Material Imprimible

Curso Ciberdelitos y Derecho Informático

Módulo 2

Contenidos:

- Nociones criminológicas y psicológicas relacionadas a la delincuencia
- Ciberdelincuentes
- Perfil habitual de los hackers
- Proceso de investigación tecnológica
- Cadena de custodia
- Análisis forense informático
- Investigación en Really Simple Syndication

Nociones criminológicas y psicológicas relacionadas a la delincuencia

El filósofo italiano Cesare Beccaria planteaba que "Los delitos deben ser calificados según el daño infligido a la sociedad.", mientras que el poeta alemán Heinrich Heine expresaba que **"**Todo delito que no se convierte en escándalo no existe para la sociedad".

Debemos entender a la conducta como el primer elemento básico del delito, y esta conducta se establece como el comportamiento humano de carácter voluntario, negativo o positivo, dirigido hacia un propósito.

Lo que queremos remarcar con esto es que solo los seres humanos pueden efectuar conductas positivas o negativas, ya sea por una actividad o una inactividad. El comportamiento es voluntario porque es una decisión puramente del sujeto y es a razón de un propósito, ya que tiene un fin al realizarse la acción u omisión.

Para proceder en la temática es importante que veamos nociones criminológicas y psicológicas relacionadas a la delincuencia. En primer término, definamos estas dos disciplinas. La criminología es una ciencia social e interdisciplinaria que tiene como fin estudiar al delito, al delincuente, el control social, las conductas desviadas, y la víctima, a razón de comprender al autor de los hechos y las distintas motivaciones que lo llevaron a efectuar determinados ilícitos.

Por su parte, la psicología es una disciplina académica y una profesión que estudia y analiza a la conducta y los procesos mentales de las personas y de grupos sociales en distintos contextos, cuya área de estudio envuelve todos los aspectos de la experiencia humana.

La psicología criminal es una disciplina que estudia los fenómenos psicológicos relacionados a los actos delictivos.

Una persona que ejerza dicha profesión puede desarrollar distintas tareas, tales como realizar y difundir técnicas de persuasión y comunicación para el análisis de testimonios, colaborar en una investigación delictiva elaborando perfiles psicológicos, establecer programas de rehabilitación para delincuentes, y efectuar investigaciones teórico

prácticas sobre la conducta, personalidad y motivación del criminal que auxilien a un análisis científico del delincuente.

A lo largo de la historia se han realizado diversas investigaciones criminológicas. A razón del presente módulo, creemos relevante desarrollar las teorías de Cesare Lombroso, Benigno Di Tullio y Sigmund Freud, quienes hablaron respecto a la conducta y la criminalidad.

Para el criminólogo italiano Cesare Lombroso la comisión de delitos era un hecho anormal. Los criminales van a ser individuos anormales, insensibles, con una personalidad de psicopática, y por eso creía necesario efectuar una clasificación de los criminales en función de su informe clínico, sus características físicas y su personalidad, para, de esta manera, poder realizar un diagnóstico de delincuencia y para poder actuar desde la prevención.

Para el segundo autor en cuestión, el psiquiatra italiano Benigno Di Tullio, la criminología se va a tratar de una disciplina que estudia las conductas que son entendidas como antisociales criminales. Este análisis lo va a efectuar a partir de una serie de casos que pueden considerarse normales, anormales o patológicos, y de esta manera, va saber discernir cuáles son las situaciones y condiciones que lleva a un individuo a realizar o no ciertos actos característicos.

Di Tullio realizó un análisis respecto la personalidad de los delincuentes para establecer los comportamientos antisociales. Para eso, efectuó un tratamiento médico en el que se analizó al paciente desde todas las implicancias factibles para poder llevar a cabo un estudio profundo de su personalidad y del propio individuo. A partir de este autor, la criminología comenzó a emplear teorías biológicas y psicológicas, incorporando, de esta manera, estas ciencias para el análisis de los comportamientos delictivos.

Para Sigmund Freud, el padre de la psicología, el criminal proyecta a través de los actos ilícitos sus conflictos psicológicos.

Este autor expresa que el humano es innatamente un delincuente y, además, plantea dos características fundamentales en el criminal: un alto nivel de egocentrismo y una tendencia hacia la destrucción, las cuales van a manifestar una deficiencia en la valoración afectiva.

Asimismo, va a destacar que la mayoría de las personas que realizan crímenes son trabajadores que no mantienen una profesión, que tuvieron problemas familiares, que fracasaron en su educación, que vienen de familias disfuncionales y que sufrieron de abusos.

Además, considera que en las primeras infancias las principales motivaciones en el desarrollo de estilo de vida son las actividades precozmente desadaptadas, la falta de sentimiento de comunidad y la privación que mantiene el menor.

