Seguridad de la Información y Ciberseguridad en Laboratorios de Informática Forense. Necesidades de las fiscalías

Cistoldi, Pablo
pcistoldi@ufasta.edu.ar
Facultad de Ingeniería, UFASTA
Parra de Gallo, H. Beatriz
bgallo@ucasal.edu.ar
Facultad de Ingeniería, UCASAL
Luz Clara, Bibiana
bluzclara@ucasal.edu.ar
Facultad de Ingeniería, UCASAL
Aráoz Fleming, José
jafleming@ucasal.edu.ar
Facultad de Ingeniería, UCASAL
Dorado, Jhon G.
jdorado@ucasal.edu.ar
Facultad de Ingeniería, UCASAL
Greco, Fernando
fmartingreco@ufasta.edu.ar
Facultad de Ingeniería, UFASTA
Ambrústolo, Mariela
ambrus@fi.mdp.edu.ar
Facultad de Ingeniería, UNMdP

Abstract*. El presente trabajo tiene por objetivo analizar los requerimientos de las fiscalías en cuanto al tratamiento de la evidencia digital. A partir de la formulación de la problemática expresada por los fiscales, en cuanto a las condiciones legales y procesales que se deben respetar cuando se trata de la evidencia digital, se analiza el modo en que un Laboratorio de Informática Forense debería responder a las mismas. El trabajo tiene como resultado un análisis de la situación, que puede servir de base para la implementación de acciones técnicas y procedimentales en un Laboratorio de Informática Forense, bajo criterios de eficiencia y calidad esperados.*

Palabras Clave Laboratorio de Informática Forense, Ciberseguridad**,** Seguridad de la Información.

.

Introducción

Desde la perspectiva de las fiscalías, los desafíos y necesidades suelen percibirse durante la intervención en cada caso concreto. Este enfoque, predominantemente casuístico, es utilizado también al demandar los servicios de un Laboratorio de Informática Forense. Ello hace necesario realizar un análisis multidimensional, que permita identificar y sistematizar un conjunto de factores de interés para el abordaje de una solución tecnológica a las demandas de las fiscalías.

Así, se plantea como objetivo del presente trabajo el análisis profundo de los factores señalados, tanto desde la demanda de las fiscalías como desde la normativa procesal forense y la intervención tecnológica requerida.

Según Kaspersky [1] la ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos

de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes.), es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras. Así, en el presente trabajo, se toma el término de ciberseguridad para referenciar cualquiera de los componentes de un sistema de información (hardware, software, estructura de datos, conectividad y comunicación con el usuario) y sus características técnicas propias, asociándolo a los conceptos de seguridad de la información y de seguridad informática.

Para resguardar la seguridad de la información se hace necesario tomar un conjunto de medidas preventivas para mantener la confidencialidad, integridad y disponibilidad de los datos de que se trate y queremos preservar.

La información puede encontrarse en distintos formatos, y todos por igual requieren privacidad y cuidado, pues puede ser utilizada por terceros inescrupulosos que la acceden sin derecho, la divulguen o utilicen para fines no queridos, o bien pueden alterarla o hacerla desaparecer. Estos efectos perniciosos también pueden ser causados involuntariamente por quienes tienen algún tipo de contacto con los diversos contenedores de información. Si se trata de pruebas, esto adquiere una trascendencia aún mayor, pues son los elementos de los que las partes pueden valerse para llevar un caso a buen puerto.

La eliminación de estos riesgos será el objetivo de la seguridad de la información.

La seguridad informática es uno de los aspectos de la seguridad de la información, aunque no el único. Se debe procurar la confidencialidad, integridad y disponibilidad de la información. La seguridad de la información puede planificarse, y también es posible llevar un registro de los eventos o incidentes de vulnerabilidad, para mejorar continuamente su preservación, evitar problemas legales y conflictos derivados de la falta de cuidado, y garantizar el cumplimiento de los imperativos establecidos en la ley de protección de datos personales.

La norma ISO 27001 fija las pautas para la mejor manera de resguardar la seguridad de la información. Esta norma proporciona requisitos para gestionar un sistema de seguridad de la información. El mismo pretende preservar la confidencialidad, integridad y accesibilidad de la información a través de un proceso sistemático de gestión de riesgos con el objetivo de brindar confianza a las partes interesadas involucradas.

En un proceso judicial, la seguridad de la información probatoria presenta desafíos particulares. En especial, la evidencia digital debe ser preservada mediante una adecuada cadena de custodia y/u otros procedimientos idóneos, ya que es volátil y debe ser protegida para evitar su contaminación, destrucción, modificación, inaccesibilidad o uso indebido. Además, es replicable, lo cual, entre otras cosas, dificulta el control de un uso indebido. Por ello, debe llevarse un registro que indique qué personas tienen acceso a la misma, para evitar su manipulación y deslindar responsabilidades.

