Fraude informático y el contexto colombiano

El ritmo que acompaña los avances tecnológicos en términos de fraude, no es el mismo de los controles ni de las alertas ni de la cultura de prevención y, menos aún, del marco jurídico que los cobija.

Sara Gallardo M.

El fraude informático avanza a un ritmo que supera todos los controles, las alertas, la cultura de prevención y ni qué decir del marco jurídico que lo rodea. Entorno que, según los futurólogos tecnológicos, no tiene nada de halagador.

Las predicciones de Scott Klososky, una de las voces más autorizadas en tales vaticinios, son para preocuparse y hacer un llamado a prestar más atención a un flagelo mundial que parece no tener límites. “Creo que estamos cerca de algún tipo de Pearl Harbor (1941). Una suerte de evento digital que acabe con numerosas compañías. Hasta que eso no ocurra, la gente no le prestará suficiente atención a la seguridad informática. Dicho evento podría suceder en los próximos cinco años”, le dijo al diario El Tiempo.

De ahí la necesidad de analizar con distintos expertos las condiciones del

presente, las tendencias y hasta el pasado. “Hace unos meses el Departamento de Defensa de los Estados Unidos liberó el documento denominado *Seguridad de los sistemas computarizados*[1], que conservaba como clasificado desde el 11 de febrero de 1970. Es decir, un documento de hace 46 años. Al revisarlo, se detectó que, en términos de los controles, pareciera que se hubiera quedado congelado en el tiempo, lo que me produjo la siguiente reflexión: -¿No hemos cambiado ni evolucionado?, manifestó Jeimy J. Cano M., director de la revista y moderador de la reunión convocada con tales fines.

Los invitados Recaredo Romero, director regional para América Latina de la División de Investigaciones y Disputas de KROLL; Natalia Baracaldo, directora del Departamento de Ciencias Contables –CIJAF- y Luis Eduardo Daza, especialista en fraude informático, del Departamento de Ciencias Contables de la Universidad Javeriana, asistieron puntuales a la cita.

“La idea es que profundicemos en las diferencias que rodean esa tendencia que está afectando y dando vueltas entre las organizaciones y el público general: el fraude informático, el ciberdelito y las otras modalidades del cibercrimen”, puntualizó Jeimy J. Cano, para dar comienzo al debate con la primera pregunta:

¿Cuál es diferencia entre un delincuente informático y un fraude informático? ¿Qué es delincuencia informática por fraude informático? ¿Existe alguna diferencia?

Recaredo Romero
Director Regional para América Latina de la
División de Investigaciones y Disputas
KROLL

[1] Department of Defense (1970) Security controls for computer systems (U). Report of Defense Science Board Task Force on Computer Security. Febrero. Recuperado de: http://seclab.cs.ucdavis.edu/projects/history/papers/ware70.pdf

El delincuente informático es el perpetrador y el fraude informático, la conducta. Y me atrevería a orientar la pregunta a la función que le damos al fraude informático. Existe una larga variedad de definiciones, una de ellas referida a quien usa el engaño a través de medios informáticos. Esa sería una diferencia entre el fraude informático y el delito informático. El primero, es un delito específico y el segundo contempla una variedad de acciones ilegales, que no son necesariamente fraude. Lo que quiere decir que el delito informático es un concepto más amplio que el fraude informático.

Luis Eduardo Daza Giraldo
Especialista en Fraude Informático
Departamento Ciencias Contables
Pontificia Universidad Javeriana

El delincuente informático, es el sujeto, el perpetrador, también identificado en otro tipo de delitos y fraudes. Es esa persona envuelta en los grandes mitos y realidades que más adelante tendremos oportunidad de precisar. A veces, es muy difícil poder identificar el delincuente informático, principalmente por las características de anonimato de su actividad. El segundo aspecto es diferenciar entre fraude y delito informático. Este último está tipificado por cada país como una conducta punible. En otras palabras, hay situaciones –que aunque son fraude, no están contempladas como delito. De ahí algunos asuntos en nuestra legislación colombiana, que aunque no son tipificadas como delito, sí caben en la categoría de fraude. Para dar un ejemplo muy sencillo, en Colombia, la evasión tributaria no es un delito, es una conducta reprochable desde el punto de vista administrativo. Eso mismo pasa en el tema informático, hay unas conductas específicas tipificadas en la ley como delito informático y otras que no alcanzan a quedar ahí, que uno podría catalogar como fraude informático.