Según Sigmund Freud, "Todo hombre es innatamente un criminal, es decir, inadaptado. Conserva en su plenitud esta tendencia durante los primeros años de su vida, la adaptación de la sociedad comienza después de la victoria sobre el complejo de Edipo, un período de lactancia, que comienza entre el cuarto y sexto año de edad y termina en la adolescencia. Aquí el desarrollo del individuo sano y del criminal son hasta el momento, iguales. En el período de lactancia el individuo normal consigue reprimir las genuinas tendencias criminales de sus impulsos y el criminal dirigiéndolas en un sentido social, fracasa en esta adaptación. Influyo en la formación del criminal desde recién nacido un medio ilimitado de apoderarse de todo, y este pulso de posesión se exterioriza en acciones caníbales del niño. Los descuidos en la educación, pueden influir en la posterior del niño con la sociedad".

A finales de la década 1970, surge la psicología con un enfoque criminológico. Esta rama científica se focalizó en la investigación del tratamiento, prevención y rehabilitación de las conductas criminales.

A partir de las ciencias de la conducta, podemos distinguir tres frentes: la psicología biológica, los procesos cognitivos y el despliegue de una investigación compuesta por el

estudio integral de las carreras criminales. De esta forma, los investigadores arriban a una conclusión de que los delincuentes piensan a modo de compartimientos.

Desde las diversas investigaciones criminológicas se estableció que para la elaboración de un perfil psicológico con criminales es sumamente relevante tener en cuenta las características sociales que diferencia a ciertos individuos de los demás, ya sea por sexo, estado civil, edad, raza, posibilidad de cometer algún ilícito, antecedentes policiales, madurez sexual, vínculos, status, entre otros.

Sobre la base de esto, se establece que elaborar el perfil de un delincuente infiere aspectos psicosociales, como su motivación, comportamiento y personalidad, con el objetivo de que se pueda puntualizar un mismo comportamiento habitual en el conjunto de individuos asociados a efectuar ciertos ilícitos. Dentro de los rasgos de las personalidad delictivas nos encontramos con la agresividad, la indiferencia afectiva, el egocentrismo y el fracaso afectivo.

Por otra parte, dentro de los rasgos cognitivos de los criminales hayamos la facilidad de distracción, la baja autoestima, la confianza extrema en sí mismo, el sentimiento de que el mundo es propio de beneficio, la escasa empatía, la interpretación del mundo como un lugar hostil, la incapacidad de demostrar agradecimiento, la falta de pensamiento crítico y la atribución de su comportamiento a otras personas.

Por último, dentro de los rasgos de comportamiento característicos de los delincuentes encontramos a la ansiedad, la insensibilidad, el aislamiento, la baja tolerancia, la impulsividad, el bajo autocontrol, la necesidad de aprobación, la alta tendencia a tomar riesgos, la visión a corto plazo, la impaciencia, la rebeldía, la insatisfacción y la frustración.

Ciberdelincuentes

Según el investigador mexicano Julio Téllez Valdés, los delitos informáticos presentan las siguientes características principales:

- Son conductas criminales de cuello blanco, en tanto que solo un determinado número de personas con ciertos conocimientos, en este caso técnicos, puede llegar a cometerlas

- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando
- Asimismo, son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico
- A su vez, provocan serias pérdidas económicas, ya que casi siempre producen grandes beneficios a aquellos que las realizan
- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundos y sin una necesaria presencia física, pueden llegar a consumarse
- Son muy sofisticados y relativamente frecuentes en el ámbito militar
- Además, presentan grandes dificultades para su comprobación, debido a su mismo carácter técnico
- Por último, tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

A partir de las características del delito informático, debemos considerar cuáles son las causales y las motivaciones para la perpetuación de los mismos.
Por motivos pecuniarios, lo que implica mayor motivación en el robo es el dinero o artículos de valor. Por ende, los sistemas que suelen ser más vulnerables a actos fraudulentos son los relacionados a pagos, ventas y compras, ya que en estos sistemas suele ser más sencillo convertir transacciones fraudulentas en ganancias. Por motivos parecidos, los bancos, las empresas constructoras y compañías de seguros son más susceptibles a los fraudes que las demás.

