UNIVERSIDAD NACIONAL DE LA MATANZA

Escuela de Posgrado

Maestría en Informática

Tesis de Maestría

Título: Metodología de análisis forense informático para la obtención de evidencia digital en Base de Datos

---

Autora: ***Esp. Ing. Cintia Verónica Gioia***

Director de Tesis: ***Mg. Ing. Jorge Esteban Eterovic***

Buenos Aires - Argentina

Junio 2019

Agradecimientos

A mi hija por comprender mis tiempos dedicados a escribir.

A mi marido compañero incondicional en todo momento.

A mis padres por alentarme siempre.

A mi Director de tesis por guiarme, orientarme y ayudarme con sus sabios consejos y gran experiencia.

Al Departamento de Ingeniería e Investigaciones Tecnológicas y a la Secretaría de Ciencia y Tecnología de la Universidad Nacional de la Matanza que me han brindado un gran apoyo y motivación.

A los profesionales amigos que contribuyeron con el aporte de sus puntos de vista, conocimiento, experiencia y consejos.

A todas las personas e instituciones que han contribuido directa o indirectamente a mi formación y desarrollo profesional en el campo de la informática forense.

RESUMEN

En la actualidad la tecnología brinda la posibilidad de recopilar y almacenar gran cantidad de información en base de datos y recuperarla en segundos. Ante esta situación, crecen los delitos informáticos asociados y la necesidad de aplicar computación forense en dichas bases, donde se plantea el desafío de obtener evidencia digital válida como medio de prueba para su efectiva sanción dentro de un proceso judicial. Prevenir los riesgos de invalidar una prueba se convierte en una responsabilidad y un reto profesional.

En este trabajo se propone una metodología forense específica para base de datos relacionales basada en una metodología forense informática general que guía, unifica y garantiza la confiabilidad de las actividades que realiza el perito informático centradas en la obtención y el análisis de evidencia digital. Asimismo, se plantea la obtención de evidencia digital a partir de la configuración y ejecución de auditorías de datos universales aplicables a cualquier motor de base de datos. La metodología planteada sobrepasa las limitaciones o retos tecnológicos individuales de cada tipo de base de datos y la dependencia de expertos en dichas tecnologías que ofrecen soluciones según su visión tecnócrata, en ocasiones incluso, sin garantizar la admisibilidad judicial de la evidencia digital.

PALABRAS CLAVE: Evidencia Digital en Base de Datos - Metodología Informática Forense - Metodología Forense en Base de Datos - Auditoría de Información de Base de Datos - Informática Forense

ABSTRACT

The technology currently makes it possible to collect and store a large amount of information in the database and retrieve it in seconds. For this reason, associated computer crimes are growing as well as the need to apply forensic computing on these bases, so the challenge of obtaining valid digital evidence as a means of proof for its effective sanction in a judicial process is raised. It becomes a responsibility and a professional challenge to prevent the risks of invalidating a proof.

This thesis work proposes a specific forensic methodology for a relational database based on a general computer forensic methodology, which guides, unifies and guarantees the reliability of the activities of the computer expert to obtain and analyze the digital evidence. In addition, it is proposed to obtain digital evidence from the result of the configuration and execution of universal data audits applicable to any database engine. The proposed methodology exceeds the individual technological limitations or challenges of each type of database and the dependence of experts on these technologies that offer solutions according to their technocratic vision, sometimes even without guaranteeing the judicial admissibility of digital evidence.

PALABRAS CLAVE: Database Digital Evidence - Forensic Computing Methodology - Database Forensic Methodology - Database Information Audit - Forensic Computing

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

"La Justicia no será servida hasta que aquellos que no están afectados estén tan indignados como los que lo están."- Benjamín Franklin.

"Todos somos ignorantes. Lo que ocurre es que no todos ignoramos las mismas cosas."- Albert Einstein.

"Lo correcto es correcto, incluso si todos están en su contra y lo incorrecto es incorrecto, incluso si todos están de acuerdo." - William Penn.

Capítulo 1 - Introducción

Las organizaciones se encuentran continuamente expuestas a amenazas de seguridad internas y externas sobre sus datos. Los datos de los sistemas de información son el activo más importante para la consecución de los objetivos y la continuidad de las organizaciones. El hecho de que esos datos y sus operaciones sean manipulados por seres humanos directamente o a través de una variedad de aplicaciones o servicios, las hace vulnerables a ataques externos o internos y les agrega un componente de error, voluntario o no, que implica un riesgo para la organización en la cual la información puede verse comprometida y accedida por personas no autorizadas.

La incorporación de las tecnologías de información a la vida cotidiana, en todos sus ámbitos, ha marcado la necesidad de incluir los distintos medios informáticos como elementos de carácter investigativo y probatorio, tanto sean usados como medio o fin en la comisión de delitos informáticos.

Las bases de datos son uno de los principales tesoros corporativos que proteger en las empresas o entidades gubernamentales. Gran parte de esta información puede estar compuesta por datos sensibles propios de las

organizaciones o por datos personales de terceros. Por tal motivo, dichas bases podrían ser afectadas por acciones maliciosas de diversos tipos, como lecturas, alteraciones o copias de datos críticos, incluso sin ser advertidas, comprometiendo así la confidencialidad de cierta información, la cual por ley debe ser objeto de especial cuidado.

En la actualidad la tecnología brinda la posibilidad de recopilar y almacenar gran cantidad de información en base de datos y recuperarla en segundos sin mayor esfuerzo. Ante esta situación crecen los casos de delitos informáticos asociados y la necesidad de, además de administrar los permisos y autorizaciones sobre los datos, aplicar también mecanismos complementarios de auditorías para la obtención de trazabilidad de operaciones que sirvan como evidencia de acciones maliciosas o detección de potenciales riesgos.

Gran parte de esta información crucial para la organización está compuesta por datos personales de terceros nacionales o internacionales, que por una u otra razón forman parte de las bases de datos. Por esta razón, es necesario facilitar la puesta en práctica y el cumplimiento de leyes de protección de datos personales tanto nacionales[1] como del exterior[2] [3] [4].

El crecimiento de las transacciones electrónicas y vía Internet, así como el auge de los servicios de base de datos en la nube, incrementan la necesidad de proteger los accesos de red y remotos a la información, haciendo que la labor del aseguramiento de la información en las bases de datos sea cada vez más exigente y especializada.

[1] Ley 25.326 de Protección de los Datos Personales; Decreto Reglamentario 1558/2001; Decreto Reglamentario 1160/2010. Buenos Aires, Argentina.

[2] Reglamento General de Protección de Datos (RGPD) a nivel de la Unión Europea, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Entró en vigor el 25 de mayo de 2016 y fue de aplicación el 25 de mayo de 2018. En España, el RGPD dejó obsoleta la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) de 1999, siendo sustituida el 6 de diciembre de 2018 por la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, acorde con el RGPD.

[3] Ley Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (30 de julio de 2002), la cual se promulgó en Estados Unidos con el propósito de monitorizar a las empresas que cotizan en bolsa de valores, evitando que la valorización de las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor.

[4] Acuerdos de Basilea de supervisión bancaria o recomendaciones sobre regulación bancaria emitidos por el Comité de Basilea de Supervisión Bancaria. Desde 2009, todos los demás países significativos del G-20 están representados, así como algunas de las mayores plazas bancarias como Hong Kong y Singapur.

Como ha sucedido a lo largo de la historia todo avance de la tecnología puede ser utilizado tanto para beneficio de la sociedad, como también para la ejecución de actividades ilícitas.

En general las organizaciones almacenan y administran sus datos en Base de Datos. Los Sistemas de Gestión de Base de Datos (en sus siglas SGBD) permiten el almacenamiento, manipulación y la consulta de los datos que resguardan. El sistema de permisos y autorizaciones del propio SGBD es la barrera universalmente implantada para proteger a los datos almacenados en dichas bases. Los administradores de Base de Datos gestionan las mismas bajo políticas y procedimientos de seguridad de la información que especifican las reglas para acceder, compartir, distribuir, conseguir, clasificar e inventariar la información.

De este modo, las políticas de información trazan procedimientos y responsabilidades específicas, definen las áreas, sectores, grupos o personas que comparten la información, los permisos, formas de acceso y de distribución de la misma, como también los responsables de actualizar y dar mantenimiento a la información.

Existe el riesgo potencial que un usuario con permisos de acceso a una tabla puede acceder a la misma, por dentro o por fuera de la aplicación, sin ser descubierto y realizar acciones maliciosas pudiendo afectar la integridad o disponibilidad de los datos, según los permisos que posea, como también acceder a información sensible o confidencial que por ley deben ser objeto de privacidad.

Prevenir los riesgos de acceder o manipular información sensible se convierte en una responsabilidad y un reto profesional difícil de llevar a cabo para aquellos que trabajan cotidianamente como Administradores de Seguridad de Bases de Datos, quienes son responsables de garantizar la integridad, confidencialidad, disponibilidad y fiabilidad de la información.

En este contexto se desprende la necesidad de configurar y ejecutar auditorías de datos sobre las bases de datos para obtener la trazabilidad y evidencia de las actividades de los usuarios, y a partir de los mismos analizar las acciones y aplicar controles.

Las configuraciones de las auditorías son cruciales para detectar, controlar y registrar información de las actividades como también para prevenir futuras

acciones maliciosas, según patrones de comportamiento que pudieran evidenciar potenciales riesgos. La implantación de estos controles posibilita obtener mejoras continuas en la seguridad de las bases de datos, ya que permiten ajustar tanto de forma preventiva como reactiva la seguridad de las mismas.

La información resultante de la ejecución de las auditorías permite analizar los distintos tipos de vulnerabilidades que pudieran existir en la configuración de seguridad de los SGBD. A través de la evaluación de las vulnerabilidades y de las potenciales amenazas determinar la exposición a los riesgos.

Los resultados de la aplicación de auditorías, como también los archivos de logs, pueden ser recolectados, analizados y presentados como evidencia digital ante potenciales conductas delictivas asociadas a la manipulación de los datos resguardas en las bases. De esta manera a través de la aplicación de las auditorías de datos, basadas en la aplicación de políticas de seguridad en tiempo real, se logra detectar y prevenir intrusiones, proteger los datos y controlar la integridad de los mismos.

Es importante considerar que la ejecución de soluciones de auditorías de datos propia de cada tipo de SGBD en muchas ocasiones afectan el rendimiento y productividad de las mismas, lo cual termina provocando la desactivación de las mismas por parte de los mismos administradores de Base de Datos, con el fin de no afectar la operatoria de los sistemas asociados [1], pero sí afectando la obtención de información valiosa que podría ser relevante como evidencia en la investigación de un delito informático.

Considerando que existe diversidad de bases de datos implementadas sobre diferentes sistemas gestores de base de datos, los cuales a la vez se pueden instalar en diversos sistemas operativos y plataformas, incluso dentro de una misma organización, se requiere disponer de tiempo y de personal especializado en cada tecnología involucrada.

Al disponer de bases de datos, en especial si contienen datos personales, nacen algunas obligaciones legales que no pueden ser soslayadas por las organizaciones sin arriesgarse a la imposición de importantes sanciones por parte del Estado, tales como las leyes de protección de datos. Las bases de datos de

[1] Ben-Natan,Ron.How to Secure and Audit Oracle 10g and 11g. Taylor & Francis Group, LLC 2009.

las empresas almacenan información crítica para el funcionamiento operacional y comercial de las mismas, lo que hace que cualquier tratamiento que afecte de forma negativa a los datos almacenados o se divulgue información secreta o estratégica pueda afectar de forma significativa al negocio.

Los SGBD, al igual que todos los sistemas informáticos, contienen vulnerabilidades que pueden ser aprovechadas tanto por terceras personas no autorizadas para acceder a la información, como también por usuarios con permisos de acceso cometiendo ataques intencionados o errores humanos, como también errores de aplicaciones. Dichas vulnerabilidades pueden ser a causa de problemas de seguridad propios del SGBD o por una mala configuración por parte del Administrador de Base de Datos, tanto técnicas o por omisión u error en las políticas o procedimientos de seguridad.

Cuando el incidente a investigar está relacionado a ejecutar un tratamiento de la evidencia a digital sobre la información almacenada en una base de datos entra en juego el análisis forense sobre base de datos.

Cada día se necesita más la aplicación de **Informática Forense de Base de Datos**, donde se plantea el desafío de obtener evidencia digital válida como medio de prueba para su efectiva sanción. Entonces surge la necesidad de avanzar en las técnicas y procedimientos usados para realizar una investigación forense de base de datos que pueda identificar de manera efectiva y eficiente los hechos acontecidos, respondiendo a las preguntas claves del análisis forense; qué, cómo, cuándo y quién.

La identificación, recolección, análisis, interpretación y presentación de esta clase de evidencia digital por un lado requiere del auxilio de expertos en base de datos, pero que también posean formación y experiencia en informática forense, con conocimientos sobre los aspectos legales y procesales que hacen a la actuación pericial.

La exigente labor que hoy en día se requiere de especialistas en informática forense obliga a los mismos a mantener un conocimiento detallado tanto a nivel de metodologías de prácticas forenses, procesos vinculados y el uso de herramientas específicas. Aunque también deben conocer las legislaciones asociadas al tratamiento de la evidencia digital, con el fin de llevar a cabo tanto

investigaciones forense informáticas particulares como la producción de pruebas que puedan ser usadas ante un tribunal de justicia u organismos del orden público, garantizando la validez jurídica y científica de la evidencia digital y su valor probatorio en el marco de una causa o investigación judicial.

Frente a la heterogeneidad de tecnologías asociadas a las bases de datos y la complejidad de su administración y configuración surge la necesidad de contar con una **metodología específica de análisis forense informático que garantice la obtención de evidencia en Base de Datos** de forma universal, confiable, segura, justificable, repetible, reproducible y trazable.

Capítulo 2 - Estado del Arte

En este capítulo se detallan y analizan diferentes conceptos y fundamentos relacionados a aspectos legales, procesales, técnicos y metodológicos, que en su integración contribuyen a un sólido marco teórico y de estudio de la problemática específica a plantear, considerando las variadas dimensiones de la labor forense informática y la interacción de la misma con expertos de otras disciplinas, como investigadores, abogados, criminalistas, funcionarios públicos, entre otros.

Para comprender y analizar con profundidad los retos de la informática forense en forma general y específica en base de datos se analizaron diversas fuentes de información, estudios relacionados y su aplicación en diferentes contextos.

La digitalización de la información obliga a que no siempre se busque un rastro o una huella física con un reactivo químico o magnético, sino a través de técnicas y herramientas informáticas que buscan la evidencia digital oculta en un código binario, que sujeto a intervención humana, electrónica y/o informática es extraído de un medio tecnológico informático (Di Iorio, Castellote & Bruno, 2017). En estos casos para llegar a la verdad o al esclarecimiento de los hechos, tanto los fiscales, jueces, abogados, incluso organizaciones o particulares, necesitan el auxilio de la ciencia forense informática, de manera de poder aplicar el uso de las tecnologias de información para recuperar y procesar la evidencia digital.

2.1. Aspectos Legales

2.1.1. Los Delitos Informáticos

El significado más utilizado para definir el concepto de **delito informático**, en términos prácticos, es aquel que lo describe como conductas indebidas o ilegales donde interviene un dispositivo informático como medio para cometer un ilícito o como fin u objeto del delito mismo (Sain & Azzolin, 2017).

Como fin para cometer un delito, se refiere a ataques informáticos a bienes informáticos, sea a computadoras, servidores, diversos tipos de dispositivos informáticos, redes, comunicaciones, incluso a programas específicos, sitios Web, base de datos, archivos, entre otros. Un ejemplo de ataque informático es el caso de una base de datos, siendo el objeto del crimen de un empleado de una compañía que instala y ejecuta un programa malicioso a fin de dañar e inutilizar el servidor donde está alojada la misma.

En cambio, es un medio para cometer un ilícito cuando se considera al uso de dispositivos informáticos como medio comisivo de delitos, en general delitos tradicionales, que con el auge de las nuevas Tecnologías de Información y Comunicaciones (TIC) crecen en magnitud, alcance y perjuicio o incluso prosperan a través de nuevas modalidades delictivas que solo pueden darse a través del uso de la tecnología. Una muestra de este caso es un adulto que accede desde su celular a una red social por medio de la cual contacta a un menor con fines sexuales, siendo el delito de Grooming[1] el hecho ilíctio en sí.

La masividad del uso de diversos dispositivos tecnológicos ha facilitado un nuevo medio digital para la comisión de delitos tradicionales (estafas, fraudes, etc.) como también la aparición de nuevas conductas delictivas (por ejemplo, el acceso no autorizado a un sistema informático, etc.).

Se definen los delitos informáticos como “aquellas conductas que: a) atacan a las propias tecnologías de la computación y las comunicaciones; b) incluyen la utilización de tecnologías digitales en la comisión del delito; o c) incluyen la utilización incidental de las tecnologías en la comisión de otros delitos, y en consecuencia, la computadora pasa a ser una fuente de datos digitales probatorios” (Di Iorio, Castellote & Bruno , 2017, p.95).

El Departamento de Justicia de los Estados Unidos define a los delitos informáticos como “cualquier acto ilegal que requiera el conocimiento de tecnología informática para su perpetración, investigación o persecución”[2].

[1] El delito de Grooming se refiere a cuando un adulto contacta a un menor de edad, a través de Internet u otros medios digitales, mediante la manipulación o el engaño y ocultando su condición de adulto; con una finalidad sexual, logrando que el niño o niña realicen acciones de índole sexual.

[2] Tobares Catalá, G. H. (2010) Delitos Informáticos: Edit. Advocatus. Nota 23 de la página 28.

Según Gustavo Sain, tal como explica en su libro “Delitos Informáticos. Investigación criminal marco legal y peritaje” (Sain & Azzolin, 2017, p9-10), las diferentes definiciones existentes de delitos informáticos en la actualidad utilizan cuatro criterios de clasificación. El primer criterio es “legal” considerando que los hechos indebidos relacionados con dispositivos informáticos son considerados delitos informáticos siempre y cuando dichas conductas esten tipificadas y se encuentren penadas por la ley. El segundo criterio es el “técnico”, según las definiciones se refieren a conductas que involucran cualquier tipo de dispositivos informáticos o dispositivos electrónicos o tecnologías de la información, siendo condicionante el lugar que ocupa la tecnlogía en el hecho, más que en la naturaleza delictiva del mismo. La tercera clasificación es el “entorno”, donde por ejemplo algunos los limitan a los hechos que se manifiestan en Internet. El cuarto criterio considera que los delitos informáticos son aquellos que requieren “la aplicación de técnicas y herramientas informáticas en el proceso de investigación” para la resolución de un caso judicial, por ejemplo, en un caso de homicidio que requiera investigar las últimas comunicaciones privadas de la víctima y se aplica análisis forense a su dispositivo móvil .

Si bien no todos los delitos informáticos se relacionan con Internet, es a partir del uso masivo del mismo que empiezan a crecer de una manera casi incontrolable tanto en cantidad como en modalidades delictivas. La tecnología está cada vez más presente en todas las investigaciones de potenciales delitos, incluso al considerar también al uso de herramientas informáticas para la investigación y análisis forense de delitos tradicionales.

Con la expansión y popularización de Internet, la mayoría de los delitos informáticos son anónimos en tanto que en la red se permite la creación de identidades falsas de usuarios y la mayoría de los servicios más utilizados son gratuitos y no requieren de procedimientos de autenticación complejos. Además, son transnacionales tanto en el sentido que se pueden cometer desde una computadora y afectar a otra computadora y sus datos en otro punto del planeta, como también en el sentido en que los datos e información que transportan las redes atraviesan distintas jurisdicciones y países, en los cuales las leyes pueden variar. La escena del crimen no se asocia a un espacio físico, sino a un espacio

virtual (Sain & Azzolin, 2017, p11). Este tipo de conductas son inmediatas en cuanto a tiempo de emisión y recepción, ya que con el uso de Internet se acortan las barreras de tiempo y el espacio por la instantaneidad de las comunicaciones (Sain & Azzolin, 2017, p90).

2.1.2. Los Delitos Informáticos en Argentina

En el año 2008 se sancionó en Argentina la **Ley 26.388 de "Delitos Informáticos"**[1] (sancionada el 8 de junio y promulgada de hecho el 24 de junio del mismo año). Esta ley realiza reformas e incorporaciones de algunos artículos existentes del **Código Penal** (C.P.) de la Nación Argentina, incorporando a las nuevas tecnologías como medios de comisión de distintos tipos de delitos previstos en el mismo y brindando un importante aporte el cual llenó un vacío legal existente hasta ese momento en el Derecho Argentino.

Previo a la sanción de esta ley, ante la aparición de los primeros delitos cometidos a través o contra los sistemas informáticos, Argentina no estaba preparada penalmente para enfrentarlos (Sain & Azzolin, 2017, p39).

Las garantías constitucionales en el Derecho Penal son principios limitadores plasmados en artículos de la Constitución Nacional que son de vital importancia para la preservación de las libertades individuales. Por un lado, hay que considerar que un hecho es considerado delito si está tipificado en el Código Penal como tal, según el **Principio de Legalidad del Derecho Penal**[2], lo cual implica la prohibición de castigar conductas no encuadradas en un tipo penal. Establece que nadie puede ser penado por hechos que no fueran delictivos según la legislación aplicable al momento de cometerse. Encuentra su razón en que nadie puede ser castigado por aquello que no podía preverse que sería interpretado como delito, ya que no existe crimen sin una ley previa. Al no estar tipificado el delito informático, el vacío legal y la falta de sanción de normas se

[1] Ley 26.388 de Delitos Informáticos disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm, Sitio Web Infoleg (de Información Legislativa del Ministerio de Justicia y Derechos Humanos de la Nación).