Natalia Baracaldo
Directora Departamento Ciencias Contables –CIJAF-
Pontificia Universidad Javeriana
Mi respuesta la oriento desde la jurisdicción actual. Con el fraude financiero, sucede lo mismo. En algunos países está tipificado en los códigos penales y en otros no es así. En Colombia existe una normatividad específica, que ayuda a tipificar específicamente los temas relacionados con delitos informáticos. Sin embargo, puede haber conductas enmarcadas en asuntos de fraude, tales como el engaño, que ni siquiera pertenecen a la categoría de delitos informáticos. De ahí que la respuesta sea muy amplia y dependa del contexto desde el cual se mire. En nuestro país, se trata de un asunto incipiente, muy nuevo y prácticamente desconocido. Quienes están más salvaguardados están en el sector financiero. Allí es donde existen las mejores medidas, para cuidar ese precioso activo que es la información. En ese orden de ideas, ellos protegen la información ya sea del delito informático o de malas prácticas en su contra. Pero, cualquier persona puede cometer algo en contra de la información y ni siquiera está tipificado ni siquiera existe. De ahí que no podamos referirnos a un delincuente informático.

Jeimy J. Cano M.
Director Revista Sistemas
ACIS
¿Este tipo de conductas (fraude informático) están tipificadas en la legislación colombiana? ¿Hay casos con fallos concretos? De no ser así, ¿cuál es la razón?, ¿por qué?, ¿cuáles son las carencias para que no lo estén?

Natalia Baracaldo
En nuestro país, la tipificación de los delitos no es un tema exclusivo del ambiente informático y considero que el Código Penal se queda corto en muchísimos aspectos. No sabría decir si por quienes emiten este tipo de

Luis Eduardo Daza señala las nueve categorías de delitos informáticos tipificadas en la ley colombiana.

normas o si falta que la Academia se pronuncie. Lo que sí es evidente es que hay una falencia. Dentro de la Ley 273 de 2009, se quedan por fuera infinidad de asuntos. Pensando la pregunta desde otro contexto, en el sentido de las responsabilidades frente al control interno de la información, se exige a muchas empresas que los revisores fiscales sean quienes dictaminen sobre la tecnología de la información orientada a protegerla. Un revisor fiscal es un contador de profesión, ¿qué puede saber de delitos y de fraudes informáticos, inclusive de seguridad de la información? En mi opinión, no sólo existen vacíos normativos, también en quienes manejan estos temas, en términos de conocimiento y buenas prácticas.

Jeimy J. Cano M.
¿Está tipificado o no el delito informático?

Luis Eduardo Daza
Está tipificado; por lo menos así se llama dentro de la ley colombiana, la 1273 de 2009.

Sara Gallardo M.
Editora Revista Sistemas
Pero, ¿no específicamente el fraude?

Luis Eduardo Daza Giraldo
En la ley colombiana están tipificados como nueve categorías de delitos, incluso hasta daños físicos en equipos, daño informático y acceso no autorizado. Sí existen fallos concretos, pero siguen siendo muy pocos. Uno de los aspectos a tener en cuenta con relación a nuestras autoridades en el país, es que como se trata de temas relativamente muy recientes, la preparación técnica de los funcionarios para atender tales hechos es escasa y deficiente. Quienes combaten ese tipo de delitos enfrentan el reto de actualización y de una formación más avanzada. En los diferentes expedientes judiciales –doscientos, para citar una cifra-, que manejan los fiscales figuran casos de robo, hurto, lavado de activos, estafa y tal vez sólo uno es delito informático y, en consecuencia, la prioridad para su investigación será, probablemente, una de las últimas. Y

además se preguntan: "¿qué hago con este proceso?, ¿a qué investigador se lo asigno?". En otras palabras, se trata de un tema que genera angustia y, por lo tanto, deciden trabajar sobre lo conocido y aplazar lo demás. Esta situación explica por qué se conocen muy pocos fallos o condenas. Su complejidad y la falta de preparación técnica en lo penal la determinan.

Sara Gallardo

¿Existen cifras sobre el porcentaje de cuántos casos de los que manejan los fiscales, corresponden a delitos informáticos?

Luis Eduardo Daza

Hay algunos informes con bajos resultados finales de productividad. En las noticias se informa sobre algunos casos muy connotados acerca de acciones de *hacking*, pero son la excepción. Y, lo grave de todo esto, es que la gran mayoría de delitos informáticos quedan en la impunidad. En el caso, por ejemplo, de un fraude financiero a través de una tarjeta de crédito, si la entidad bancaria devuelve el dinero al tarjetahabiente, hasta ahí llega el asunto. Se cometió el delito, pero no se hizo nada para iniciar una acción legal, porque la víctima (el tarjetahabiente) al final no sufrió una pérdida. Tal hecho, por los montos individuales menores, no incentiva los procesos penales y obstaculiza su éxito de investigación y sanción.

Recaredo Romero

Con relación a si está o no tipificado el fraude, me gustaría "medir el vaso, medir el hielo". En otras palabras, la tecnología va a una velocidad muy distinta a la de las normas. Eso sucede en la normatividad nacional e internacional. El fraude informático no está tipificado en la ley. Algunas conductas sí lo están, con las cuales en un caso de fraude informático, se podrían apalancar la investigación y el proceso.