En estos casos, contar con un protocolo de actuación segura es de gran ayuda para la tarea. Un protocolo establece una base metodológica para el desarrollo de acciones determinadas y específicas, desde la recolección y la preservación, hasta el

análisis que se vuelque en el informe y/o presentación final. Su cumplimiento ofrecerá una garantía de que las evidencias serán adecuadamente tratadas, manteniendo su aptitud probatoria y respetando las exigencias legales. En la práctica, un protocolo es una guía a seguir para el mejor desarrollo de los procedimientos y reglas básicas que se deben atender y cumplir sobre obtención, identificación, embalaje, traslado, recepción, almacenamiento y procesamiento de las evidencias digitales, conformando un documento único con requisitos mínimos que deben ser respetados por quienes deseen llevar adelante las tareas periciales. Los protocolos brindan un marco jurídico adecuado a dichas prácticas, conformando un cuerpo de indicaciones dedicadamente elaboradas e institucionalizadas, que deben ser seguidas para la obtención de resultados satisfactorios. La implementación de una normativa de gestión adiciona a este protocolo una perspectiva de mejora continua que posibilita que el diseño de este instrumento se implemente, mantenga y mejore, alineándolo a la decisión estratégica de cada organización

Este artículo está conformado de la siguiente manera: la Sección 1 contiene el Análisis de los Factores que marcan la demanda de las fiscalías, la Sección 2 describe las cuestiones legales y procesales en las que se deben enmarcar estos factores, mientras que la Sección 3 describe la respuesta técnico-informática que podría tomarse como base para responder a la demanda señalada; y la Sección 4 hace el abordaje del tema desde la gestión de la calidad en los Laboratorios de Informática Forense. Por último, la Sección 5 describe las conclusiones del trabajo.

1 – Análisis de los Factores que marcan la Demandas Tecnológicas de las Fiscalías

Los riesgos y exigencias en esta materia varían de acuerdo con la fase de actuación informático-forense en que se presenten. Por ejemplo, los riesgos de pérdida de información que aparecen en la fase de identificación no son los mismos que los propios de la fase de análisis.

Asimismo, deben contemplarse los riesgos que se presentan entre fase y fase, y los que pueden surgir una vez terminada la actuación propiamente pericial. Incluso puede ser conveniente adoptar medidas, dentro del ámbito de atribuciones propias del laboratorio, frente a la actuación de terceros (abogados o peritos de parte, por ejemplo).

Las fiscalías, y el sistema de justicia en general, necesitan que los laboratorios informático-forenses tengan un desempeño confiable. El grado de compromiso y la eficiencia con los cuales los laboratorios preservan la seguridad de la información y la seguridad informática impactan en la confiabilidad de sus servicios. Ello implica la necesidad de contar con instalaciones, equipamiento, herramientas, competencias y conductas adecuadas para prevenir riesgos de esta índole, por ejemplo: Sistemas de vigilancia frente a nuevas formas de amenaza, y matrices de riesgo actualizables; Sistemas de respuesta frente a eventos adversos, entre otros.

¿Cuáles son los datos digitales que, si se pierden, se corrompen o no son accesibles en tiempo oportuno comprometen la suerte del caso? La respuesta a esta pregunta depende de un conjunto de factores entre los que se destacan:

1. Requisitos de Usabilidad
2. Prevención de Acceso y Uso Indebido
3. Datos ilícitos y no pertinentes
4. Contenido y Contexto
5. Datos y Contenedores
6. Prioridades y prácticas alineadas

7. Procedimientos adecuados a cada fase de actuación forense

A continuación, se detalla cada uno de ellos

1.1 - Requisitos de usabilidad para los datos con valor investigativo y/o probatorio

Se considera que los datos con valor investigativo y/o probatorio deben ser:

- **Lícitos**. Su obtención, conservación y análisis no deben haber sido contrarios a la ley. Este es un aspecto "formal", vinculado con derechos y garantías constitucionales (art. 18 de la Constitución Nacional y concordantes de las Constituciones Provinciales, derechos sobre los datos personales, etc.).
- **Pertinentes al caso**. Es decir, deben vincularse con los hechos investigados y/o controvertidos. Según las circunstancias, la conservación o análisis de datos no pertinentes puede llegar a ser una conducta ilícita, con consecuencias legales (ya analizaremos brevemente esta cuestión).
  - En fases de investigación preliminar (predominantemente unilateral), la pertinencia puede ser provisoria, potencial, especialmente cuando todavía no se ha formulado una hipótesis mínimamente sólida sobre los hechos. En tales casos, esa pertinencia puede llegar a confirmarse o descartarse en momentos posteriores.
  - En fases de litigio, los hechos controvertidos ya están delimitados. Los datos con valor probatorio sólo pueden estar referidos a esos hechos, sea en modo directo o en modo indirecto (cadenas de indicios).
  - La pertinencia tiene grados, y está ligada al abordaje del caso que adopta cada parte (ej.: pedidos de medidas cautelares, anticipos probatorios, juicio oral, entre otros).

En este punto es importante considerar el resguardo tecnológico más adecuado de la evidencia, ya que la guarda de los dispositivos en el Depósito Judicial puede no garantizar la inalterabilidad de los mismos, mientras que si se resguarda en el Laboratorio de manera unívoca en un servidor (por ejemplo), puede tener mayor probabilidad de mantener la integridad de la evidencia, atendiendo además a las condiciones climatológicas, de espacio y otros que se presentan en los ámbitos utilizados para el resguardo de las pruebas y evidencias.

