Fraudes y fallas de seguridad, investigaciones internas

Sara Gallardo M.

Ante el aumento de casos, invitamos a un grupo de expertos para debatir sobre la dinámica que deben adelantar las organizaciones en materia de seguridad y controles.

Anuar Fernando Torres

Hilda Chaparro

Mayor Fredy Bautista

Oscar Ruíz

Los delitos informáticos van en aumento, de acuerdo con las últimas estadísticas reveladas por la Dirección de Policía Judicial (Dijín) y el Departamento Administrativo de Seguridad (DAS).

En lo que va corrido del presente año, las empresas del país han perdido 6.6 billones de pesos como consecuencia de delitos relacionados con la tecnología informática. Y de las cuentas bancarias de personas naturales han sido sustraídos 311 mil millones de pesos.

Así mismo, los casos reportados frente a 2006 han tenido un incremento del 71%, según los mismos informes.

Ese panorama que año tras año muestra mayores debilidades, ha hecho que la seguridad informática con todas las aristas que la componen, tenga su propio espacio dentro de las actividades más sobresalientes de la Asociación Colombiana de Ingenieros de Sistemas (ACIS).

Basta citar las Jornadas anuales, la encuesta nacional –publicada en este número-, y la edición especial de la revista con la realización del tradicional foro dedicado a esos temas, que tuvo como invitados al mayor Fredy Bautista, director de Delitos Informáticos de la Dijín; a Anuar Fernando Torres, jefe del Departamento de Auditoría de Sistemas del Banco Davivienda S.A.; y, a Oscar Eduardo Ruíz, consultor y director general de Internet Solutions.

En el marco de la reunión, Hilda Chaparro, presidenta de la Junta Directiva, además de abrir el debate, manifestó a los participantes su complacencia porque en la Asociación se estuvieran abordando aspectos de tanta trascendencia, relacionados con la seguridad informática, a partir de los más recientes fundamentos teóricos y los avances de la tecnología.

"Mi bienvenida tiene que ver con la seguridad como política de Estado y no como un asunto de 'boom' informático, en la medida en que tiene directa relación con el ciudadano del común y el ambiente empresarial de cualquier dimensión", precisó la recién posesionada en ese cargo directivo de ACIS.

Apreciación enfatizada por el moderador Jeimy J. Cano, acompañado de Francisco Rueda, director de la revista; Beatriz E. Caicedo, directora ejecutiva de ACIS; y, Sara Gallardo editora de la publicación.

Jeimy J. Cano
Moderador

De acuerdo con las estadísticas internacionales los ataques internos son más frecuentes que los externos. Esta situación nos habla sobre una dinámica importante que dentro de las organizaciones se debe adelantar en materia de seguridades y controles.

En este contexto, las investigaciones internas son un elemento fundamental que debe estar articulado con la atención de incidentes y sus aspectos operacionales. Sin embargo, variables como las jurídicas, las de procedimientos y manejo de relaciones públicas establecen retos importantes para que las investigaciones que se adelanten cuenten con

los requisitos y formalidades correspondientes.

Después de esta breve introducción, procedo a formular el primer asunto por debatir.

¿Qué es una investigación interna? ¿Cuáles son las mayores diferencias con las adelantadas por un ente de policía judicial? ¿Cuál es su alcance?

Oscar E. Ruíz B
Consultor y Director General
Internet Solution

Una investigación interna es el proceso de análisis de una amenaza o una alerta generada por un sistema o un ser humano; puede ser iniciada -"trigger" en nuestro argot-, por un simple "chisme de pasillo" o por la manifestación de una persona, que por su ética y moral, alerta de alguna conducta de otro empleado interno o simplemente, por el rastreo de auditoría, desde el punto de vista de un sistema de información o por un suceso en un video desde la seguridad física.

La investigación interna lo que busca es analizar un incidente basándose en un procedimiento, el cual es esencial para desarrollar la investigación; se debe tener una metodología que lo lleve a uno a determinar si puede ser un incidente administrativo o algo que vaya más allá de la organización y que puede pasar esa línea en la que se conforma un delito, hecho que debe confrontarse.

Mayor Fredy Bautista
Director Delitos Informáticos
Dijín

La investigación interna como su nombre lo indica se realiza dentro de una organización que ha presentado alguna falla en alguno de sus

procesos o procedimientos, y tiene como finalidad establecer de qué se trata el incidente detectado por el mismo personal técnico o por los sistemas y controles.