Asimismo, los sistemas mecanizados van a ser más propicios a los fraudes y a las pérdidas. Los motivos son:

- Manejan grandes volúmenes de información en los cuales, generalmente, opera poco personal, lo que dificulta la verificación de todas las partidas

- A veces los registros tienen carácter transitorio y podrían extraviarse los detalles de lo ocurrido, quedando solo los efectos
- Pueden llegar a sobrecargarse los registros magnéticos, lo que podría ocasionar la pérdida, la evidencia o la sucesión de acontecimientos
- Los sistemas no son personales, figuran en un formato ilegible y están auditados escasamente por individuos cuya preocupación más relevante son los aspectos técnicos del sistema y su equipo

En la creación de un sistema importante es complejo poder asegurar que se han previsto todas las situaciones, y es factible que en las previsiones que se hayan pensado hayan quedado vacíos sin cubrir. Los sistemas suelen ser rígidos y no siempre se piensan o cambian con la misma velocidad que con la que se generan los acontecimientos, lo cual puede llegar a ser otro motivo de carencias.

Pocos individuos del personal correspondiente al proceso de datos tiene noción del completo alcance del sistema, y el lugar de cálculo suele llegar a tratarse de un centro de información. De igual modo, el centro de cálculo va a procesar muchas cuestiones parecidas de las transacciones. En estos centros hay personal muy capaz, que opera por iniciativa propia la mayor parte del tiempo y podría ser complejo establecer unos niveles comunes de supervisión y control.

Asimismo, el fraude y el error no van a ser equiparables, ya que a veces, los errores son bastántes disímiles a la actividad fraudulenta. Cuando aparecen desemejanzas, no se suele pensar que se han generado por un fraude, y la investigación puede culminarse previo a llegar a dicha conclusión. Por eso, se suele iniciar buscando errores del sistema y de programación. Si fracasa esta interveción, se indaga respecto a fallos operativos y técnicos. Recién cuando todas estas operaciones no hayan dado resultados satisfactorios, empieza a pensarse que podría tratarse de una maniobra fraudulenta.

Es importante comprender que el sujeto activo de estas modalidades delictivas tiene ciertas características y mantienen habilidades que no suelen presentar la mayoría de los criminales. A su vez, tenemos que tener en cuenta que ellos, para el uso de los sistemas

informáticos y habitualmente por su trabajo, pueden encontrarse en ambientes laborales estratégicos donde se opera información de carácter sumamente sensible.

Estos delincuentes suelen ser muy hábiles en la utilización de los sistemas informatizados, y en general, la perpetuación de estos delitos no suele explicarse por situaciones de pobreza, ni por poca inteligencia, ni por falta de educación, ni por inestabilidad emocional. Asimismo, en estos casos, los sujetos activos suelen ser individuos listos, motivados y decididos, que toman los retos tecnológicos a modo de desafíos.

Perfil habitual de los hackers

Como características habituales de estos individuos tenemos, en general, a la mentalidad turbada, problemas financieros, beneficio personal, odio a la organización, búsqueda de prestigio y búsqueda de reconocimiento. Esta conducta, a partir de la cual se va a acceder sin autorización a un sistema de información, atenta gravemente contra la estructura de seguridad que se mantenga.

El objetivo del accionar del hacker suele ser muy diversa, ya que a partir de su accionar buscará filtrar, destruir o alterar la información que mantenga el sistema, ya sea de forma total o parcial.

Proceso de investigación tecnológica

Según el escritor británico Philip Kerr, “La información es la parte vital de cualquier investigación criminal, y si esa información está contaminada, entonces todo el cuerpo investigador resulta envenenado”.

Previo a indagar profundamente en la cuestión del proceso de investigación de la informática forense, es preciso que se tenga una noción básica respecto a las normas de la evidencia y la investigación preliminar. Resulta fundamental la presentación de pruebas en cualquier proceso judicial, pero en materia de evidencia informática resulta ser un desafío aún mayor. Por esto, se necesita tener conocimientos respecto a la materia, y un particular cuidado a la hora de no alterar y preservar el medio de prueba.

Para que un medio pueda ser tenido en cuenta como prueba del hecho, el mismo tiene que ser relevante y competente a la cuestión, con el objetivo de responder un interrogante pericial relevante para la causa, como por ejemplo, quién efectuó el delito.
El objetivo del investigador va a ser dirigir la investigación policíaca respecto a un hecho punible, integrando la labor que despliegan los demás especialistas en sus áreas de experticia.
En el lugar del hecho, este despliegue se efectúa con la participación de distintos profesionales. Sin embargo, cuando se dan situaciones en las cuales, ya sea por el lugar, modo o tiempo, no es factible contar con el auxilio de estos, es el momento en que el investigador deberá desarrollar las técnicas y practicar procedimientos requeridos para realizar su trabajo y, también, desplegar la inspección técnica para recolectar y preservar cualquier clase de evidencia digital, las que podrán ser de utilidad para la localización, la identificación y la persecución de los autores y responsables de la perpetuación del acto ilícito.

La labor del investigador, posterior a mantener conocimiento de un acto delictivo, va a constar se una serie de procedimientos. Al arribar al lugar se tiene que efectuar un análisis de este, con el objetivo de preservarlo y proceder a su inspección.