Recaredo Romero indica que la tecnología va a una velocidad muy distinta a la de las normas y, por tal razón, el fraude informático no está tipificado en la ley.

Según Recaredo Romero (derecha), el fraude no está tipificado, pero se le puede conectar con delitos informáticos que sí lo están.

Jeimy J. Cano M.
¿En lo penal?

Recaredo Romero
Exactamente y con conexión al delito informático. El fraude, específicamente, no está tipificado, pero se le puede conectar con delitos informáticos que sí lo están. Por ejemplo, con el delito de acceso abusivo a un sistema informático. Ese delito está presente en muchas conductas y fraudes. Así que la norma tiene carencias, pero es algo natural, mientras el ritmo de la tecnología y el sistema normativo sean distintos. Ya, por lo menos, tenemos en Colombia unas conductas tipificadas como delitos informáticos.

Jeimy J. Cano M.
¿Existen en Colombia estadísticas sobre fraude informático? ¿Cuáles son las conductas más habituales?

Recaredo Romero
Con relación a estadísticas, cito los resultados del informe global de fraude que elabora KROLL anualmente. En el año 2015, de las once tipologías de fraude que mide el estudio, el "robo de información, pérdida o ataque" se ubicó en tercer lugar como tipología más frecuente a nivel internacional. En Colombia, esa tipología fue la número uno y afectó al 27% de las empresas que participaron en el estudio.

Sara Gallardo
¿De cuántas empresas?

Recaredo Romero
Del total de la muestra, el 27%. Es preciso anotar que el estudio mide específicamente el fraude detectado. El fraude real, que incluye el no detectado, es probablemente significativamente más alto. Dentro de las tipologías más comunes en el ámbito empresarial está la captura y robo de información para venderla y hacer uso de la misma; también el robo de identidad es prevalente. En el sistema financiero, los datos personales, cuen-

tas bancarias, claves de acceso a tarjetas, entre otros aspectos, tienen una alta demanda en el mercado negro. Se trata de actividades de bajo riesgo y alta retribución para el delincuente, lo cual incentiva la actividad ilícita. La transnacionalidad de esas tipologías, dificultan investigar el delito informático. Dentro de las tendencias, estamos ante unos encadenamientos productivos, por llamarlos de alguna manera, donde tenemos muchos eslabones que participan en la cadena; desde los desarrolladores de los *softwares* maliciosos, hasta los que capturan datos, los que los comercializan y los que hacen uso de esos datos para obtener un beneficio económico. Entonces, tenemos una multitud de actores ubicados en distintos países. Afortunadamente, la colaboración judicial es creciente y está aumentando la eficacia en la persecución de estos delitos, la cual ha sido tradicionalmente muy baja. Algo que se ha vuelto tremendamente frecuente y que se espera siga en aumento es el *ransomware*, o secuestro de información; una tendencia global que está afectando también a Colombia. Esta es una actividad que va a ser difícil de contrarrestar, mientras existan empresas y personas dispuestas a pagar "el rescate". Frente a lo que se ve a futuro, *Internet de las cosas* tendrá gran incidencia, por la interconexión al gran *software* y el boom de los bienes electrónicos; los carros, las casas y los sistemas del hogar estarán conectados. Así que podrá resultar lo mismo que estamos viendo ahora, el secuestro de información, a cambio de un rescate, además de pasar a metodologías todavía más sofisticadas.

Jeimy J. Cano

Adicionalmente al planteamiento de Recaredo Romero, el ransomware ha sufrido una evolución. Ya no sólo se pide rescate, sino que con el pasar del tiempo sin pagarlo, los atacantes comienzan a borrar los archivos retenidos. En otras palabras, queda capturado el equipo.

El director de la revista y moderador del foro Jeimy J. Cano se refiere a la evolución del ransomware.

Luis Eduardo Daza (segundo de derecha a izquierda) advierte sobre la dificultad para medir la acción criminal en la red.

Recaredo Romero
Agregaría que con el *ransomware* está sucediendo lo mismo que ocurría con la extorsión y los secuestros tradicionales. Hay casos en que la gente paga el rescate y se le piden pagos adicionales. O casos en que las víctimas vuelven a ser atacadas por ser percibidas como proclives al pago. Adicionalmente, lo más común hasta el momento es, yo retengo tu información hasta que me pagues el rescate. Pero se empiezan a presentar incidentes en los que se amenaza a la víctima con hacer pública la información, a no ser que se pague rescate.

Sara Gallardo
¿Con relación a las tendencias mencionadas, que en muchos lugares ya son un hecho, hay cifras específicas?