Su diferencia con las adelantadas por los entes de policía judicial se cifra en la respuesta ante la misma entidad en términos de su alcance. Dicho alcance está orientado en varios sentidos; uno de ellos en detectar las fallas para tomar el curso a seguir y corregir los errores. Este proceso puede convertirse en la columna vertebral de una investigación, la cual si llega a las instancias penales tiene un significado preponderante.

En tal sentido, una buena investigación interna contempla excelentes procedimientos ajustados a las normas vigentes, a unas buenas prácticas de recolección y preservación de evidencias, entre otros aspectos.

Anuar Fernando Torres.
Jefe Departamento
Auditoría de Sistemas
Banco Davivienda S.A.

Lo primero para hablar de una investigación interna es que hay una "manifestación", un hecho que representa una situación de la cual todavía no conocemos su alcance. En la investigación interna por lo general, es importante tener en cuenta que no existe el conocimiento de la magnitud real del evento que se está tratando.

Cuando decimos que existe una "manifestación" o alerta, se debe identificar si está originada por una falla administrativa o un evento de dolo. Hay que diferenciar los hechos para determinar el procedimiento a seguir. La denominada investigación interna es un proceso sistemático que busca identificar las causas de un problema. Es decir, un procedimiento ordenado y metódico.

Este tipo de investigación se denomina "interna" porque existe la solicitud dentro de una organización para iniciar y realizar el proceso. En otras palabras, por el origen o la fuente, que no es más que la ubicación de la "manifestación", la cual viene acompañada de un requerimiento de los interesados, no siempre de la administración.

Otra característica es que existe un desconocimiento del alcance de esta

"manifestación". Inicia por dentro, pero puede ir hacia el exterior, juntando las dimensiones interna y externas de la organización. En ese momento, surge la necesidad de establecer contacto con los entes judiciales. Vale la pena aclarar que, aunque se trate de una investigación interna, no tiene que ser adelantada necesariamente por personas vinculadas a la organización.

Otra claridad necesaria es el entendimiento: "Qué es lo que se está pidiendo que se investigue".

Para resumir, los principios que orientan y definen una investigación interna son tres: una manifestación dentro de la organización; una solicitud del interesado -por lo general del ambiente interno de la organización-; y, un desconocimiento del alcance de las causas.

Jeimy J. Cano

¿Cuáles son los elementos prácticos que se deben tener en cuenta para adelantar una investigación interna, de manera tal que jurídica y procedimentalmente se acoja a las disposiciones legales y administrativas de la organización?

Anuar Torres

Lo primero es que el fraude como tal no es un hecho aislado, sino un elemento sistémico de la organización. Es decir, que compromete a toda la empresa. Por tal motivo, la investigación no puede ser un hecho de una persona particular; toda investigación de fraude tienen múltiples componentes: tecnología, gente, financiero, seguros, operación, procesos, entre otros.

En tal sentido, el profesional que va a realizar ese tipo de investigaciones debe tener unas capacidades intelectuales superiores para poder manejar todos los dominios de la organización. Lo que quiere decir que se trata de un equipo con competencias profesionales y personales específicas.

¿Quién lo debe realizar en la organización? Depende de cada empresa. De acuerdo con las normas internacionales las recomendaciones se orientan a que sea un área especializada, que pueda actuar con independencia. Así mismo, la madurez de la entidad también influye en ese sentido.

Otro asunto es la confianza de la persona que solicita la investigación. ¿En quién confía? Si cuenta con un grupo de auditoría interna, un consultor independiente o una auditoría externa, ¿cuál le merece esa confianza? ¿Qué capacidad observa en ellos con relación al problema? En esto prima una decisión administrativa.

Pero más allá de quién debe realizar la investigación, la problemática se cifra en cuáles son las calidades que debe

tener el equipo investigador. Ahí está la dificultad. Si una organización no cuenta con áreas especializadas para este tipo de trabajos, necesariamente debería considerar la posibilidad de recurrir a entes externos, como las autoridades competentes o consultores que garanticen imparcialidad e idoneidad.

Oscar E. Ruíz B.

Los elementos prácticos yo los defino en tres aspectos básicos, como las "materias primas".

El primero son los procedimientos. Es necesario tener cubierto todo ese tema, porque el manejo del incidente o la investigación es circunstancial; si esta se origina en el departamento de IT, esta área no puede participar en la investigación, en la medida en que no puede ser juez y parte. Así mismo, si se origina en Auditoría. Dadas las circunstancias, ni una ni otra podrían formar parte del comité interinstitucional de investigación.

