Introducción

Los delitos informáticos en Colombia cobran gran importancia a causa de las millonarias pérdidas de activos que reportan las empresas y los usuarios, a esto se suman, las indemnizaciones, pago de pólizas y pago de seguros, evidenciando una clara falla en el sistema de seguridad informático implementado por parte de las empresas y personas afectadas.

Pero más alarmante es el hecho de ver vulnerada la intimidad, integridad de las personas y peor aún sus datos personales, información que es comercializada por parte de los ciberdelincuentes de manera inescrupulosa y vendida al mejor postor, así sea un simple correo o una foto intima, es sujeto de negociarse en las redes sociales y ventanas de mercados virtuales a nivel mundial.

De ahí que en este ensayo se quiera hacer una reflexión en cuanto a la historia, evolución y práctica de los delitos informáticos en Colombia, como apoyo a la búsqueda de soluciones y recomendaciones que permitan mejorar u optimizar los sistemas de seguridad informáticos, sus procesos y procedimientos. No se pretende hacer un análisis o una investigación, lo que se quiere es reflexionar sobre una serie de eventos que se convirtieron en costumbre, error tras error, desconociendo la historia y en muchos casos la normatividad existente en cuanto al tema.

Debido a los cambios tecnológicos y nuevas herramientas informáticas que existen en la actualidad, se ha generado un ambiente de inseguridad mucho más amplio. Se pensaría que a mayor tecnología, mayor seguridad, pero realmente al inundar el mercado con nuevos productos, bienes y servicios tecnológicos, el usuario está entrando en un vicio virtual desmedido que lo

ciega a los controles de seguridad que debe adoptar para proteger su información y sus datos, es esta actividad consumista la que no tiene límite, al punto de preferir la tecnología que la seguridad informática.

De manera que con este trabajo se quiera hacer énfasis en los errores cometidos por los usuarios al emplear herramientas informáticas, la necesidad de generar controles de seguridad adecuados y la importancia de conocer, difundir y aplicar la normatividad existente en temas de protección, sanción y penalización en la que puede verse inmerso un delincuente informático.

El origen, evolución y estado actual de la práctica de delitos informáticos en Colombia

Este ensayo tiene como objetivo general describir la normatividad y situación de la seguridad informática durante los últimos años en Colombia, para ello se elabora un marco teórico acerca del origen, evolución y estado actual de la práctica de delitos informáticos, así mismo se relacionan los sectores y/o tipos de victimas más susceptibles al delito informático.

Por lo anterior se hace necesario definir delito informático o ciberdelicuencia, es toda aquella acción, típica, antijurídica y culpable, dada por vías informáticas cuyo objetivo es destruir y dañar ordenadores, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

Entre las principales modalidades de delitos informáticos según expertos en tecnología forense, referencian que esta clase de crímenes se encentran agrupados en el Código Penal Colombiano, mencionando los siguientes; acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño Informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales, hurto por medios informáticos y semejantes y transferencia no consentida de activos, delitos amparados por la Ley 1273 de 2009.

Al mismo tiempo el Código Penal Colombiano incluye delitos que pueden ser cometidos por medios informáticos, en este contexto se relacionan algunos como son; los delitos contra la intimidad, la usurpación y cesión de datos reservados de carácter personal, delitos contra el honor, calumnia e injuria, estafa, defraudaciones de fluido eléctrico e incluye de forma expresa la defraudación en telecomunicaciones siempre y cuando se utilice un mecanismo para la realización de la misma, o alterando maliciosamente las indicaciones o empleando medios clandestinos, delitos relativos a la propiedad intelectual (Cómo proteger las creaciones y proyectos desarrollados en una empresa), delitos relativos a la propiedad industrial, delitos relativos al mercado y a los consumidores, publicidad engañosa cuando se hagan alegaciones falsas o manifiesten características inciertas sobre los mismos, causando un perjuicio grave y manifiesto a los consumidores.