- **Relevantes**. En otras palabras, deben conducir a dilucidar y/o probar cuestiones concretas y determinadas.
  - El ámbito de pertinencia es un conjunto de cuestiones (a averiguar y/o probar). La relevancia y la conducencia son específicas para una o más cuestiones. Cada elemento investigativo o probatorio, debe ser fundamental o, al menos, importante, para la averiguación o prueba de esas cuestiones concretas.
  - La relevancia admite graduaciones. En comparación con otros elementos investigativos o probatorios con los cuales se cuenta, y eventualmente en función de su grado de integración con ellos. En un extremo, el aporte poco añade a otros elementos de prueba (datos superfluos). En el otro, no existen otras pruebas o elementos sobre ese punto o cuestión (datos cruciales).
  - La relevancia de un elemento probatorio se valora en su contexto de uso (ej.: al pedir medidas cautelares, al discutir posibles fórmulas conciliatorias, en la etapa de producción de prueba...).

- La relevancia de los datos se complementa en mayor o menor medida con la relevancia de la interpretación pericial y con la relevancia de la valoración judicial.

● **Confiables**. De nada sirve contar con elementos probatorios lícitos, pertinentes y relevantes si no son confiables, es decir, si no son convincentes.

- La confiabilidad de los datos también presenta graduaciones: en relación al contexto de uso. Confiabilidad comparativa entre los elementos probatorios con los cuales se cuenta. Este punto debe ser analizado conjuntamente con la relevancia de cada elemento. Confiabilidad comparativa con los elementos probatorios de la parte contraria. Adecuación a los estándares legales de prueba, que rigen para cada tipo de proceso judicial (ej.: penal, civil, laboral, etc.) y en cada etapa de esos procesos (ej.: medidas cautelares, conciliación, sentencia definitiva)
- Para poder ser defendida adecuadamente en un litigio, la confiabilidad debe abarcar, al menos, estos aspectos: infraestructura, herramientas, procedimientos, capacidades y conducta de los expertos.
- Además, debe distinguirse entre la confiabilidad de los datos en sí mismos, (por ejemplo: su origen e integridad), la confiabilidad de la interpretación pericial de esos datos y la confiabilidad de la valoración probatoria por parte de jueces y abogados.
- También debe considerarse la confiabilidad desde el punto de vista de la subjetividad de cada partícipe en el acto judicial, en cuanto al grado de confianza que le ofrece la infraestructura judicial puesta a disposición de la evidencia, y que cada uno percibe desde su propio enfoque y según el rol que cumple.

● **Fácilmente accesibles y utilizables**. Este requisito tiene varios aspectos, que dependen del contexto de uso:

- Disponibilidad en tiempo oportuno (por ejemplo, para el cumplimiento de los plazos procesales, para solicitar medidas urgentes o medidas cautelares, etc.)
- Costos razonables
- Facilidad para extraer información de valor (sea a través de la labor pericial, sea en forma directa por jueces y abogados)

1.2 - Prevención de acceso y uso indebido

Es imprescindible adoptar los recaudos necesarios para evitar o minimizar el uso indebido de los datos, sea por integrantes de la organización o dependencia, o por terceros.

Este requisito se aplica tanto a los datos con valor investigativo y/o probatorio, como a los datos de origen ilícito y los datos no pertinentes al caso. El acceso o el uso indebido pueden afectar el curso de un proceso judicial o las probabilidades de éxito de un caso, pero también puede lesionar o amenazar derechos desvinculados del caso (sea de alguna de las partes o de un tercero ajeno). Y en ciertas circunstancias, también puede generar consecuencias para las personas y entidades responsables de la custodia de datos y/o involucradas en su uso indebido. Entre estas posibles consecuencias podemos encontrar las sanciones penales (en particular, cabe destacar las que prevé el Código Penal en

los arts. 153 bis y 157 bis[1]), responsabilidad pecuniaria por daños y perjuicios, y la pérdida de confiabilidad.

Este aspecto es de suma importancia, y los procedimientos y procesos técnicos fijados en el Laboratorio, deben abundar en todos los aspectos posibles para garantizar la confidencialidad de la información. Estas características deben ser una nota distintiva del Laboratorio de Informática Forense.

En algunos casos, el resguardo de la privacidad puede tornar conveniente acudir a medidas de disociación y anonimización de ciertos datos (por ejemplo, de terceros menores de edad), especialmente al elaborar dictámenes periciales o efectuar presentaciones en juicio.

En el marco de las actividades investigativas y de las medidas cautelares, mantener la reserva de los datos suele ser esencial para garantizar el éxito de esas medidas. Esta reserva es temporal.