Los pasos son:

- Para su aseguramiento, deberán ocupar lugares, objetos, armas o instrumentos, utilizando para tal fin cualquier medio idóneo para lograrlo, tales como cuerdas, cintas, barrera de funcionarios, entre otros
- Luego se deberá identificar a personas que pudieran suministrar información sobre la presunta comisión del delito, para su posterior citación y/o traslado, a fin de recibirles sus respectivas entrevistas
- Posteriormente se va a tratar de identificar, localizar y capturar a los posibles responsables o partícipes en el hecho, así como los objetos, armas o instrumentos que pudieran relacionarlo con el mismo

- Después se deberá auxiliar al técnico-criminalista en la práctica de las experticias pertinentes, tales como inspección técnica, levantamiento planimétrico, trayectoria balística, entre otros
- Por último, se va a realizar cualquier otra diligencia necesaria para la investigación.

Para fijar, anotar, dibujar y conservar los datos captados, es necesario que el investigador criminal cuente con herramientas indispensables y necesarias a utilizar para tomar nota, tales como bolígrafo, lápiz, marcador, cuaderno, agenda, block, entre otros. Poder realizar una reconstrucción de los hechos le va a brindar al investigador la posibilidad de entender todas las circunstancias vinculadas con la realización de los ilícitos, utilizando para ello las evidencias inspeccionadas, preservadas, recolectadas y analizadas.

Los diferentes elementos que se usarán para la comisión del crimen le van a permitir al investigador efectuar tres maneras distintas de reconstrucción: la reconstrucción funcional, la reconstrucción relacional, y la reconstrucción temporal.

- La reconstrucción funcional se efectúa a partir del señalamiento de la función de cada elemento dentro de la escena del hecho, así como la manera en que estos operan y cómo son utilizados
- La reconstrucción relacional Esta parte de basarse en los indicios que manifiestan una correspondencia con algún objeto en la escena del hecho y su carácter relacional con los otros elementos que ser encuentren. Se focaliza en la interacción en conjunto o entre cada uno de los elementos indiciarios
- Por último, la reconstrucción temporal se realiza con elementos que nos sitúan en la línea temporal del despliegue del ilícito y en relación con los indicios hallados.

El término análisis forense se utiliza para el proceso de análisis de una copia completa de un sistema que ha sido vulnerado. Dicho análisis va a abarcar distintas áreas: una de las

mismas es la recolección del material de carácter probatorio a partir medios electrónicos, entre otras clases de dispositivos de comunicación y de almacenamiento, puntualizando en el principio de la inmediatez de la prueba pericial.

Se deberá adquirir toda la información vinculada con cada una de las plataformas y documentos digitales que se estudien. En otras palabras, se debe estar al tanto respecto a las modificaciones, consultas, sustracciones o adiciones que puedan vincularse con distintas áreas, como podría tratarse, por ejemplo, de un registro contable, desde que se haya creado hasta el momento de la pericia.

Otra de las áreas pertinentes va a ser la recuperación de información que haya sido borrada, destruida, alterada u oculta en los distintos dispositivos de almacenamiento tecnológicos.

La siguiente área se va a encargar de descifrar las claves de acceso de los ordenadores personales y dispositivos de almacenamiento, así como cualquier otro tipo de dispositivo a partir de herramientas y metodologías de análisis de encriptación.

Y las últimas dos áreas son la de detección de los intrusos en las redes, y la de garantizar la confiabilidad y autenticidad de las evidencias digitales adquiridas.

Cadena de custodia

Se va a entender por cadena de custodia a la totalidad de las medidas que deben tenerse en cuenta para poder preservar la integridad e identidad de los elementos que constituyan la evidencia de hechos delictivos, a fin de garantizar su correspondiente eficiencia durante el debido proceso judicial.

Es fundamental garantizar que los elementos de prueba requeridos para el juicio sean idénticos a los que se hayan recolectado en primer lugar, es decir, que no hayan mantenido modificaciones o adulteraciones a lo largo del proceso.

Asimismo, se debe tener especial cuidado en evitar cuestionamientos respecto del levantamiento y la custodia de los elementos o rastros que se presentan en el juicio, expulsando cualquier sospecha sobre su procedencia y dejando en claro que se corresponden con los efectivamente secuestrados en la escena del crimen.

Para llevar adelante esa actividad, es preciso acreditar el método utilizado y el personal que lo practicó. En definitiva, si las pruebas no se bastan a sí mismas, es decir, si es preciso identificar los objetos o huellas del delito, el sitio en que fueron encontrados, o la persona que tuvo a su cargo esa tarea, resulta central prestarle atención al levantamiento y la conservación de ese material. Porque si el método es incorrecto, el almacenamiento inadecuado o la persona incapaz de cumplir su cometido, el trabajo será inútil y la evidencia inservible.