Resulta oportuno relacionar los daños asociados a delitos informáticos, estos perjuicios se pueden agrupar en dos métodos, el primero hace referencia a los daños y destrozos físicos en los ordenadores, computadores o sistemas de seguridad y vigilancia, donde la característica de este método es el deterioro y no tiene ánimo de lucro, su pretensión es la de sabotear o neutralizar los sistemas como por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en los equipos, son una serie de conductas destinadas a la destrucción física del hardware y el software de un sistema. El otro método está dirigido a causar daños lógicos, son todas aquellas conductas que producen, como resultado, la destrucción, inutilización, o alteración de datos, programas, bases de datos información, documentos electrónicos, contenidos en cualquier soporte lógico, sistemas informáticos o telemáticos que permitan la intrusión del delincuente quien busca acceder a las bases de datos, la suplantación de identidad, el hurto de activos, o con la pretensión de causar

destrozos irrecuperables de la información empresarial, destrucción de los sistemas de protección informática, hurto de secreto comercial. Este tipo de daño puede alcanzar diferentes formas desde la más simple que se pueda imaginar como el borrado de archivo de una empresa, borrado de contabilidad, borrado de listado de clientes, hasta la utilización de los más complejos programas lógicos destructivos (crash programs), sumamente riesgosos, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo o simplemente hurto de bases de datos o información susceptibles de venta en el mercado negro.

Con respecto a lo anterior se establece: los tipos de organizaciones y tipos de personas que cometen los delitos informáticos pueden variar según su experiencia, capacitación y objetivo final, en ese mismo sentido es común encontrar personas con escaza práctica (novatos), y personas que cometen delitos de manera personal e independiente hasta llegar a la delincuencia organizada, mediante redes virtuales y reuniones clandestinas estandarizan sus métodos de ataque cibernético rentables les proporcionen activos para ser ofertados en el mercado negro son los llamados sujetos activos.

> Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso informático, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. (Acurio Del Pino, 2010, p.15)

Con el tiempo se ha podido identificar a los autores de delitos informáticos son muy diversos y la diferencia entre sí, es la naturaleza de los delitos cometidos. Según las investigaciones forenses en el mercado negro se venden y negocian un sin número de cuentas de correos electrónicos, estas bases de datos permiten a los ciberdelincuentes escoger sus víctimas y ejecutar sus ataques, todo depende de la información alcanzada a descifrar en cada correo electrónico o cuenta bancaria, para este evento los delincuentes emplean el sistema de captación de información conocido como ingeniería social, en informática es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica la pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos, pero son los mismos investigadores forenses son quienes describen al sujeto activo variable y no ostenta un determinado estatus social o económico. Sutherland (2005) afirma "El sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional" (p.16). De esta manera los avances tecnológicos han permitido mejorar los sistemas de comunicación y unir al mundo mediante redes virtuales e informáticas, estas tecnologías llevan consigo beneficios pero a la vez sin su adecuado empleo y las medidas de seguridad óptimas, la tecnología en el ambiente informático puede causar daños irreparables desde económicos como físicos. Desde el inicio de la Internet todas las generaciones viven los avances del siglo XXI se han visto en la obligación de adaptarse a los cambios tecnológicos en acelerado crecimiento, es este afán que cede a los errores más usuales y comunes aprovechados por los delincuentes informáticos, en Colombia es común emplear celulares, laptops, Tables, y dispositivos móviles para hacer transacciones bancarias,

consultar datos personales, participación en redes sociales de mayor popularidad entregando toda la información necesaria para los trabajos de ingeniería social, estas tecnologías facilitan muchos procesos haciendo la vida más fácil y agradable a las personas, esa misma tecnología permite a los ciberdelincuentes cometer sus delitos indiscriminadamente sin piedad alguna. Se piensa que es importante educar a la población en el manejo y aplicación de la tecnología, sin embargo en Colombia la Educación en informática se asienta al manejo de Computadores y programas básicos de uso familiar y comercial no contemplando la seguridad informática como factor fundamental de prevenir y evitar los daños causados por la delincuencia, se considera que la educación en Colombia debe analizar esta problemática y establecer una estrategia de soluciones prontas ante una crisis que se ve venir, es importante tener en cuenta a Colombia como un país consumista y los colombianos son felices invirtiendo en tecnología moderna, así tengan equipos o aparatos que suplen las necesidades básicas del ciudadano común, se evidencia el desespero por tener el ultimo celular, el ultimo computador de mesa o la última TV, sin escatimar recursos y sin tener en cuenta los sistemas de seguridad y medidas a adoptar.