Luis Eduardo Daza
Cuando se habla de estadísticas, el problema es medir la acción criminal en la red. Esta acción es muy difícil de realizar. En teoría hay dos tipos de delitos informáticos: los que no contemplan una intención financiera, conocidos como *hacking* y los que sí la tienen, reconocidos como *cracking*. ¿Cuál es medible? Generalmente, las estadísticas apuntan al *cracking* porque se trata de cifras asociadas a montos de dinero; mientras que las acciones de acceso a sistemas o datos no autorizados resultan difícilmente medibles. Lo más difícil en este tipo de delitos es medir. Como dije antes, las conductas de los delitos informáticos se podrían dividir entre las que son con una intención de provecho financiero y las que no. Las primeras, de alguna manera se podrían medir, o por lo menos estimar, con base en encuestas a las víctimas, ya sean personas o empresas. Al contrario, resulta casi imposible estimar los delitos informáticos no financieros, que sólo buscan acceder a unos datos o sistemas de información sin consentimiento de su titular. Algunas entidades han realizado dichas mediciones, en forma anual y otras bianual y la gran mayoría a través de encuestas en las que se

definen ciertas categorías y una metodología de estimación para cada una. De esta forma, la empresa o persona que fue víctima del ciberdelito financiero manifiesta la modalidad, el número de incidentes, el monto involucrado y demás características. Pero no hay de *hacking*.

Y esa, en mi opinión es una de las conductas, para llegar a la pregunta sobre ¿Cuáles son las más habituales? Sin tener una cifra concreta, creo que el *hacking* es una de las conductas más habituales en ese tipo de delitos, pero no se puede medir exactamente. Es como hablar de otros fenómenos como el narcotráfico, hay cifras, hay datos, hay estimaciones, pero no hay una cifra exacta. No hay una medición exacta. Se trata de hacer ejercicios o aplicar modelos para medirlo. Nosotros desde la academia ¿qué hacemos? Revisamos y seguimos estadísticas que publican algunas firmas como KROLL, KPMG y PriceWC que se aventuran a medir el fenómeno. Y ahí lo que uno ve es que hay unas tendencias, las cuales permiten medir, según sus metodologías, en dónde se puede ir clasificando y midiendo el delito informático y qué tendencia marca. KPMG venía haciendo una encuesta de fraude en las empresas para los años 2011 y 2013. Algo interesante es que para el 2013, incluyó la variable, cibercrimen. Esto es muy valioso porque hace una primera medición en las empresas colombianas. Lástima que no apareció la versión 2015 para comparar dicha medición. Esperábamos que fuera cada dos años, pero KPMG no lo hizo. No sé si lo estarán pensando hacer o retomar. El tema de estadísticas o medición de actividades ilegales, en este caso los delitos informáticos, resulta muy complejo porque se trata de medir algo que sabemos que existe, pero es clandestino.

Natalia Baracaldo

La firma KPMG ha venido haciendo lo que ellos denominan *Encuesta de fraude*, versiones 2011 y 2013. En la primera, realizaron mediciones rela-

Por primera vez en la historia de esta sección de la revista, ninguno de los invitados a la reunión era ingeniero de sistemas.

cionadas con el árbol del fraude que proponía tres categorías y en ésta medían impactos de corrupción, malversación de activos, e información financiera fraudulenta. En la encuesta del año 2013, contemplan la ramificación del cibercrimen, en donde entran las conductas a las que nos hemos referido. En ese estudio de 2013 vale la pena destacar que el impacto económico de estos actos vandálicos está representado en una cifra cercana a los 550 millones de dólares, sin tener en cuenta lo no cuantificado. De dicha encuesta sale el cibercrimen. En el año 2011, el valor total de los fraudes cuantificados fue de 950 millones de dólares; para el año 2013, la cifra de lo cuantificado ascendió a 3.600 millones de dólares. Sin embargo, no quiere decir que en ese lapso hubiesen ocurrido esos fraudes. Más bien, es que se venían gestando y lo que salió a la luz en esos períodos, fue lo que venía de atrás. Por ejemplo, Interbolsa y Saludcoop, para citar algunos. Tales casos no fueron específicamente gestados por el cibercrimen, pero sí fueron utilizadas herramientas informáticas. Es importante entonces, verificar la incidencia que tiene el tema de lo informático. Las cifras de lo que propone KPMG en su encuesta versión 2013, es que el 23% de los ataques cibernéticos, obedece a deslealtad de empleados. Es decir, que en ese porcentaje, se están gestando desde el nivel ocupacional y personas dentro de la organización, fraudes relacionados con el cibercrimen. Allí hay otras cifras importantes de mencionar, como que el 39% de los ataques cibernéticos fueron detectados de manera accidental. Digamos que en esa cifra, se mencionan dos cosas, el impacto o la incidencia de cómo se detectaron ataques cibernéticos. No es común que los delitos informáticos se denuncien a través de los canales organizacionales, obedece más a un tema de accidente -como veíamos en noticias recientes- a que la persona tuvo mala ortografía o escribió mal el *password.* Se podría decir entonces que no hay controles en la tecnología de informa-

ción, a través de un canal de denuncias. En los ataques cibernéticos, no es efectivo un canal de denuncias para detectarlo, lo cual es muy preocupante. Incluso, están las cifras, del Rasmussen College (2012), las cuales señalan que el delito cibernético ha venido creciendo tanto en los últimos años, que llegará un momento, en el cual tenga muchísima más incidencia que el narcotráfico, la trata de personas u otro tipo de delitos y ante la opinión pública sean más graves.