Lo más habitual es que sean fuerzas policiales las que, primeramente, tomen conocimiento respecto a la comisión de un hecho delictivo, por lo que deben accionar, en primer lugar, para verificar respectivamente la información. Va a ser fundamental el tiempo transcurrido hasta que las fuerzas de seguridad se constituyan en el lugar del hecho y, además, cómo delimiten el perímetro de la escena del hecho, ya que estas dos acciones dan comienzo a la protección de las evidencias que contenga el lugar.

Luego de que se efectúan de las diligencias iniciales, se debe proceder con la inspección e identificación de los distintos indicios que se hallen, de carácter físico, biológico, químico, de índole material o digital. Asimismo, es fundamental, al momento de recolectar los elementos indiciarios, tener el debido cuidado para no alterarlos ni destruirlos, con el fin principal de conservar su integridad, la manera en que fueron encontrados, y que, de igual forma, arriben al especialista, quien deberá realizar el análisis o pericia correspondiente. Además, se va a procurar que la recolección se efectúe utilizando los medios más adecuados en función a la clase de muestra.

Es esencial que cada muestra que se recoja sea identificada correctamente, describiendo de dónde se obtuvo, a qué corresponde, qué cantidad, qué peso, qué volumen, quién efectuó el levantamiento, a qué hora, entre otras cuestiones. Además, la muestra deberá contener fijada la rotulación pertinente, que mantendrá la firma del funcionario público interviniente.

La fuerza de seguridad que se encargue del caso es la que se encargará de la observación preliminar, la valoración, el análisis, la documentación y la fijación de la escena del crimen, y además, realizará la correspondiente Acta de Secuestro, la recolección de evidencia, el embalaje respectivo, así como el rotulado.

A su vez, es menester que los que realicen las acciones de recolección, embalaje y rotulación de los elementos indiciarios preserven las condiciones de protección y bioseguridad, como lo son el uso de gafas de protección, guantes, equipos especiales, barbijos, etc.

Siempre que sea factible, se procederá a registrar los elementos con fotos antes del embalaje, durante el embalaje y al terminar de embalar y rotular. El embalaje es un paso muy importante, ya que los laboratorios ni ninguna otra institución aceptarán elementos de prueba que no se encuentren embalados, rotulados, sellados y con el debido listado de la cadena de custodia.

La información que debe contener el etiquetado y rotulado de las evidencias físicas es la siguiente:

- número de expediente
- número de listado de la cadena de custodia
- funcionario que recolecta la prueba
- órgano de investigación correspondiente
- número de inspección técnica
- clase de delito
- descripción del elemento
- lugar y fecha en donde se recolectó la evidencia
- y letra o número que corresponda en función al orden de fijación y recolección

El procedimiento de solicitar los análisis pertinentes a los laboratorios y demás instituciones que se encuentren autorizados, deben tener como fin brindar información que confiera un agregado de valor a la investigación. Por esta razón, tiene que tener el objeto de estudio que se precisa de este análisis.

Si el material no está correctamente embalado, rotulado y con el registro correspondiente, ningún personal recepcionará la evidencia. De ahí la importancia de la correcta entrega. Asimismo, quien recepcione los elementos deberá dejar plasmada su

participación en el registro de continuidad de cadena de custodia, lo cual siempre se realizará con la presencia de quien esté efectuando la entrega.

También es importante manifestar que el registro de cadena de custodia deberá tramitarse con un solo ejemplar original sin ningún tipo de copias, y se dejará la constancia correspondiente tanto de la entrega del formato como de las muestras.

Por último, cabe destacar que cuando ya se encuentren ejecutadas las sentencias, ya sea de carácter absolutoria o condenatoria, el juzgador de dicha sentencia va a disponer cuál será el destino final de los elementos de prueba.

Análisis forense informático

Cuando hablamos de análisis forense informático nos referimos a la tarea que efectúan los técnicos, peritos, y demás especialistas de los medios informáticos, con el objetivo de recolectar evidencias que le confiera adquirir información respecto al responsable del delito informático que se indaga, tratando continuamente de no alterar las evidencias mientras se están investigando.

Asimismo, se puede definir como una técnica de reconstrucción de una secuencia de sucesos, que lo que busca es recrear, a partir de distintas metodologías, lo que ha sucedido en dispositivos digitales.