Coincido plenamente en que el grupo debe ser interdisciplinario, del que formen parte: abogados, el comité que hace la respuesta a incidentes a nivel tecnológico y el área judicial. La parte legal de la compañía y el área judicial o los entes de control deben mantenerlos involucrados, sea de una forma u otra en la primera fase preparatoria, mientras se determina si el incidente es solo de carácter administrativo. En tal caso, solo participaría el equipo legal de la compañía, y si transgrede a la parte legal, habría que recurrir a los entes de control, involucrando dentro de ese procedimiento a quienes ejercen tal labor desde adentro de la empresa.

La segunda materia prima es el área de tecnología, independientemente de que se tenga una infraestructura para responder a esa investigación. Así como existe el circuito cerrado de televisión en la vida real, para grabar y reproducir una escena de un atraco, identificar algún sospechoso, algún cable, entradas, salidas, movimiento de personal, igual está en la parte digital. En ese contexto figuran los grabadores y analizadores de tráfico en tiempo real para la parte digital; con el uso de diferentes tecnologías es posible tener evidencia e indicios de lo que pudo haber pasado en la parte física del edificio o en la parte lógica del sistema de información de la compañía.

Ahí debo resaltar lo siguiente: muchas veces se responde al incidente sin las debidas precauciones y sin las herramientas forenses; cuando no existe la certeza de que se está manipulando la evidencia de forma segura, aunque el procedimiento esté bien realizado, ese desconocimiento puede comprometer la evidencia contaminándola y haciéndola inadmisible.

De ahí la importancia de la preparación, del conocimiento necesario

sobre el tema y de contar con una tecnología apropiada. No solo los Firewalls, IPS o ese tipo de herramientas tecnológicas, sino desde lo más básico en donde está la evidencia, el *host* y el tráfico de la red.

De ese análisis que se haga y de esa recopilación, depende el éxito de una investigación digital; por ejemplo, si hay un *log* y yo lo abro, lo edito, lo modifico, lo contaminé y eso ya no servirá como evidencia en la investigación.

El tercer ingrediente es la idoneidad del personal. Coincido también con eso. Si se va a realizar una investigación por un fraude, el equipo debe ser especialista en el tema. Si es una intrusión o fuga de información debe estar el equipo experto que se encargue de adelantar la investigación.

Muchas veces si la compañía tiene suficiente bagaje puede hacerlo a nivel interno, pero se presentan situaciones en donde es inevitable tener que recurrir a terceros. Más aún, cuando la misma organización está comprometida; en ese caso el tema ya no es de investigación interna.

Jeimy J. Cano

Entonces ¿quién debería realizar la investigación?

Oscar E. Ruíz B.

Un grupo interdisciplinario y circunstancial. Si se tiene en IT, un 'hackeo' de un webserver, IT pasa a ser el primer sospechoso; así de sencillo, porque dentro de una estructura de tales características cuando sucede un evento de vulneración, pues lo más probable es que haya ocurrido por personas del mismo equipo de IT o por negligencia de quienes integran esa área; en tal sentido, no es posible permitir que un investigado participe de su propia investigación. Quizá sea necesario involucrar a una persona de auditoría que sepa de la parte tecnológica y buscar un tercero que le apoye, adicionando el grupo de entes de control y el grupo legal.

Este último debe integrarse en todas las investigaciones, porque es el responsable de decidir si esto o aquello se puede hacer o no, desde el punto de vista legal, de cara a la compañía, sobre sus activos e intereses y definiría que esta fuera de su marco de trabajo como lo son elementos privados de una persona. Por ejemplo investigar un correo corporativo, pero un correo personal tiene dificultades para hacerlo, y es otro tema; correspondería ya a una investigación en curso por parte de un ente de control. En tal dirección es necesario contar con el apoyo del grupo legal para que oriente las acciones a seguir, dentro del marco jurídico que lo permita, sin incurrir en violaciones al debido proceso.

Así mismo, los entes de control pueden manifestar una sospecha de IT y de Auditoría, entonces se terceriza por completo la investigación; es usual recurrir a una de las grandes compañías auditoras reconocidas o a otras compañías también especializadas en el tema de investigación digital. Todo depende y es circunstancial, si los grupos de control están de acuerdo y trabajan de la mano con este tercero; de esa manera la compañía va a saber qué es lo que hace y como se desarrolla la investigación. Se ha preparado para saber con exactitud frente a cualquier situación cómo actuar y qué tipo de áreas poner en marcha para iniciar la investigación.

Anuar Torres

¿Qué pasa cuando el fraude es la Junta Directiva?

Oscar E. Ruíz B.