[2] El Principio de Legalidad en el Derecho Penal es uno de los principios más importantes del derecho penal en la actualidad, cuya esencia es: "nullum crimen nulla poena sine praevia lege" (no hay delito ni pena sin ley previa), el cual emana del artículo 18 de la Constitución Nacional.

hacía sentir aún más con el crecimiento de modalidades delictivas que como fin o medio hacían uso de las tecnologías y entornos digitales. Esto sumado a que en el Derecho Penal la analogía[1] está prohibida en los tipos penales, dada la vigencia del **Principio de Estricta Legalidad**, no se puede encuadrar un hecho en un determinado delito aplicando una norma jurídica a un caso que no está incluido como tipo penal específico, pero que resulta ser similar. El Principio de Legalidad es también una herramienta que funciona como garantía para evitar que alguien sea perseguido por aquello que no podía prever que fuera delito, siendo a su vez el Código Penal, un catálogo cerrado ("numerus clausus")[2] que no puede ser extendido por la sola interpretación judicial. El Principio de Legalidad encuentra su expresión práctica en la formulación de los tipos penales, que es la forma legislativa de establecer las conductas prohibidas en el ámbito penal y que pueden ser clasificados en cuanto a su forma de realización como delitos de acción o delitos de omisión.

El Código Penal Argentino[3] organizó su parte especial, es decir aquella en la que describe los tipos penales, en torno a los bienes jurídicos[4] susceptibles de ser afectados, de tal manera que siempre deba tenerse esta tipificación a la vista a la hora de juzgar si una conducta es lícita o no. En virtud de lo señalado, resultó necesario modificar el Código Penal a fin de extender la penalización de ciertas acciones que se consideraban ilícitas, y que fueran **cometidas mediante el uso de las nuevas Tecnologías de Información y Comunicaciones (TIC) o dirigidas contra bienes informáticos**.

[1] A esta prohibición de analogía, también se la conoce como "prohibición de la analogía in malam partem". Cabe aclarar que no se opone el uso de la analogía para excluir o atenuar la responsabilidad penal conocido como "analogía in bonam parte".

[2] En su trabajo "Property and Collective Undertaking: The Principle of Numerus Clausus" Dorfman sostiene que el principio del "numerus clausus" de los derechos reales es "un límite a la legislación privada", es decir, a la autonomía privada, en la creación de nuevas formas de derechos reales y que el fundamento de tal limitación se encuentra en la idea de que crear nuevos derechos reales corresponde al legislador democrático. Disponible en: https://almacendederecho.org/el-principio-del-numerus-clausus-de-los-derechos-reales/

[3] Código Penal de la Nación Argentina disponible en el siguiente enlace: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm.

[4] El bien jurídico hace referencia a los bienes, tanto materiales como inmateriales, que son efectivamente protegidos por el derecho, como por ejemplo la salud y la vida

Es por aplicación de este principio que el Derecho Penal reconoce sólo dos factores de atribución de responsabilidad. Por un lado, la **culpa**, donde la responsabilidad se atribuye por imprudencia, negligencia o impericia y por el otro el **dolo**[1], donde se manifiesta la voluntad de realización del tipo delictivo, guiada por el conocimiento de sus elementos objetivos, es decir, que para afirmar su presencia deberemos afirmar la presencia de dos elementos: conocimiento y voluntad[2]. Como señala el Dr. Zaffaroni: "Sus disposiciones distinguen claramente la culpa del dolo, reconociéndose las eximentes de fuerza mayor y el caso fortuito, como también la buena fe, el estado de necesidad y la legítima defensa"[3].

Al sancionar la Ley N° 26.388 se asumió que las nuevas tecnologías podrían ser utilizadas como posibles medios de comisión de distintos delitos y que debían ser expresamente tipificados en el Código Penal Argentino. La Ley 26.388 no es una ley especial del Código Penal que regula los delitos informáticos en un cuerpo normativo separado con figuras propias y específicas, sino es una ley que modifica, reemplaza y agrega figuras típicas a diversos artículos ya vigentes en el mismo para poder tipificar los delitos informáticos. A lo largo de su articulado incorpora nuevas definiciones y tipifica diversos delitos informáticos.

La reforma de la Ley 26.388 siguió los lineamientos del Convenio sobre la Ciberdelincuencia de Budapest del 23 de noviembre de 2001[4]. Los bienes jurídicos[5] alcanzados por la reforma son: 1) delitos contra la integridad sexual; 2) delitos contra la libertad, específicamente la violación de secretos y de privacidad; 3) delitos contra la propiedad; 4) delitos contra la seguridad pública; 5) delitos contra la Administración Pública.

---

[1] En los actos jurídicos, el dolo implica la voluntad maliciosa de engañar a alguien o de incumplir una obligación contraída. En el derecho el término dolo se usa con significados diferentes. En derecho penal, el dolo significa la intención de cometer la acción típica prohibida por la ley. En derecho civil se refiere a la característica esencial del ilícito civil, en el incumplimiento de las obligaciones designa la deliberada inejecución por parte del deudor y, por último, es un vicio de los actos voluntarios.

[2] Fontan Balestra, C. (1998). Derecho Penal - Introducción y Parte General. Buenos Aires: Abeledo-Perrot

[3] Zaffaroni Eugenio Raúl; "TRATADO DE DERECHO PENAL - PARTE GENERAL"; Ed. Ediar; Buenos Aires; 1998; pág. 326.

[4] Convenio sobre la Ciberdelincuencia, Budapest, 23 de noviembre de 2001, Serie de Tratados Europeos nro. 185, Council of Europe/Conseil de L´Europe, disponible en: www.coe.int.

[5] El bien jurídico hace referencia a los bienes, tanto materiales como inmateriales, que son efectivamente protegidos por el derecho, como por ejemplo la salud y la vida.

La Ley 26.388 generó un número limitado y específico de tipos penales y la reforma o actualización de otros ya existentes (Dupuy & Kiefer, 2017, p.10).

La ley brinda el valor jurídico probatorio al **documento electrónico**, donde el término documento comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

Se resalta la tipificación como delito del **acceso indebido a sabiendas a un sistema o dato informático de acceso restringido por cualquier medio sin la debida autorización o excediendo la que posea,** como también **la publicación indebida de una comunicación electrónica que no esté destinada a ser pública y que puede causar perjuicios a terceros** y **la revelación de hechos, actuaciones, documentos y datos que por ley sean secretos.**

La Ley penaliza a quien **acceda, proporcione, revele o inserte directa o indirectamente datos ilegítimamente a un banco de datos personales**. También reconoce como modalidades delictivas a la **estafa informática** y al **daño informático**, entre otros.

La ley contempla además los **delitos que puedan cometerse con herramientas informáticas** como calumnias e injurias, divulgación de secretos, defraudación, amenazas, comercialización y suministro de medicamentos sin autorización por internet, instigación a cometer delitos, instigaciones basadas en la ley antidiscriminatoria, intimidación pública, impedimento arbitrario del pleno ejercicio de los derechos y garantías fundamentales reconocidos en la Constitución Nacional.

Otro de los aspectos importantes a tener en cuenta es el surgimiento de la "**prueba informática**", su validación o equiparación a la "prueba documental" sin atentar contra las garantías constitucionales. En las investigaciones de delitos informáticos gran partes de las pruebas son intangibles y transitorias.

En el Anexo 1 del presente trabajo se detalla y analiza cada artículo de esta Ley 23.388, como también de otras leyes nacionales cuyos artículos se relacionan con delitos informáticos, como ser la Ley 25.506 de Firma Digital[1] que reconoce y

[1] Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje.

establece las condiciones para el empleo de la firma digital y su eficacia jurídica y la Infraestructura de Firma Digital de la República Argentina.

2.1.3. Delitos Transnacionales y Marco Legal Internacional. Convenio de Budapest

Los delitos que se cometen en y a través de la red pueden tener carácter transnacional, ya sea porque son cometidos por personas que operan en diferentes países, a causa de que las víctimas están en un país distinto o porque la prueba está alojada en servidores ubicados en países distintos al que lleva adelante la investigación. Es por esto que las investigaciones suelen requerir la intervención de diferentes Estados (Ferreyra, La Convención de Cibercrimen de Budapest y América Latina, 2018).

La información que se necesita acceder en una investigación puede no estar en la computadora del sospechoso, sino alojada en servidores externos, en la "nube"[1], que incluso pueden estar alojados en otro país. En estos casos, la investigación y recolección de evidencia requiere muchas veces la cooperación internacional.

Argentina tiene una estructura federal, por lo que, ante la presunta comisión de la mayoría de los delitos, interviene la justicia penal ordinaria de la provincia que se trate. Ante casos excepcionales legalmente establecidos es competencia de la justicia nacional o federal. Esta estructura federal ya plantea controversias acerca de la ley aplicable y la determinación del juez competente (ya sea para decidir en un caso o sólo obtener la prueba). Los casos son más problemáticos cuando se involucran diferentes países, ya que no todos los países aplican las mismas reglas para determinar la jurisdicción y la competencia judicial. Para lo cual en estos casos es necesario establecer cuál es la normativa de derecho internacional que rige la relación con cada Estado, tanto en convenios bilaterales como tratados internacionales (Di Iorio, Castellote & Bruno, 2017, p.151-152).

[1] La computación en la nube (del inglés "cloud computing"), conocida también como servicios en la nube, informática en la nube, nube de cómputo, nube de conceptos o simplemente "la nube", es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.

En el mundo conviven múltiples legislaciones relacionadas con la transferencia internacional lo que dificulta establecer una estrategia global en términos de la utilización de servicios de cómputo en la nube (González Allonca, y otros, 2019).

El instrumento internacional aplicable a estas cuestiones es la Convención de Criminalidad de la Unión Europea, también denominado el Convenio de Ciberdelito de Budapest[1]. Este convenio fue elaborado por el Consejo de Europa en Hungría el 23 de noviembre de 2001 y entró en vigor en el 2004, con la finalidad de acordar cuestiones básicas de la política penal de los países participantes del mismo, con el objetivo primario de prevenir la cibercriminalidad y hacer frente a los delitos informáticos, armonizando las leyes entre países aplicando una legislación apropiada y uniforme de manera que los hechos puedan ser investigados por cualquiera de los Estados miembros. Es el primer convenio internacional que aborda de manera específica el tema de cibercrimen transnacional estandarizando métodos de combate contra crímenes informáticos para la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Trata, entre otros temas, infracciones de derechos de autor, fraude informático, pornografía infantil, los delitos de odio y violaciones de seguridad en la red.

La tarea involucra cuestiones no solo de legislación sino de cooperación internacional, como también adecuarse a las nuevas normas de protección de datos personales de Europa, asegurando que toda la circulación de información, que es necesaria en causas penales, tenga las debidas garantías y protecciones.

El tratado está abierto para que otros países de cualquier continente puedan adherirse al mismo. Más de 56 países de todo el mundo forman parte del tratado internacional. Están adheridos países como Estados Unidos, Italia, España, Japón, Canadá, Israel, República Dominicana y Panamá. La Argentina adhirió al Convenio de Budapest en noviembre de 2017 y forma parte oficialmente desde mayo de 2018. Chile, Paraguay, Costa Rica y Panamá son otros de los países de Latinoamérica adheridos. Las acciones estipuladas en este Convenio obligan a que cualquier Estado que pretenda unirse a él, deba adecuar su regulación según lo establecido en el tratado.

[1] Convenio de Budapest, versión en español disponible en https://rm.coe.int/16802fa41c.

Los principales objetivos se centran en la tipificación de las conductas ilícitas, así como el establecimiento de las medidas procesales idóneas para su investigación, siendo de especial relevancia la coordinación y cooperación de las fuerzas de los países adheridos. Según Marcos Salt[1], "se trata más que nada de discutir todas las formas novedosas que resultan necesarias para poder obtener prueba en formato digital (evidencia digital) cuando la evidencia no está alojada en el país que la necesita, sino en un servidor en el extranjero".

El acceso transfronterizo de datos se refiere a las distintas formas que existen para que el sistema penal de un país pueda acceder a información que necesita en una causa, bajo jurisdicción de ese país, pero con pruebas alojadas en otra jurisdicción.

En cuanto a la clasificación de los delitos informáticos se estableció la existencia de las siguientes categorías: 1) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; 2) Infracciones informáticas; 3) Delitos vinculados al contenido; 4) Delitos vinculados a la violación de la propiedad intelectual y otros derechos afines (Di Iorio, Castellote & Bruno , 2017, p.143-144).

2.1.4. Protección de Datos Personales en la República Argentina

En materia de protección de datos personales en la República Argentina se aplica la Ley 25.326 (Ley de Habeas Data, año 2000)[2], Decreto 1558/2001[3], Decreto 1.160/2010[4] y las Disposiciones DNPDP (Dirección Nacional de

[1] El abogado argentino Marcos Salt, coordinador del Programa Nacional contra la Criminalidad Informática del Ministerio de Justicia y Derechos Humanos de la Nación y representante de Argentina en las reuniones del Consejo de Europa. Es coordinador académico de un programa de la Subsecretaría de Justicia y Política Criminal que en el año 2018 trabajó en lograr que la Argentina integre la convención de ciberdelito de Budapest.

[2] Ley 25.326 de Protección de los Datos Personales disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

[3] Decreto Reglamentario 1558/2001. Poder Ejecutivo Nacional (P.E.N.) disponible en http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=70368

[4] Decreto Nº 1.160/2010. Poder Ejecutivo Nacional (P.E.N.) disponible en http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=170508

Protección de Datos Personales, órgano descentralizado del Ministerio de Justicia y Derechos Humanos de la Nación)[1].

La Ley 25.326 de Protección de los Datos Personales, 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 estos 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 (González Allonca, y otros, 2019).

La Ley 25.326 define los principios generales relativos a la protección de datos personales, desde derechos de los titulares hasta las figuras de usuarios y responsables de archivos, registros y bancos de datos. El control, las sanciones, la acción de protección de los datos personales están vinculados a esta Ley.

Considerando el importante papel que las bases de datos desempeñan en el mundo tecnológico, surge el derecho de las personas a protegerse frente a la intromisión de los demás. El régimen de protección de los datos personales permite que las personas ejerzan su legítimo poder de disposición y control sobre los datos de carácter personal referidos a su persona que se encuentran registrados en base de datos de terceros. Los ciudadanos tienen la facultad de consentir la recolección, obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles por un tercero, sea el Estado o un particular. Y este derecho a consentir el conocimiento y tratamiento de sus datos personales les da la facultad de saber en todo momento quién dispone de sus datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

La Ley de Protección de Datos Personales exige que todo aquel que efectué operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación,

[1] Las diferentes Legislaciones y Jurisprudencias referidas a protección de datos se pueden consultar del sitio Web http://www.protecciondedatos.com.ar/. En esta página se puede consultar toda la información necesaria para conocer y entender cómo funciona el sistema de Protección de Datos Personales establecido en la República Argentina por la Ley 25.326 (también conocida como Ley de Habeas Data), legislación, jurisprudencia, novedades, enlaces de interés a web sites nacionales e internacionales y servicios ofrecidos.

relevamiento, evaluación, bloqueo, destrucción, y en general, el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, interconexiones o transferencias, debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento de este tipo de información.

El Decreto 1558/01 estableció que la Dirección Nacional de Protección de Datos Personales es el organismo encargado de dictar las normas y procedimientos técnicos relativos al tratamiento y condiciones de seguridad de los archivos, registros, bases y bancos de datos públicos y privados. La Dirección Nacional de Protección de Datos Personales es el órgano de control de la ley, primero en América Latina y el tercero del hemisferio sur.

Argentina cuenta con una amplia tradición en materia de protección de datos personales, que se manifiesta en tres niveles distintos. Previamente a Ley 25.326, se encuentra la Constitución Nacional que, luego de su reforma en el año 1994, incluyó el artículo 43 que, en su párrafo tres, contempla el llamado habeas data, de la siguiente forma: "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística". Como se advierte, esta reforma de la Constitución Nacional ha establecido un instituto que carecía de antecedentes en el derecho federal, aunque ya se encontraba en las constituciones provinciales: la acción de habeas data [1] . Se trata de un procedimiento especialmente necesario a partir del aumento del uso de las computadoras, que pueden compilar la información y datos personales afectando el honor y la privacidad de las personas[2]. La acción también está establecida para tomar conocimiento de estos datos y exigir la supresión, rectificación, confidencialidad o actualización (Gonzalez Allonca, y otros, 2019).

[1] Palazzi, P (2002). *La transmisión internacional de datos personales y la protección de la privacidad*. Buenos Aires, Argentina.

[2] Peyrano, G (2002). *Régimen legal de los datos personales y el habeas data*. Buenos Aires, Argentina: De Palma., 2002.

Es imprescindible considerar la interpretación y la aplicación que hacen los jueces de estas normas. A partir de este desarrollo legislativo, Argentina fue declarada país adecuado por la Unión Europea en materia de Protección de Datos Personales, de conformidad con la Directiva 95/46/CE [1] (Gonzalez Allonca, y otros, 2019).

2.1.5. Protección de Datos Personales a Nivel Internacional

A nivel internacional rigen leyes de protección de integridad y confidencialidad de los datos personales. Existen leyes que se están promulgando continuamente en todo el mundo sobre la protección de datos personales, ya sea de datos considerados privados por las personas, datos del sector salud, financieros, etc.

En este aspecto toma relevancia el nuevo **Reglamento General de Protección de Datos (RGPD) 2016/679**[2] que es el nuevo reglamento de la Unión Europea (UE) relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismos.

Con esta nueva normativa de protección de datos de la UE, que empezó a regir a partir del año 2018[3], todas las empresas están obligadas a comunicar las brechas de seguridad que pudieran producirse, por lo que deberán extraer información constante sobre los intentos de intrusión y los accesos no autorizados y notificarlos en el plazo correspondiente. También es obligatorio comunicar los detalles del fallo a las personas cuyos datos hayan podido verse afectados.

El RGPD tiene por objetivo garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar.

[1] Parlamento Europeo (1995): "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data."

[2] Reglamento (UE) 2016/679 Del Parlamento Europeo, se puede descargar del sitio de la Agencia Estatal del Boletín Oficial del gobierno de España desde el enlace: https://www.boe.es/doue/2016/119/L00001-00088.pdf (visitado en mayo de 2019).

[3] El RGPD entró en vigor el 25 de mayo de 2016 y fue de aplicación el 25 de mayo de 2018, dos años después durante los cuales las empresas, las organizaciones, los organismos y las instituciones se fueron adaptando para su cumplimiento.

Esta ley no sólo es de aplicación para todas las empresas europeas, sino también para aquellas empresas internacionales que gestionen datos de usuarios residentes en la Unión Europea y realicen tratamiento de datos como consecuencia de su oferta de bienes o servicios destinados a ciudadanos europeos, por lo que deben contar para tal efecto con un responsable visible en Europa. El reglamento se aplicará al intercambio de datos transfronterizos y establece estándares mínimos para el tratamiento de datos en cada país.

La nueva normativa pretende devolver a los ciudadanos el control de sus datos personales y garantizar en la UE estándares de protección elevados y adaptados al entorno digital, en un mundo de teléfonos inteligentes, redes sociales, banca por internet y transferencias globales. También incluye nuevas normas mínimas sobre el uso y transmisión de datos para fines judiciales y policiales. Sienta las bases de una normativa de privacidad que se adecúa a la tecnología hoy presente con la finalidad de tomar las medidas preventivas adecuadas para proteger al usuario frente a los abusos en los tratamientos de sus datos, y evitar así que las empresas u organismos que efectúan el tratamiento de los mismos infrinjan la normativa.

En España, el RGPD dejó obsoleta la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD)[1] de 1999, siendo sustituida el 6 de diciembre de 2018 por la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, acorde con el RGPD y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Una de las claves de este Reglamento se centra en analizar el **impacto de privacidad**, que implica analizar el impacto en el tratamiento de datos cualquier proyecto informático. Este análisis de Privacidad por Diseño involucra determinar cómo se van a recolectar los datos de usuarios y clientes, cómo se va a informar a los clientes el tratamiento y uso que se le dará a sus datos personales, cómo y dónde se va a almacenar la información, analizar si la información recolectada es excesiva o no, definir mecanismos de acceso a la información y quién podrá acceder y/o realizar acciones sobres los datos personales y desde dónde.

[1] Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personales; Madrid, España. Disponible en https://www.lopd-proteccion-datos.com/sites/default/files/03-Ley-Organica-15-1999-LOPD.pdf.

Según lo que se expresa en el artículo 5 "Principios relativos al tratamiento"[1], del capítulo II del reglamento, los datos deben ser tratados de manera lícita, leal y transparente en relación con el interesado; recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; exactos y, si fuera necesario, actualizados; mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Si bien con la Ley Orgánica LOPD se exigía información sobre quién se encuentra detrás de todo tratamiento de datos y qué tratamiento se iba a hacer de los mismos, con el nuevo Reglamento Europeo de Protección de Datos RGPD se tiene que detallar la información de forma más precisa detallando: la identidad de los responsables de la gestión de los datos, la identidad o categoría de los destinatarios de los datos personales, los fines del tratamiento a que se destinan los datos personales y el fundamento jurídico para dicho tratamiento, el tratamiento que se le dará a los datos, el plazo de conservación de los datos o los criterios para determinarlos, transferencias de datos a otras organizaciones o países con el detalle del destino, entre otros, para cumplir con el **deber de información**.