Es importante tener en cuenta dos ejes fundamentales al aplicar estas técnicas. Por un lado, qué hizo un usuario remoto en el ordenador de alguien más. Esto va a incluir la reconstrucción de acciones, la lectura de los archivos de registros y la localización de los orígenes. Por el otro, se distingue qué ha hecho la gente en su computadora. Acá debemos incluir la búsqueda de ciertas fases y tipo de archivos, la desencriptación elemental, la recuperación de archivos borrados y la observación de las áreas interesantes de la computadora.

Proceso fundamental de análisis forense en lo que respecta a la investigación en seguridad

La primera fase es la fase de identificación. Sobre esta se puede expresar que la calidad de la información, así como acotar el ámbito de la misma, es un factor crítico para el

éxito de una investigación. Para un investigador es igualmente nocivo tanto el desconocimiento de información como el disponer de un volumen inmanejable de la misma.

En el primer caso, es decir, ante el desconocimiento de información, el investigador puede llegar a conclusiones erróneas, y en ambos casos, o sea, desconocer información y disponer de un gran volumen de la misma, puede lograr no llegar a presentar ningún resultado concluyente. Por lo tanto, es importante conocer los antecedentes concretos del caso, así como la situación actual. Esta información permitirá al investigador posicionarse y tomar las decisiones que le permitan determinar la estrategia a poner en práctica en la búsqueda de las evidencias.

Durante esta fase es fundamental realizar ciertos pasos, sin los cuales no será factible avanzar. Los mismos son:

- Realizar un planeamiento adecuado y una correcta identificación de los medios y las herramientas a utilizar, además de verificar que se cuenta con los conocimientos y procedimientos requeridos para efectuar el despliegue profesional
- Reconocer si la información está en los dispositivos o debe ser obtenida a partir del proceso mismo
- Rever el contexto jurídico que impacta en el dispositivo, escenario, elemento o material que se va a analizar
- Requerir las autorizaciones imprescindibles, además de información en función a cuáles son las circunstancias, sobre qué se debe obrar, quién puede encontrarse presente, quién está a cargo, quien tendrá que intervenir y cuáles son los límites del despliegue
- Requerir la explicación pormenorizada de los dispositivos, qué identificaciones tienen en el dispositivo, qué son cada uno de estos y cuáles provienen del distribuidor o fabricante, clases de dispositivos, los usos factibles y aplicaciones de los dispositivos, etc.

- Por último, puntualizar los medios y capitales implicados, dispuestos de mantener cualquier clase de evidencia importante. Con esto no solo nos referimos a los dispositivos informáticos, sino además a la documentación que podría mantener información afín a la causa.

Cuando ya se encuentren identificados los distintos dispositivos se pasa a la segunda fase, que es la fase de recopilación. Esta parte del proceso supone la documentación y obtención de la clase de información que se precisa y del entorno del cual se deba adquirir la evidencia.
Acá hay que ser prudentes, ya que muchas veces hay una sola posibilidad de capturar dicha información, por lo que este despliegue se tiene que efectuar en la manera más eficiente posible y con las garantías más elevadas de que se va a adquirir el resultado que se precisa. La recopilación de información simplemente deberá cumplir con dos postulados: ser sistemático y respetar el orden de prioridad en función a la volatilidad de la información.

Es importante tomar a consideración una serie de pautas:

- Seguir indicaciones de buenas prácticas que sean reconocidas
- Tener un registro cronológico del despliegue de recopilación de la información
- Y emplear listas para ir chequeando, a razón de no pasar por alto ninguno de los pasos fundamentales o elementos que pueden tener información importante.

Cuando se esté realizando la recopilación se tiene que ser sumamente cuidadoso y verificar continuamente que se esté obrando dentro de los requisitos y condiciones de legalidad que necesitan este tipo de situaciones. Si bien puede no tenerse en mente la toma de acciones penales, es preciso tomar las medidas que se requieran para no vulnerar la situación de privacidad que se debe mantener y tener las autorizaciones propicias del dueño de los equipos, así como de los responsables de la empresa o de los sistemas en cuestión.

La correcta ejecución de la fase de preservación va a resultar de vital importancia para el despliegue de la investigación forense.

De todas las etapas que compone el análisis, las tareas empleadas en esta son las más reconocidas, inclusive por personas con poco o nulo conocimiento de la investigación de esta índole, pero principalmente por los individuos que comienzan a desarrollarse en el ámbito forense.

Las labores de preservación tienen como fin contar con una copia íntegra e idéntica de la información contenida en los dispositivos sometidos a análisis. Asimismo, esta fase mantiene implícitas acciones que involucran el manejo de las evidencias adquiridas, debido a que la identificación de estas implica la utilización de herramientas y metodologías de búsqueda, composición, localización y procesos que de alguna manera podrían contaminar o alterar su respectivo contenido. Debido a esto, antes de iniciar las labores de recopilación, el investigador deberá crear, como mínimo, dos copias de la información contenida en los dispositivos, con los que trabajará posteriormente.