Uno está preparado para poner a funcionar sus controles internos, frente a cualquier eventualidad, pero cuando se trata de la Junta Directiva, integrada por agentes externos a la organización, el tema se escapa de los mecanismos de control internos y no se puede iniciar una investigación interna, porque a los entes de control disponibles para hacerlo, no se les definió el alcance a este nivel.

Ya no es el modelo de la compañía, sino el país, el cual cuenta con los entes de seguridad interna. Por ejemplo, en el mencionado caso de fraude en Cajanal, intervinieron la Contraloría, Fiscalía, Procuraduría y el Departamento Administrativo de Seguridad (DAS), esto aplica para entes públicos o privados. Así que en un evento de tal naturaleza, sube el nivel y se debe orientar la investigación con parámetros diferentes.

Anuar Torres

En el escenario en que la Junta Directiva es la que comete el dolo, ya no se puede hablar de investigación interna. Tal situación se sale del contexto de la organización, para afectar al grupo de inversionistas. Esto hace la diferencia entre un fraude corporativo y un fraude dentro de la empresa.

Mayor Fredy Bautista

Una investigación de ese orden debe contemplar tanto la capacidad técnica, es decir, contar con las herramientas tecnológicas; y, con la capacidad humana que en el caso descrito deberá ser asumida por entes externos. Pero, hay que enfatizar esos requerimientos tanto para el ámbito interno como por fuera de la organización. Cualquiera sea el caso, debe existir una sincronía total con el marco legal; con el respaldo absoluto de todas las garantías y libertades de los involucrados en el proceso.

Fácilmente, una investigación puede llevar a transgredir o vulnerar algún derecho como el de la misma intimidad, el libre acceso a la información o el desarrollo de la personalidad, entre otros.

Todos sabemos que la investigación tiene un fin, pero en muchas ocasiones los efectos pueden perjudicar a la misma organización y lo que se está investigando puede revertirse en contra.

No solo por la vulneración de estos derechos, sino porque dentro del mismo éxito de dicha investigación se puede estar violando el derecho al debido proceso y la cadena de custodia. El mismo procedimiento de recolección de estas evidencias que pueden convertirse en elementos probatorios, si la investigación se sale de ese ámbito interno y llega al contexto penal, pasarían a ser pruebas presentadas en juicio que estarían viciadas y afectarían en forma negativa todo el camino recorrido en esa investigación interna.

Anuar Torres.
Quisiera aportar algunos elementos que considero importantes en la investigación interna:

Lo primero es tener claridad sobre cuáles son los objetivos de la gerencia; qué es lo que nos están pidiendo que investiguemos; adónde quiere llegar realmente la gerencia. Lo segundo es definir el marco regulatorio, entendido como lo que

Los asistentes estuvieron de acuerdo en la claridad de los objetivos para adelantar una investigación interna.

ya comentó el Mayor Bautista, pero adicionalmente todos los intereses que pueden existir. Si hay una póliza de seguros, qué es lo que pide esa póliza; si figuran unas políticas de procedimiento; y, considerar el mismo contrato de trabajo, para determinar hasta dónde se puede llegar con la investigación.

En el caso de existir una reglamentación jurídica, la investigación tiene que ajustarse a ella, lo mismo si se trata de unos lineamientos internos, a los cuales debe estar alineada.

Eso nos lleva a otro punto relacionado con la necesidad de conocer muy bien el negocio. Porque es imposible iniciar una investigación si no se tiene ese conocimiento, así la adelante un agente externo.

Otro punto importante es el relacionado con las evidencias para entender lo sucedido: qué hizo el delincuente; qué buscaba; cuáles fueron sus motivaciones; a dónde pretendía llegar. Así mismo, hay que determinar el alcance del fraude para detectar si cobija a una sola persona, a un equipo o se trata de una organización delictiva la que está detrás.

Es de vital importancia la vinculación a ese proceso de un abogado, para garantizar que las pruebas y evidencias cumplan con todos los requerimientos de orden legal. Los expertos en tecnología también son indispensables, en la medida en que la mayoría de negocios o actividades empresariales están soportados en componentes tecnológicos.

Por lo general la solicitud de investigación se orienta a demostrar si hay una pérdida y a establecer responsabilidades; a que se identifiquen los responsables y a demostrar la intencionalidad. Igualmente, los métodos utilizados y es ahí donde las pistas de auditoría y las evidencias tecnológicas cobran mayor importancia, por son estas las que permiten llegar a tales conclusiones.