Por otro lado, dado el carácter eminentemente técnico del acceso a datos digitales, no se debería permitir que personal no especializado utilice los dispositivos originales ni a los equipos y herramientas del laboratorio. El riesgo de manipulación inexperta de la evidencia es común con otras áreas periciales. Debe tenerse presente que, cuando un caso finaliza, los datos digitales dejan de ser pertinentes (salvo que algunos de esos datos abastezcan bases de datos de un modo permitido por la ley).

El Laboratorio de Informática Forense es responsable de mantener el ciclo de vida de la información desde que llega el dispositivo a peritar hasta que se borra la última imagen forense una vez cumplido el plazo de resguardo en el Laboratorio. Se debe garantizar el acceso a la información cada vez que sea requerido. Por ello es importante mantener un resguardo redundante de las imágenes forenses, considerando la estructura de los contenedores de la probable evidencia digital atendiendo además a las particularidades de cada caso. Aquí la gestión del espacio de almacenamiento y el óptimo estado de la infraestructura del Laboratorio es de vital importancia.

1.3 - Datos ilícitos y datos no pertinentes: ¿qué hacer?

La protección de los datos personales es un deber ineludible[2]. Cuando en un caso se incorporan datos ilícitos o no pertinentes, aquí no existen requisitos de usabilidad, ya que esos datos no deben ser utilizados. Deben considerarse ajenos a la organización o dependencia, y es ineludible

---

[1] *ARTÍCULO 153 BIS. - Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.*

ARTÍCULO 157 bis. -Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

[2] La citada Ley 25326, en su primer artículo, al definir su objeto, se refiere al deber de protección de los datos personales de la siguiente manera: *"La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional." [...]*

adoptar las medidas necesarias para restituirlos o eliminarlos, según corresponda.
Esto presenta dificultades, ya que en un mismo contenedor o dispositivo suelen coexistir datos pertinentes y datos no pertinentes. Y esa es solamente una parte de la complejidad del problema, ya que muchos de los datos digitales contenidos en un dispositivo están referidos a personas ajenas al proceso judicial.
También debe tenerse presente que, cuando un caso finaliza con un pronunciamiento firme, los datos digitales dejan de ser pertinentes (salvo que algunos de esos datos abastezcan bases de datos de un modo permitido por la ley[3]).

1.4 - Contenido y contexto

La preservación de la información con valor investigativo y probatorio puede gestionarse de formas y con contenedores variados. Para ello, es necesario distinguir entre dos posibles funciones de los datos: función documental y no documental. Si bien esta diferencia no siempre es clara ni posible, la distinción conceptual ayuda a escoger las mejores medidas de aseguramiento de la información, una vez recolectados los dispositivos y/o los datos.
Los datos de contenido poseen un valor que los asimila a la prueba documental. Están destinados a exteriorizarse hacia las personas como representaciones de una determinada realidad (texto, imágenes, audio, video). En cuanto a esta característica, no interesa si han sido producidos por la voluntad humana (ej.: filmación casera) o por un dispositivo (ej.: filmación de cámara de monitoreo). Respecto de su integridad, la identidad bit a bit puede ser importante, pero también lo es la no alteración de su aptitud representativa. Incluso, pueden adoptarse procedimientos de mejora de dicha aptitud (ej.: procesamiento de imágenes, representaciones 360), o requerir procedimientos de conversión de formatos debidamente documentados. De ahí que, a la hora de garantizar la seguridad de la información que proveen estos datos, haya que priorizar su capacidad representativa, mediante el empleo correcto y documentado de herramientas y métodos fiables en cada eventual mejora, combinación o cambio de formato. Un caso especial lo constituyen los documentos que contienen las formalidades legalmente exigidas para realizar o probar determinados actos jurídicos.
Algunos datos de contexto pueden servir como apoyo probatorio de datos documentales (ej.: los metadatos de fecha y hora agregados en la imagen de una foto o en un video; el valor hash del archivo de un contrato, etc.). Pero ello no siempre ocurre. Muchos de estos datos se producen en el marco del funcionamiento de sistemas informáticos, y obedecen a la lógica de esos sistemas. Esto no impide su búsqueda y utilización como información de valor investigativo o probatorio en sí mismo.

---

[3] Cabe destacar que el art. 16 inc. 5) de la ley citada establece de modo específico que: "*La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos".*
A continuación, en el art. 17 incs. 1 y 2, la Ley prevé excepciones al deber de eliminación de los datos de la siguiente forma: "*ARTÍCULO 17. — (Excepciones). 1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros. 2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado." [...]*

Datos en memoria volátil, logs, algunos tipos de metadatos, aplicaciones informáticas, etc., pueden contener valiosos indicios. Desde esta perspectiva, los datos mencionados presentan semejanza con otros tipos de rastros y evidencias materiales.

Existen pautas comunes para los procedimientos de preservación y custodia de la información contenida en sistemas informáticos. Pero, de acuerdo con la función o finalidad (documental o no documental) que se asigne en cada caso concreto a un conjunto de datos, puede ser necesario añadir medidas específicas.

1-5 Datos y contenedores

La acumulación de dispositivos contenedores de datos puede generar problemas de seguridad (por ejemplo, debido a falta de instalaciones adecuadas), y afectar la disponibilidad oportuna de los datos.