La llegada a Colombia en la práctica de la delincuencia informática no tiene un origen exacto o una fecha específica. Para los estudiosos del tema se considera que esta práctica se instituye formalmente cuando la Legislación Colombia incluye en su normatividad los delitos informáticos y establece penas por su ocurrencia, siendo Colombia el primer país que penaliza los delitos informáticos bajo el auxilio de la Ley 1273 de 2009, denominada de la protección de la información y de los datos, y a diferencia de otros países también se imponen las sanciones económicas más altas del Código Penal colombiano. La pena económica más baja está en 100 salarios mínimos mensuales legales vigentes, cerca de los 60 millones de pesos, en casos de delitos informáticos la máxima puede llegar a los 600 millones de pesos, dependiendo del delito

cometido, sin embargo la justicia colombiana diverge de esta ley y surgen diferencias desde el punto de vista de cada juez.

> En Colombia no sé si es por desconocimiento de los fiscales o de los jueces, pero muchos delitos informáticos están siendo juzgados como delitos clásicos, y ubican al delito informático como una circunstancia de agravación que se usa para aumentar la pena. (Díaz García, 2010, pag12).

A pesar de que esta clase de delitos se cometen en Colombia por más de una década y bajo el auspicio de la Cibercriminalidad, aunque posteriormente fue decretada la legislación colombiana para desafiar las amenazas Informáticas, para algunos jurídicos esta normatividad es tardía. De acuerdo con los estudios realizados en 2008 por (CISCO) certificación básica o inicial es CCNA que significa Cisco Certified Networking Associate, según los cuales el país registraba una de las calificaciones más bajas en seguridad informática en comparación con otros seis países de Latinoamérica con un resultado de 62 puntos de 100 posibles, lo que deja ver una ventaja delincuencial informática considerable.

Por lo anterior expuesto, en Colombia esta normatividad toma importancia a partir de la inversión extranjera y la necesidad de generar condiciones de seguridad para las transacciones bancarias entre otras importantes actividades realizadas por medio de las redes digitales. Se deduce que fue la presión extranjera la que obligo a países como Colombia a generar mecanismos de defensa, traducidos a mecanismos jurídicos, pero queda un sin sabor en cuanto al control de la educación informática, especialmente los sitios clandestinos donde se enseña a ser un sujeto activo de la informática, o lugares abiertos al público donde se promueve y se hace apología al delito informático. Se considera por lo tanto la importancia de evaluar estos denominados café

Internet y realizar una investigación más exhaustiva para identificar sitios de entrenamiento de ciberdelincuentes además de implementar controles jurídicos para estos establecimientos.

Ahora bien sería interesante hablar de la evolución de los delitos informáticos en Colombia. Como punto de partida se tiene la ley marco para delitos informáticos y que corresponde a la Ley 1273 del 2009 por la cual se modifica el código penal colombiano y se adhieren artículos para sancionar este tipo de delitos estableciendo penas y multas a los infractores.

Con respecto a esta Ley se considera como un avance que permite enfrentar la amenaza frente a temas de seguridad informática, durante sus ponencias Kevin Mitnick, experto en seguridad informática quien participó en el evento tecnológico Campus Party celebrado en Bogotá desde hace algunos años. Considera la normatividad positiva, debe evolucionar y adaptarse al compás de la tecnología, día a día las tendencias y sistemas cambian, mejoran y evolucionan, entonces las leyes se van quedando obsoletas, Mitnick estadunidense que fue encarcelado durante 5 años por delitos informáticos, se dedica en la actualidad a burlar la seguridad de grandes empresas para después elaborar sistemas seguros, ya desde la legalidad.

En ese mismo sentido se puede decir para la ley en Colombia no satisface los requerimientos de seguridad informática quedando vacíos que permiten a los ciberdelincuentes mantener su actuar delictivo, existe un vacío en seguridad inmenso donde sólo se tratan los casos que más suenan a escala nacional e internacional, pero muchos de los pequeños siguen descuidados.

Uno de esos vacíos a la ley puede ser interpretada desde el punto de vista de cada lector, es así para los jueces en Colombia que no son expertos en el tema pueden deliberar de formas distintas, esto ha permitido que casos jurídicos sean archivados por falta de evidencia, y es porque Colombia no tiene expertos jurídicos en el tema, dejando a los ciberdelincuentes libres para actuar acomodando la ley a su conveniencia.