Jeimy J. Cano

¿Existe un modus operandi del defraudador informático? ¿Cuáles podrían ser los síntomas que revelen un posible fraude informático?

Luis Eduardo Daza

En buena parte de estos asuntos aplica la teoría general del fraude. El modus operandi del defraudador se presenta interna y externamente, hechos que coinciden con la teoría del fraude en general. Es decir, afuera de las organizaciones están los defraudadores interesados en vulnerar u obtener beneficios de la compañía. Dentro del ámbito interno de las empresas, yo diría, que los fraudes se pueden dar en todos los niveles, desde la alta dirección, digamos, desde un nivel directivo y medio, hasta un nivel netamente operativo. ¿De qué depende? Según la teoría general del fraude, un enfoque tradicional de finales de los años 60 propuesto por Donald Cressey, los funcionarios cometen fraude por motivación, oportunidad o racionalización. Sin embargo, luego se añade el concepto de la capacidad a estos tres elementos. Sin duda, es un aspecto fundamental en este tipo de conductas asociadas a los delitos informáticos, porque la capacidad del sujeto determina el alcance que pueda tener para acceder a la información o datos. Entonces, dependiendo de la modalidad del fraude de que estemos hablando se pueden identificar diferentes perfiles y modos de actuar. Por ejemplo, un alto directivo tiene mucha más capacidad de acceso a cierta información, que muchos otros

Jeimy J. Cano (fondo) indaga sobre el modus operandi del defraudador informático.

funcionarios de la empresa no lo tienen. Hay muchos altos directivos que tienen acceso a todo. Algunos, por buena práctica, renuncian a dichos privilegios y dicen, “yo no quiero tener claves de nada”, “yo no quiero tener acceso a ningún sistema”, “a mí pásenme la información requerida”. En cambio, hay otros funcionarios que su capacidad es limitada al nivel de acceso que se haya fijado según las políticas o protocolos de seguridad. Digamos, por ahora, que diferenciar el acceso a los sistemas de información es una de las buenas prácticas que existen porque delimita la capacidad y establece perfiles diferentes.

¿Cómo se ven los síntomas? También yo diría, hay que aplicar la teoría general del fraude. ¿Cómo sabe uno que de pronto alguien está involucrado en ese tipo de fraudes? Hay que revisar los temas y las conductas personales; por ejemplo, los cambios repentinos o injustificados de estilo de vida, aquellas personas que se quedan siempre hasta altas horas de la noche, o en horarios no habituales o en fines de semana; relaciones muy cercanas con ciertos proveedores o clientes. Yo aplicaría la teoría del fraude. Los síntomas son esos comportamientos inusuales, son aquellas conductas que podrían ir descubriendo ese tipo de fraude, según el área de desempeño laboral o funcional de la persona. Sin duda, hay que volver a poner la lupa en aquellas personas que tienen cierta capacidad y además están ubicados en áreas críticas o de alto impacto. Porque cada categoría de fraude tiene sus propias condiciones.

Natalia Baracaldo

KPMG tiene en cuenta una tipificación dentro de su nuevo árbol de fraude: la piratería, los accesos no autorizados y el vandalismo. En el tema de piratería, creo que todos nos hemos hecho una idea desdibujada, desde el señor que está en el mercado informal o que quienes la realizan manejan unos perfiles muy bajos. Puede que sea esa la línea final de toda la cadena, pero la

verdad, es que en términos de piratería, todo obedece a grandes cabezas, a grandes corporaciones. Si miramos el tema de la música, hoy en día existen plataformas como *Napster*, o *Spotify*, que se han visto inmersas en temas de piratería, en términos de derechos de autor. Desde la óptica en que se mire es necesario hacer una diferenciación. Si se trata de la reproducción no autorizada, piratería hecha por una organización grande o si se refiere a distribución, la cual cae en mercados más oscuros, densos y sobre los que el control finalmente se pierde. Los accesos no autorizados, podrían darse directamente en las organizaciones. Por ejemplo, con los accesos abusivos a sistemas informáticos de las entidades. Por ejemplo, la persona que su puesto de trabajo era en el área contable y luego pasó a tesorería, a quien se le presenta una necesidad familiar y ve la oportunidad de cometer un acto ilegal, en el marco de un acceso no autorizado. ¿Cuál sería el modus operandi de la persona? Ellos lo hacen una vez, dos veces y se dan cuenta que lo pueden repetir y le proponen al amigo. Un caso muy sonado el del tesorero de Bavaria, quien cometió uno de los actos de fraude financiero de miles de millones de pesos, de mayor repercusión en nuestro país, hace aproximadamente ocho años. Por otro lado, los robos de identidad, también a través de accesos abusivos a la información o a través de las páginas de internet con las entidades financieras. Y por último, podemos hablar de un tema de vandalismo, donde apenas voy a mencionar los temas de suplantación de destrucción de la información y de *software* malicioso. En ese ambiente es posible encontrar personas muy capaces, a veces ni siquiera profesionales, pero sí muy hábiles con los asuntos de sistemas. Particularmente, participo en investigaciones de fraude financiero, donde uno se ve inmerso en escenarios con personas discapacitadas o mujeres embarazadas.