En el Reglamento RGPD, el **consentimiento** por parte de los clientes, en el uso o almacenamiento de sus datos personales, no será válido si se basa en el silencio, inacción u omisión por parte del cliente o usuario, es decir, dejó de ser válido el consentimiento tácito. El consentimiento debe ser claro y afirmativo. Es obligatorio que se produzca una declaración explícita del dueño de los datos o una acción positiva que otorgue su conformidad para poder considerar que dicho

[1] Reglamento (UE) 2016/679 Del Parlamento Europeo, el cual se puede descargar del sitio de la Agencia Estatal del Boletín Oficial del gobierno de España desde el enlace: https://www.boe.es/doue/2016/119/L00001-00088.pdf

consentimiento es “inequívoco”, además de informado y específico. Las empresas o plataformas online deberán disponer de sistemas que puedan garantizar y probar que se ha otorgado el consentimiento por parte del dueño de los datos.

El **tratamiento** de los datos será lícito si el interesado dio su consentimiento o si el tratamiento es necesario para la ejecución de un contrato, para el cumplimiento de una obligación legal, para proteger intereses vitales del interesado o de otra persona física, entre otros (artículo 6, capítulo II de RGPD)

Respecto al tratamiento de datos de menores se dispone de una regla que establece que la **edad en la que los menores** pueden prestar por sí mismos su propio consentimiento para el tratamiento de sus datos personales en el ámbito de los servicios de la sociedad de la información (por ejemplo, redes sociales o aplicaciones móviles) es de 16 años. Sin embargo, esa edad se puede rebajar y cada Estado miembro puede establecer la suya propia, fijando un límite no inferior en ningún caso a los 13 años. Por ejemplo, el límite en España se ha dispuesto en los 14 años, si es menor a esa edad, es necesario que padres o tutores den su consentimiento a la organización que quiera tratar los datos personales.

En el RGPD es primordial también la **transparencia**, facilitando a los usuarios los derechos de acceso, rectificación (corrección o modificación), cancelación (dejar de consentir el uso de sus datos personales), portabilidad (derecho a trasladar los datos a otro proveedor) u oposición (negar o no consentir el uso de sus datos personales), como también los derechos de reclamación o queja y derecho al olvido (mediante la rectificación o supresión de datos personales).

Como parte de la transparencia cobra relevancia el lenguaje claro y comprensible sobre las cláusulas de privacidad, como también, el derecho a ser informado fehacientemente si los datos personales han sido atacados y en tal caso brindar información sobre el hecho, las acciones realizadas y por realizar al respecto, de manera de comunicar cuando se ponga en riesgo su privacidad o intimidad

Es esencial para cumplir con el RGPD que las empresas dispongan de una infraestructura tecnológica que pueda garantizar el tratamiento y almacenamiento seguro de los datos de sus clientes o usuarios, con el establecimiento y el cumplimiento de **medidas de seguridad** claras, como también medidas técnicas y organizativas. Estas medidas deben abarcar desde los accesos seguros a los

servidores, sistemas y base de datos, procedimientos seguros de resguardo de copias de seguridad, medidas especiales para evitar fuga de datos o alteración maliciosa de los datos, registro de las acciones sobre los datos sensibles, cifrado de datos sensibles, medidas de protección contra ataques de denegación de servicio o daños a los sistemas y bases de datos en general, entre muchas otras medidas de seguridad.

Para el RGPD es esencial velar por un nivel de seguridad que brinde la capacidad de incluir la seudonimización[1] y el cifrado[2] de datos personales; garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento de los datos; la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento (artículo 32).

RGPD obliga a reforzar los controles sobre la forma en que las empresas u organismos recopilan, usan y comparten los datos. Es importante que las organizaciones adopten un enfoque preventivo en cuanto a la adquisición, la gestión y el uso de los datos para evitar sanciones, pero sin pecar de exceso de cautela.

Acerca de la obligatoriedad del cifrado de las bases de datos, la RGPD, en su artículo 34, establece la no obligatoriedad de comunicar un incidente de seguridad si los datos están cifrados, en caso contrario es obligatorio hacerlo en las primeras
72 horas, tanto a la Agencia Española de Protección de Datos (AEPD) como al interesado, según lo indicado en los artículos 33 y 34.

Los estándares regulatorios actuales, no solo de la Unión Europea, abogan por el cifrado de los datos como método para proteger los mismos y evitar sanciones regulatorias. En este sentido, la recomendación general es migrar a aplicaciones y base de datos a entornos seguros, tanto de programación como de motores de

[1] Seudonimización es un procedimiento de gestión de datos donde se reemplazan campos de información personal dentro de un registro de datos por uno o más identificadores artificiales o pseudónimos.

[2] El cifrado es la práctica de codificar datos con el fin de modificar su formato original para que no sea posible leerlo.

bases de datos (Oracle, Microsoft SQL, etc.), actualizados a las últimas versiones y con las configuraciones de seguridad adecuadas.

Fuera de la Unión Europea hay varios estándares a mencionar. A continuación, se describen los más relevantes.

El **Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago ("Payment Card Industry Data Security Standard")** [1] o en sus siglas denominado PCI DSS, fue desarrollado por un comité conformado por las compañías de tarjetas de débito y crédito más importantes, el comité denominado PCI SSC ("Payment Card Industry Security Standards Council"). El PCI DSS fue desarrollado como una guía que ayuda a las organizaciones que procesan, almacenan y/o transmiten datos de titulares de tarjeta, a asegurar dichos datos, con el fin de evitar los fraudes que involucran tarjetas de pago de débito y crédito. Ayuda a comerciantes e instituciones financieras a comprender e implementar estándares para políticas de seguridad, tecnologías y procesos continuos que protegen sus sistemas de pago contra violaciones y robo de datos de titulares de tarjetas.

De este modo, las compañías que procesan, guardan o transmiten datos de tarjetas deben cumplir con el estándar PCI o arriesgan la pérdida de sus permisos para procesar las tarjetas de crédito y débito, enfrentar auditorías rigurosas o pagos de multas. Los datos del titular de la tarjeta deben ser ilegibles en cualquier lugar donde se almacenen o transmita mediante el uso de criptografía sólida (es decir, cifrado de disco) con procesos y procedimientos de administración de claves asociados.

IIROC [2], la **Organización Reguladora de la Industria de Inversiones de Canadá**, es una organización nacional autorregulada, establecida en el año 2008, que supervisa a todos los operadores de inversión y las actividades comerciales en los mercados de deuda y capital en Canadá. Su objetivo es mantener mercados justos y ordenados y regular todo el comercio relacionado con valores dentro del país. La disposición requiere proteger la información del cliente, que

[1] PCI (industria de tarjetas de pago) Normas de seguridad de datos disponible en https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

[2] Investment Industry Regulatory Organization of Canada (IIROC) https://www.iiroc.ca/Pages/default.aspx

puede incluir el cifrado de dichos datos, protegiendo aún más las claves de cifrado para garantizar la confidencialidad de la información del cliente.

La **FCA ("Financial Conduct Authority")**[1] es un organismo regulador de las firmas financieras que prestan servicios a los consumidores y mantiene la integridad de los mercados financieros en el Reino Unido; fundada el 1 de abril de 2013. Es uno de los organismos reguladores del sector financiero más respetados a nivel mundial y también de los más estrictos y exigentes. FCA también exige el cifrado de los datos del cliente en movimiento, en reposo y respaldado y el almacenamiento seguro, mediante la aplicación de medidas de seguridad de vanguardia.

2.2. Informática Forense

2.2.1. Introducción a la Informática Forense

En primer lugar, es importante explicar que se entiende por **evidencia digital**. De manera general se la conoce como la prueba electrónica, y en su acepción dentro del ámbito probatorio, puede ser considerada como cualquier información almacenada o transmitida en forma digital, la cual podrá utilizarse en un juicio. Eoghan Casey[2] define a la misma como "cualquier dato que puede establecer que un crimen se ha ejecutado o puede proporcionar un enlace entre un crimen y su víctima o un crimen y su autor". Luego especifica que la misma es un "tipo de evidencia física construida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales" (Casey, 2011). Las evidencias digitales son aquellas extraídas de un medio informático, y de igual manera se pueden utilizar como evidencia en un juicio. Se entiende como evidencia digital a los datos almacenados o transmitidos usando tecnología informática que sirva de soporte para la construcción de un caso a investigar.

[1] FCA ("Financial Conduct Authority") consultar información en el enlace https://www.fca.org.uk/

[2] Eoghan Casey es un estadounidense experto en informática forense, investigador y autor, que ha llevado a cabo una amplia gama de investigaciones digitales, incluyendo las violaciones de datos, fraude, delitos violentos, robo de identidad y la actividad criminal en línea.

Si se lleva la Ciencia Forense al plano de los sistemas informáticos, entonces se habla de **Análisis Forense Digital o Informática Forense**. La misma hace su aparición como una disciplina criminalística auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar al proceso. La misma tiene como objeto la investigación de hechos con relevancia jurídica o para la simple investigación privada en sistemas informáticos y desarrolla técnicas idóneas para ubicar, reproducir y analizar evidencias digitales con fines legales. Esta disciplina se aplica tanto en la investigación de delitos tradicionales (homicidios, fraude financiero, narcotráfico, terrorismo, etc.), como en los propiamente relacionados con las tecnologías de la información y las comunicaciones, entre los que destacan la piratería de software y comunicaciones, la distribución de pornografía infantil, el robo de identidad, las intrusiones y el "hacking"[1] en organizaciones, entre otros (López Delgado, 2007).

La **informática forense** es un conjunto multidisciplinario de teorías, técnicas y métodos de análisis que brindan soporte conceptual y procedimental a la investigación de la prueba indiciaria informática. Podemos decir que "La informática forense es un método probatorio consistente en la revisión científica, tecnológica y técnica, con fines periciales, de una colección de evidencias digitalizadas para fines de investigación o legales" (Darahuge & Arellano González, Manual de Informática Forense, 2011; p.9).

Según el Instituto Nacional de Ciberseguridad INCIBE[2], la informática forense es "El proceso de investigación de los sistemas de información para detectar toda evidencia que pueda ser presentada como medio de prueba fehaciente para la resolución de un litigo dentro de un procedimiento judicial".

El **perito judicial o perito forense** es un profesional dotado de conocimientos especializados y reconocidos, a través de sus estudios superiores, que suministra información u opinión fundada a los tribunales de justicia sobre los **puntos**

[1] Hacking: es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de estos y los mecanismos para protegerse de aquellos que saben hacerlo.

[2] El Instituto Nacional de Ciberseguridad (INCIBE) es un organismo dependiente del Ministerio de Economía y Empresa de España través de la Secretaría de Estado para el Avance Digital. Tiene su sede oficial en la ciudad de León (España). Es la entidad de referencia en el desarrollo de la ciberseguridad y la confianza digital de ciudadanos y empresas, especialmente aquellas que gestionan infraestructuras críticas.

litigiosos o de pericia que son materia de su dictamen. El perito decodifica cierta información (sea por ejemplo un ADN o evidencia digital) y la recodifica para su presentación ante el juez de manera comprensible. Es un especialista, conocedor de su ciencia, que debe aplicar su conocimiento en un ámbito judicial, con el fin de aportar información que, de acuerdo con los principios de la criminalística, contribuyan al esclarecimiento o prueba de los hechos.

El perito judicial debe entregar un **dictamen pericial** en donde debe producir una explicación consistente para cada **punto pericial** propuesto, con términos técnicos-científicos y concluyendo de una manera clara que pueda ser comprendida por quien lo lee y no es idóneo en la materia.

Existen dos tipos de peritos, los nombrados judicialmente **de oficio** y los propuestos por una o ambas **partes** (y luego aceptados por el juez o el fiscal). Los peritos judiciales o forenses en todas sus especialidades actúan frente a la autoridad judicial que ha solicitado sus servicios, como testigos idóneos fedatarios, ejecutando tareas técnicas específicas en base a los conocimientos científicos y experiencia propios del área, dejando de lado cualquier tipo de prejuicio u opinión en torno al caso de estudio. Los **peritos oficiales** actúan en nombre de una institución como funcionarios públicos cumpliendo con la totalidad de la legislación que regulan dicha figura (ejemplo Policía, Gendarmería, etc.).

El **perito informático forense** es un perito judicial involucrado en procesos en los que los hechos controvertidos están relacionados directamente con bienes y servicios informáticos (Dupuy & Kiefer, 2017).

Es importante aclarar que la informática forense es aplicable tanto **en casos judicializados como en investigaciones particulares solicitadas por empresas u organismos**, en estos últimos casos los peritos de parte pueden actuar como **consultores o asesores técnico-forenses**. De todas formas, cada caso debe ser tratado como si fuera a juicio, de esta manera cualquier investigación en informática forense podría presentar evidencias digitales admisibles en un proceso judicial.

Según el FBI[1], "la **informática forense** es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional". Por lo tanto la **informática forense** abarca desde la identificación, preservación, adquisición, procesamiento, análisis, documentación, hasta la presentación de la evidencia digital.

El principal objetivo de la misma es la recolección de la evidencia para la persecución y procesamiento judicial de los delincuentes. Son tres los **requisitos básicos que deben cumplir los investigadores forenses en informática** respecto a sus métodos de trabajo: (1) Utilizar medios forenses estériles (para obtener copias de información no contaminadas) (2) Mantenimiento y control de la integridad del medio original (3) Etiquetar, controlar y transmitir adecuadamente las copias de los datos, impresiones y resultado de la investigación.

Sintetizando, se puede afirmar que "la informática forense es la informática como la medicina legal es la medicina". (Darahuge & Arellano González, Manual de Informática Forense, 2011, p.16).

En definitiva, puede ser utilizada tanto en los distintos fueros judiciales, como en la labor diaria de organismos oficiales o privados y hasta en ámbitos particulares o personales.

Las legislaciones relacionadas a la admisibilidad de la **evidencia digital** fundan sus parámetros en cuatro conceptos: (Heredia, 2011)

1) **Autenticidad**: Es la característica que resalta la no alterabilidad de los medios originales en la escena del posible delito.
2) **Confiabilidad**: Establece si efectivamente los medios probatorios aportados provienen de fuentes creíbles y verificables. La misma está en función de la manera en que se sincronice el registro de las acciones efectuadas por los peritos y un registro íntegro de los mismos.
3) **Suficiencia**: Se refiere a la presencia de toda la evidencia necesaria para adelantar el caso.
4) **Conformidad**: Los medios de prueba, que son regulados por el Nuevo Código Procesal Civil y Penal, sólo se valorarán y producirán si los mismos han sido

[1] FBI: Siglas en Inglés de la Agencia Federal de Investigación "Federal Bureau of Investigation", es la principal rama de investigación criminal del Departamento de Justicia de los Estados Unidos.

obtenidos e incorporados al proceso por un procedimiento constitucionalmente legítimo.

Actualmente existen grandes **debates** entre juristas y expertos técnicos en cuanto a las exigencias de la evidencia informática para que la misma pueda aceptarse como prueba en un proceso legal. Cada día hay más leyes y normativas que regulan las actividades relacionadas con la informática y el uso (o mal uso) que se hace de ella. Muchas de estas leyes obligan a las empresas u organizaciones a conservar una serie de datos relacionados con la utilización que se hace de la información contenida en los sistemas informáticos (registros de actividad o auditorías), los cuales podrían ser de gran utilidad para los investigadores forenses. Sin embargo, se plantea la disyuntiva del valor probatorio de los mismos. Es destacable la ambigüedad existente en el valor de las pruebas informáticas desde el punto de vista pericial, lo cual ocasiona gran incertidumbre desde el punto de vista jurídico. (López Delgado, 2007)

A la hora de realizar un análisis forense es fundamental tener presente el **principio de intercambio de Locard**[1], el cuál sentó las bases de la ciencia forense, y que expresa lo siguiente “siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto”. Esto significa que cualquier tipo de delito, incluidos los relacionados con informática, dejan un rastro por lo que mediante el proceso de análisis forense se pueden obtener evidencias digitales válidas.

La **informática forense** implica un trabajo detallado, minucioso, que debe realizarse con mucho cuidado en cada uno de los pasos a ejecutar desde el momento de la adquisición de la evidencia hasta la redacción del informe y la ratificación en el juicio. Considerando que **una pericia nunca es igual a otra**, aunque puedan existir actividades o situaciones comunes, siempre va a aparecer alguna diferencia que la haga única. En este sentido es muy importante la capacitación y la investigación continua de los peritos informáticos, considerando el gran abanico de tecnologías y escenarios que hacen de esta ciencia un infinito de posibilidades e investigación constante.

[1] Edmon Locard fue un criminalista francés, considerado uno de los principales pioneros en el tema. Es famoso por enunciar el conocido "Principio de intercambio de Locard".

En la rama judicial no existe un estudio o especialización para que los profesionales de la misma obtengan los conocimientos necesarios para la interpretación técnica, por tal motivo es necesario que los peritos informáticos forenses puedan realizar informes a modo de que se puedan entender los resultados obtenidos en un proceso judicial. (Cano, 2016)

Es necesario mantener un conocimiento detallado no solo de procedimientos, técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del hecho, sino también, de las normas y regulaciones legales asociadas con las pruebas y el derecho procesal. (Cano, 2016, p22).

Además, un especialista en informática forense requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido. El conocimiento del informático forense abarca el conocimiento no solamente del software sino también de hardware, redes, seguridad, base de datos, etc.

Una tarea crítica y primordial en el trabajo forense es la **cadena de custodia**. Es un proceso mediante el cual se conserva la integridad tanto física como lógica de las evidencias. La misma corresponde al registro de identificación cronológica del movimiento y manejo de evidencia potencial. Si la misma no existiese automáticamente causa la invalidez de la prueba. Consiste en un informe detallado que documenta la manipulación y el acceso a las pruebas objeto de la investigación. La información contenida en este informe debe ser conservada adecuadamente y mostrar los datos específicos, en particular todos los accesos con fecha y hora determinada. (Marqués Arpa & Serra Ruiz, 2014)

La cadena de custodia permite asegurar la **confiabilidad** de la información recolectada y registrar la **trazabilidad** exacta de la misma, es decir, saber en todo momento, en qué lugar está la prueba, desde su detección, hasta su disposición final. Es un componente fundamental que asegura que la evidencia digital recolectada se pueda seguir metodológica y procesalmente, en todo momento, registrando incluso bajo **responsabilidad** de quién está en cada momento, ya que cada vez que intervienen nuevas personas u organismos, también cambia el responsable que la recibe e interactúa con la misma. Con estos registros, si la evidencia es adulterada en algún punto, es posible saber quién debía protegerla

en ese momento. Es importante considerar que la cadena de custodia no asegura la legalidad o legitimidad, ni tampoco protege por sí misma al derecho a la privacidad.

Aunque la evidencia puede ser legítima o admisible, cuando el perito está presentando sus resultados en un juicio, las preguntas acerca de las habilidades del perito informático y conocimiento pueden afectar su credibilidad, así como la confiabilidad del proceso empleado. El no poder explicar, competentemente y con precisión, la aplicación de un proceso o procesos puede producir cuestionamientos sobre el conocimiento y credibilidad del perito. Básicamente, **las pericias complejas deben ser realizadas por personal calificado y experimentado que posea un apropiado nivel de conocimientos y entrenamiento**. Dado que la tecnología está avanzando continuamente, es importante que el perito o investigador forense reciba entrenamiento continuo.

El principal objetivo es evitar la contaminación o la recolección ilícita de la evidencia digital. La "Doctrina del fruto del árbol envenenado", acuñada por la Corte Norteamericana[1], hace referencia a las pruebas obtenidas de manera ilícita, las cuales impedirán posteriormente ser utilizadas en un proceso judicial, desestimando cualquier medio probatorio obtenido por vías ilegítimas. La teoría se refiere a que si la fuente de la prueba (el árbol) se corrompe, entonces cualquier cosa que se gana de él (el fruto), también lo está. En la metáfora legal, en este caso, las pruebas contaminadas son la fruta y la adquisición de evidencia ilegítima u obtención ilícita son el árbol envenenado. Cualquier prueba obtenida por medios ilegales resulta contaminada, como también todas las pruebas que puedan desprenderse de la misma, por la ilegalidad de la primera, así la ilicitud de la obtención de la prueba se transmite a las pruebas derivadas o relacionadas, que son igualmente excluidas del proceso.

En el libro el Rastro Digital (Di Iorio A. H., 2016, p53). se define la **Criminalística** "como la ciencia aplicada, que, mediante el empleo del método científico, técnicas y conocimientos aportados por otras disciplinas, busca y

[1] Carrió Alejandro, *Garantías Constitucionales en el Proceso Penal*, ob. cit., pág.162. Sobre la génesis de la expresión, relata este autor que su origen se remonta al caso "Silverthorne Lumber Co. Vs. United States", 251 US 385 (1920) en el que la Corte estadounidense decide que el Estado no puede intimar a una persona a que entregue documentación, cuya existencia es descubierta por la policía a través de un allanamiento ilegal.

estudia las evidencias materiales vinculadas con presuntos hechos delictivos, con el objeto de auxiliar a los órganos que lo procuran y administran justicia, brindándoles elementos reconstructores, identificadores y probatorios para que conozcan la verdad técnica e histórica de los hechos que investigan". Hoy no solo se buscan huellas físicas, sino digitales. De la pronta adaptación y capacidad de respuesta que tenga la justicia con el auxilio de la criminalística dependerá la calidad de las respuestas frente a estos nuevos desafíos. El doctor Rodríguez Manzanera [1] enuncia la criminalística como el conjunto de conocimientos aplicables a la búsqueda, descubrimiento y verificación científica de un delito en particular y del presunto responsable de éste. **Tales definiciones posibilitan la integración de la Informática Forense al campo de la Criminalística**, siendo que la misma no se limita al campo de las Ciencias Naturales, auxiliando a expertos ante el desafío de decidir cuáles evidencias buscar, dónde y cómo hacerlo, y de qué modo analizar las evidencias. (Di Iorio A. H., 2016, p.52-54)

En lo que hace a la informática forense y los principios criminalísticos, la "escena del hecho" puede llegar a estar distribuida en diferentes lugares físicos, constituyendo entre todos ellos una "escena virtual".