La copia original se debe preservar en custodia, la primera copia se emplea para proceder con las fases de análisis y, en la circunstancia de deber reproducir una prueba ya realizada, como la primera copia ya ha sido modificada, se tendrá que volver a obtener una nueva copia a partir de la segunda copia que se realizó.

Acá es necesario aclarar que si bien en esta instancia el ámbito de actuación no tiene en cuenta las acciones judiciales, en la cual el protocolo es un requisito fundamental, una mala praxis o una acción descuidada de las acciones de preservación no será tenida en cuenta como una práctica profesional.

Dentro de los requisitos de una correcta investigación nos encontramos con que las acciones deben ser repetibles, por lo que siempre se debe disponer de la posibilidad de reproducir la situación de partida de manera íntegra. Asimismo, es importante aclarar que es sumamente relevante la utilización de las medidas de seguridad que se requieran en cada caso para evitar el borrado, la modificación o el sobre grabado cuando se esté realizando una copia.

De igual modo, las copias efectuadas deben poder identificarse de forma unívoca, a razón de que se pueda comprobar su exactitud y su falta de manipulación. Para este tipo de tareas, es muy común que se empleen programas que utilizan las funciones "Hash", con fin de que se pueda verificar de manera sencilla la integridad de las copias de la información de análisis.

Después de la fase de preservación se pasa a la fase de análisis. En esta fase, las tareas de análisis de los datos se van a desplegar sobre la información duplicada, nunca será sobre los originales.

Las características que deberá mantener un buen analista son:

- El analista debe ser metódico y sistemático, ya que sus actividades se van a fundamentar en el método científico, por lo que se plantearán de manera idónea diversas hipótesis y se buscará información para validarlas.
- También debe trabajar de manera repetible, ya que, como dijimos anteriormente, se deben poder replicar los pasos para así permitir arribar a la obtención de las conclusiones respecto a lo que se desea determinar. Siguiendo la misma sucesión de pasos se debe poder arribar a iguales condiciones.
- Por último, un buen analista debe tomar decisiones basadas en el raciocinio. La totalidad de las decisiones y las acciones tomadas deberán estar fundamentadas en buenas practicas, de manera de que pueda ser mostrado ante otros especialistas, asegurando el proceder correcto del proceso de análisis desplegado. En relación a los antecedentes conocidos, los medios disponibles, el objetivo que se persigue y las evidencias que se han podido obtener, cada análisis va a ser único y particular.

Asimismo, se han establecido procedimientos de forma genérica para desplegar las búsquedas de evidencias específicas y las técnicas de análisis de la investigación que se estén realizando. Estos procedimientos metodológicos van a tornar más sencillas las pautas para efectuar los análisis.

A partir del uso de metodologías de análisis basadas en técnicas y procedimientos, se arriba a la extracción de los datos que mantiene la información que, al mismo tiempo, tras ser contextualizada y analizada, brinda respuestas a las situaciones que plantean las investigaciones.

Sin embargo, esto no siempre se trata una tarea fácil de realizar, y a veces, la información se encuentra en varios datos dispersos, o también se puede dar que una parte de los datos que forman esta información se hayan borrado o el disco en sí mismo se haya dañado o formateado, por lo que se hace imprescindible la aplicación de herramientas específicas y técnicas para recuperar dicha información.

En relación al estado en que se encuentre la información, se aconseja contar con servicios especializados de especialistas en esta clase de actividades que ayuden tanto a obtener la información como a preservarla debidamente.

Otra de las cuestiones a realizar durante el análisis es la adquisición de la información no observable de los ficheros, como son los metadatos, cuyo provecho ha sido demostrado de forma empírica en varias situaciones en las que se ha logrado conocer cuál fue ciclo de vida de la información, la autoría de la creación, horas, fechas, accesos, alteraciones, entre muchos otros datos.

Luego de desarrollar todas las fases descriptas, se llega a la fase de presentación, que es la fase en la cual el investigador va a arribar una conclusión puntal. Dicha conclusión deberá quedar plasmada en un informe de manera precisa, clara, y entendible para cualquiera que no sea idóneo en la temática, independientemente de que esta pericia mantenga carácter extrajudicial o judicial.

Este informe debe ser siempre riguroso, profesional, respetuoso, argumentativo y previsor. Quedará bajo la responsabilidad del analista forense mantener una copia de todo lo que se pueda precisar, empleando los medios que garanticen la confidencialidad e integridad de la información, para que, dado que sea necesario, pueda retomar las actuaciones y realizar exposiciones o dar las explicaciones que se soliciten.