Jeimy J. Cano

Es de resaltar la importancia de todas las intervenciones y sobre ellas hay dos puntos en los que quisiera enfatizar. Uno es el contexto legal. A la luz de estos temas creo que hay una sentida necesidad de las áreas asesoras desde el punto de vista legal, las cuales empiezan a introducirse en asuntos del derecho informático. Es casi una consecuencia de la evolución tecnológica y la tecnología formando parte del negocio.

Es interesante observar cómo los abogados hoy en día se han visto abocados a repensar todo lo que han aprendido en el tema del derecho relacionado con los mundos *on* y *off line.*

Así mismo, el entorno obliga a quienes manejan los aspectos tecnológicos, a entender desde esa perspectiva (la legal) qué es lo que el Derecho establece como norma u orientación, para poder poner en marcha la investigación. Un asunto bien importante para las áreas que asesoran a las empresas desde el punto de vista jurídico.

Hace poco leía el último número de la revista *IEEE Security & Privacy* de mayo, que aborda el tema de los ciberseguros y considero que es pertinente hacer un comentario en este sentido.

Los seguros que en la actualidad están vigentes para los bancos y otras organizaciones establecen sus cláusulas en elementos tecnológicos de hace 20 años. Se refieren a pérdidas de información, transferencias de mensajes vía télex, conexiones por fax; conexiones vía telefónica (dial up), entre otros que hacían parte de la operación normal de las empresas hace 20 años. De otra parte, la manipulación de la página web, la suplantación o robo del nombre de dominio, engaños vía *phishing* y manipulación de identidad, entre otros medios, no son cubiertos por las pólizas todo riesgo ofrecidas en la actualidad por los entes aseguradores.

Hace poco, algunos estudiantes de la Facultad de Derecho de la Universidad de los Andes, en el curso Internet: Principios de Seguridad y Aspectos Legales, ofrecido durante

El moderador Jeimy J. Cano (centro) enfatizó en el contexto legal como una necesidad de las áreas asesoras.

el primer semestre de 2007, hicieron una investigación en las empresas de seguros colombianas y se pudo detectar tal panorama. Lo que refleja que las organizaciones todavía no ven los ciberseguros como una forma adicional para luchar contra el fraude, el cibersecuestro, el ciberterrorismo o cualquier otro evento similar.

En tal sentido, los ciberseguros son un elemento fundamental que le permite a la organización exigirse a sí misma para mejorar sus competencias frente a incidentes de seguridad que puedan llegar a materializarse. Alguien decía que para cometer un fraude lo que se necesita es una motivación; como dicen los psicólogos "toda idea lleva al acto".

Para finalizar este comentario, el profesionalismo, además de conocer y saber usar la tecnología, son componentes para tener en cuenta de cara a las investigaciones, en la medida en que permiten avanzar para tener sistemas menos inseguros. Se dice que "no hay crimen perfecto, sino investigaciones imperfectas".

Francisco Rueda

¿Y no será que la legislación también requiere actualización, así como lo exigen los seguros? Luego la pregunta es si la legislación actual es suficiente para enfrentar todas esas problemáticas.

Mayor Fredy Bautista

En este momento lo que se está haciendo es utilizar lo que ya está consignado en el Código Penal como conductas delictivas para realizar casi una analogía o una comparación. Allí los fiscales y los jueces tienen que jugar con la norma y hacer ver una conducta delictiva.

Hay varias iniciativas para fortalecer esos aspectos legales, pero es una necesidad sentida, armonizar la actual legislación frente a la problemática que se está presentando sobre nuevas conductas delictivas.

Anuar Torres.

Esa obsolescencia de legislación y las deficiencias internas de políticas tecnológicas se debe básicamente a una "invasión de tecnología" que ha sido aplicada al negocio, pero no se ha hecho una apropiación de tales herramientas, entendida como la comprensión de la tecnología, sobre cómo funciona. Por lo general, se operan los elementos tecnológicos, se ponen a funcionar dentro de la organización, pero sin entender sus principios y conceptos. En tal sentido y a manera de ejemplo, si no se entiende lo que es un secuestro de dominio, pues no se va a legislar sobre el particular.

Oscar Ruíz

Un elemento que impulsaría en gran parte el tema de legislación y para que las empresas se organicen en el tema de investigación interna, es la

apropiación de modelos que ya están funcionando como los equipos de respuesta de incidentes en seguridad de la información CSIRT (Computer Security Information Response Team).

El Gobierno está participando en el comité del CICTE (Comité Interamericano contra el Terrorismo) de la OEA y ese comité busca implementar a nivel de política de Estado la protección de infraestructura y la conformación de CSIRTs a nivel local y en Latinoamérica.