La recolección puede efectuarse en un **allanamiento o prueba anticipada** o dentro de un proceso normal, pudiéndose efectuar de manera **local o remota**, según la naturaleza y ubicación de la evidencia y de forma **visible o encubierta**, según el tipo de investigación y con las **autorizaciones judiciales pertinentes**. El análisis de evidencia es el corazón de la pericia informática y está constituido por el conjunto de tareas a realizar a los efectos de analizar el contenido de la evidencia digital para confirmar o refutar una situación que se plantea (Presman, Gustavo; ADC Por los Derechos Civiles, 2018).

Si bien es recomendable no acceder al contenido de los equipos encendidos que contienen la evidencia digital para evitar su contaminación, existen ciertas ocasiones donde se requiere acceder al equipo en vivo con previa autorización del juez y sólo sobre aquellos aspectos de la investigación que han sido indicados. Lo mismo sucede si se necesita recolectar la prueba digital mediante el uso de criterios superficiales, a fin de identificar potenciales elementos relevantes

[1] Rodríguez Manzanera, L. (1976). Manual de introducción a las Ciencias Penales, Cap. La Criminología. Secretaría de Gobernación, México, D.F. p.389.

para la investigación antes de, por ejemplo, secuestrar todos los equipos (a este procedimiento se lo denomina "**Triage**"). (Presman, Gustavo; ADC Por los Derechos Civiles, 2018).

Asimismo, es importante considerar los escenarios donde se necesite obtener una **prueba anticipada,** es decir, la producción de prueba pericial antes de la presentación de una demanda, sin intervención judicial (en general se aplica en casos donde pudiera resultar imposible o muy dificultosa recolectar la evidencia digital pasado un tiempo). También pueden acontecer escenarios de **preconstitución de prueba**, donde la actuación del perito es protocolizada por un escribano para dar fecha cierta de los hechos constatados, dar fe de las operaciones que efectúe un perito ante él, asegurar y depositar elementos de prueba.

2.2.2. La Evidencia Digital

La **evidencia digital** es un término utilizado de manera amplia para describir "cualquier registro generado por o almacenado en un sistema computacional" (Committee IT/012, 2003).

La evidencia digital es cualquier dato o registro de información procesada electrónicamente, almacenada y/o transmitida por una computadora o dispositivo electrónico, que sujeto a intervención humana, electrónica y/o informática es extraída de un medio tecnológico informático, pudiendo ser de valor para una investigación o caso judicial en curso. De esta manera, ciertos datos o evidencias tendrán simplemente el valor de **pistas** para seguir avanzando en el esclarecimiento de los hechos, mientras que otras evidencias y su decodificación técnica tendrán valor como **prueba** ante un tribunal de justicia.

Se define a la **evidencia digital** como el conjunto de datos o información en formato binario, como por ejemplo archivos, capturas de tráfico o conexiones de red, imágenes de discos o tarjetas, o memoria volátil del sistema atacado, entre otros. En otras palabras, es todo aquel elemento que pueda almacenar información de forma física o lógica que puede llegar a ayudar a esclarecer un caso. Como ejemplos se puede citar un archivo de fotografía en un celular, un

archivo de video de una cámara de seguridad, una línea de texto en un log de transacciones, el registro de acceso a un sitio web, datos en el registro de auditoría de una aplicación, datos de una ocurrencia en los registros de eventos del sistema, un mensaje de texto, un correo electrónico, etc. No solo el contenido visible de un archivo es evidencia digital, sino también los metadatos del mismo.

En el marco procesal, una evidencia requiere su adecuada preservación, análisis y presentación para transformarse en fuente de indicios. Son los testigos o los expertos quienes hacen "hablar" a las evidencias dotándolas de un valor indiciario (Di Iorio, Castellote & Bruno, 2017, p79).

La evidencia digital puede ser dividida en tres **categorías**: (Cano, 2016, p21)

1. Registros almacenados en el equipo de tecnología informática (documentos, imágenes, correos electrónicos, archivos de aplicaciones, grabaciones, etc.).
2. Registros generados por los equipos de tecnología informática (registros de auditorías, registros de transacciones, registros de eventos, registros varios de logs, etc.).
3. Registros que parcialmente han sido generados y almacenados en los equipos de la tecnología informática (vistas parciales de datos, consultas en base de datos, acceso a redes, etc.).

La evidencia digital presenta **particularidades** que la diferencian de las restantes clases de evidencia física. Las características propias de la misma, advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de informática forense. La evidencia es volátil (puede desaparecer), es anónima, duplicable (de manera exacta), frágil (es alterable, modificable y eliminable). (Cano, 2016, p22)

Las evidencias pueden cumplir **dos funciones, orientadora o probatoria**. La función **orientadora** es cuando la evidencia proporciona una pista que permite avanzar en una investigación, donde la pista por sí misma no acredita el hecho investigado (por ejemplo, una dirección IP asociada a un domicilio real). La función **probatoria** es cuando la evidencia puede ser invocada como prueba de los hechos que afirma una de las partes del proceso (por ejemplo un archivo de video donde se puede visualizar el momento del crimen).

Al pretender emplear la evidencia digital como probatoria, la misma debe poseer **cuatro características esenciales para su admisibilidad** en un proceso judicial: **relevancia, suficiencia, validez legal y confiabilidad** (Di Iorio A. H., 2016, p10).

La **relevancia** de la evidencia digital se basa en el principio de criterio de selección de misma. La evidencia debe ser útil a la investigación en curso y a los puntos probatorios o de pericia del caso concreto, sin ser sobreabundante o superflua (art. 338 CPP).

La **suficiencia** implica que las evidencias digitales deben ser suficientes a los fines investigativos o en respuesta a los puntos de pericias para que puedan ser ofrecidas como pruebas ante un tribunal.

Para garantizar la admisibilidad de la evidencia debe haber sido obtenida respetando las garantías y formas legales y así poder tener **validez legal**. Cumpliendo con las disposiciones legales y reglamentarias de actuación, sin adoptar decisiones o acciones que afecten a los derechos fundamentales sin previa autorización judicial o ajenas al área de incumbencia.

El proceso de tratamiento de la evidencia digital debe cumplir con ciertos requisitos de **confiabilidad** en los procedimientos aplicados para garantizar la confiabilidad de la evidencia: a) **Justificable** (justificación de todos los métodos y acciones realizadas en el manejo de la evidencia digital); b) **Auditable** (documentación de todas las acciones sobre la misma); c) **Repetible** (obtener los mismos resultados si se aplica el mismo procedimiento, con las mismas herramientas, en las mismas condiciones, en cualquier momento); d) **Reproducible** (se deben obtener los mismos resultados si se aplica el mismo procedimiento, con herramientas distintas, en condiciones distintas, en cualquier momento y sin restricciones). La confiabilidad de la evidencia digital como prueba está dada por aspectos básicos en cómo se obtuvo, cómo se preserva y quién la realizó.

Cualquier especialista externo, consultor o perito de parte puede ser capaz de evaluar el proceso y determinar si se ha aplicado una metodología, técnica o proceso adecuado.

Con la finalidad de no perder la admisibilidad de la evidencia digital es importante considerar una serie de **pautas generales para el tratamiento de la evidencia digital**. (Airala & Rapetti, 2007)

Es esencial **minimizar el contacto con la evidencia digital original** de manera de preservarla debidamente para la presentación en un juzgado. La evidencia digital es sumamente frágil, el simple hecho de acceder a un archivo modificaría la última fecha de acceso del mismo. Por tal motivo debe tomarse los recaudos necesarios desde el primer contacto con la evidencia digital, realizando la recolección de la manera óptima, eficiente, profesional, preservando la evidencia sin contaminarla, para evitar que se impugne la evidencia más adelante o se pierda información por no haber preservado de manera correcta un dispositivo. Se deben aplicar todas las técnicas necesarias para mantener la inalterabilidad de la evidencia digital.

Otra pauta esencia es **duplicar la evidencia digital y no sobre la original**. A la evidencia se la puede duplicar de manera exacta obteniendo una copia perfecta del original. El trabajo sobre la evidencia digital duplicada asegura que la original no será alterada en caso de un uso incorrecto o inapropiado del proceso forense que se aplique, ya que, si los datos en la evidencia digital duplicada se alteran o se destruyen, se puede recurrir a otra copia. Además, disponer de un duplicado posibilita al perito aplicar diferentes técnicas o herramientas para lograr el mejor resultado y permite el trabajo en paralelo de varios especialistas de informática forense sobre los mismos datos, o en partes de los datos, optimizando tiempos y recursos. Trabajar con una copia exacta de los datos facilita llegar a conclusiones más completas en el análisis forense, ya que no existe el riesgo en su manipulación ni la limitación de acciones por temor a alterar la evidencia digital original.

En los casos que sea realmente necesario e inevitable, **justificar y pedir autorización para acceder a la evidencia digital original.** El acceso a la evidencia original debe ser realizado por un especialista competente y con la capacidad de justificar y atestiguar las implicaciones de las acciones. Con el mismo criterio **justificar, advertir y pedir autorización para cualquier acción que pudiera implicar alteración de la evidencia digital original.** Cualquier acción que implique o pudiera implicar una alteración física o lógica irreversible de

la evidencia digital original debe ser previamente informada, obtener la debida autorización judicial y ser documentada completamente. El perito debe ser capaz de identificar correctamente la magnitud de cualquier cambio y dar una explicación detallada del por qué era necesario o inevitable el mismo.

Es obligatorio **conservar y mantener la cadena de custodia** de manera que las personas que realicen cada acción con la evidencia digital original se responsabilicen de lo actuado, y documentarlo en forma completa y fidedigna.

Es primordial el **uso de herramientas y técnicas adecuadas a cada caso,** asegurando que el uso las mismas no disminuya la admisibilidad de la evidencia, por ejemplo, por utilizar herramientas sin licencia o que se desconoce su funcionamiento.

De ningún modo **emprender un examen pericial más allá del nivel de conocimiento y habilidad que posea un perito**. Es esencial que el perito sea consciente del límite de su conocimiento y habilidad ya que abordar un examen más allá de las habilidades, es aumentar el riesgo de daño, incluso efectuando cambios de los cuales el examinador no es consciente o no entiende y por consiguiente puede ignorar, contaminando la evidencia digital.

El **método de presentación no debe alterar el significado de la evidencia.** Se debe presentar la información de una manera que sea tan representativa del original como sea posible. Hay que considerar que, tanto la evidencia digital como el dictamen pericial y el testimonio del perito son considerados elemento de material probatorio.

Todas las actividades y acciones sobre la evidencia digital en sus diferentes etapas **deben cumplir con las disposiciones legales y reglamentarias propias de la actuación del perito.** Cuando una acción implique injerencia en derechos fundamentales (como secuestro de dispositivos o análisis de datos personales), se deberá constatar la previa autorización judicial, sin adoptar decisiones o acciones que sean ajenas a la propia incumbencia.

Es necesario poder **describir los procesos empleados durante un examen correctamente y explicar la metodología seguida** para ese proceso brindando claridad al proceso.

Para poder **asegurar integridad de la evidencia digital de la evidencia**, se utiliza la **firma digital**[1] de la misma, la cual se aplica tanto a la evidencia digital en sí como a todo los informes y documentación presentada. Se denomina firma digital a la cadena alfanumérica de longitud fija que se obtiene tras aplicar un algoritmo matemático de Hash[2] a un archivo (o valor de entrada). Este valor del hash identifica inequívocamente al archivo, asegurando que, ante cualquier variación del contenido de la misma, si se vuelve a aplicar el algoritmo de hash, el valor que lo identifica se vería modificado, por lo cual se deduciría una manipulación de la evidencia original. A estas funciones también se las conoce como funciones resumen y se caracterizan por ser irreversibles (dado un valor de hash no se puede computar o deducir el valor original que dieron lugar al mismo) y deterministas (las mismas entradas dan siempre las mismas salidas).

La evidencia digital puede convertirse en un factor fundamental dentro de un proceso judicial, aunque en general puede tener dificultades para ser llevada a los altos tribunales, ya que no es tan impactante un registro digital que evidencia un cambio malicioso sobre un dato como la huella digital sobre un arma de fuego. No puede omitirse que en la actualidad dicha evidencia sigue siendo frágil y volátil, pues la información que reside en los medios electrónicos de almacenamiento está expuesta a ser borrada, modificada o eliminada sin dejar rastros y, por lo tanto, puede tornarse en una desventaja para el sistema judicial que no tenga los mecanismos adecuados para su efectivo desarrollo. (Darahuge & Arellano González, Manual de Informática Forense III, 2016)

2.2.3. Los Peritos Forenses

Lo **peritos forenses** deben estar capacitados en la técnica pericial específica, en la metodología a seguir y en la legislación vigente actualizada. Las buenas

[1] La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales. Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje. La firma digital no implica asegurar la confidencialidad del mensaje; un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma holográficamente.

[2] El algoritmo de hash es un algoritmo matemático irreversible que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud. Ejemplos de algoritmos Hash más usados son el MD5, SHA1, SHA2.

prácticas del perito y la realización de una investigación conforme al derecho influyen drásticamente para que la investigación sea admitida y sea eficaz en un juicio. La práctica pericial debe respetar los medios de prueba admitidos en derecho y la jurisdicción y competencia de los jueces y tribunales dónde deba desarrollarse la práctica tecnológica. (Vila Avendaño, 2018, p18-19)

El **perito informático forense** es un perito forense involucrado en procesos en los que los hechos controvertidos están relacionados directamente con bienes y servicios informáticos, pudiendo cumplir el rol de perito de oficio o de parte.

El **perito de oficio** es un auxiliar de la justicia, que debe estar inscriptos en la Corte de Justicia, para lo cual debe disponer de un título habilitante de su especialidad. Se reunirá con las partes en casos que sea necesario y en los cuales se precise realizar las tareas periciales frente a las mismas.

El **perito de parte** es un perito designado por alguna de las partes como auxiliar de la parte que lo convoca (y luego aceptados por el juez o el fiscal), y junto con el perito de oficio ambos ejercen influencia en el juicio. Pueden ser convocados para presentar informes periciales propios, analizar los informes presentados por la otra parte, o incluso con fines de asesoramiento general.

Los **peritos oficiales** actúan en nombre de una institución sea Policía, Gendarmería, entre otras. Como funcionarios públicos deben cumplir con la totalidad de la legislación que regulan dicha figura (Ley de Ética Pública, Ley de administración financiera y de los sistemas de control del sector público nacional, Código de Ética de la función pública, etc.). No es necesario que posean título habilitante de la especialidad.

2.2.4. Tipos de Datos

Dependiendo los tipos de casos a peritar, aparecen distintos tipos de datos a analizar (Vila Avendaño, 2018):

1. **Datos volátiles**: datos en la memoria del sistema de dispositivos encendidos, que pueden perderse al ser reiniciados o apagados los mismos. Estos datos cambian o se pierden con facilidad. Son en general datos contenidos en la

memoria RAM[1] ("Random Access Memory", memoria de acceso aleatorio, donde se vuelvan los procesos a ejecutar por el microprocesador) o en memoria caché[2] (memoria utilizada por el microprocesador para reducir el tiempo de acceso a datos ubicados en la memoria principal que se utilizan con más frecuencia y así las solicitudes futuras a esos datos se puedan atender con mayor rapidez). También se encuentran alojados en tablas de enrutamiento[3], procesos en ejecución, etc. Usualmente son datos asociados a fecha y hora del sistema, servicios y procesos en ejecución, lista de usuarios autenticados o que han iniciado sesión en el equipo, claves de acceso, archivos en uso, aplicaciones en ejecución, procesos de memoria, contenido del portapapeles, archivos temporales, archivos de registros, contenidos de la caché, archivos ocultos, estado de las conexiones de red, puertos de red abiertos, información o datos almacenados remotamente, como también indicios de presencia de malwares, datos cifrados, conexiones activas, entre otros.

2. **Datos no volátiles**: datos persistentes, es decir, que se mantienen después que los equipos son apagados, que se encuentran en general en discos rígidos u otros dispositivos de almacenamiento persistentes removibles, como dispositivos USB, tarjetas de memoria SIM[4], CD-ROM, unidades de disco duro externas, etc. Estos datos en general corresponden a datos contenidos en archivos, documentos, logs, directorios, datos de aplicaciones instaladas, etc.
3. **Datos transitorios**: datos transitorios en la memoria o caché.

---

[1] En la RAM se cargan todas las instrucciones que ejecuta la unidad central de procesamiento (procesador) y otras unidades de las computadora o dispositivos electrónicos, además de contener los datos que manipulan los distintos programas. Se denominan de acceso aleatorio porque se puede leer o escribir en una posición de memoria con un tiempo de espera igual para cualquier posición, no siendo necesario seguir un orden para acceder (acceso secuencial) a la información de la manera más rápida posible.

[2] La caché es una memoria que se sitúa entre la unidad central de procesamiento (CPU) y la memoria de acceso aleatorio (RAM) para acelerar el intercambio de datos. Cuando se accede por primera vez a un dato, se hace una copia en la caché; los accesos siguientes se realizan a dicha copia, haciendo que sea menor el tiempo de acceso medio al dato. Cuando el microprocesador necesita leer o escribir en una ubicación en memoria principal, primero verifica si una copia de los datos está en la caché; si es así, el microprocesador de inmediato lee o escribe en la memoria caché, que es mucho más rápido que de la lectura o la escritura a la memoria principal.

[3] Una tabla de enrutamiento es un archivo de datos en la RAM que se usa para almacenar la información de rutas para redes remotas y redes conectadas directamente.

[4] SIM: Tarjeta inteligente comúnmente utilizada en telefonía móvil (en sus siglas en inglés, "Subscriber Identity Module").

4. **Datos temporales**: archivos de naturaleza temporal.

El orden de volatibilidad de la evidencia se basa en la susceptibilidad al cambio. Se debe recolectar primero los datos que sean más susceptibles al cambio o con posibilidad que se pierdan.

La recolección de datos volátiles contribuye de manera significativa a muchas investigaciones forenses siempre y cuando dichos datos estén disponibles para la captura y análisis. Permiten recuperar información que no se almacena en discos duros o medios persistentes, como ser procesos que evidencian qué aplicaciones se estaban ejecutando (las cuales podrían ser programas maliciosos que los atacantes utilicen solo en memoria) o abordar los problemas que las nuevas tecnologías como el cifrado pueden causar durante el curso de un análisis en frío o tradicional.

2.2.5. Escenarios de Adquisición de Datos

La adquisición de datos desde la fuentes de evidencia digital se realiza mediante la técnica de **clonación forense**, la cual consiste en una copia idéntica del medio de almacenamiento, bit a bit, para evitar alterar la muestra original a analizar.

En este sentido es importante aclarar los siguientes conceptos:

- Una **imagen o clonación forense** es una copia exacta, sector por sector, bit a bit, de un medio de almacenamiento. El resultado final de esta imagen es un archivo conteniendo una copia exacta del dispositivo de origen, el cual puede tener diferentes formatos, donde la extensión del archivo es la manera más viable de indicar su formato (algunos formatos como ".DD", son open source o de fuente abierta, mientras otros como ".E01"[1] son propietarios.). De esta manera, es posible trabajar con la imagen como si se hiciera sobre el original.
- Una **copia forense** que es una copia a nivel de sistema de archivos, de uno o varios archivos que constituyen la evidencia lógica. Es un vuelco de los

[1] Los productos "EnCase Forensics de Guidance Software" utilizan un formato cerrado para las imágenes forenses .E01. Este formato puede contener información del caso y comprimirse, entre otros aspectos.

archivos sin almacenar ciertos datos como los sectores o información interna de los medios de almacenamiento.

Los escenarios periciales de adquisición de datos pueden tener infinitas variantes considerando el universo tan cambiante y dinámico de las tecnologías de computación y comunicaciones. En forma general se pueden determinar los escenarios según el estado de encendido del equipo, el tipo de dispositivo y la ubicación de los datos.

Según el estado de encendido del dispositivo

1) **Adquisición de sistemas apagados (análisis en frío)**

- En esta adquisición es más simple evitar la alteración de las evidencias del sistema ya que solo se recopila información persistente. Se basa en la adquisición de datos no volátiles.
- Los escenarios posibles van desde equipos apagados, de los cuales se pueden retirar los dispositivos de almacenamiento involucrados y se dispone de adaptadores necesarios y capacidad de almacenamiento para el clonado, hasta equipo apagados de los cuales no se le pueden retirar los dispositivos de almacenamiento involucrados y se debe evaluar conectar el dispositivo de almacenamiento al dispositivo a peritar o ejecutar un clonado a través de la red. También incluyen los medios de almacenamiento removibles.
- Ventajas:
  - Permite efectuar una imagen física del medio (copia bit a bit).
- Desventajas:
  - No se pueden recolectar datos volátiles.
  - No es posible efectuar el análisis de un dispositivo que se encuentra encriptado y para el cual no se conoce la clave.

2) **Adquisición de sistemas encendidos (análisis en caliente o en vivo)**

- La adquisición en vivo se realiza principalmente para recolectar información de datos volátiles, aunque también se aplica a datos no volátiles.
- Los escenarios posibles van desde análisis en vivo de sistemas que sí pueden ser copiados o se puede obtener una imagen de los mismos, donde es

recomendable utilizar luego máquinas virtuales para emular el entorno adquirido y lograr un entorno fiel a la realidad a analizar. Como también análisis en vivo de sistemas que no pueden ser copiados ni se puede hacer una imagen forense debiendo interactuar directamente con ellos.