Investigación en *Really Simple Syndication*

Entendemos que la web llamada "social", o también Web 2.0 surge como una generación secundaria de web fundada en sociedades de usuarios. Se habla de una evolución, ya que se pasa de una web limitada de carácter informativa y utilizada por especialistas, a una web comunitaria, donde para cualquiera es sencillo participar. Surgen así aplicaciones web muy poderosas y fáciles de usar, focalizadas en el destinatario.

Según la Universidad de Murcia, "RSS" son las siglas de *Really Simple Syndication*, un formato que cumple con el estándar *Extensible Markup Language*, es decir, XML, para compartir contenido en la web. El formato RSS se utiliza para difundir información actualizada a usuarios que se han suscrito a una fuente de contenidos.

Para visualizar los contenidos RSS se puede utilizar el navegador de internet. No obstante, este formato permite distribuir contenidos sin necesidad de un navegador, utilizando un *software* diseñado para leer dichos contenidos. Las últimas versiones de los principales navegadores permiten leer los RSS sin necesidad de programas adicionales. Esto se conoce como redifusión web o sindicación web, una traducción incorrecta, pero de uso común.

Asimismo, la Universidad de Murcia expresa que habitualmente el término RSS es usado erróneamente para referirse a fuente web, independientemente de que el formato de dicha fuente sea RSS o no. Fuente web se refiere al medio de redifusión web, mientras que RSS se refiere al formato de dicha fuente web.

Originalmente el único formato de fuente web era RSS, así que se usaban de manera indistinta ambos términos. Sin embargo, el formato Atom es, actualmente, otro formato popular de fuente web. Una cuestión a tener en cuenta es que no toda fuente web tiene formato RSS, ya que algunas tienen formato Atom. En ocasiones, las páginas web ofrecen una fuente web en formato Atom y erróneamente la señalan como RSS.

Para poder recibir noticias RSS es necesario contar con un blog o sitio en internet que mantenga el servicio RSS. Este es un contexto que se da habitualmente, puntualmente en los blogs, ya que, por defecto, suelen mantenerlo habilitado. El servicio RSS se logra

visualizar de manera sencilla a partir de un logotipo, generalmente de color naranja, que tiene el texto “RSS”, o en su defecto, tres arcos.

Asimismo, otro requisito para poder recibir dichas noticias es tener un programa que sea lector de RSS. El mismo puede encontrarse instalado en la computadora, puede estar en la web y hasta puede utilizarse desde la casilla de correo electrónico.

A partir de la instalación del programa RSS o por medio la utilización *online*, se tendrán que configurar la páginas de las que se quiere obtener actualizaciones. Este es un procedimiento muy fácil de realizar. Cuando se dan de alta estas páginas se admiten, de forma directa, los artículos nuevos y las noticias de esas páginas web consideradas de interés. Estos se incluyen en los canales deseados, también llamados feeds, con la virtud de tener todas estas páginas web compiladas en un único espacio.

El alimentador RSS va a favorecer la gestión, así como facilitar la publicación de noticias e información varia en distintos blogs o sitios. Debemos entender que el RSS es una manera estandarizada de reparto de la información que se encuentra online a los lectores de las páginas web, y que dicha información se va a distribuir a partir de los canales o fuentes RSS.

Gracias a este sistema, los lectores mantienen una herramienta de utilidad para estar informado respecto a las webs y noticias que son de interés, almacenando y conservando toda la información que se requiere en un solo espacio que, además, se actualiza de automáticamente.

A su vez, el RSS le brinda al lector un ahorro de tiempo muy considerable respecto a la lectura de noticias e información. Basta con abrir el lector RSS para que el usuario visualice rápidamente cuáles son las actualizaciones más recientes y qué noticias han publicado las distintas páginas en las que se encuentra suscripto. Además, a partir de lo expuesto es necesario aclarar que los investigadores pueden beneficiarse significativamente del RSS, ya que con esta herramienta pueden ahorrar mucho tiempo de trabajo.

Algunas ventajas de usar RSS para acceder a contenidos, las cuales fueron descriptas por el especialista en informática madrileño Iván Lasso.

- La primera ventaja es que seleccionamos nuestras propias fuentes de contenidos. No hay selección previa hecha por terceros, sino que nosotros elegimos, sin importar que tan minoritaria o popular sea la fuente. Esto nos da mayor poder de criterio personal en la selección de información.
- A su vez, ahorramos tiempo al poder visualizar el contenido publicado por todas esas fuentes desde un solo lugar
- Por último, visualizamos los contenidos de una manera uniforme.

El filósofo italiano Marco Aurelio expresaba que "Nada tiene tanto poder para ampliar la mente como la capacidad de investigar de forma sistemática y real todo lo que es susceptible de observación en la vida".