Con la apropiación de este modelo que ya es un estándar en otros países como en Europa y Estados Unidos, el Gobierno tendrá que adecuar su legislación, y se hará una apropiación de este modelo a la cultura empresarial y gubernamental. Será un efecto dominó.

Jeimy Cano

A la luz de una investigación interna ¿cómo establecemos relaciones o nexos con los entes de policía judicial si queremos judicializar el caso? ¿Cuáles restricciones o cuidados debemos tener?

Mayor Fredy Bautista

El tema principal en ese sentido es la confianza. En eso estamos trabajando; en generar una confianza desde la policía judicial hacia las organizaciones públicas y privadas, porque a nadie le gusta que cualquier incidente de seguridad se ventile o se conozca. Esto trae consecuencias sobre el buen nombre, de tipo económico u otras similares, que agravan el daño que ya ha sufrido la organización.

En primera instancia debo anotar que estamos trabajando con los principales gremios en esa dirección de generar la confianza necesaria para adelantar las investigaciones, y esto lo estamos haciendo con las principales empresas relacionadas con el tema de la tecnología y aquellas cuyos procesos se desarrollan por completo a través de sistemas.

Colombia en este momento está viviendo un problema bastante grave; la Fiscalía puede tener cerca de 6 mil o 7 mil investigaciones por fraude represadas. Primero, porque se está depurando el entorno y mirando cuáles ameritan poner a funcionar todo el aparato judicial, de manera de no desperdiciar esfuerzos. Segundo, porque ha rebasado la capacidad investigativa en cuanto al número de fiscales y ese mismo problema se presenta dentro de la policía judicial. Para este período del año, tenemos igual número de fraudes que conocimos el año anterior. Se trata de fraudes informáticos reportados, más los que están en curso y a la espera en la Fiscalía para ser atendidos.

El problema existe, es latente y no podemos taparnos los ojos, pero lo que también hay que determinar aquí, es que muchas veces cuando iniciamos el proceso de investigación no encontramos eco en las empresas. Las demoras en la entrega de la información que requerimos para agilizar las investigaciones son de hasta tres meses.

Ahí encontramos varias trabas. O no han diseñado un mecanismo de rápida respuesta para suministrar la información a los entes judiciales o no desean que se avance mucho en la investigación, precisamente para proteger su nombre o cualquier otro aspecto.

No hay una respuesta rápida para las autoridades y cuando nos disponemos a trabajar con la Fiscalía sobre investigaciones que tienen 4 o 5 meses, descubrimos que no existe la información solicitada, después de uno, dos o hasta tres requerimientos hechos por parte de la policía judicial.

Otro asunto es el relacionado con el primer respondiente y ya pasamos a la parte procedimental. Nadie quiere asumir la responsabilidad dentro de la organización para dar la cara a la policía judicial, aspecto directamente relacionado con la generación de confianza. Es decir, el hecho de que un empleado esté presente y suministre las pruebas, no quiere decir que esa persona vaya a formar parte del sujeto procesal o sea responsable de esa acción.

Las organizaciones deben definir quiénes son las personas autorizadas y responsables para manejar el incidente en todos esos efectos y de esa manera allanar el camino para que la policía judicial pueda llegar a recolectar la evidencia o material probatorio.

El código establece que el respondiente es la primera persona que tiene contacto con un elemento material probatorio que le infiere al investigador la posibilidad de convertirse en una evidencia, que podría materializar en una audiencia de juicio y terminar siendo una prueba. En otras palabras, se va rotando la responsabilidad dentro de las organizaciones

Mayor Fredy Bautista

–en su mayoría privadas- y es difícil concretar esos procesos.

El tercer punto es el desconocimiento de los afectados sobre la forma de dar a conocer a la policía judicial o a la autoridad el conocimiento del hecho. El código establece 3 o 4 formas.

El primero es la denuncia penal; básicamente un escrito en el que la organización narra en forma cronológica los hechos sucedidos y detalla los procedimientos que adelantó cuando conoció el caso. Identifica cuáles son las personas relacionadas con la investigación interna; en este punto es necesario acreditar la idoneidad de quienes participaron en esos pasos a efecto de decir que el procedimiento de preservación y recolección fue el adecuado.

Cuando en ese procedimiento estuvieron presentes varias personas y la organización no quiere profundizar en esos datos por las implicaciones que pueda tener, la ley permite que una investigación se abra en calidad de averiguación. Uno de los principales temores que uno encuentra, en particular, en la empresa privada cuando van a poner en conocimiento un hecho es que a nadie le gusta ir a sindicar o señalar directamente a una persona. Y, para eso, está precisamente el engranaje completo de la administración de justicia en aras de hallar el responsable.