- En el casos de datos volátiles, además del volcado de memoria principal se recomienda, por ejemplo, descargar también los archivos de paginación e hibernación de la computadora para contar con más información al momento del análisis, entre otros de interés según el caso o tecnología.
- Ventajas:
  - Adquirir datos volátiles.
  - Permite efectuar la adquisición o análisis de información de equipos que no pueden ser apagados (ejemplo: servidores críticos).
  - Permite obtener información descifrada de dispositivos móviles o volúmenes cifrados evitando la necesidad o incluso la imposibilidad de desencriptar la información a posterior (por ejemplo, a un volumen cifrado que está montado descifrado sobre una máquina encendida, se le puede aplicar una recolección en vivo en estado descifrado, y de este modo hacer una copia forense de la información en plano de un disco cifrado del cual no se tiene la contraseña).
- Desventajas:
  - Existe grandes riesgos de contaminar el sistema de manera accidental o involuntaria ya que las herramientas y comandos pueden cambiar las fechas y horarios de acceso a los archivos, utilizar bibliotecas compartidas, desencadenar la ejecución de software malicioso (“malware”), forzar el reinicio del dispositivo, entre otros.
  - La manipulación del equipo encendido genera cambios o modificaciones controladas.
  - El proceso es más lento que la adquisición en sistemas apagados. Es necesario encontrarse en el sitio para efectuar la adquisición.
  - Si el equipo se encuentra expuesto a ataques desde el exterior, puede que las evidencias se alteren en una adquisición en caliente.

Según el tipo de equipo o dispositivo

1) **Adquisición de datos en almacenamientos masivo**, los cuales pueden ser internos o externos a los dispositivos y varían de tecnologías desde unidades de discos duro HDD (en inglés: "hard disk drive"), unidades de estado sólido SSD (en inglés: "solid state drive"), USB, CD-ROM, memorias SD SSD (en inglés: "secure digital"). Según las capacidades, configuraciones y estado de los mismos se debe evaluar si es necesario o posible hacer clonado. Se pueden encontrar discos cifrados e incluso en cifrado de discos en mal estado.
2) **Adquisición de datos en dispositivos móviles o celulares.**
3) **Adquisición de datos en cámaras de videograbación.**
4) **Adquisición de otros tipos de dispositivos, como ser TV inteligentes, etc.**

Según la ubicación de los datos

1) **Locales**, pudiendo ser sistemas, sitios web, base de datos instalados localmente en computadoras o servidores de una empresa**,** o datos locales almacenados en un dispositivo, entre otros.
2) **En la nube**, involucra base de datos, archivos y datos almacenados en la nube, pudiendo estar ubicados incluso en territorio extranjero.

2.2.6. La Prueba Anticipada y la Preconstitución de Prueba

La **prueba anticipada**, se refiere a la producción anticipada de actos periciales. Está constituida por aquel material relevado antes de la presentación de una demanda, sin intervención judicial; ya sea para ser utilizado en la demanda o para una instancia de negociación previa o extrajudicial (Darahuge & Arellano González, Manual de Informática Forense III , 2016). El objetivo de la prueba anticipada es la producción de prueba pericial que pudiera resultar imposible o muy dificultosa pasado un tiempo. Como también la exhibición, resguardo o secuestro de documentos concernientes al objeto de la pretensión.

La prueba anticipada surge ante la necesidad de congelar la realidad de la información en un momento dado, según la volatilidad y la fragilidad de la evidencia digital, fácilmente destruible o alterable con el fin de asegurar su sobrevida durante el proceso. Tiene como fin preservar la prueba, para ser

utilizada posteriormente en el proceso en función de los argumentos de cada una de las partes.

Cabe destacar que para su utilización posterior se requiere tomar los siguientes recaudos: 1) Recolectar información personal o pública. 2) La misma debe estar certificada ante escribano público. 3) Para la prueba informática, debe estar autenticada mediante un código confiable de digesto matemático o hash. 4) Su correspondiente cadena de custodia.

Aunque la recolección efectuada constituye un hecho definitivo y difícil de repetir, son provisionales, debido a que generalmente requieren una prueba de informes complementaria y/o prueba pericial. Son susceptibles de revisión, pero no deben modificarse durante su empleo judicial, ya que en dicha inalterabilidad se funda gran parte de su poder probatorio.

En muchas oportunidades la urgencia para preservar prueba informática no soporta siquiera los tiempos procesales de la prueba anticipada prevista por los códigos, por lo cual se recurre a la **Preconstitución de Prueba**, que es la actuación de perito protocolizada por un escribano para dar fecha cierta de los hechos constatados, dar fe de las operaciones que efectúe un perito ante él y asegurar y depositar elementos de prueba. Se debe considerar que el escribano no conoce de la especialidad informática ni de la metodología y las operaciones técnicas, por lo cual lo que certifica tiene ser considerado un indicio o documento relevante o genere convicción suficiente en el juez para tomar algún tipo de resolución. Brinda fundamento para hacer un reclamo judicial sobre una base objetiva.

2.2.7. La investigación forense

Los **argumentos judiciales** tienen tres componente: los **hechos invocados**, la **prueba aportada** para demostrar que esos hechos existieron y la **ley** aplicable a los hechos probados. Antes de llegar a litigar ante la justicia los hechos, la prueba y la ley deben estar integrados para resistir la argumentación de la otra parte. **Para llegar a poder presentar un caso viable es indispensable la investigación** para ayudar a conocer la verdad de los hechos y confirmar, o no, si

ocurrieron, si tienen carácter delictivo, si las evidencias o indicios obtenidos son suficientes para saber cómo ocurrieron los sucesos, si los sospechosos participaron del ilícito, si hay personas concretas involucradas, etc.

Según el curso de la investigación, las evidencias recolectadas y el esclarecimiento de los hechos pueden plantearse diferentes escenarios. Un Fiscal puede persuadir a las partes promoviendo acuerdos totales y parciales alternativos al juicio, se puede exigir o aconsejar la adopción de medidas que, si afectan derechos, deben ser requeridas al juez. También surgir la solicitud de medidas de algunas de las parte. Cuando no sea posible o legítimo arribar a acuerdos entonces interviene el juez o tribunal imparcial. Si en el curso de la investigación, no se recogieron o preservaron correctamente las pruebas necesarias para demostrar existosamente los hechos que se invocan ante el juez, el caso no está resuelto.

La investigación tiene como objetivo esclarecer los hechos investigando: qué conducta se produjo, por quién o quiénes, dónde, cuándo, cómo, mediante qué, por qué, para qué, a quiénes o a qué afectó. Mediante la labor investigativa se busca obtener pruebas. Los peritos aportan piezas de información significativas que constituyen insumos para el esclarecimiento de los hechos y las acciones posteriores.

2.2.8. Informática Forense en Base de Datos

Es importante entender la diferencia entre ***informática forense*** y la ***informática forense en base de datos***. El *forense de base de datos* enfoca su investigación específicamente en la base de datos en sí y el servidor que la contiene, es decir la capa de datos. No se incluye dentro del universo de su investigación el servidor de aplicaciones, el servidor web o las aplicaciones que interactúan con los usuarios. A continuación, se presenta una ilustración explicativa en la Figura 1: (Cano, 2016)

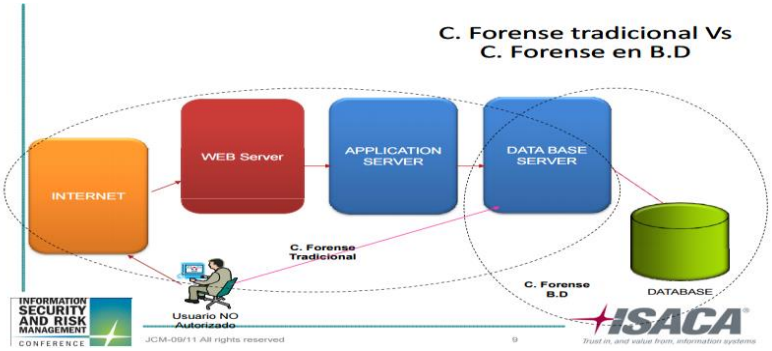

Figura 1: Esquema conceptual de ISACA

Jeimy J. Cano en su investigación afirma que las principales limitaciones actuales en *computación forense en base de datos* se deben a la dependencia de la misma con herramientas propias de cada sistema manejador de las bases, al elevado nivel de experiencia y conocimiento requerido sobre las mismas, a la alta probabilidad de modificación de datos en el proceso de extracción de los mismos y a la falta de un procedimiento estándar que apoye al análisis forense. Esto provoca que se generen dudas sobre la confiabilidad de las herramientas utilizadas y la validez de las pruebas obtenidas. En consecuencia, no se puede soslayar la incertidumbre que existe sobre el hecho de cuestionar si la información recogida es exacta, completa, clara, precisa, veraz y objetiva. (Cano, Computación Forense: Conceptos y reflexiones, 2011).

No existe a la fecha un procedimiento estándar específico para adelantar y apoyar el análisis forense sobre base de datos. Existen sólo estudios públicos detallados para Oracle y MS SQL Server. Incluso algunos SGBD disponen de herramientas o tecnologías que pueden utilizarse para análisis forense, pero no existe una metodología estándar de cómo utilizarlas con éxito para tal fin (Cano, Computación Forense: Conceptos y reflexiones, 2011).

Es relevante destacar el trabajo de tesis “Estado del arte de la aplicación de técnicas antiforense en bases de datos Oracle. Conceptos y retos para los informáticos forenses” (Ferro Rodriguez & Santiesteban, 2010) donde se plantea como trabajo futuro la necesidad del desarrollo de una “Herramienta general de análisis de fuentes de evidencia”.

Se resalta también el trabajo de tesis “Análisis de los principales sistemas de gestión de bases de datos ante ataques básicos” (Armendariz Perez, 2016) cuyo objetivo principal consistió en realizar una serie de ataques sobre cuatro de los gestores de bases de datos más conocidos (MySQL, PostgreSQL, Microsoft SQL Server y Oracle) y posteriormente analizarlos y ver si eran capaces de responder a las cuatro preguntas clave del análisis forense: qué, cómo, cuándo y quién ha realizado el ataque. Si bien este trabajo no estableció una metodología estándar para el análisis forense sobre base de datos, siendo su foco más que nada técnico y específico por cada SGBD, realiza una comparación muy interesante sobre la facilidad de obtener los datos y la calidad de los mismos procurando no utilizar herramientas de terceros, sino utilizando las propias herramientas de cada gestor. Plantea escenarios donde se aplican análisis forenses ante ataques internos y externos tanto sobre SGBD sin auditorías como con auditorías configuradas, comparando finalmente los resultados obtenidos en cada uno de los cuatros SGBD estudiados.

2.3. Marco Normativo y Metodológico

2.3.1. Aplicación práctica de las normas en las actuaciones periciales

Las normas y modelos enunciados a continuación son una referencia general de aplicación a la práctica forense informática nacional e internacional. Es preciso que los profesionales informáticos no solo cuenten con las capacidades y habilidades del ámbito del saber de su materia, sino que al momento de actuar en una práctica forense respeten los principios forenses, que se basan en una actuación metódica con los recaudos necesarios para evitar alterar la evidencia digital y mantener la debida cadena de custodia a lo largo de todo el proceso o en las etapas en que interviene.

No existen normas obligatorias o estrictas a aplicar en la práctica forense informática, pero si guías o referencias claras a tener en cuenta en el tratamiento de la evidencia digital en sus distintas instancias, cuyo objetivo es la preservación correcta e inalterable de la evidencia digital.

Es importante conocer los estándares, pero esto no implica que a través de los mismos se obtengan directrices o lineamientos para cada escenario a peritar, por lo que la profesionalidad y experiencia del perito es esencial para el éxito de la pericia. Si bien se plantean diferentes escenarios de actuación acompañados de buenas prácticas, en los casos reales cotidianos existen particularidades y no todas las recomendaciones son viables o aplicables, por lo que se ha de particularizar la actuación del perito según las características y circunstancias de la misma.

Por este motivo a la hora de llevar a cabo una actuación de captura de evidencias se debe tener en cuenta las características principales de la información que se desea recopilar, es decir, cuál es la naturaleza de la evidencia que se desea recopilar y el estado de la misma para determinar cuál es la mejor forma o vía de actuación que garantice el éxito de la misma. Para ello se debería elaborar un protocolo de actuación adecuado y "ad hoc" para cada caso específico (López Rivera, 2012).

Las variables por considerar a la hora de capturar la evidencia digital son: (López Rivera, 2012)

- Las características de la información: la información contenida, el formato de la información y el medio que contiene la información.
- Los estados de la información: almacenada estáticamente, almacenada dinámicamente en procesamiento, en tránsito, desplazamiento o en movimiento.

A continuación se detallan las normas nacionales e internacionales de mayor relevancia, que han sido de gran referencia al presente trabajo.

2.3.2. Norma ISO/IEC 27.037:2012 y vinculadas

Tal como define IRAM [1] una norma es un documento que establece, por consenso y con la aprobación de un organismo reconocido, reglas y criterios para usos comunes y repetidos. Es decir, establece las condiciones mínimas que debe reunir un producto o servicio para que sirva al uso al que está destinado.

Una norma es un documento técnico basado en la experiencia y elaborado a partir de las necesidades de la actividad. Proporciona reglas, directrices o características para las actividades o sus resultados, con el fin de conseguir un grado óptimo de orden en un contexto dado, está disponible al público, establecida por consenso de las partes interesadas, dirigida a la promoción de beneficios óptimos para la comunidad y aprobada por un organismo Nacional o Internacional reconocido.

Según ISO[2], la normalización es una actividad que tiene por objeto establecer, ante problemas reales o potenciales, disposiciones destinadas a usos comunes repetidos, con el fin de obtener un nivel de ordenamiento óptimo, en un contexto dado, que puede ser tecnológico, político o económico.

A partir del año 2012 los organismos internacionales ISO junto con IEC ("International Electrotechnical Commission") incorporan dentro de su línea de

[1] IRAM es el Instituto Argentino de Normalización y Certificación. IRAM es una asociación privada sin fines de lucro, de interés público creada en 1935 como organismo de normalización. Es el único representante argentino ante organizaciones internacionales y regionales de normalización, como la Asociación Mercosur de Normalización (AMN) y la Comisión Panamericana de Normas Técnicas (COPANT), y ante las organizaciones internacionales: International Organization for Standardization (ISO) e International Electrotechnical Comission (IEC), en este caso, en conjunto con la Asociación Electrotécnica Argentina (AEA). Fue reconocido como organismo de normalización argentino en 1937, ratificado en 1994 por el decreto PEN 1474/1994. Contribuye con normas para todos los sectores como ser economía, la industria, el comercio, la salud, el cuidado del ambiente y la educación. Lidera los comités técnicos nacionales que analizan los documentos en estudio, canaliza las propuestas nacionales, fija la posición de Argentina ante estos organismos y está presente en la conducción de varios de los comités técnicos internacionales.

[2] Las normas ISO son definidas por la Organización Internacional de Normalización, más conocida por sus siglas en inglés: ISO (International Organization for Standardization). Es una entidad internacional dedicada a promover y favorecer el desarrollo de normas y regulaciones internacionales de fabricación, comercio y comunicación en todo el mundo para asegurar la calidad, seguridad y eficiencia de productos y servicios, brindando estándares internacionales.

ISO/IEC 27000[1] una seria de normas internacionales ISO/IEC 27037:2012[2], ISO/IEC 27040:2015[3], ISO/IEC 27041:2015[4], ISO/IEC 27042:2015[5], ISO/IEC 27043:2015[6] y ISO/IEC 27050:2015[7] de aplicación a la práctica forense informática, destinadas a estandarizar el tratamiento de la evidencia digital promoviendo un conjunto de procesos fundamentales y buenas prácticas con la finalidad de preservar la integridad de la evidencia digital contribuyendo a su admisibilidad, valor probatorio y relevancia en procedimientos judiciales o disciplinarios.

La norma ISO/IEC 27.037:2012[8] es una guía internacional que brinda lineamientos para la identificación, recolección, adquisición y preservación de la evidencia digital (ISO/IEC 27.037, 2012).

La mencionada norma es un estándar establecido para el primer contacto con la evidencia electrónica, la cual está claramente orientada al procedimiento de la actuación pericial en el escenario de la recolección, identificación y secuestro de la evidencia digital, sin detallar la fase de análisis de la evidencia o posteriores.

Proporciona buenas prácticas con respecto al proceso de manejo de la evidencia digital, la prioridad de recolección según orden de volatilidad así como orientación en los procedimientos de intercambio de evidencias digitales entre intervenientes, manteniendo la debida cadena de custodia.

---

[1] La familia de normas ISO/IEC 27.000 es un conjunto de estándares desarrollados por ISO e IEC que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, las cuales pueden adquirirse y consultarse desde la página oficial de ISO https://www.iso.org/standard

[2] ISO/IEC 27.037:2012. "Information Technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence": Guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales.

[3] ISO/IEC 27.040:2015 "Information technology - Security techniques - Storage security": Guía para el almacenamiento seguro de la evidencia digital.

[4] ISO 27.041:2015. "Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method": Guía para garantizar la idoneidad y adecuación de los métodos de investigación.

[5] ISO 27.042:2015. "Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence": Guía con directrices para el análisis e interpretación de las evidencias digitales.

[6] ISO 27.043: 2015. "Information technology - Security techniques - Incident investigation principles and processes". Guía que desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.

[7] ISO 27.050:2015, "Information technology - Security techniques - Electronic discovery - Part 1: Overview and concepts": Guía del proceso de descubrimiento, adquisición y manipulación de datos electrónicos.

[8] La norma ISO/IEC 27.037:2012 se puede adquirir en https://www.iso.org/standard/44381.html

Incluye directrices de preservación de la evidencia y la cadena de custodia para dispositivos digitales de almacenamiento de todo tipo, desde los sistemas de almacenamiento masivos y externos, dispositivos móviles, sistemas conectados en red, sistemas de circuito cerrado de televisión digital o sistemas de alta dispoibilidad.

Los principios fundamentales de la evidencia digital en los que se basa son la relevancia, confiabilidad y suficiencia a la hora de tener en cuenta qué información o qué dispositivos se van a adquirir como parte de la investigación, donde la cadena de custodia es primordial para evitar la nulidad en cualquiera de las etapas, basadas en procesos auditables y repetibles (López Rivera, 2012). Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital para garantizar la admisibilidad de la misma.

La **relevancia** es una condición técnicamente jurídica, que habla sobre aquellos elementos que son pertinentes a la situación que se analiza o investiga, con el fin de probar o no una hipótesis que se ha planteado alrededor de los hechos. Todo aquello que no cumpla con este requisito será irrelevante y excluido del material probatorio recabado para efectos del caso bajo estudio. (Semprini, 2017)

La **confiabilidad** busca validar la repetibilidad y auditabilidad de un proceso aplicado para obtener una evidencia digital. Esto es, que la evidencia que se extrae u obtiene es la que deber ser, y que, si un tercero sigue el mismo proceso, deberá obtener resultados similares verificables y comprobables. (Semprini, 2017)

Finalmente, el tercer principio es la **suficiencia**, la cual está relacionada con completitud de pruebas informáticas, es decir que, con las evidencias recolectadas y analizadas tenemos elementos suficientes para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada. (Semprini, 2017)

Esta norma ha determinado que estos tres principios, establecen las condiciones necesarias y suficientes para que los expertos en informática forense recaben, aseguren y preserven elementos materiales probatorios sobre medios digitales, los cuales podrán ser revisados y analizados por terceros interesados.

Las **tipologías de dispositivos y entornos** tratados incluyen equipos y medios de almacenamiento y dispositivos periféricos, sistemas críticos (alta

exigencia de disponibilidad), ordenadores y dispositivos conectados en red, dispositivos móviles y sistemas de circuito cerrado de televisión digital.

Los aspectos claves para el manejo de la evidencia digital en los que se basa la norma ISO 27.037 son: (López Rivera, 2012)

- **Aplicación de Métodos:** La evidencia digital debe ser adquirida del modo menos intrusivo posible tratando de preservar la evidencia original y en la medida de lo posible trabajar sobre copias forenses.
- **Proceso Auditable:** Las tareas, procedimientos y la documentación generada deben ser validados y contrastados por las buenas prácticas profesionales. Se debe proporcionar trazas y evidencias de lo realizado y sus resultados. El proceso debe ser traceable.
- **Proceso Reproducible:** Los métodos y procedimientos aplicados deben de ser reproducibles, verificables y argumentables. Se debe considerar la realización de informes al nivel de comprensión de quienes puedan dar validez y respaldo a las actuaciones realizadas.
- **Proceso Defendible**: Deben detallarse las herramientas utilizadas, las cuales deben ser licenciadas, validadas y contrastadas en su uso para el fin en el cual se utilizan en la actuación.

La norma establece un **modelo genérico** de tratamiento de las evidencias digital, basado en **procesos bien diferenciados**:

- **Identificación:** Consiste en localizar e identificar las potenciales informaciones o elementos de prueba en sus dos posibles estados, el físico y el lógico según sea el caso de cada evidencia.
- **Recolección y Adquisición:** Se refiere a la recolección de los dispositivos y la documentación que puedan contener la evidencia que se desea recopilar o bien la adquisición y copia de la información existente en los dispositivos. Relacionada con la incautación y secuestro de los dispositivos.
- **Conservación/Preservación:** Se refiere a las acciones de dirigidas a conservar la cadena de custodia, la integridad y la originalidad de la evidencia digital, para garantizar su utilidad, y que a posterior pueda ser admisible como elemento de prueba en un juicio.