En complemento la Ley 1273, existen normas anteriores como la Ley 44 de 1993 sobre derechos de autor cuyo objetivo es proteger la propiedad física y moral de los autores de obras otorgándoles la titularidad, en sus Artículos 51 y 52 del Capítulo IV impone sanciones drásticas a sus infractores. Otra norma importe es la Ley 599 de 2000 el Código Penal Colombiano Capítulo Único del Título VII que determina los Delitos contra los Derechos de Autor.

Resulta oportuno resaltar uno de los aspectos que logro fijar la Ley 1273 en Colombia radica en la explotación de pornografía infantil dio sus inicios en revistas y posteriormente a la internet migrando del papel a los sistemas digitales y virtuales al punto de llegar a ser incontrolable inundando el mercado negro virtual sin restricciones ni controles, entonces en el 2001 se promulga en Colombia la Ley 679 que trata del estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con niños menores de edad, lo que impulso la necesidad de generar mecanismos jurídicos para controlar este flagelo más popular en las redes virtuales.

También existe el Decreto 1360 de 1989 para reglamentar la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor.

Pero aún más importante es el artículo 15 de la Constitución Política de Colombia de 1991 sobre el Habeas Data para proteger a todas las personas en su derecho a la intimidad personal, familiar y a su buen nombre.

A lo anterior se podría deducir que existe un buen marco Jurídico, subsidiario, complementario etc. Pero el problema radica en dos aspectos. El primero hace referencia a la falta de divulgación, promoción y aplicación de la normatividad y el segundo hace énfasis en la capacitación, se establece que en Colombia no existen expertos jurídicos en temas informáticos dejando la interpretación de la norma al libre albedrío como se mencionó anteriormente.

Sobre la base de las consideraciones anteriores Colombia podrá seguir firmando convenios como el Convenio de Cibercriminalidad suscrito en Budapest, Hungría, en 2001 y vigente desde julio de 2004, generando leyes, acuerdos, tratados pero si en Colombia no se genera la cultura de la difusión y promoción de las normas vigentes muy seguramente se podría pensar que en temas jurídicos no se está haciendo la tarea en seguridad informática.

Como recomendación para apoyo al sector jurídico en Colombia se podría generar una ley que ordene a entidades públicas y privadas la certificación ISO 27001 o de otro tipo en gestión de seguridad Informática, esta iniciativa puede ser amparada en la ley 872 del 2003 que ordena la creación del sistema de Gestión de Calidad SGC en las instituciones del Estado, de esta manera se lograra subsanar en alguna medida los vacíos encontrados en la ley 1273 de 2009.

Por ello los marcos de las observaciones anteriores la seguridad informática no solo es un problema del Estado, es importante fraccionar responsabilidades a los niveles que corresponda,

en el caso de las empresas formalmente constituidas el compromiso de fortalecer la estructura y funcionamiento de los controles necesarios para la prevención de este tipo de delitos en el territorio nacional.

Dado que el CEO Chief Executive Officer, director ejecutivo de la empresa es responsable final del desempeño y acciones de la empresa, por esta razón las políticas de seguridad informática de una empresa deben pasar por manos y revisión del CEO, además el CEO como mayor autoridad de la empresa tiene que velar por la ejecución de la estrategia para el cumplimiento de estas políticas.

De allí el CIO Chief Information Officer, director de información, pasa reporte directamente al CEO, y siempre está monitoreando que las estrategias y políticas de seguridad informática planteadas en las empresas se cumplan.

Como resultado es importante seleccionar de la manera más profesional y efectiva el personal que labora o tiene responsabilidad directa con seguridad informática, a pesar que este tema es gestión y talento humano no se puede descuidar una selección particular de funcionarios con habilidades y características especiales en informática.

A fin de lograr un buen trabajo y un buen desempeño en la empresa hay que tener cierta seguridad en el área de información, manteniendo la integridad, disponibilidad y confiabilidad de la información que el encargado de la seguridad en informática será responsable de planear, coordinar y administrar los procesos de seguridad informática de la empresa. Aplicar la metodología de análisis de riesgo para evaluar la seguridad informática en la organización.