Recaredo Romero

A la hora de revisar el modus operandi para establecer el perfil del perpetrador, es oportuno diferenciar entre el

Recaredo Romero (derecha) explica las diferencias que rodean a los actores internos y externos, en términos del fraude informático, dentro de una organización.

actor interno y el externo. Y dentro de los actores internos, aquellos que actúan de manera maliciosa y los que son negligentes. Al contrario de lo que pudiera pensarse, un número significativo de incidentes de seguridad informática son generados por actores internos. Es importante fortalecer la conciencia de seguridad informática en los empleados y hacer que todo el mundo sea responsable de crear un entorno seguro. Los empleados con escasa cultura de seguridad, aquellos que por desinformación o porque no les gusta la inconveniencia que genera la seguridad e intentan evadir las políticas de la empresa, facilitan mucho la actuación de los *hackers*. El factor humano es usualmente el eslabón débil en cualquier programa de seguridad informática. Respecto a los actores externos, nos encontramos los *hackers* criminales, los cuales buscan generalmente un beneficio económico, los *hacktivistas*, cuyo propósito es principalmente generar daño o avergonzar a la víctima, y los *hackers* patrocinados por gobiernos. Es importante tener presente que las tácticas de los *hackers* han ido evolucionando. Se ha pasado del "golpear y correr" al "infiltrar y permanecer". Una medida de protección de uso creciente en las organizaciones es la gestión de incidentes de seguridad informática con agentes inteligentes. Estos agentes ayudan a detectar incidentes o alertas en tiempo real y proporcionan soluciones inmediatas en forma automática para controlar los incidentes.

Jeimy J. Cano

En un mundo digitalmente modificado como lo establecen los académicos Michael Porter y James E. Heppelmann[2] (2015) la seguridad y el control se convierten en un elemento clave que genera valor a los productos y servicios. En este sentido, ¿qué tipos de controles se deben tener en cuenta para prevenir el fraude informático? ¿Son los mismos que se aplican en seguridad de la información o como controles generales de TI?

[2] Porter, M. y Heppelmann, J. (2015) How Smart, connected products are transforming companies. Harvard Business Review. Octubre.

Natalia Baracaldo

En mi concepto, el tema del control tiene que analizarse como un todo. El control interno es un proceso organizacional y existen los controles que pueden ser compartidos. Por ejemplo, al modelo COSO, relacionado con el control interno, la organización para cumplir sus objetivos debe determinar los ámbitos de cumplimiento, financiero y operativo. Lo informático está implícito en los tres. En la Ley *Sarbanes Oxley*, en el año 2002, posterior a fraudes financieros, en la sección 404 de Control sobre información financiera, se obliga a que las organizaciones contemplen un control interno sobre ésta. Aunque allí no se está hablando específicamente de fraude informático, sí vemos la necesidad de que tengan controles internos de tales características. En ese orden de ideas. ¿qué efecto tiene esto en el ámbito colombiano? Pues que eso va aplicar para aquellas empresas colombianas que coticen en bolsa. ¿Pero cuántas empresas colombianas cotizan en bolsa? Un mínimo porcentaje de la economía. Es decir, que por normatividad, las empresas no están obligadas a tener unos sistemas informáticos muy fuertes. En las empresas de familia, las pymes y las microempresas, piensan que el riesgo informático más grande es un virus que afecte el computador. Tales compañías no cuentan con un back-up de la información. ¿Cuál es el tema crucial? Regulación, porque las empresas no tienen la obligatoriedad en Colombia de contar con un sistema de información fuerte; ni desde la seguridad de la información ni desde el fraude informático. ¿Dónde es palpable el tema del fraude informático? En las grandes organizaciones con prácticas de gobierno corporativo y de control interno. Tales empresas comienzan a tener dependencias antifraude. ¿Y cuál es el porcentaje de estas compañías en el país? Un porcentaje muy pequeño.