La norma diferencia los roles y responsabilidades de los intervinientes a partir de la fase en la que se involucran en la pericia, diferenciando habilidades de quienes deben recolectar y preservar la evidencia con respecto a quienes deben procesar o revisar y presentar la misma. En el caso de esta norma se establece como rol principal, en las etapas enunciadas, el primer interviniente o DEFR ("Digital Evidence First Responder").

El resto de la familia de normas vinculadas a al tratamiento de la evidencia digital, ISO/IEC 27.040/27.041/27.042/27043/27.050[1], enuncian en su conjunto buenas prácticas orientadas a la fase análisis e interpretación, procesamiento, revisión y presentación de evidencia digital y determinan roles específicos para cada tarea, complementando a la ISO/IEC 27.037.

La norma ISO 27.040:2015 (ISO/IEC 27040, 2015) es una guía de recomendaciones relacionado con el almacenamiento seguro de la evidencia digital. Enuncia los riesgos existentes y detallas las buenas prácticas incluyendo modelos de auditorías y revisiones para controlar y garantizar el almacenamiento seguro de las evidencias (Vila Avendaño, 2018).

La norma ISO 27.041:2015 (ISO/IEC 27041, 2015) es una guía para garantizar la idoneidad y adecuación de los métodos de investigación. El desarrollo general se basa en la captura y análisis de requerimientos y en el diseño, implementación, verificación, validación y aseguramiento de procesos a aplicar en el tratamiento de la evidencia digital.

La norma ISO 27.042:2015 (ISO/IEC 27041, 2015) es una guía orientada al análisis e interpretación de la evidencia digital desde la identificación (evidencia digital potencial), análisis (evidencia digital), hasta que es aceptada como prueba en un juicio (evidencia digital legal). Incluye las partes e información que debe contener un informe pericial. El estandar diferencia modelos de análisis que pueden plantearse desde el análisis estático al análisis en vivo. El análisis estático se plantea basado en el método de inspección tradicional de contenido de archivos, datos borrados, etc. El análisis en vivo o en caliente se refiere al estudio de evidencias digitales en sistemas encendidos como memorias RAM, dispostivos

[1] Las normas ISO/IEC 27040/27041/27042/27043/27050 se pueden adquirir en https://www.iso.org/standards.html

móviles, redes, etc. En el caso de analisis en vivo diferencia en los que pueden o no ser copiados u obtener una imagen de los mismos. (Vila Avendaño, 2018)

La norma ISO 27.043:2015 (ISO/IEC 27043, 2015) es una guía que desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.

La norma ISO 27.050:2015 (ISO/IEC 27043, 2015) es una guía que aplica al proceso de descubrimiento, adquisición y manipulación de datos electrónicos

Al ser normas internacionales, la aplicación de dichas normas en Argentina[1], conlleva a analizar restricciones en lo que hace a la ley nacional vigente, a la estructura del Derecho y a la característica de un país federal, de manera de ajustarla a la realidad del país y no superponerse con la ley o reglamentación, considerando que las normas siempre están por debajo de la ley. Por otro lado, no debe dejarse de lado los códigos de procedimientos de cada una de las provincias y jusridicciones en el país. Por tal motivo se deben considerar como un conjunto de buenas prácticas que acompañan al trabajo técnico sin causar modificaciones o controversias con ningún código procesal.

2.3.3. Modelo EDRM

El modelo internacional **EDRM ("Electronic Discovery Reference Model")**[2], es un modelo de referencia del descubrimiento electrónico creado en 2005 ante la ausencia de estándares y directrices en el mercado. Actualmente se encuentra vigente la versión 2014[3] (EDRM, 2014). El descubrimiento electrónico (también conocido como **e-discovery**) se refiere a cualquier proceso en el que se busca,

[1] En abril del año 2019 IRAM ("Instituto Argentino de Normalización y Certificación") organizó y conformó una Comisión de Informática Forense con integrantes referentes en la temática, ante la necesidad de la adopción de las normas ISO relacionadas a Informática Forense, con el fin de obtener una base aplicable a la regulación de la actividad de actuación en el ámbito judicial y cooperativo Institucional en la República Argentina. Las normas ISO/IEC vinculadas a informática forense son parte del comité técnico "ISO/IEC JTC1/SC27 IT Security Techniques", del cual IRAM es miembro participante.

[2] El modelo EDRM ("Electronic Discovery Reference Model") fue desarrollado en 2005 por George Socha Jr., fundador de Socha Consulting LLC, con sede en St. Paul, Minnesota, y Tom Gelbmann, director gerente de Gelbmann & Associates en Roseville, Minnesota. Los estándares son distribuidos por EDRM, LLC, una coalición de consumidores y proveedores que desarrollan recursos de e-discovery y gobierno de la información. EDRM es presentado bajo licencia de Creative Commons en http://edrm.net.

[3] La especificación completa del modelo EDRM ("Electronic Discovery Reference Model") se puede consultar accediendo al enlace https://www.edrm.net/frameworks-and-standards/edrm-model/.

localiza, asegura y examina datos electrónicos con la intención de usarlos como evidencia digital. El modelo EDRM es un marco conceptual que describe los estándares para la recuperación y el descubrimiento de datos digitales.

Este modelo también menciona una serie de etapas o fases en las cuales se brindan mejores prácticas de manera global para el tratamiento de la evidencia, las cuales van desde la identificación, preservación, recolección, procesamiento, análisis, revisión, producción y presentación de la evidencia digital.

El modelo EDRM plantea ideas en forma general sin puntualizar en ningún dispositivo en concreto, siendo un conjunto de metodologias que se pueden considerar de manera universal para cualquier tipo de dispositivos.

El diagrama EDRM representa una vista conceptual del proceso, con fases planteadas en un modelo que no es lineal o de cascada, sino un proceso iterativo, como puede verse en la Figura 2.

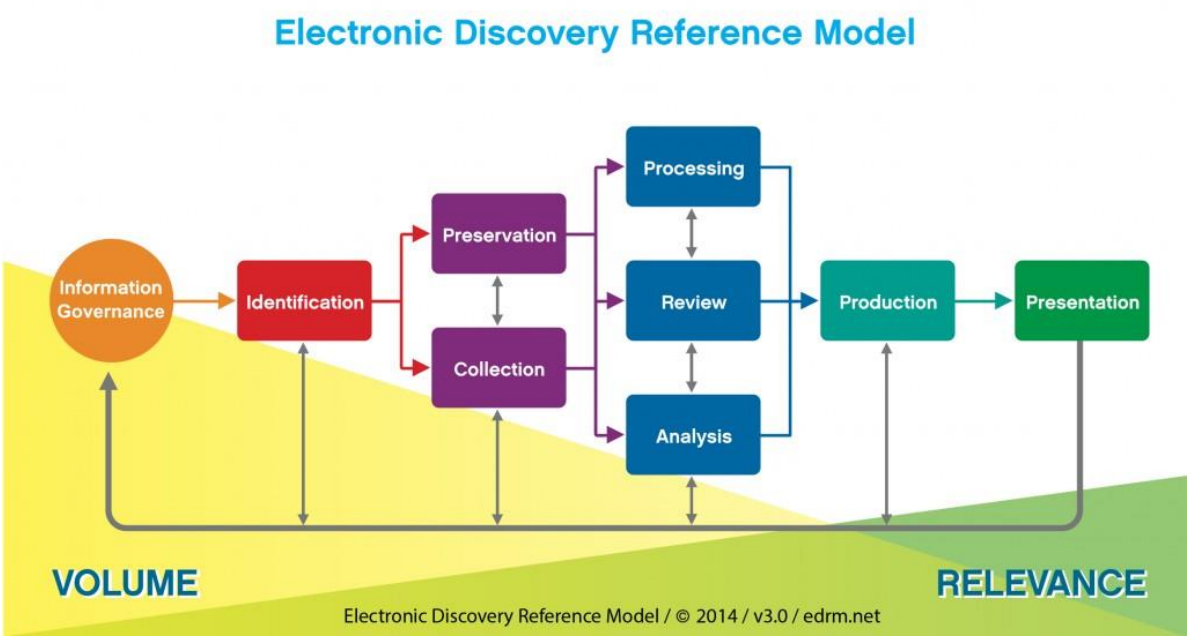

Figura 2: EDRM

Al ser planteado como un proceso iterativo todas las fases retroalimentan al modelo y el final retroalimenta al inicio nuevamente. Mientras se avanza en la investigación se pueden encontrar nuevas fuentes de evidencia que no se recolectaron al inicio o nuevas personas involucradas, lo cual implica una retroalimentación del proceso que puede originar, por ejemplo, nuevos allanamientos o nuevos artefactos a recolectar o analizar. De esta manera se

podría repetir la misma fase varias veces, conduciendo a un conjunto más preciso de resultados o se podría también pasar nuevamente sobre las fases anteriores, refinando el enfoque para una mejor comprensión de los datos que surgen. El proceso permite iterar infinitamente hasta que se llegue algún tipo de decisión por parte del jurado.

A medida que se avanza en la ejecución de las fases el volumen de información se va reduciendo, enfocándose en la información con mayor relevancia.

Consta de 9 fases o etapas:

- Gestión de la información: Fase de implementación de procesos de gestión de la información y riesgos asociados, en caso de una solicitud de e-discovery.
- Fase de Identificación: Fase de desarrollo y ejecución de estrategias para la identificación y validación de potenciales fuentes de información almacenadas electrónicamente (ESI, “Electronically Stored Information”). Identificación de fuentes de información útiles y relevantes para el caso de investigación y determinación de su alcance, amplitud y profundidad. Incluye la identificación tanto de personas como de sistemas asociados a las ESI. Se identifica a los custodios de las ESI. Dado que el alcance de los datos puede ser abrumador en esta fase, se intenta reducir el alcance general durante esta fase, por ejemplo, limitando la identificación de documentos a un cierto período o término de búsqueda para evitar una solicitud excesivamente onerosa.
- Fase de Preservación: Fase en la que se activa la preservación de los datos potencialmente relevantes identificados en la fase anterior. Se los debe aislar inmediatamente protegiéndolos de forma que sea luego legalmente defendibles, razonables, amplios, pero a medida, auditables y repetibles. Asegurarse que la ESI está protegida contra alteración inapropiada o destrucción.
- Fase de Recolección: Fase en la que se realiza la recolección de la información potencialmente relevante. La misma deber ser recogida teniendo en cuenta los preceptos de la fase de preservación. En esta fase se realiza la adquisición de la evidencia digital en vivo o en equipos apagados, respetando el orden de volatilidad de la evidencia.

- Fase de Procesamiento: Fase en la que se reduce el volumen de ESI y se la convierte, si es necesario, a formas más confortables para su posterior revisión y análisis. Se aplican acciones sobre la información recolectada en la etapa anterior para permitir la visualización de los metadatos, el filtrado, la normalización del formato y la reducción de la cantidad de archivos para su posterior revisión.
- Fase de Revisión: Fase de evaluación de la ESI para determinar la revelación del descubrimiento electrónico de los datos. Diferentes plataformas de revisión de documentos ayudan en tareas relacionadas con este proceso, incluyendo la rápida identificación de documentos potencialmente relevantes, y el filtro de documentos según varios criterios (como palabras clave, rango de fechas, etc.).
- Fase de Análisis: Fase para obtener una adecuada comprensión del contenido de la información recolectada, a través de la organización de los mismos en subconjuntos lógicos de una manera eficiente. Evaluación de contenido y contexto de la ESI, incluyendo patrones clave, tópicos, personas y temas de discusión.
- Fase de Producción: Fase destinada a preparar y producir de manera eficiente y en un formato útil los resultados de la investigación, a fin de reducir tiempos, costos y errores, cumpliendo de esa manera en tiempo y forma con los plazos comprometidos, utilizando mecanismos de entrega adecuados.
- Fase de Presentación: Etapa en la que se muestran los resultados de la investigación, utilizando presentaciones con muestras relevantes y contundentes extraídas de la información recolectada inicialmente en las primeras etapas, con el fin de eventualmente obtener más información y/o validar los hechos.

El EDRM puede ser usado como guía de reglas de mejores prácticas para descubrir, recopilar y asimilar datos electrónicos durante un proceso legal, incluido el descubrimiento de pruebas criminales.

2.3.4. Modelo PURI (Proceso Unificado de Recuperación de Datos)

El modelo PURI (Proceso Unificado de Recuperación de la Información) es el resultado de un proyecto de investigación iniciado en el 2011 en la Facultad de Ingeniería de la Universidad FASTA por un grupo de investigación en sistemas operativos e informática forense[1]. El modelo PURI se encuentra desarrollado y detallado en el Anexo III de la "Guía Integral de Empleo de la Informática Forense" (Di Iorio A. H., 2016)[2] y en el libro "El rastro digital del delito. Aspectos técnicos, legales y estratégicos de la Informática Forense"[3] (Di Iorio, Castellote & Bruno , 2017, capítulo 3).

PURI es un modelo teórico de las tareas involucradas en la aplicación forense de las ciencias de la información. Establece una guía de labores a desempeñar desde el área técnico-informático forense, organizándolas en fases, actividades y tareas que sirve de asistencia a la justicia para mejorar técnicamente la recuperación de la información en pericias. A su vez, el modelo se complemetna con las técnicas para llevar a cabo cada una de esas tareas y las herramientas disponibles que ejecutan dichas técnicas (Di Iorio, Castellote & Bruno , 2017, capítulo 3).

[1] En el año 2014 se crea el Info-Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, siendo la sede actual del grupo de investigación. Info-Lab es una iniciativa conjunta de la Universidad FASTA, la Procuración General de la Suprema Corte de Justica de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredón, que nuclea en la ciudad de Mar del Plata a un equipo interdisciplinario de investigadores científicos y tecnológicos con el objeto de desarrollar soluciones a las demandas en el campo de la informática forense y su aplicación.

[2] La "Guía Integral de Empleo de la Informática Forense en el Proceso Penal" (segunda edición, abril 2016) se puede descargar del enlace http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/1592/PAIF.pdf?sequence=1 en forma gratuita. La misma surge en el marco del proyecto "Protocolo de Actuación en Informática Forense a partir del Proceso Unificado de Recuperación de Información - PAIF-PURI", acreditado por el Ministerio de Ciencia, Tecnología e Innovación Productiva de la Nación e incorporado al Banco Nacional de Proyectos de Desarrollo Tecnológico y Social de la República Argentina, mediante Res. 062/14 de la Secretaría de Articulación Científico-Tecnológica. El proyecto PAIF-PURI, iniciado en junio de 2014, tenía como objetivo inicial el desarrollo de un Protocolo de Actuación en Informática Forense para ser adoptado y promovido por el Ministerio Público de la Provincia de Buenos Aires como estándar oficial de trabajo, en base a lo establecido en el Proceso Unificado de Recuperación de Información (PURI). A partir de nuevos requerimientos planteados por las autoridades del Ministerio Público, en particular, en lo que respecta a los lineamientos referidos al abordaje de los casos, la planificación y gestión de la investigación penal y la litigación, se extendió el proyecto original para contemplar estos aspectos en el protocolo validado resultante, dando lugar a la guía mencionada.

[3] El libro "El rastro digital del delito. Aspectos técnicos, legales y estratégicos de la Informática Forense" se puede descargar de forma gratuita del enlace http://redi.ufasta.edu.ar:8080/xmlui/handle/123456789/1593. El libro es producto del trabajo desarrollado por proyectos de investigación del Grupo de Investigación en Sistemas Operativos e Informática Forense de la Universidad FASTA y por el Info-Lab entre los años 2010 y 2016.

Se basa en un proceso formado por un conjunto de fases sucesivas, donde cada fase posee objetivos y particularidades específicas y se interconectan entre sí como un todo. Las series de fases a seguir pueden diferir según el caso origen a resolver y a las características del objeto sobre el que realizar las tareas forenses, pudiendo abordarse el proceso en diferentes fases.

El modelo PURI es "un esquema[1] teórico de las tareas involucradas en la aplicación forense de las ciencias de la información", donde las tareas se agrupan en actividades y las actividades en fases. Es un esquema dado que es una representación gráfica o simbólica de las tareas involucradas en la informática forense. El modelo se complementa con técnicas y herramientas asociadas a las mismas, para cada una de las tareas.

Se presenta a continuación un gráfico explicativo de las fases que intervienen en el modelo PURI (Di Iorio, Castellote & Bruno , 2017, p.279):

Figura 3: Modelo PURI

Se entiende por **fase** a cada uno de los estados sucesivos en el que puede encontrarse un proceso de recuperación de información que se ejecute sobre el modelo. Estas fases son sucesivas debido a que llevan un orden lógico (Di Iorio, Castellote & Bruno , 2017, p.279).

[1] Según el diccionario de la Real Academia Española un esquema es la representación gráfica o simbólica de cosas materiales o inmateriales.

Cada **fase** del modelo PURI está compuesta por **actividades** (al menos una), donde cada actividad engloba un conjunto de **tareas**. Cada una de las actividades y las tareas pueden realizarse o no, según el caso o servicio a realizar y el objeto de estudio (Di Iorio, Castellote & Bruno , 2017, p.279).

En PURI se entiende por **actividad** al conjunto de tareas forenses relacionadas entre sí y agrupadas en función del objetivo que persiguen, sugiriendo un orden en el que se podrian ser llevadas a cabo. De este modo, una **tarea** en PURI es un trabajo específico y atómico dentro de una actividad y arrojan un resultado concreto. A su vez, cada tarea puede ser realizada aplicando una o varias **técnicas** y estas técnicas implementadas por diversas **herramientas** sugeridas. Una técnica es un procedimiento, una serie de pasos a realizar para llevar a cabo una tarea y las herramientas son los programas, aplicaciones o infraestructuras que implementan una o varias técnicas.

La fase de **relevamiento** o identificación abarca la investigación que se realiza para conocer el caso a trabajar e identificar los posibles objetos de interés. En un entorno judicial se corresponde con las medidas de “exploración” o labores investigativas del caso o con las labores de “reconocimiento o exploración” en caso de trabajos privados no judicializados. Se prioriza los objetos según la volatilidad de los datos y el interés sobre cada uno. Abarca actividades de identificación de documentación legal y técnica, como de identificación de infraestructura tecnológica.

La fase de **recolección** abarca las acciones y medidas necesarias para conseguir los equipos físicos sobre los que se realizará el trabajo forense y/o fuentes de datos sobre los cuales se deberá trabajar posteriormente, es decir las posibles fuentes de evidencia digital. En un caso judicial este hecho puede implicar un “secuestro” del efecto durante un allanamiento o en la escena del hecho o una “presentación espontánea” en el caso. Las actividades que componen esta fase son la detección de la infraestructura tecnológica y la recolección de los objetos (tareas de secuestro, embalaje y transporte).

La fase de **adquisición** involucra las tareas en la que se obtiene el “contenido” a analizar, abarcando todas las actividades en las que se obtiene la imagen forense del contenido que se analizará. Esta fase se puede realizar “in situ” en el

lugar del hecho o durante un allanamiento, o bien en un laboratorio forense luego de haber recolectado los objetos. Las actividades de esta fase abarcan la adquisición de datos persistentes, datos volátiles, paquetes de red y tarjetas inteligentes, como también la validación, el resguardo y el transporte no supervisado.

La fase de **preparación** involucra las actividades técnicas de preparación del ambiente de trabajo del informático forense, la restauración de las imágenes forenses, el volcado de datos, junto con su correspondiente validación. Como también la selección del conjunto de técnicas y herramientas apropiadas, a fin de dejar preparado el entorno para su posterior extracción y análisis. En esta fase es esencial identificar las tecnologías de la información en el objeto, como ser sistemasoperativos, cantidad de particiones, etc.

La **fase de extracción y análisis** comprenden las tareas forenses de extracción de la información de las imágenes forenses y posibles fuentes de evidencia digital, la selección de la potencial evidencia digital y su análisis en relación al caso y a los puntos periciales o requerimientos de servicio forense. Las tareas de extracción y análisis se plantean en la mismas fase, ya que si bien son dos labores independientes, se realizan en conjunto y están íntimamente vinculadas entre sí.

Las actividades de extracción se separan en tres niveles teóricos independientes de las tecnologías o plataformas en particular: extracción a nivel de aplicación, extracción a nivel de plataforma y extracción a bajo nivel. Las actividades de análisis se dividen en análisis de contenidos, es decir de la información propiamente dicha que surge de los datos extraídos y el análisis de relaciones entre los distintos elementos extraídos.

La **fase de presentación** comprende el armado de los informes necesarios y la presentación del caso en un juicio o a los solicitantes. Las actividades involucradas son el armado de un informe pericial claro, preciso y concreto incluyendo la documentación de todas las actividades y tareas realizadas, como también la preparación de la información a presentar en una eventual presentación en un juicio o quienes hayan solicitdo el servicio forense.

En todas las fases se asegura la trazabilidad y la correcta preservación y custodia de los objetos secuestrados, a fin de garantizar la cadena de custodia, según protocolos y recomendaciones vigentes.

El modelo plantea que las fases iniciales de relevamiento y recolección son de tipo exploratorio y es esperado que sean ejecutadas por un profesional con perfil orientado a la investigación donde el técnico tenga un rol de asistencia y asesoramiento. En cambio las fases subsiguientes mencionadas son netamente de informática forense donde se espera que las tareas involucradas sean llevadas a cabo por profesionales especializados en la temática, con la asistencia de los investigadores del caso.