Implementar la Política de seguridad informática de la organización, procedimientos para aplicarla y monitorearla con nuevas tecnologías permiten acceder de manera muy fácil a la red, pero no es problema mientras esta actividad no sea dañina o inescrupulosa, la red permite disfrutar de las redes sociales, compartir con amigos, descargar fotos, videos, imágenes en si un mundo de bondades virtuales a las que años atrás era imposible acceder, sin embargo el permitir tanto acceso a la información se puede llegar a ser víctima de un cracker.

> En general se tiene la idea de que un hacker es un pirata informático que se infiltra en sistemas informáticos sin autorización, ilegalmente, para robar, modificar o destruir información. Esta visión, en realidad, es errónea. De esa definición se desprende el concepto de cracker. (Solano, 2008, p.17).

Con el objeto de establecer responsabilidades, es el auditor quien debe hacer cumplir los controles y mantener una observancia de estos controles, lo que se considera que en el nivel de control el auditor tiene la mayor de las responsabilidades, es esta persona la encargada de capacitar, orientar y prevenir al personal de los riesgos informáticos que se pueden presentar en la empresa, de esa manera fortalecemos la seguridad informática.

De acuerdo a lo expuesto anteriormente se Considera que el CEO (Gerente General) y CIO (Gerente de Sistemas) tienen responsabilidad compartida, por esta razón debe haber un canal de comunicación constante entre el Auditor, el CEO y CIO y más cuando deben hacer parte en las funciones de planeación, se hace esta salvedad ya que en muchas empresas los niveles directivos son los que con más frecuencia infringen las políticas de seguridad informática, por los afanes del comercio o simplemente por el mal empelo de las herramientas informáticas.

Se puede inferir la importancia de establecer responsabilidades al momento de ejercer los controles y la administración de la seguridad informática, para así mismos ser determinantes en el rol que desempeña cada miembro de la organización, y ser claros que cada uno tiene una compromiso, algunos en un grado mayor y otros e un grado menor, pero la seguridad informática y su administración y control es una responsabilidad compartida.

Paralelamente es transcendental que las responsabilidades no queden en un documento sino que también es imperativo capacitar al personal frente al tema, e indispensable realizar pruebas de vulnerabilidad y exámenes frente a este conocimiento, de esta manera el control es más llevadero y permite al auditor una mayor eficacia y eficiencia al momento de ejercer sus funciones, de idéntica manera es evidente que además de ejercer controles, se deben identificar las vulnerabilidades presentadas en los procesos de seguridad informática.

Por ello el 5 de Enero de 2009 el Congreso de la república de Colombia promulgo la ley 1273, en esta ley se tipifican los delitos informáticos, los artículos relacionados allí tienen como objetivo proteger el uso informático y sancionar con penas y multas los delincuentes que se valen de los sistemas y medios tecnológicos para cometer infracciones.

Una de las ventajas encontradas en esta ley es la protección de los datos personales en especial datos que comúnmente las personas van dejando en las redes sociales, sistemas informáticos y especialmente en internet.

Los avances tecnológicos permiten que las personas puedan manipular bases de datos, realizar transacciones bancarias, pago de servicios, hacer amigos, estudiar, interactuar con el

mundo y para eso emplean en gran medida la internet, sin embargo detrás de esta maravillosa herramienta se encuentran en la clandestinidad una serie de personas con habilidades especiales, o algunos con escaso entrenamiento, u otros por simple diversión que recopilan datos, estudian sus víctimas y atacan sigilosamente, estos malhechores son conocidos como los ciberdelincuentes independientemente cual sea su fin.

En Colombia anualmente se lleva a cabo el Campus Party reconocido como el mayor evento de tecnología, creatividad, ocio y cultura digital en red del mundo. Se gestó en España desde 1997 como un encuentro anual en el que, durante varios días, se reunían miles de participantes con sus computadores, procedentes de todo el país y otras naciones. Tiene un carácter generalista y formativo, que congrega a las distintas plataformas y colectivos del mundo de la informática, creando un punto de encuentro propicio para el intercambio de ideas y conocimientos, actividad que se realiza en Colombia desde el 2014, en el encuentro realizado para 2014 Matías Katz famoso hacker argentino quien figura entre los 10 Hacker más trascendentales del mundo, realizó una ponencia donde se enfatiza la amenaza informática especialmente en PC, Smartphone, e internet, resaltando que la privacidad no solo está amenazada por los espionajes estatales y privados sino también por fallas en el software y el hardware además del descuido, la ignorancia y la imprudencia de los usuarios, en esta misma ponencia destaco las transacciones bancarias inseguras siendo un jugoso y rentable objetivo para los ciberdelincuentes.