El manejo de efectos propios de otras disciplinas periciales nos muestra que no siempre es posible preservar los contenedores de información. Un automóvil siniestrado en un determinado lugar, o el grado de alcohol en sangre que presenta el sospechoso, son contenedores de información con valor probatorio. No será posible presentar en juicio ese automóvil o esa sangre, pero sí se podrá extraer la información de un modo fiable, e incorporarla bajo otro formato (ej.: fotografías, filmaciones, tickets de alcohotest, actas, operaciones y dictámenes periciales, testimonios de funcionarios y peritos). Para ello, se requieren procedimientos seguros. Estas y otras analogías podrían ser útiles para el manejo de datos en formato digital, siempre de acuerdo con un balance riesgo-beneficio.

A su vez, la circunstancia de que una misma información puede ser registrada en múltiples formatos, exige extender las medidas de seguridad. Por ejemplo, las copias forenses, los borradores de dictámenes y el conocimiento adquirido por peritos y técnicos (registrado en sus recuerdos personales) deben ser objeto de recaudos específicos para evitar filtraciones y usos indebidos.

1.6 - Prioridades y prácticas alineadas

La ponderación del valor investigativo o probatorio de los datos digitales en cada caso concreto debe integrarse con la priorización de casos y actividades vistas desde el conjunto de casos.

Los distintos tipos de fenómenos criminales tienen un impacto social o personal diferente, según sea el tipo de derecho afectado, la intensidad de la afectación, el impacto social causado o el riesgo de reiteración.

El mayor nivel de vigilancia y aseguramiento de la información debe darse respecto de los datos críticos en los casos críticos. Las matrices de riesgos deberían elaborarse bajo estas pautas, siguiendo el principio de Pareto.

De este modo, las políticas de seguridad de la información y de ciberseguridad estarán alineadas, por un lado, con las exigencias de gestión del caso y, por el otro, con las orientaciones de priorización de casos establecidas en el Ministerio Público.

La comunicación y coordinación adecuadas con las fiscalías son, en sí mismas, una herramienta imprescindible, máxime cuando muchas fuentes de riesgo pueden abrirse o neutralizarse fuera del laboratorio. Igualmente, los obstáculos que pudieran existir en la comunicación y la coordinación no son impedimento para la elaboración y cumplimiento de políticas, ya que éstas permitirán delimitar más claramente las responsabilidades y brindarán seguridad a los peritos e integrantes del laboratorio.

1.7 - Procedimientos adecuados a cada fase de actuación forense

Desde otro ángulo, los riesgos y exigencias en esta materia varían de acuerdo con la fase de actuación informático-forense en que se presenten. Por ejemplo, los riesgos de pérdida de información que aparecen en la fase de identificación no son los mismos que los propios de la fase de análisis.

Asimismo, deben contemplarse los riesgos que se presentan entre fase y fase, y los que pueden surgir una vez terminada la actuación propiamente pericial. Incluso puede ser conveniente adoptar medidas, dentro del ámbito de atribuciones propias del laboratorio, frente a la actuación de terceros (abogados o peritos de parte, por ejemplo). Una exigencia del debido proceso judicial es que cada parte pueda tener acceso a la información probatoria que poseen las otras partes. Existen excepciones a esta regla, pero son, precisamente, excepciones, y la duración del secreto o reserva es, aún en estos casos, limitada en el tiempo. Frente al riesgo de que las otras partes hagan uso indebido de la información a la cual acceden, la capacidad de acción de los laboratorios es limitada. Ello no obsta a la posibilidad de desplegar procedimientos y estrategias que contribuyan, en alguna medida, a minimizar dichos riesgos, reducir su impacto o remediar sus consecuencias

2 – Marco legal y procesal que impacta sobre los factores señalados

Los datos que se analizan deben haber sido obtenidos de modo legal, es decir cumpliendo los requisitos necesarios para que la prueba pueda ser considerada. En la sección 1.1 se ha detallado acerca de los criterios de licitud, pertinencia al caso, relevancia, confiabilidad y facilidad para la accesibilidad y utilización de los datos, que deben cumplirse con todo rigor.

2.1. Datos pertinentes y no pertinentes:

La protección de los datos personales es un deber ineludible. Cuando en un caso se incorporan datos ilícitos o no pertinentes, aquí no existen requisitos de usabilidad, ya que esos datos no deben ser utilizados. Deben considerarse ajenos a la organización o dependencia, y es ineludible adoptar las medidas necesarias para restituirlos o eliminarlos, según corresponda.

Esto presenta dificultades, ya que en un mismo contenedor o dispositivo suelen coexistir datos pertinentes y datos no pertinentes. Y esa es solamente una parte de la complejidad del problema, ya que muchos de los datos digitales contenidos en un dispositivo están referidos a personas ajenas al proceso judicial.