Sara Gallardo M.

¿Los indicios tienen el mismo alcance de una averiguación?

Los indicios son todos los señalamientos y demás elementos que nos permiten inferir que en efecto una persona puede tener alguna responsabilidad en el hecho. Mientras la averiguación es una figura para abrir un proceso bajo esas características.

La empresa ya sabe quién es la persona, pero no quiere asumir el costo que esto representa frente a la familia y al conocimiento público.

En este momento, la Fiscalía General de la Nación está buscando fortalecer una Unidad de Delito Informático, cuya génesis es la unidad de propiedad intelectual y telecomunicaciones. Un ejemplo concreto que vale la pena comentar es el caso de Corfiboyacá, asignado a esa unidad en el que se cometió un fraude, precisamente por la equivocada utilización de un sistema informático. Se trata del primer caso relacionado con un hurto o fraude grave que llega a esa instancia, a una unidad especializada.

¿Cómo establecer las relaciones con los entes de policía judicial? Básicamente existe la denuncia; hay que

mejorar algunos procedimientos de respuesta inmediata, los cuales permiten desplazar equipos de tal naturaleza a las empresas en donde han ocurrido incidentes cibernéticos. Por ejemplo, hemos desplazado equipos cuando se está ejecutando un fraude "en vivo", en el momento preciso, a entidades financieras porque lo comunican en forma inmediata y porque creemos que es un hecho que requiere que el sistema judicial actúe en esa forma.

Tenemos la capacidad de desplazar esos equipos para hacer la recolección de esa evidencia, pero no contamos con los suficientes para atender la creciente demanda. Por esa razón, establecemos en forma estratégica cuáles son los casos que ameritan una acción inmediata de ese estilo.

Sobre las restricciones y cuidados que debemos tener sugeriría que se debe hacer una revisión y que es prioritario leer el Código de Procedimiento Penal. Dicho Código tiene que ver con todos, seamos o no abogados, porque de cara a las leyes actuales sobre procedimiento penal, fácilmente podemos pasar a ser testigos de un evento. Capítulos como el de la cadena de custodia que genera temor y miedo; procedimiento mediante el cual se garantiza que quien encuentra inicialmente un elemento material probatorio, esa evidencia física que no es prueba sino un indicio, un referente de que algo hay, sea la misma persona hasta cuando ese elemento llega a manos del perito, que en últimas, es quien va a observar si hay un hallazgo interesante para la investigación.

La acreditación es otro tema importante. No podemos pedirle a alguien que no tenga la acreditación suficiente a la hora de soportar los hechos ante un juez de garantías. Cuando se carece de esa idoneidad es mejor acudir a agentes externos.

Oscar E. Ruíz B.

En un caso como ese, fácilmente el abogado de la defensa podría alegar a favor de su defendido la contaminación de la evidencia, por la alteración de la fechas de operación del equipo. Una simple diferencia entre el encendido y apagado del equipo puede dar lugar a ello.

Oscar E. Ruíz B.

El tema tecnológico de respuesta de incidentes tiene un primer responsable que debe tener las cualidades y preparación adecuada. Puede ser humano con tecnología o tecnológico y automatizado.

Así como existe el circuito cerrado de televisión, en los sistemas de información existen dispositivos para gravar y reproducir el tráfico de red. Es decir, que no hay forma que algo se escape. Son 'juguetes caros' para capturas de información de 15 Tb.

Los servidores de misión crítica deben estar vigilados en forma constante para que en un caso de acceso no autorizado, puedan obtener diferente tipo de evidencia hasta el nivel de las cesiones TCP o UDP que corren en memoria, las cuales son altamente volátiles. Aquí el tiempo de oportunidad en la adquisición de este tipo de evidencia se torna en un componente crítico.

Este tipo de soluciones de adquisición de evidencia digital serán utilizadas en las empresas para el análisis forense. Son soluciones costosas, que no siempre las empresas están dispuestas a adquirir, bien sea por razones de presupuesto o porque no ven la importancia de tenerlas consigo.

Estos elementos permiten que la recolección de pruebas sea fundamental en una investigación, siempre y cuando el procedimiento se haya ajustado a los pasos necesarios para no alterarlas.

Al encapsular un archivo o un dispositivo dentro de un archivo de evidencia digital, en el fondo lo que se esta haciendo es presentar en este formato la prueba ante un juez o la instancia pertinente. Este archivo de evidencia de forma lógica cuenta con mecanismos para validar su integridad.