La ausencia de seguridad en el navegador web revela que los datos de la tarjeta de crédito empleada quedarán en poder del sitio de e-commerce de lo contrario estos datos estarán en poder del delincuente informático, puso como ejemplo lo que sucedió en 2011 con Sony, cuando los

delincuentes informáticos se llevaron miles de datos de tarjetas de crédito aprovechando esta falencia.

Además de describir un mundo infinito de delitos informáticos también ofrece servicios de protección informática como test de intrusión, en la jerga informática conocido como hacking ético. Una empresa lo contrata para probar sus sistemas informáticos ante posibles ataques o violaciones. Se firma un contrato donde se establece quiénes participarán, qué tareas desarrollarán, los sistemas que se examinarán y un compromiso de confidencialidad, esta práctica también es conocida como una consultoría de seguridad sobre el hardware, el software y las comunicaciones de una organización brindando capacitaciones de alto nivel técnico a empresas, organizaciones y usuarios finales.

Otro de los factores más comunes que afectan la seguridad informática es el manejo inadecuado e inescrupuloso de las redes informáticas y páginas de internet por parte de los empleados de una empresa, según informes de CISCO empresa global con sede en San José, (California, Estados Unidos), principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones, las empresas se enfrentan a más de 100 mil páginas contaminadas con una medida de 133 infecciones web mensuales por usuario empresarial, por lo que se considera que en la mayoría de los casos se presenten por el manejo inadecuado de las redes sociales, que facilitan el trabajo de ingeniería social permitiendo al ciberdelincuente el empleo del avance tecnológico mediante herramientas virtuales para apropiarse del patrimonio de terceros a través de diferentes modalidades delictivas como la clonación de tarjetas, la vulneración y alteración de los sistemas de cómputo para recibir servicios

y transferencias electrónicas de fondos mediante manipulación de programas o simplemente extorción o secuestro de información.

Si se revisa en internet se encuentran un sin número de páginas con información de seguridad informática, delitos, modalidades, historia etc. Describir cada delito o ahondar en el tema en este ensayo no será necesario, así se considera relevante establecer que los delitos informáticos independiente del delito cometido el ciberdelincuentes acaba buscando un lucro final. "En el 2007 la revista cara y sello público un informe donde algunas empresas colombianas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos" Boletín 103 Delitos Informáticos, Facultad de Investigación Criminal PONAL.

A propósito Fabián Zambrano Smith, Gerente del Centro de Operaciones de Seguridad de Digiware y Héctor Tamayo, coordinador de tecnología de la Cámara Colombiana de Informática y Telecomunicaciones, entidades expertas en seguridad informática en Colombia, citan que las principales fuentes para cometer delitos informáticos en Colombia son dos, la primera las redes sociales y la segunda los correos de tipo personal, se estima que los principales objetivos van dirigido a las cuentas bancarias y al número de cuentas de correos electrónicos para ser vendidas a empresas que pagan muy bien por números de listas de correos para posteriormente inundarlas con publicidad o correos no deseados.

Por lo descrito anteriormente se puede considerar que la libertad del usuario al momento de utilizar sistemas informáticos y redes sociales es la principal herramienta de los delincuentes, y esto se debe a la facilidad de las personas emplean su información personal en las redes sociales, cometiendo los errores más graves en el mundo virtual, así lo establecen los principales expertos

de tecnología forense quienes atribuyen al usuario en alto porcentaje la actividad delictiva de ciberdelincuentes por la confiabilidad con que los usuarios navegan en internet dejando datos y detalles de su información personal.

Para mitigar las acciones delincuenciales es conveniente recomendar medidas y evitar los ataques informáticos en el país. Sobre la base de las consideraciones anteriores es importante establecer medidas preventivas, disuasivas y restrictivas mitigando los riegos frecuentes encontrados en seguridad informática, basado en la normatividad nacional e internacional, recomendar controles a seguir en seguridad informática como difundir claramente la normatividad existente verificando que sea entendida, comprendida y aplicada al grupo focal dirigido. La siguiente figura es una muestra por años, de reclamaciones realizadas por usuarios afectados a causa de ataques cibernéticos en los sistemas financieros.