2.2 Reformas Procesales necesarias para la obtención de la evidencia digital en tiempo y forma

En este punto es sumamente importante destacar que, para la obtención de los datos en legal tiempo y forma nuestras vetustas legislaciones procesales deben adecuarse a los tiempos. En el mes de julio del año 2023, la Cámara de Senadores de la Provincia de Salta dio sanción definitiva[4] a una novedosa e inédita legislación en Argentina y a nivel global, un proyecto de modificación del código procesal penal de Salta que tuvo sus inicios en el mes de marzo del año 2021, cuando desde la Procuración Provincial se creó la Comisión de Reforma del Código Procesal Penal de Salta[5] ; "… para el análisis **del tratamiento de la evidencia digital** en la actualidad y

[4] Expediente Nº 91-47608/23, con origen en la Cámara de Diputados de la Provincia de Salta

[5] Resolución Nº 001179 del Procurador General de la Provincia, de fecha 17 de marzo de 2021, publicada en Edición Nº 20.952, de fecha 23 de marzo de 2021, del Boletín Oficial de Salta

proyección de una futura reforma…", que entre otros, contó con la participación de destacados expertos en temas vinculados a la interacción entre el derecho y la tecnología. Dicho proyecto ya contaba con media sanción de la Cámara de diputados de la Provincia de Salta desde el mes de mayo del año 2023.

Al abordar figuras tales como la del agente encubierto digital, la posibilidad de obtención remota de datos, la intervención de todo tipo de comunicaciones; la postura de los abogados litigantes siempre fue la del respeto irrestricto de las garantías constitucionales, de garantías individuales tales como la privacidad, la intimidad, etc.; entendiendo, obviamente, que las herramientas que la reforma proponía eran fundamentales a los fines de encarar los nuevos tiempos de la delincuencia, de la delincuencia organizada.

El avance tecnológico aplicado al delito requiere soluciones análogas y estas demandan obviamente reformas de nuestros anticuados Códigos Procesales; añejos no por falta de conocimientos o de idoneidad de sus redactores sino simple y sencillamente porque lo que en la actualidad ya es una realidad, en su época, no existía, porque los tiempos cambian, porque los móviles que hoy se usan para delinquir, hace algunos años se veían solo en las películas de ciencia ficción.

La investigación penal no osaba abordar estos temas, la evidencia física lo era todo. Hoy, se puede decir, sin temor a equivocarse, que la evidencia digital lo es todo. No existe delito en donde esta no intervenga. Y no solo cuando se habla de los delitos específicos en los que la tecnología es factor fundamental de su consumación; el grooming por citar un ejemplo, en donde nuestros niños son las víctimas. Ahí está claro el rol relevante de las TICs. En un homicidio, por ejemplo, la evidencia digital, el conocer por donde transitó el celular de la víctima, o del posible imputado, cual fue el camino que siguió ese elemento, permite arribar a altos grados de certeza en las investigaciones, permite descubrir crímenes que hubiesen quedado impunes en otros tiempos. La triangulación de antenas de telefonía móvil, los informes de las compañías telefónicas, la información existente en el propio aparato de la víctima o el autor del delito, otorgan la certeza requerida.

Esta evidencia digital se obtendrá con herramientas como las que se impulsan en el referenciado proyecto de reforma. Con el aseguramiento de los siempre volátiles datos informáticos. Con la orden de presentación pertinente. Con la posibilidad de obtenerlos de parte de las empresas proveedoras de servicios. Con la posibilidad de secuestrarlos, de obtenerlos remotamente, de introducir los agentes encubiertos digitales en el entorno virtual, en la red investigada.

Para evitar la arbitrariedad del poder, justamente el proyecto echa mano a los necesarios equilibrios, al juego de los frenos y contrapesos, poniendo en manos del fiscal la fundamentación de la necesidad de la medida, dotando al juez de la decisión de su otorgamiento, permitiendo a los que tienen que impulsar la investigación llevarla adelante, sabiendo que quienes tienen que controlarla gozan de todo el poder para ello y, finalmente, activando el eslabón de las responsabilidades para los excesos.

Un sistema de justicia que se precie de ser tal debe contar necesariamente con todos estos engranajes, máxime en el caso en análisis, el de la provincia de Salta, en donde el ministerio público no es parte del poder judicial y justamente nos encontramos en un esquema diseñado para hacer factible estos frenos y contrapesos.

Las fiscalías de nuestro país deben contar con herramientas modernas e idóneas que hagan posible su función. Para el reaseguro,

para el control posterior, el poder judicial ya cuenta con las herramientas necesarias, debe utilizarlas. Los abogados deben controlar, activar, estas últimas ante la detección de excesos o de actos reñidos con el fin buscado.

3 – Criterios tecnológicos vinculados a los factores señalados

Considerando los requisitos formulados por las fiscalías y que se pueden tomar como mandatorios para la definición de la infraestructura tecnológica adecuada y pertinente para un Laboratorio de Informática Forense, se describen a continuación aquellos criterios tecnológicos a tener en cuenta.

Por una parte, los **requisitos de usabilidad para los datos con valor investigativo y/o probatorio** acerca de la licitud, pertinencia, relevancia, confiabilidad y disponibilidad se pueden sostener en los propios principios fundamentales de la información: integridad, confidencialidad y disponibilidad. Siendo éstos los principios de base también para un sistema de seguridad de la información, que debe garantizar el cumplimiento de los mismos.