El modelo se basa en la definición de distintos niveles de conocimientos en las actuaciones del informático-forense:

- Responsable de Identificación (RI): Persona idónea para tareas de identificación y no necesariamente es informático. Puede ser un investigador judicial capacitado en la materia o personal auxiliar del Laboratorio Informático Forense.
- Especialista en Recolección: Persona autorizada, entrenada y calificada para recolectar objetos físicos pasibles de tener evidencia digital.
- Especialista en Adquisición: Persona autorizada, entrenada y calificada para recolectar dispositivos y adquirir la evidencia digital de estos.
- Especialista en Evidencia Digital: Experto que puede actuar como especialista en adquisición y además tiene conocimientos, habilidades y aptitudes que le permiten manejar un amplio rango de situaciones técnicas, tales como la realización de una pericia informática.

Las ventajas del modelo PURI es que al ser desarrollado en Argentina es un modelo factible de aplicar nacionalmente. La flexibilidad y adaptabilidad lo hacen aplicable a la realidad nacional y de cada jurisdicción. Por ejemplo, a diferencia de las normas internacionales, no plantea un equipo por cada rol sino se plantean roles y habilidades del personal que participa en cada una de las etapas, obviamente considerando que pueden ser los mismos personas cumpliendo diversos roles, lo cual es algo muy usual ante la falta de recursos humanos que se dispone. Otra característica que lo hace muy interesante es que incluye el

desarrollo de ejemplos prácticos detallados basados en pericias reales, afianzando y aclarando de este modo la teoria con los mismos.

2.4. Metodología de Auditoría Universal de Datos No Invasiva

Como marco de referencia para la configuración, ejecución y control de auditorías de bases de datos, se considera la **Metodología de Auditoría Universal de Datos No invasiva** (Gioia 2012) desarrollada como parte del trabajo de tesis “Desarrollo de una Metodología de Auditoría Universal de Datos a Nivel de Registro” para la Especialización en Criptografía y Seguridad Teleinformática en la Escuela Superior Técnica del Ejército Argentino (EST).

La metodología de auditoría universal de datos no invasiva posibilita que los auditores de base de datos puedan validar el cumplimiento de diferentes normas y legislaciones, principalmente en lo que se refiere a materia de protección de datos personales, y estándares relacionadas con la seguridad de la información y su gestión en cada organización, así como apoyar la gestión de los riesgos para asegurar la confidencialidad, integridad y disponibilidad de la información contenida en las bases de datos. La metodología es adaptable a las diferentes legislaciones de protección de datos personales de los diferentes países donde se pueda implementar, como también a las medidas o necesidades específicas de seguridad de la información de las organizaciones según las normas o estándares de seguridad en las que se basen la implementación de su Sistema de Gestión de Seguridad de la Información (SGSI) y la gestión de riesgos asociados. (Gioia & Eterovic, 2017)

Con la evidencia recolectada por las auditorías se puede conocer, analizar y controlar las actividades de los usuarios tanto para detectar acciones maliciosas que puedan afectar la confidencialidad, integridad o disponibilidad de la información, como para prevenir las mismas a futuro. Además, las ejecuciones continuas de las auditorías de datos retroalimentan a la estrategia de seguridad aplicada al motor de base de datos al detectar riesgos potenciales, por ejemplo, a

los que se expone ante el otorgamiento de determinados permisos a usuarios o aplicaciones. (Gioia & Eterovic, 2017)

Las auditorías de datos deben basarse en las políticas de seguridad de la información establecidas en la organización, por tal motivo es indispensable tener conocimiento sobre las mismas. (Gioia 2012)

Los diferentes tipos de auditorías de datos consideradas en la metodología se basan en auditar la ejecución y/o los datos vinculados a operaciones de actualización, operaciones de cambio de estructuras de datos, operaciones de lecturas, operaciones con determinada información de contexto o incluso a partir de intentos fallidos de acciones.

Las auditorías de datos no deben afectar la eficiencia de los Sistemas Informáticos asociados, de manera de evitar que por temas de disponibilidad o rendimiento las auditorías no se ejecuten. Por tal motivo al configurar las auditorías se deben evaluar los riesgos potenciales sobre los datos sensibles y configurar las auditorías de manera de orientarlas realmente donde existe la amenaza para mantener el equilibrio adecuado entre la necesidad de resguardar la seguridad de la información y la operatoria de los sistemas. (Gioia, 2012)

La ejecución de las auditorías puede producir cantidades copiosas de información, en especial las que auditan a nivel de contenidos de datos u operaciones de lecturas. Por tal motivo al momento de configurarlas se debe buscar un compromiso entre auditar demasiados datos que resulten onerosos de clasificar y agoten los recursos del sistema o auditar pocos datos causando la pérdida de registro de eventos importantes. La metodología considera la configuración de filtros de auditorías y de niveles de almacenamiento que ayudan a manejar el volumen de datos y focalizar las auditorías en acciones críticas sobre los datos más sensibles.

Los diferentes tipos de filtros de auditoria planteados permiten focalizar la obtención de evidencia en determinadas operaciones, datos sensibles, usuarios o información de contexto de las acciones sobre datos críticos. Los filtros pueden configurarse a nivel de operaciones, a nivel de datos, estructura de datos o a partir de la información de contexto de las operaciones auditadas.

De manera complementaria, la misma considera que se pueden aplicar filtros aplicados al nivel de almacenamiento de la información auditada, de manera de configurar la información auditada que se necesita almacenar, y así evitar resguardar registros completos de datos que sean innecesarios a fines de las auditorías en sí, almacenando solo aquellos campos identificatorios del registro y los campos sensibles a auditar o incluso solo las operaciones asociadas, dependiendo de los escenarios.

La metodología además establece definir el tipo de protección a aplicar a la información auditada en el almacenamiento de la misma, incluso en archivos de reportes que se emitan, considerando que la información es sensible tanto en su almacenamiento original, como también en los registros de auditorías en sí. La protección de los datos permite cumplir con normativas y regulaciones relacionadas con la privacidad de los datos y con regulaciones específicas de determinados sectores (financiero, salud, telecomunicaciones, etc.) o datos críticos para la organización en la propia solución. A nivel de almacenamiento de la información muy sensible auditada, donde se requiera un nivel de protección adicional, la metodología incluye el cifrado de datos, como también firma digital de reportes de auditorías.

Considerando que los resultados de las auditorías se pueden visualizar tanto desde los sistemas como en reportes emitidos por el mismo, se considera la aplicación de niveles de protección a la visualización que van desde la configuración de autorización de visualización, aplicación de visualización con enmascaramiento, como también visualización enriquecida, según los usuarios involucrados en el tratamiento de la información.

2.5. La Auditoria Forense

Según René Humberto Márquez Arcila[1] "La auditoría forense es una disciplina que sirve como asesor experto a quienes imparten justicia, en la investigación y obtención de evidencia, acerca de la existencia de un delito financiero o relacionado con los activos de la organización.

La función de la auditoría forense consiste en evaluar los procesos de la organización evaluando excepciones, irregularidades contables y patrones de conducta que pueden considerarse anormales; lógico y sistemático que les permite obtener evidencia legal de hechos presuntamente delictivos que podrían dañar el interés público o privado". (Márquez Arcila, 2018)

Esta disciplina permite responder a preguntas sobre qué es lo que ocurrió, cómo, dónde, cuándo, quién es responsable, etc. Para esto, requiere la utilización de técnicas para obtener información más precisa y específica, así como para realizar un análisis de mayor alcance que el de las técnicas de auditoría tradicionales. La comprensión de cómo se lleva a cabo un delito es fundamental para las organizaciones, ya que se ha convertido en una de las principales causas de pérdida financiera y reputacional en la actualidad. (Márquez Arcila, 2018)

La auditoría forense puede ser correctiva, enfocándose en los delitos que ya han sido cometidos, y también preventiva para prevenir y predecir situaciones indeseables relacionados con potenciales delitos (a partir de una matriz de riesgos). Además, también puede cumplir un rol de asesoría, capacitación y soporte durante litigios, valiéndose de diversas técnicas para la obtención de información.

[1] René Humberto Márquez Arcila, autor del libro "Auditoria Forense" del año 2018. Actualmente es vicepresidente del Sector Gubernamental del Instituto Mexicano de Contadores Públicos por el periodo 2107-2019. Autor de los libros: Fiscalización y rendición de cuentas (2013) y Auditoría de desempeño (2014).

La auditoría forense mantiene un enfoque de auditoría legal que permite obtener evidencia confiable y un programa de aseguramiento constante del riesgo de delitos sugiriendo medidas de control.

Dicha auditoría tiene como objeto de estudio los posibles ilícitos relacionados con los bienes de la organización; cometidos desde dentro o fuera de ésta y afectando sus intereses y permanencia. (Márquez Arcila, 2018)

A continuación, se describen los tres tipos de enfoques (Márquez Arcila, 2018):

1. **Pasivo**. La auditoría es diseñada para determinar la existencia de los controles y que han sido implementados y se encuentran operando. También para estar alerta cuando los controles expongan alertas.
2. **Reactivo**. Se desarrolla una investigación en respuesta a las declaraciones de delitos. En este enfoque, los procesos se enfocan en resolver la declaración específica.
3. **Proactiva**. La investigación toma lugar cuando aún no existe una declaración o aviso de delito, o incluso cuando no existe ningún fallo en controles que sugieran que un ilícito podría estar ocurriendo.

La manera de responder al riesgo de fraude consiste en comprender la diferencia entre auditoría e investigación, diseñar políticas adecuadas para responder a este riesgo y, por último, proveer de un marco para preparar un plan de investigación.

Los auditores e investigadores son diferentes, tienen distintos conocimientos y normas. Los auditores se basan en las normas de auditoría, principios contables, políticas y procedimientos. Los investigadores se basan en reglas de evidencia y procedimientos criminales o civiles. La auditoría de fraude tiene como función identificar transacciones que tienen potenciales banderas rojas, la gerencia se convierte en el juez del hecho porque la investigación está destinada a impugnar o sustanciar la acusación y proveer evidencia relacionada en donde el juez y el jurado se convierte son quienes juzgarán la verdad del hecho (Márquez Arcila, 2018).

En general, el objetivo de la investigación es resolver la acusación o sospecha de delito; sin embargo, comprendiendo el punto final del caso, los auditores pueden hacer un mejor plan para realizar la investigación. Los auditores deberían

tratar cada caso como si fuera ser llevado a juicio; en este caso, deberán seguir estrictamente los procedimientos y conducta durante la investigación.

La auditoría de fraude debe proveer una transición visible de la auditoría a la investigación. Idealmente, el reporte de auditoría forense debe convertirse en el reporte de investigación.

2.6. Familia ISO/IEC 27.000

La familia ISO/IEC 27.000 es el grupo de estándares emitida por la Organización Internacional de Normalización (ISO), dedicado a la definición de los SGSI (Sistema de Gestión de Seguridad de la Información).

Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.) o de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27.001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización

Está formada por cinco estándares internacionales abarcando los requisitos de los sistemas de gestión de la seguridad, la gestión del riesgo, métricas y medidas, guías de implantación, glosario de términos y mejora continua.

Se resaltan los siguientes estándares:

1. ISO/IEC 27.001[1]: Describe cómo gestionar la seguridad de la información en una empresa. El SGSI es el concepto central sobre el que se construye ISO 27.001. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27.001:2013. Puede ser implementada en cualquier tipo de organización, con o sin fines de lucro,

[1] ISO/IEC 27001:2013 "Information technology - Security techniques - Information security management systems - Requirements", disponible en https://www.iso.org/standard/54534.html.

privada o pública, pequeña o grande. Promueve la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

2. ISO/IEC 27.005:2011[1]: Es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO/IEC 27.001. Es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización.
3. ISO/IEC 27.006[2]: Facilita el proceso de evaluación de la eficacia del SGSI, según las normas, de forma que la evolución y la mejora continua del SGSI agregue valor a la implementación y a la organización en general.

La ISO/IEC 27.001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI según "Ciclo de Deming" o PDCA (acrónimo de Plan, Do, Check, Act y en castellano Planificar, Hacer, Verificar, Actuar) o espiral de mejora continua, la cual es una estrategia basada en la mejora continua de la calidad, en esos cuatro pasos.

[1] ISO/IEC 27005:2011 - "Information technology - Security techniques - Information security risk management") https://www.iso.org/standard/56742.html

[2] ISO/IEC 27006, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems. https://www.iso.org/standard/62313.html

Capítulo 3 – Planteamiento del Problema

3.1. Descripción del problema

En forma general en la Seguridad Informática se debe distinguir dos propósitos de protección, la Seguridad de la Información y la Protección de Datos. Ambos se diferencian en el motivo por el cual emplean medidas de seguridad de protección.

Mientras que para **la Seguridad de la Información** el objetivo es **proteger los datos en sí mismos** contra la pérdida y modificación no autorizadas; para la **Protección de Datos** el objetivo **no es proteger a los datos en sí mismos, sino el contenido de información referido a las personas, para evitar el abuso o perjuicio de las mismas**. El objetivo de la Protección de datos es proteger los datos personales de los individuos para evitar consecuencias negativas en contra de ellos. La **motivación** y la **finalidad** también difieren en ambas. La motivación de emplear medidas de protección, para la Seguridad de la Información, es el interés propio de la organización o de la persona que maneja los datos, con la finalidad de evitar daño material o inmaterial. En cambio, la motivación para la Protección de Datos es la obligación jurídica o la simple ética personal, con la finalidad de evitar consecuencias negativas contra las personas a las cuales se trata la información.

En este contexto surge un tercer propósito, que es la **Informática Forense,** y afín a este trabajo, **específicamente en Base de Datos**, cuyo **objetivo** no es la protección de datos ni el contenido de los mismos, sino la obtención de evidencia digital como medio de prueba para su sanción en un proceso judicial. La Informática Forense no busca proteger ni prevenir, sino que tiene como objetivo la obtención de evidencia digital relacionada a operaciones que hayan causado pérdida o modificaciones no autorizadas de información, o evidencia digital de operaciones relacionadas a abuso en el uso de datos personales, entre otros casos. La **motivación** de la informática forense es el interés del Juez, Fiscal,

algunas de las partes o de la propia organización. La finalidad principal es evitar invalidar la prueba.

En la siguiente Figura 4 se visualiza como interaccionan las diferentes ramas y propósitos mencionados:

Figura 4: Propósitos de protección de la Seguridad Informática

En este contexto se plantea la necesidad de una **metodología de análisis forense informático para la obtención de evidencia digital en base de datos relacionales** que, por un lado, audite las operaciones que violen las políticas de Seguridad de la Información o infrinjan las Leyes de Protección de Datos personales, y que, por otro lado, efectúe el tratamiento de la evidencia digital adecuado para la presentación de la misma ante un Tribunal de Justicia, sirviéndose, en el caso que se dispongan, de los resultados de las auditorías.

La **informática forense de base de datos**, tal como se explicó en el punto 2.2.8, enfoca su investigación específicamente en la base de datos en sí y el servidor que la contiene, es decir la capa de datos. Los problemas y riesgos que se presentan en la realización de una pericia informática de bases de datos son

diversos y se acrecientan más aún por no disponer de un procedimiento estándar específico para el análisis forense sobre las mismas.

Las bases de datos podrían ser afectadas por **acciones maliciosas o indebidas de diversos tipos**, como lecturas, modificaciones o copias de datos críticos, incluso sin ser advertidas, comprometiendo así la integridad, disponibilidad y la confidencialidad de cierta información, la cual por ley debe ser objeto de especial cuidado. La **corrupción de los datos y la revelación indebida de información** pueden ser llevadas a cabo tanto por usuarios con acceso autorizado como por atacantes con acceso desautorizado. Los ataques pueden ser internos o externos a la organización. Incluso pueden existir operaciones indebidas o críticas que se hayan llevado a cabo por error o sin intención, sin ser producidas por un ataque intencional.

Los conocimientos y experiencia técnica son una condición necesaria, pero no suficiente, **para un eficaz desempeño de los expertos en informática forense en base de datos**. La experiencia técnica en base de datos no asegura el buen proceder del profesional experto en materia pericial. Esta problemática no aplica solo a base de datos sino a los diferentes campos de la informática forense, los cuales son cada vez mas específicos y especializados, donde la necesidad de expertos concretos crece cada día, como también la **necesidad de capacitación y formación específica en el tratamiento de evidencia digital y en los aspectos legales y procesales vinculados**.

En la actualidad existen metodologías generales o guía para el tratamiento de la evidencia digital en sus diferentes etapas que se pueden aplicar a cualquier tipo de dispositivo o tecnología informática, pero no son específicas a tecnologías en particular y menos aún referidas a base de datos.

Como se ha detallado en el punto 2.3 como marco normativo metodológico, las normas y protocolos enunciadas son una referencia o guía general para la práctica forense informática nacional e internacional, para que al momento de actuar en una práctica forense, los peritos expertos tengan una referencia general de trabajo basada en los principios forenses. Estos principios forenses se basan en una actuación metódica, con los recaudos necesarios para evitar alterar la evidencia digital y mantener la debida cadena de custodia a lo largo de todo el

proceso y en las etapas en las que interviene el perito. Es importante conocer los estándares, pero esto no implica que a través de los mismos se obtengan directrices o lineamientos para cada escenario o tecnologías a peritar, por lo que la profesionalidad y la experiencia del perito es esencial para el éxito de la pericia.

Si bien se plantean diferentes escenarios de actuación acompañados de buenas prácticas a considerar, los mismos son generales y no todas las recomendaciones son viables o aplicables para el trabajo pericial sobre base de datos, por lo **que se hace necesario particularizar la actuación del perito informático cuando la fuente de la evidencia digital a obtener es una base de datos**.

En el caso particular de las base de datos, **la diversidad de sistemas de gestión de base de datos SGBD y las plataformas posibles** donde se pueden implementar, genera un abanico de opciones que conlleva incluso a tratar con expertos por cada tipo de SGBD y/o plataforma de implementación. Esta necesidad lleva muchas veces a exponer o **arriesgar el éxito de una pericia a la expertis de profesionales que omiten o desconocen cuestiones fundamentales de la aplicación de la informática forense**.

La actividad forense en base de datos habitualmente depende de herramientas propias de cada Sistema de Gestión de Base de Datos relacional (SGBD). Por tal motivo **se requiere un alto nivel de experiencia en las bases de datos específicas** y se hace necesario el acompañamiento de un Administrador de Base de Datos (DBA, “Database Administrator”) o experto en cada motor.

El hecho de que las empresas o entidades gubernamentales cuenten hoy en día con entornos heterogéneos (Windows, Linux, Mainframe, Unix, OS/400, etc.) y diferentes motores de gestión de base de datos relacionales (tales como Oracle, Microsoft SQL Server), hacen más difícil el análisis forense de las transacciones efectuadas, la recolección válida de las pruebas y el logro de la confiabilidad de las evidencias. Más aún se complejiza cuando se necesita interactuar con infraestructuras basadas en configuraciones de RAID de discos, virtualización de discos o servidores en la nube.

Existen **multitud de sistemas de gestión de bases de datos relacionales**, tanto comerciales como libres. Entre las SGBD comerciales se pueden mencionar Oracle, Microsoft SQL Server, Informix, FoxPro, IBM DB2, Sybase, dBase, etc.

Como SGBD libres las más relevantes son MySQL, PostgreSQL, Firebird, Sqlite, etc.

La evidencia digital en base de datos es muy frágil, ya que su información está continuamente expuesta a cambios por parte de las aplicaciones o usuarios que acceden y utilizan las mismas. Por defecto, la información puede ser borrada, modificada o eliminada sin dejar rastros. Las múltiples conexiones desde las aplicaciones internas y externas hacen menos sencillo el seguimiento de las amenazas y vulnerabilidades de las bases de datos.

Las bases de datos son vulnerables, ya que los administradores en general no activan características avanzadas de seguridad, en pos de no perjudicar la velocidad de sus transacciones y minimizar el uso de recursos. Las nuevas infraestructuras del ambiente computacional provocan que el trabajo de aseguramiento de las bases de datos sea cada vez más exigente y especializada.

En líneas generales, se pueden clasificar los ataques en dos tipos. Los **ataques que no requieren autenticación** son los que no necesitan usuario y contraseña, suelen ser ataques externos y aprovechan alguna vulnerabilidad en la base de datos o en las aplicaciones que acceden a ella. Los **ataques que requieren autenticación** se lanzan por usuarios que poseen las claves de acceso, porque se han conseguido de forma ilícita o porque son usuarios autorizados.

Hay ataques que por un lado se aprovechan de alguna vulnerabilidad de la aplicación que accede a la base de datos (por ejemplo **SQL Injection**) o realizan un ataque directo a la base de datos (por ejemplo **ataque de fuerza bruta o diccionario**). La vulnerabilidad “SQL Injection” se basa en la no validación de los datos de entrada en la aplicación que accede a la base de datos pudiéndose ejecutar código o sentencias no deseadas. El ataque de fuerza bruta consiste en probar todas las combinaciones posibles para intentar el acceso a la base de datos. Los ataques pueden ser **externos** como **internos**. Se considera que los ataques internos pueden ser realizados tanto por los **usuarios** de la empresa como de los mismos **administradores de base de datos**.

Dentro de las vulnerabilidades de base de datos más comunes se pueden mencionar: contraseñas vacías, débiles o por defecto, otorgamiento de privilegios

innecesarios a usuarios, características del SGBD innecesarias habilitadas, desbordamiento de búfer (por el exceso de información y peticiones que recibe), falta de actualizaciones, datos sensibles sin cifrar, denegación de servicio (DoS, ataque en el cual se niega el acceso a la información a usuarios autorizados), exposición de los medios de almacenamiento para backup (a menudo se tiene protegida la base de datos, pero no se emplea la misma seguridad para proteger las copias de seguridad).