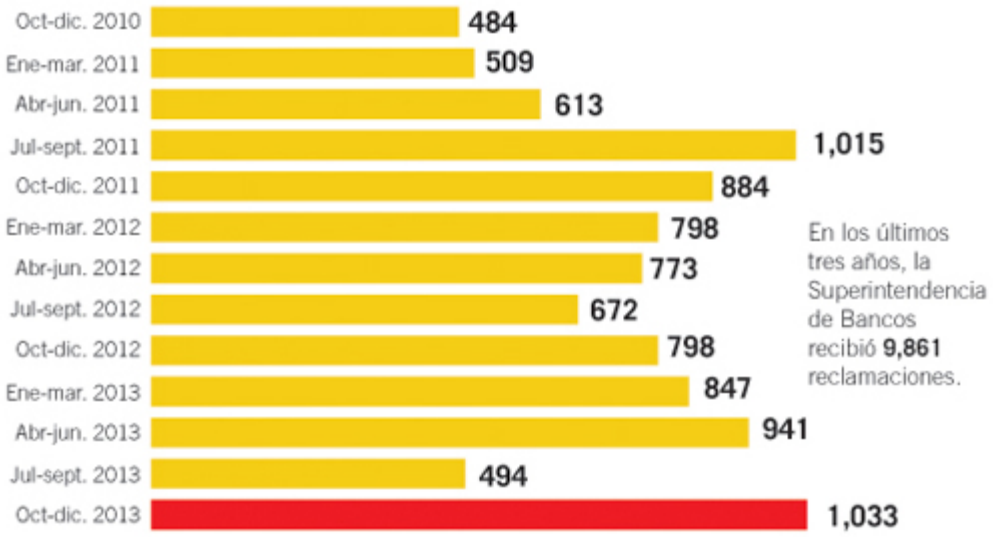

Figura 1 Reclamaciones financieras por transacciones fraudulentas en Colombia

Fuente Superintendencia de Bancos, Grafico Ramon L Sandoval.

Implementar estrategias de seguridad y generar políticas empresariales claras y definidas para el personal de empleados derivadas de su labor en la empresa y el empleo de herramientas informáticas, es importante que estas personas no visiten todos los portales, no se abran todos los correos que llegan, si la empresa tiene página web se debe digitalizar la URL, evitar entrar a paginas por favoritos y sobre todo si esta página web es bancaria, actualizar frecuentemente los antivirus, no se recomienda visitar portales en china ya que se considera como el país más inseguro en portales del mundo, evitar la consulta de los correos spam, no ingresar a paginas sospechosas de premios y procurar navegar en páginas conocidas. La empresa debe implementar un sistema de seguridad corporativo y en sus políticas dejar establecido el monitoreo constante de este sistema de manera que se puedan corregir las fallas de manera oportuna.

Es evidente entonces la necesidad de restingar la instalación de software en los equipos de la empresa y establecer controles de acceso a los sistemas informáticos mediante contraseñas de 8 dígitos intercalando caracteres con números, letras y símbolos e indispensable generar mecanismos de protección como antivirus, capacitaciones en temas de seguridad informática al personal.

Todo lo que se haga o deje de hacer en medios electrónicos será sujeto de ser vulnerado, no existen barreras para los ciberdelincuentes, aun así, existen mecanismos de seguridad que pueden ayudar para que el delincuente desista de su intento o sea capturado, lo importante es tener claro que al momento de emplear un medio electrónico informático, se está en riesgo, por esto es recomendable mantener sistemas de seguridad fuertes y denunciar cualquier intento de intrusión o delito cometido ante las autoridades judiciales, ya que muchos de estos delitos quedan en la impunidad por la falta de denuncias.

Conclusiones

El origen y evolución de los delitos informáticos en Colombia, se da con la legitimación que impone la Ley 1273 de 2009, sancionando y multando las infracciones cometidas mediante el empleo de sistemas informáticos.

Como resultado de las investigaciones realizadas por expertos en procesos forenses informáticos, es posible concluir que existe una gran diversidad de técnicas y métodos delictivos, modalidades asociadas a diferentes tipologías de delitos, así como organizaciones y clasificación de personas con ciertas características y atributos especiales conocidos como ciberdelincuentes quienes aprovechan los avances tecnológicos y el bajo nivel en seguridad implementado por los usuarios y empresas para cometer sus fechorías.