Recaredo Romero

Las bases y los conceptos básicos son los mismos. Pero sí hay algunos matices dentro de la seguridad informática, donde es importante un grado

Recaredo Romero (derecha) dice que "no hay sistemas de protección infalibles".

de especialización, sobre todo en los profesionales. Ahí, principalmente en temas como el monitoreo o la respuesta a amenazas dinámicas, sí existe una marcada diferencia, al tener profesionales con una formación y experiencia práctica, atendiendo incidentes y ataques informáticos. Así mismo, la oferta de herramientas especializadas para prevenir, monitorear, detectar y responder a las amenazas de seguridad es cada vez más amplia y sofisticada y requiere profesionales con los adecuados conocimientos técnicos. Una tendencia creciente en cuanto a controles, es el endurecimiento por parte de las organizaciones de la política de uso aceptable de tecnología de la información. Específicamente, las restricciones de acceso a sitios *web* desde computadores conectados a la red corporativa, incluyendo proveedores de servicios de email, redes sociales, chats y motores de búsqueda.

Sara Gallardo

¿Lo que quiere decir que la tecnología ha fallado? ¿Si la solución se cifra en determinar: "usted no use", "usted no acceda", "usted…", quiere decir, que los controles en términos tecnológicos fallaron?

Recaredo Romero

Ese es el desafío de esta temática. No hay sistemas de protección infalibles. Siempre se está en riesgo y la tolerancia al mismo influirá en los controles que cada uno deberá establecer. Obviamente, el sistema financiero es muy restrictivo. Habrá otro tipo de actividades económicas, en las que pueden manejar el riesgo con criterios más flexibles. Dependiendo de la naturaleza del trabajo, de los requerimientos para la esencia del negocio o la actividad realizada se establecerán políticas diferentes. La tendencia dominante es establecer restricciones generales de uso aceptable de tecnología de la información para toda la organización y permitir excepciones para personas o grupos según lo amerite la necesidad del negocio. Las amenazas son crecientes y cambiantes y hay que adaptar los controles en la misma medida.

Luis Eduardo Daza
Parto de una analogía. El tema de los controles es similar a los "cachos" o a la infidelidad. No importa cuántos controles usted coloque, si de verdad una persona tiene la intención de ser infiel, lo va a hacer. Esa persona buscará muchas maneras para lograrlo. Las organizaciones, los auditores, las áreas de riesgo, siempre están buscando imponer o verificar el cumplimiento de los controles y más controles, para minimizar el riesgo. Esa es una de sus tareas. Y se convierte en un círculo vicioso. En mi opinión, la solución no está en enfocarse en esa dirección. El reto está en crear una cultura y tener en cuenta los cambios generacionales. Por ejemplo, hoy una persona de las últimas generaciones, *millenials*, es quien dentro de una organización necesita estar conectado con el mundo o por lo menos con sus contactos. El mundo no tiene sentido si no es globalizado e intercomunicado. Esto es muy importante hoy en las organizaciones, porque la tendencia en los controles a la seguridad de la información es cada vez más restrictiva para los accesos a redes sociales e internet.

Jeimy Cano
¿Entonces, la cultura es un control?

Luis Eduardo
La cultura se vuelve en una forma complementaria del control. Volviendo a la infidelidad, si en mi casa me enseñaron a respetar, a decir la verdad, a ser honesto, etc., etc., pues al final seguramente no voy a caer en ella. Y pasa lo mismo en las organizaciones. Si la cultura dentro de la empresa es relajada, vulnerable y no está bien cimentada, si los accesos contemplan fines personales y no institucionales, hay riesgo. En muchas ocasiones la información de algunas empresas tiene niveles muy altos de confidencialidad, es decir, no es posible compartirla ni con la familia. Hace poco supe de un atraco en un banco del país, porque un empleado de esa oficina divulgó fotos en sus cuentas personales de redes sociales

Hoy, las organizaciones ponen en práctica más y más controles, según Luis Eduardo Daza (izquierda).

El uso de las redes sociales y los smartphones, de acuerdo con Natalia Baracaldo, pueden ser la mayor fuente de riesgo.

y con esa información los delincuentes supieron dónde estaban las bóvedas o caja fuerte y la ubicación. Se trata de un tema de cultura y un reto generacional.

Jeimy J. Cano M.

¿Qué tendencias futuras se ven en el fraude informático? ¿Se apalancan en las tendencias de la delincuencia digital moderna?

Recaredo Romero

Algunos ejemplos ya los hemos anotado. Agregaré que crecen las amenazas a los teléfonos inteligentes. Los dispositivos móviles actuales contienen mucha información personal y cada vez más son objeto de ataques. Por ejemplo, hay aplicaciones que camuflan en juegos aparentemente inofensivos que posteriormente descargan un componente malicioso. Las vulnerabilidades siguen siendo frecuentes en *Android*, el sistema operativo más utilizado del mundo, a pesar del lanzamiento de nuevas versiones que ponen énfasis especial en la seguridad. Sin duda, los teléfonos inteligentes son un área de atención, toda vez que su uso es extendido y cada vez somos más dependientes de ellos.