Respecto de la **prevención de acceso y uso indebido** de la información, va de suyo que debe ser la principal característica de control en todas las aplicaciones informáticas para la gestión de la evidencia digital, requiriendo además la definición de plataformas de hardware suficientemente robustas como para evitar el acceso indebido o ataques de ciberseguridad sobre los activos tecnológicos.

Tanto para las exigencias de integridad, confidencialidad y disponibilidad de los datos como para la prevención de acceso y uso indebido, existen una gran variedad de herramientas tecnológicas de protección. como, por ejemplo, un sistema de seguridad perimetral, basado en la propuesta de [2] que se basa en la implementación de servidores virtuales que reemplacen a los equipos físicos, atendido por un software tipo firewall que permita la posibilidad de aumentar o disminuir recursos según sea necesario, y así atender la demanda sobre los mismos.

Otro de los requerimientos de la fiscalía menciona la **protección de datos personales** como deber ineludible de la organización judicial, corriendo por parte de los responsables tecnológicos la definición de los procedimientos y procesos técnicos más adecuados, para ajustar el Laboratorio de Informática Forense a las cuestiones básicas de reserva, privacidad y confidencialidad de la información. Esta tarea, aunque técnica, requiere del asesoramiento de profesionales del derecho expertos en protección de datos, para definir por ejemplo, los contratos de confiabilidad que deben firmar todos los actores judiciales, así como los términos y condiciones de uso de las aplicaciones e instalaciones del Laboratorio de Informática Forense. Al respecto el Reglamento General de Protección de Datos Personales de la Unión Europea (UE 2016/679)[3] define el concepto de datos personales como "*…toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona…"*

Es decir, cualquier información que permita identificar a una persona física se considera datos personales, por ello, muchos de los datos involucrados en las evidencias digitales toman el carácter de "datos

personales", y en ese sentido, es necesario considerar todas las instancias tecnológicas necesarias y suficientes para su protección y uso correcto. En particular, esta normativa aborda las siguientes cuestiones sobre los datos personales: la calidad de los datos, la legitimación de su tratamiento, los derechos de los interesados o propietarios de los datos, la excepciones y limitaciones, la confidencialidad y seguridad del tratamiento de los datos y la existencia de una autoridad de control, incluyendo además un conjunto de directivas expresamente señaladas para los servicios informáticos afectados, los proveedores de servicios de comunicaciones electrónicas, la confidencialidad en el tratamiento, el tráfico de datos y datos de localización. En todos los casos, parte de la necesidad de que las distintas organizaciones responsables de administrar datos personales consideren las técnicas más avanzadas y los costos involucrados para garantizar un nivel de seguridad adecuado al riesgo existente.

En relación a los criterios señalados por la Fiscalía respecto del **Contenido y Contexto**, no habría distinción entre datos de contenido y de contexto, ya que toda la información asociada a una evidencia digital (sea ésta contenido propio o metadatos), revisten la misma importancia en cuanto a que deben ser protegida adecuadamente, sin importar su función.

Los requerimientos de las fiscalías respecto de los **Contenedores de los datos** si resultan una problemática de gran interés para los responsables tecnológicos de un Laboratorio de Informática Forense, coincidiendo con la fiscalía acerca de la necesidad de extremar las medidas de seguridad de acceso cuando se trata de evidencia digital en resguardo durante mucho tiempo. Aquí se plantean dos cuestiones de índole práctica que son muy difíciles de resolver:

- La obsolescencia de los dispositivos electrónicos que contienen esas evidencias digitales
- La exigencia de espacios de almacenamiento cada vez más voluminosos para resguardar las evidencias digitales

Frente a esta problemática, de suma urgencia en el ámbito judicial, se considera de utilidad el trabajo de "Preservación digital a largo plazo: estándares, auditoría, madurez y planificación estratégica" [4] que inicia con un estudio sobre los estándares que se utilizan para la preservación digital, los mecanismos de auditoría necesarios para el cumplimiento de dichos estándares, el nivel de maduración de la organización que marca la distancia entre los requerimientos de las fiscalías y la respuesta que se brinda desde el Laboratorio de Informática Forense, y plantea las directrices para la planificación estratégica de una línea de acción dirigida a dar respuesta a esta problemática.

En referencia a las **prioridades y prácticas alineadas** se coincide con las consideraciones previamente realizadas sobre este punto y se agrega el análisis de los factores que contribuyen a la pérdida de información que, en el caso que nos ocupa, reviste particular importancia. En este sentido se puede considerar el trabajo de [5] en el que se identificaron 5 factores que provocan la pérdida de información: los recursos humanos de la organización, el presupuesto disponible, el conocimiento del personal tecnológico, los desastres naturales y los agentes externos maliciosos. Todos ellos presentan impactos diferentes, y exigen respuestas apropiadas, basadas en el estudio pormenorizado de las características de la organización judicial (cultura de la seguridad vigente, disponibilidad de recursos, compromiso de la dirección en líneas de acción concretas destinadas a la seguridad informática del entorno, entre otras).