Por otro lado al comparar la normatividad colombiana frente a la normatividad internacional, se observa que Colombia es uno de los primeros países en penalizar los delitos informáticos, sin embargo la falencia se evidencia en la falta de promoción, capacitación y correcta divulgación de esta normatividad, lo que deja vacíos jurídicos en los entes encargados de impartir justicia. En este sentido se estima que cada juez interpreta la ley a la medida de su conocimiento y practicidad.

Después de haber mencionado algunos de los controles más relevantes que se pueden emplear en seguridad informática, se concluye que una de las principales fallas es la identificación y aceptación de responsabilidades, falta de compromiso por parte de los usuarios

que emplean los equipos informáticos, falta de cultura de seguridad, y la inminente necesidad de establecer políticas gerenciales, claras, objetivas y aplicables.

El sistema de seguridad informático actual que poseen las grades, pequeñas y medianas empresas en Colombia, no es suficiente ante el reto de enfrentar tecnología y delincuencia, al respecto de estas vulnerabilidades se considera que las transacciones bancarias y financieras realizadas a través de las redes, no garantiza la protección de los activos, a esto se suma la complicidad de los empleados en entidades y empresas, quienes facilitan las acciones del ciberdelincuente, por esto se estima que a pesar de existir normatividad frente al tema, las herramientas, controles y sistemas de seguridad en Colombia no son los ideales. Debido a estos factores se hace necesario generar un procedimiento de protección basado en sistemas de gestión de calidad por lo que se recomienda que toda empresa pública y privada en Colombia se certifique en la norma internacional ISO 27001 Gestión de seguridad de la información.

Tabla de Figuras

Referencias

Acurio Del Pino, S. (2005). *Delitos Informáticos*. Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Baratta, A. (1999). *Derecho Penal Mínimo*. Colombia: Editorial Temis S.A.

Correa, C. (1990). *El Derecho Informático en América Latina.* Colombia: Editorial Temis S.A.

Controles de seguridad. (2010). *Seguridad en los centros de Cómputo*. Recuperado de http://uvmsistemas.weebly.com/uploads/2/5/5/4/2554403/sesin_4_seguridad_en_centros_de_cmputo.pdf

COUNCIL OF EUROPE. (2001). *Convenio sobre la Ciberdelicuencia.* Recuperado de http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF

El congreso de Colombia. (2009). *Ley 1273 de la protección de la información y de los datos*. (Edición 47.223) Colombia: Diario Oficial.

Chinchilla. Z. (2013). *Herramientas Telemáticas*. Recuperado de http://datateca.unad.edu.co/contenidos/100201/HT2013Exe/leccin_4_riesgos_y_proteccin_en_internet.html

Grancha. E. (2013, 05,06). *Delitos de cuello blanco*. Revista del Instituto de investigación en Criminología y Ciencias Penales de la UV. Recuperado de http://www.uv.es/iccp/recrim/recrim13/recrim13n02.pdf

Cámara Colombiana de Informática y Telecomunicaciones. (2011). *Delitos Informáticos. La confianza, principal herramienta de los delincuentes*. Recuperado de http://www.ccit.org.co/files/SEGURIDAD%20INFORMATICA/Delitos_Informaticos.pdf

Legalidad informática. (2013). *Los retos de la privacidad, innovación, derecho y seguridad*. Recuperado de http://legalidadinformatica.blogspot.com/

Mitnick, K. (2007). *El arte de la intrusión*. México. Alfaomega Grupo Editor, S.A. de C.V.

Marquez, C. (2007). *El Delito Informático*. Colombia: Editorial Leyer.

Norton. (2013). *Reporte Norton 2013*, Recuperado de http://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf

Organización de los Estado Americanos. (2014). *Tendencias de Seguridad Cibernética en América Latina y el Caribe.* Recuperado de http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Symantec. (2014). *Informe sobre Amenazas a la Seguridad en Internet*. (Vol. 19) Recuperado de http://www.symantec.com/es/mx/security_response/publications/threatreport.jsp

Universidad Politécnica de Valencia. (2008). *Hacking y ciberdelito.* Recuperado de http://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf?sequence=1