Natalia Baracaldo

En escenarios en perspectiva, el uso de redes sociales, *smartphones*, entornos a los que nos hemos vuelto adictos, esclavos, pueden ser la mayor fuente de riesgos en los sistemas de delitos informáticos. En sentido contrario a tal perspectiva sobre el futuro del delito informático, los temas de piratería tienden a disminuir, porque hoy se han creado empresas para descarga de música, películas, videos, etc. Ahora las personas tienen la música en sus móviles, sin pagar ni exponer los equipos a virus. Esto también depende de la jurisdicción. En China, en Asia se tipo de aplicaciones no se pueden tener.

Luis Eduardo Daza

La tendencia de la delincuencia informática va en dos vías. Una, la denominaría como la irreverencia o el irrespeto al *status quo* y está basada en tecnología. Es decir, con la aparición de ciertos fenómenos como la

economía colaborativa hemos cambiado los principios de riqueza que ya no están en la cantidad de propiedades, sino en la facilidad para acceder a bienes o servicios, apoyados en los desarrollos tecnológicos. Algunos ejemplos notables de esta nueva forma de acceder a la economía colaborativa o *sharing economy* es Uber ó Airbnb. El caso de Uber es muy significativo para entender cómo este negocio, basado en una plataforma tecnológica desarrolla un servicio de transporte sin tener la propiedad de un solo vehículo; esto se ha convertido en todo un reto para los taxistas tradicionales, autoridades, usuarios y otros jugadores. Para volver a la respuesta, cito este ejemplo para ilustrar que los negocios lícitos hoy no tienen fronteras, pero al mismo tiempo las organizaciones criminales y ciberdelincuentes se aprovechan de las mismas ventajas tecnológicas.

La segunda tendencia la podría denominar como la asimetría regulatoria. Es decir, los ciberdelincuentes saben perfectamente que en la red tienen un panorama inmenso, casi ilimitado, de posibilidades para reali-zar actividades que resultan claramente ilegales según las normas penales de cada país. Sin embargo, la red no tiene una jurisdicción penal específica. Esta situación es aprovechada por los delincuentes para favorecer sus intereses y evadir las posibles acciones legales que debieran asumir.

Conclusiones

Recaredo Romero

El mundo está cada vez más interconectado y dependemos de la tecnología en los negocios y nuestra vida cotidiana. Esto nos expone a riesgos crecientes e infortunadamente no existen métodos infalibles de protección. No obstante, podemos mitigar en forma significativa el riesgo de fraude y otros riesgos informáticos mediante la implementación de estrategias adecuadas orientadas a prevenir la ocurrencia de incidentes y a responder de manera rápida y efectiva cuando estos suceden. Defender el perímetro sigue siendo necesario, pero no es suficiente. Un buen programa de seguridad informática requiere prestar atención a estos tres pilares fundamentales: personas, procesos y tecnología.

Natalia Baracaldo

Queda de manifiesto que en todos los sectores de la economía, el ciberdelito debe ser contemplado como un riesgo, frente al cual se debe dar una respuesta, que desde mi experiencia debería ser la mitigación; lo mejor en materia de mitigación es la imposición de controles, los cuales deben formar parte de la cultura organizacional. Es importante que las empresas y hasta los ciudadanos del común sean conscientes sobre cómo el conocimiento y la prevención en estos temas, se vuelve un arma para combatir los delitos cibernéticos.

Luis Eduardo Daza

Para concluir, quisiera decir que los ciberdelincuentes se aprovechan del anonimato que se puede dar en la red y también saben de las debilidades técnicas de las autoridades para investigar estas conductas. Por lo tanto, debemos asumir una gran responsabilidad en el manejo de nuestros propios datos y cuidar la información que manejamos de las empresas o negocios a nuestro cargo. En cuanto a los delitos informáticos en las empresas, se requiere un trata-

miento con enfoque basado en riesgo para distinguir mecanismos de prevención y controles acordes con el nivel de riesgo identificado. Por último, las organizaciones deben tener en cuenta los cambios en su estructura por el avance tecnológico y de comunicaciones, los cambios culturales de las personas que llegan al mundo laboral y los tipos de controles, según el diferente rol de sus empleados.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas "Uno y Cero", "Gestión Gerencial" y "Acuc Noticias". Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista Infochannel de México y de los diarios "La Prensa" de Panamá y "La Prensa Gráfica" de El Salvador. Investigadora en publicaciones culturales. Gerente de Comunicaciones y Servicio al Comensal en Andrés Carne de Res, empresa que supera los 1800 empleados; corresponsal de la revista IN de Lanchile. En la actualidad, es editora en Alfaomega Colombiana S.A., firma especializada en libros universitarios, y editora de esta revista.*