Respecto de los **procedimientos adecuados** para el tratamiento forense de la evidencia digital, existe ya un grado de maduración importante respecto de la aplicación de metodologías y herramientas forenses que cumplen con los principios científicos y de buenas prácticas que exige la justicia. Dichos elementos se encuentran incluso apoyados por las normas ISO/IEC de la serie 27k que brindan recomendaciones específicas para las tareas de búsqueda, recolección, adquisición, análisis y preservación de la evidencia digital.

4 - Criterios de calidad aplicables a los Laboratorios de Informática Forense

Las políticas de seguridad de la información y de ciberseguridad de los laboratorios informático-forenses pueden adaptarse y aplicarse a otros ámbitos de trabajo afines, tales como los equipos de investigación en entornos digitales o los equipos de análisis de grandes masas de datos, los técnicos en el uso de herramientas de análisis de smartphones, o el personal idóneo en recolección.

Todos estos aspectos propios de la tecnología deben atender los requerimientos que en tal sentido hacen las fiscalías a los Laboratorios de Informática Forense.

Tomando como base la familia de normas ISO/IEC 27000, se deben considerar especialmente aquellas con impacto directo en las distintas fases del proceso forense que involucra a las evidencias digitales, tales como:

- ISO/IEC 27001:2017 Requisitos del Sistema de Gestión de la Seguridad de la Información
- ISO/IEC 27002:2017 Guía de Buenas Prácticas de Seguridad de la Información
- ISO/IEC 27017:2015 Guía de seguridad para Cloud Computing
- ISO/IEC 27018:2019 Buenas Prácticas en controles de protección de datos para aquellos proveedores de servicios de computación en cloud computing
- ISO/IEC 27032:2012 Ciberseguridad, Estructuras Críticas
- ISO/IEC 27033-5:2013 Protección de las comunicaciones entre redes mediante redes privadas virtuales (VPN)
- ISO/IEC 27037:2013 Directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de Evidencias Digitales Potenciales
- ISO/IEC 27042:2015 Guía con Directrices para el análisis e interpretación de las Evidencias Digitales
- ISO/IEC 27043:2015 Principios y Procesos de Investigación para la recopilación de Evidencias Digitales
- ISO/IEC 27100:2020 Descripción de la ciberseguridad y los conceptos relevantes, incluida la forma en que se relaciona y se diferencia de la seguridad de la información.
- ISO/IEC 27110:2021 Conjunto mínimo de conceptos para definir los marcos de ciberseguridad
- ISO/IEC 27701:2019 Requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Información de Privacidad (PIMS)

Este conjunto de normas y guías puede generar un espacio confiable y de amplia garantía para el manejo de la evidencia digital, además de servir de guía para la definición de los procedimientos técnicos y operativos que deben respetar los distintos actores involucrados en la manipulación de la evidencia digital, brindando un marco conceptual de enfoques y herramientas que permite la gestión a largo plazo permitiendo el abordaje temprano de situaciones nuevas y diferentes desafíos mediante una

estructura sistemática de gestión con enfoque en la prevención de riesgos.

Conclusiones

Saliendo de las exigencias de cada caso concreto, y desde un ángulo más general, las fiscalías (y el sistema de justicia en general) necesitan que los laboratorios informático-forenses tengan un desempeño confiable.

El grado de compromiso y la eficiencia con los cuales los laboratorios preservan la seguridad de la información y la seguridad informática impactan en la confiabilidad de sus servicios. Ello implica la necesidad de contar con

- Instalaciones, equipamiento, herramientas, competencias y conductas adecuados para prevenir riesgos de esta índole
- Sistemas de vigilancia frente a nuevas formas de amenaza, y matrices de riesgo actualizables
- Sistemas de respuesta frente a eventos adversos

Por otra parte, es importante que las políticas de seguridad de la información y de ciberseguridad de los laboratorios informático-forenses pueden adaptarse y aplicarse a otros ámbitos de trabajo afines, tales como los equipos de investigación en entornos digitales o los equipos de análisis de grandes masas de datos, los técnicos en el uso de herramientas de análisis de smartphones, o el personal idóneo en recolección.

Referencias Bibliográficas

[1] “Que es la ciberseguridad”, AO Kaspersky Lab. (2023). Online: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[2] Morales, F., Toapanta, S., & Toasa, R. M. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. Revista Iberica de sistemas e tecnologías de informacao, (E27), 553-565.

[3] Reglamento General de Protección de Datos Personales de la Unión Europea (UE 2016/679) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02002L0058-20091219

[4] Bodero Poveda, E., De Giusti, M. R., & Morales, C. (2022). Preservación digital a largo plazo: estándares, auditoría, madurez y planificación estratégica. Revista Interamericana de Bibliotecología, 45(2).

[5] Bustamante Garcia, S., Valles Coral, M. A., & Levano Rodriguez, D. (2020). Factores que contribuyen en la pérdida de información en las organizaciones. Revista Cubana de Ciencias Informáticas, 14(3), 148-164.