Francisco Rueda

¿En ese sentido, las empresas están preparadas? ¿Saben qué hacer y como recoger las pruebas? ¿Falta una cultura de esa naturaleza?

Anuar Torres

Uno debería observar el contexto empresarial colombiano, para responder a la pregunta sobre si las empresas

Anuar Torres

están o no preparadas para administrar evidencias. En condiciones ideales ese tipo de mecanismos debería existir. Pero la realidad es que las organizaciones que cuentan con los dispositivos para hacerlo, son muy pocas.

Aquí vale la pena hacer un juicio al respecto. Las empresas que tienen elementos de seguridad los han dispuesto pensando en cómo soportar un negocio, pero sus sistemas no han sido diseñados o concebidos para enfrentar una ataque. Herramientas existen muchas, pero la cultura de tecnología del país no está preparada para enfrentar los riesgos que genera la tecnología por sí misma.

Por lo tanto, los mecanismos de preservación de evidencia o de defensa no son incorporados de manera nativa, sino como complemento; una respuesta ante un hecho no entendido plenamente.

Francisco Rueda

Esa infraestructura y su montaje son costosos. ¿Es una razón para que los empresarios duden en ponerla en marcha y solo lo hagan hasta cuando sucede algún evento?

Anuar Torres

Hay un problema cultural de fondo, de conciencia. El empresario colombiano crea un negocio, por lo general motivado por una necesidad de subsistencia personal. Si debe implementar tecnología busca la más económica que responda en forma rápida a sus requerimientos. Solo cuando ha solucionado el problema de subsistencia, considera la posibilidad de pensar en otros asuntos, olvidando que esta y la permanencia de su empresa están íntimamente ligadas y que uno de los principales componentes para lograrlo es el adecuado uso y puesto en marcha de la tecnología informática.

Sara Gallardo M.

¿Y la obsolescencia de la tecnología tiene que ver con esos aspectos que se están abordando?

Jeimy J. Cano

Ese es un aspecto clave en el tema de las investigaciones. En algunas ocasiones se han materializado fraudes en un sistema OS2 o peor aún, en un AS400, lo que dificulta el proceso completo de la investigación.

Se trata de tecnologías que no son masivas, con otras características y propósitos. Es decir, que las herramientas actuales para hacer análisis forense tienen limitaciones en estas plataformas. Habría que pensar en que se requieren herramientas nativas en los sistemas operacionales mencionados para poder actuar en el caso de un incidente. De lo contrario, la recopilación de pruebas en esos sistemas sería cuestionable, desde el punto de vista de su manipulación.

En ese contexto, hay que coleccionar originales de los sistemas operacionales para poder instalarlos en las máquinas y proceder a la virtualización de los servidores. Es un hecho que la obsolescencia tecnológica afecta e impacta las investigaciones internas.

Conclusiones

Anuar Torres

La investigación interna es un tema que está en pleno desarrollo, asociado por lo general con tecnología y auditoría forenses. De ahí que las preguntas giren en torno a quién debe adelantarla.

El fraude siempre ha existido y seguirá existiendo. En la medida en que la tecnología y los entornos empresariales han evolucionado, las modalidades delictivas se han sofisticado, lo cual exige para su investigación y análisis profesionales especializados, con competencias profesionales y personales específicas.

En lo que se refiere a los temas legales, tecnológicos y de negocio, esos profesionales deberán desarrollar con los grupos de investigación conocimientos de las ciencias humanas que permitan entender aspectos tales como el lenguaje verbal y no verbal de un individuo; sus motivaciones y necesidades. Elementos tan importantes como un análisis de computación forense.

Oscar E. Ruíz B.

Afrontar el reto de las investigaciones internas por fallas en los sistemas de información, fraude, sabotaje o cual fuere el motivo, requiere el previo establecimiento de las Políticas de Seguridad de la Información, la conformación del CSIRT y el uso de tecnología y/o conocimientos específicos para su desarrollo.

Las seis etapas para el manejo de incidentes son: Preparación, Identificación, Contención, Erradicación, Recuperación y Lecciones Aprendidas; quizás esta última sea la más importante porque retroalimenta cada experiencia, identifica errores en los que se pudo haber incurrido y permite tomar los correctivos para que el incidente no vuelva a pasar o sea manejado en la forma correcta.

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. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Corresponsal de la revista Infochannel (México). Autora del libro "Lo que cuesta el abuso del poder". Corresponsal en Colombia del Diario "La Prensa" de Panamá y revista IN de Lanchile; editora de esta revista.*