Incluso podrían surgir casos asociados a **errores humanos**. Se consideran **errores humanos de usuarios finales, errores por uso o desarrollo inapropiado de las aplicaciones o incluso errores del propio administrador de base de datos.** A diferencia del usuario final, los administradores del sistema tienen todo tipo de privilegios y acceso. En consecuencia, sus errores pueden tener mayor impacto y ser más difíciles de restablecer.

Para avanzar de manera confiable en un análisis forense en una base de datos, debe existir aseguramiento (buenas prácticas de seguridad) en el sistema de administración de base de datos. Los administradores o responsables de las base de datos deberían además de **administrar la seguridad a nivel general**, **conocer donde se almacena la información sensible, la cual está más expuesta a amenazas**.

No existe a la fecha un procedimiento estándar para adelantar y apoyar el análisis forense sobre base de datos. Existen sólo documentos específicos basadas y enfocadas en herramientas específicas principalmente de Oracle y MS SQL Server. En consecuencia, existe, por parte del investigador forense, una alta probabilidad de modificación involuntaria de datos mientras realiza la extracción de los mismos en las bases de datos, causando la invalidación de la prueba, perdiendo o corrompiendo la evidencia digital necesaria para que se pueda considerar en un proceso legal.

Esto provoca que **se generen dudas sobre la confiabilidad de las técnicas y herramientas utilizadas** y en consecuencia de la validez de las pruebas obtenidas. No se puede eludir la inseguridad que existe sobre si la evidencia digital obtenida es exacta, completa, clara, precisa, veraz y objetiva.

Por otra parte, en relación con la obtención de datos que puedan servir como prueba válida, en general los SGBD mantienen por defecto la información

histórica de los cambios realizados sobre los datos mientras los mismos estén involucrados en transacciones no confirmadas, una vez confirmadas las mismas, dependerá de cada motor y sus configuraciones el tiempo y forma en que el historial de cambios se almacene. Entonces **surge la necesidad de implementar técnicas especializadas de auditorías de datos,** propias de cada tipo de motor, que garanticen el resguardo de las operaciones realizadas sobre los datos que se consideren críticos para poder brindar información evolutiva de los datos para los potenciales análisis forenses.

En este punto es importante resaltar la complejidad de la implementación, análisis, resguardo, seguimiento y control de estas auditorías, las cuales dependen de especialistas en cada tipo de SGBD, que según la solución implantada pueden incluso perjudicar el rendimiento de las operaciones normales, lo cual ocasiona, en muchos casos, que se decida desactivarlas.

Disponer de mecanismos de auditorías de datos posibilita resolver uno de los problemas, que es la **complejidad en determinar el usuario** (y a partir de él intentar deducir la persona responsable) que ha originado la incidencia, así como obtener evidencia digital más completa para demostrarlo. En este sentido es que se hace primordial la aplicación de la **auditoría con fines forenses**. Disponer de estas auditorías permitirían no solo resolver el quién, el cuándo, el qué, el cómo, entre otras preguntas; sino también investigar y **analizar los sucesos o eventos a través de una línea de tiempo con trazabilidad**. Incluso la recolección y análisis de ciertos **archivos de log** sería un gran aporte. Lo cual también es algo complejo, ya que en general en las empresas u organismos no existen implementados mecanismos de resguardo adecuados de los archivos de logs o configuración de auditorías para lograr la **trazabilidad de la evidencia digital** y de los eventos críticos o sensibles de su entorno.

Otro escenario problemático es el gran volumen de **evidencia digital por procesar, pero con poco tiempo disponible para su análisis,** debido a que no se dispone de metodologías que clasifiquen la información asociada o técnicas y herramientas que simplifiquen la visualización de los datos recolectados y faciliten el análisis, revisión y la presentación de la evidencia. La falta de tiempo y la

urgencia es algo habitual, que se complica aún más cuando hay que analizar grandes volúmenes de información.

En este punto también resaltar que lo que se persigue ante un análisis pericial es responder los **puntos de pericias** que se plantean, por lo cual es importante recolectar la evidencia digital relevante según los mismos, aunque estos en ocasiones pueden ser lo suficientemente amplios o ambiguos, impidiendo establecer como filtrar la información relevante, es decir, **no siempre se cuenta con requerimientos claros, concretos y específicos al caso**.

Frecuentemente estas pericias involucran a grandes bases de datos, en general operativas, las cuales son críticas para la organización involucrada, más aún según la naturaleza de la misma (por ejemplo, el caso de hospitales o centros de salud). Se debe garantizar la integridad y la continuidad de las bases de datos, pero al mismo tiempo, extraer los datos de forma segura para interpretar los hechos y así poder probar las acciones que se han realizado. Por tal motivo, al ser imposible en estos casos hacer una adquisición de sistemas apagados o desconectar la red y menos aún secuestrar los servidores es necesario realizar análisis en vivo.

Al realizar un análisis en vivo de las bases de datos, se debe interactuar directamente con los datos en el momento o en el mejor de los casos se pueden hacer copias forenses de determinados archivos (por ejemplo, archivos de resguardos, logs, etc.), tal como se explicó en el punto 2.2.5.

Resulta clave poder realizar un **seguimiento eficiente** de los autores del hecho, de los objetos de estudio desde diferentes puntos de vista e investigar la magnitud del hecho mientras se protege los activos y tiempos de la organización. Frente a esta situación se plantea la necesidad de un proceso de identificación y clasificación de las fuentes de evidencia y posibles escenarios asociados, acompañados de pautas o criterios lógicos a seguir, para minimizar el impacto en la organización; alterando lo menos posible la operatoria de la empresa y, que la obtención y tratamiento de la evidencia digital sea correcto a nivel procesal y legal, obteniendo los permisos necesarios del fiscal y o el juez para las adquisiciones en vivo.

Las decisiones que se tomen deben estar debidamente justificadas y detalladas en la cadena de custodia. Incluso evaluar ante la posibilidad de

desconexión de los equipos o secuestro de los mismos, el **costo y las consecuencias** del período de tiempo en que las bases de datos y los sistemas asociados no estarían disponibles, la reinstalación, la puesta en marcha, revalidación, etc., tanto en la empresa como en el laboratorio de informática de forense donde se lleven los equipos o imágenes a peritar. Se puede considerar la alternativa de basar el **análisis forense a partir de los archivos de resguardo** ("backups"), según el contenido, rango de fechas que se necesite analizar y las fechas de los archivos de backups disponibles; obviamente rescindiendo la posibilidad de obtención de información volátil que se podría obtener al interactuar directamente con los servidores.

Dependiendo del escenario planteado para las adquisiciones en vivo se necesita tener acceso a los servidores de las BD, en estos casos se debe lograr que algún empleado o representante de la empresa nos indiquen la ubicación de los servidores y nos brinden las claves de acceso de forma voluntaria, sin mediar presión.

No solo se debe peritar la base de datos, sino también el **servidor que la contiene** (sea físico o virtual) de manera de investigar y recolectar evidencia sobre posibles ataques o vulnerabilidades explotadas al **servidor de base de datos**, incluso analizar archivos borrados o corruptos, cuentas de usuarios extrañas, la implementación del nivel de seguridad en relación a las políticas establecidas en la empresa, y determinar también si el servidor se encuentra comprometido o fue manipulado intencionalmente, entre otros.

Es relevante verificar y documentar la sincronización de los relojes del sistema, para poder obtener una **línea de tiempo de las acciones y la trazabilidad hasta el origen del hecho**.

Asimismo, el empleo de la evidencia digital en los procesos judiciales presenta **complejos problemas jurídicos vinculados con el derecho a la intimidad, las posibles afectaciones a terceras personas**, etc. lo cual se intensifica en el caso de bases de datos a periciar que contengan datos personales.

En el caso de las bases de datos **que almacenan datos personales**, se deben tomar todas las medidas necesarias para no violar los derechos fundamentales y garantías de protección de datos personales que dispone la **Ley**

sobre datos personales de trabajadores, clientes, pacientes, menores, usuarios, etc., descriptos en el punto 2.1.4. Más aún si los datos personales se relacionan a ciudadanos o empresas de la comunidad europea donde rige **el nuevo Reglamento General de Protección de Datos (RGPD) 2016/679**, o regulados por alguna otra ley internacional según la naturaleza de los datos, descriptos en el punto 2.1.5. Más allá que, desde el punto de vista de la ética el perito está obligado a guardar el secreto profesional, siendo consecuente con la información encontrada en sus actuaciones tanto por código ético como perito o por mandato civil como ciudadano, se deben fijar medidas de actuación para asegurar la protección de los datos personales. Esta protección no solo debe enfocarse en las fases de recolección, transporte y análisis, sino una vez finalizada las pericias y la investigación, se debe asegurar que se destruyan de forma fehaciente.

En efecto, la **protección de la privacidad de la información, no se conforma de manera exclusiva con la cadena de custodia**. Como se detalló en el punto 2.2.1, la **cadena de custodia** es un elemento que permite asegurar la confiabilidad de la información recolectada, implica la trazabilidad estricta de la misma, pero no protege por si sola al derecho a la privacidad. La privacidad requiere por supuesto confiabilidad, pero también respeto estricto de las normas procesales que resguardan el legítimo proceso asegurado constitucionalmente.

Podríamos estar en presencia de una cadena de custodia bien realizada, con una trazabilidad adecuada, con preservación estricta, pero que se haya realizado a partir de una acción ilegal o ilegítima. Por ejemplo, es ilegítima en el caso de una recolección de datos personales, que excede los límites de lo permitido, accediendo no sólo a la información estrictamente necesaria para responder los puntos de pericias, preservando otros elementos que nada tienen que ver lo solicitado.

Los **casos delictivos en general relacionados a base de datos** están relacionados a investigaciones por competencia desleal, fuga de información (robo de información), la modificación o eliminación valiosa (con fines de ocultamiento de información, fraudes, beneficios particulares, para perjudicar a la empresa dañando su imagen o reputación, causar pérdida de información valiosa de la empresa o hasta incluso afectar a trabajadores o clientes de la misma, perjuicios económicos, entre otros), ataques de denegación de servicio, etc.

Es muy habitual que la conclusión sea que los ataques se han producido **por parte de los empleados de la propia organización**, pero también se encuentran casos donde los daños son producidos **por atacantes externos**. Puede ser también que se necesite peritar una base de datos para verificar por ejemplo registros contables, ante una supuesta estafa, o el tratamiento que se le da a los datos personales que almacena **a partir de una denuncia**.

El analista forense de base de datos deberá tener en cuenta no solo incluir en el proceso forense los **datos persistentes**, sino los **datos no persistentes** y emplear estrategias para la recolección de datos y sus estructuras sin alterar la integridad de las mismas, afectando la operatoria lo menos posible. La **recolección debe ser realizada considerando la volatilidad de los datos y estructuras**, sin excluir los archivos de log y de auditoria, que son de gran aporte para la trazabilidad y la reconstrucción de los hechos en una línea de tiempo.

Todas las acciones que se lleven adelante deben ser registradas, al igual que todas las herramientas y técnicas utilizadas indicando sus capacidades y resultados, incluso registrar los posibles cambios que puedan introducirse en la base de datos al efectuar actividades, de manera de **garantizar la debida cadena de custodia y asegurar la confiabilidad y la trazabilidad del proceso**.

Prevenir los riesgos de invalidar una prueba se convierte en una responsabilidad y un reto profesional difícil de llevar a cabo para aquellos que trabajan como analistas forenses de bases de datos. Luego de investigar y analizar diversas normas, metodologías y técnicas, se puede afirmar que **no existe en la actualidad una metodología forense específica de base de datos** (de aplicación independiente del tipo de motor de base de datos), que permita guiar cómo identificar, recolectar y analizar de manera integral las fuentes de evidencia digital en las mismas, permitiendo reconstruir la secuencia de eventos en el tiempo y que sean admisibles en un proceso judicial.

Incluso, **tampoco existe una metodología forense informática general detallada** a tal punto que sirva de base para a partir de la misma especificar a lo que a la base de datos refiere. En general son metodologías genéricas, o se enfocan en determinadas fases. Algunas se basan en una metodología muy global o conceptual y los detalles los indican a través de ejemplos y no en la

propia metodología. Otras hacen mucho hincapié en temas legales y procesales, incluso de fueros específicos, y no en temas metodológicos o tecnológicos. Se plantean metodologías con un exceso de fases y otras, todo lo contrario.

En general, las metodologías estudiadas no plantean etapas enfocadas a la planificación, análisis de factibilidad, análisis de capacidades o riesgos, ni tampoco actividades de seguimiento y control o de evaluación de resultados con fines de calidad o mejora continua.

Si bien no siempre es fácil definir o decidir a priori todos los pasos a realizar, ya que los escenarios pueden ser infinitos**, existe la necesidad de una metodología aplicable a base de datos** que brinde determinadas guías, pautas o criterios lógicos a seguir ante decisiones, en especial drásticas, tanto desde el punto de vista técnico, como legal y procesal, basada en la naturaleza de los datos, brindando confiabilidad y trazabilidad al proceso.

Asimismo, se plantea la necesidad del diseño de una **metodología de tratamiento de la evidencia digital general** (basada en ideas y conceptos de las metodologías estudiadas) en la cual se detallen fases y actividades que no están definidas, diferenciadas o destacadas en las metodologías actuales, la cual sirva de base para el diseño particular de la **metodología aplicable a base de datos**.

A través de la aplicación de la metodología propuesta, se espera lograr una mejora la confiabilidad del análisis forense en base de datos, brindando garantías en todo el proceso.

3.2. Hipótesis de trabajo

Disponer de una metodología de análisis forense informático específica de base de datos relacionales garantiza la confiabilidad de las diversas actividades a realizar por parte del perito informático forense y de la admisibilidad de la evidencia digital obtenida.

Además, si la metodología mencionada se basa en la configuración preventiva de auditorías y la recolección de resultados de las mismas como evidencia digital admisible, posibilitaría no solo obtener información más valiosa del contexto de los hechos, sino reconstruir los sucesos o eventos en una línea trazable de tiempo.

3.3. Objetivos

Objetivo General

- Elaborar una metodología de análisis forense en base de datos relacionales que sirva de guía para la actuación pericial garantizando la confiabilidad de las actividades de identificación, recolección, adquisición y análisis de evidencia digital admisible como prueba en un proceso judicial.

Objetivos Específicos

- Analizar normativas, metodologías y estándares relacionados con la admisibilidad y tratamiento de la evidencia digital.
- Comprender el marco legal y procesal en el que se desarrollan las actividades forenses informáticas.
- Investigar metodologías forenses informáticas aplicables a base de datos.
- Desarrollar una metodología forense informática general como base de la específica de base de datos relacional.
- Desarrollar una metodología forense aplicable a las actividades del forense de base de datos relacional.
- Definir de qué manera la información obtenida a partir de la ejecución de auditorías de datos se puede considerar como fuente de evidencia digital válida.
- Incluir en la metodología forense de base de datos el tratamiento de la información obtenida a partir de auditorías de datos.
- Integrar la metodología forense de base de datos basada con la metodología de auditoría universal de Datos.

3.4. Límites

A nivel tecnológico, la metodología de análisis forense de base de datos relacionales propuesta es aplicable a la actuación pericial sobre cualquier tipo de sistema de gestión de base de datos relacional.

La metodología de análisis forense de base de datos relacionales propuesta tiene como principal foco los datos contenidos en las base de datos, es decir la base de datos en sí y no el servidor que la contiene.

Como base de la metodología específica de base de datos relacional, se especifica una metodología general integral que se puede considerar como referencia para cualquier actuación pericial informática.

La metodología no especifica reglas o directrices para casos donde las bases de datos están contenidas en la nube o correspondan a bases de datos no relacionales.

La metodología no describe las particularidades de casos donde las bases de datos están contenidas o sincronizadas en dispositivos móviles.

En relación con los aspectos legales vinculados a la actuación forense, la metodología se basa en la legislación de la República Argentina. No enfoca su aplicación en un fuero específico, por lo cual podría utilizarse en casos del fuero civil, comercial, penal, laboral, etc.

La metodología puede ser aplicable tanto a casos judicializados como privados y ser utilizada tanto por peritos de oficiales, de parte u oficiales. Independientemente que sean casos judicializados o no, la metodología considera la ejecución de actividades y procedimientos necesarios para la admisibilidad de la evidencia digital en un proceso judicial.

En lo referido a la Protección de Datos Personales, además de la ley nacional de Protección de Datos Personales Ley 25.326, la metodología se enfoca también en ciertos requerimientos del nuevo Reglamento General de Protección de Datos (RGPD) 2016/679, de la comunidad europea.

Capítulo 4 – Solución Propuesta

4.1. Descripción General de la Solución

La solución propuesta comprende el desarrollo de una **metodología de análisis forense informático para la obtención de evidencia digital en base de datos relacionales (AUDBForense)**.

AUDBForense está basada en la aplicación de dos metodologías propias de base de datos (Ver Figura 5):

- ✓ **Metodología de auditoría universal de base de datos (AUDB).**
- ✓ **Metodología forense informática en base de datos (ForenseDB)**.

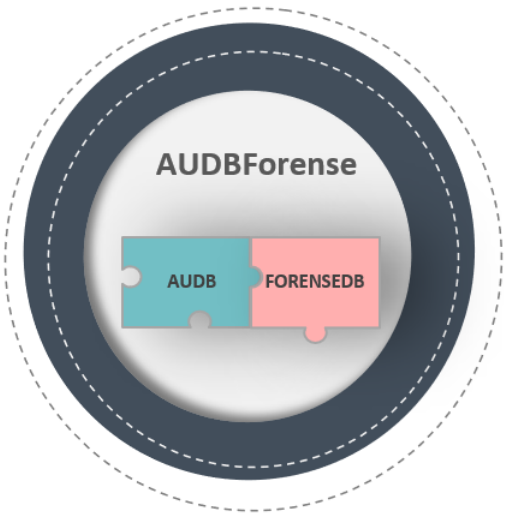

Figura 5: Metodología AUDBForense

AUDB actúa como base de generación de evidencia digital para la investigación forense. **ForenseDB** se nutre y realimenta a la auditoria forense **AUDB**.

La metodología **AUDB** es una versión mejorada y ampliada de la **metodología de auditoría universal de datos no invasiva (Gioia 2012)**, explicada en forma general en el punto 2.4., a la cual también se incorpora principios de la **auditoría forense** en base de datos. En la siguiente Figura 6 se puede visualizar las fases de AUDB.

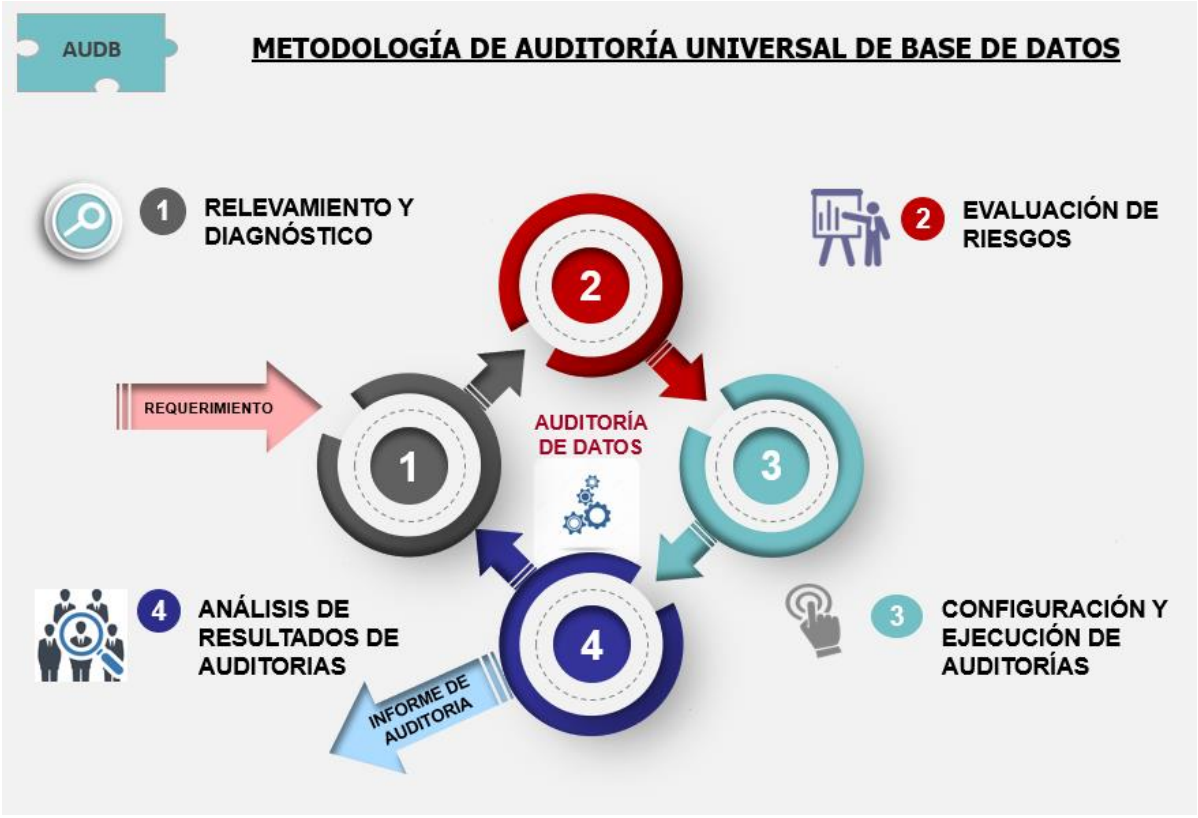

Figura 6: Metodología AUDB

Como parte de la solución y como base de la metodología ForenseDB se plantea el diseño propio de una metodología informática forense aplicable a cualquier tipo de evidencia digital, es decir, a evidencia digital universal (**UDE, Universal Digital Evidence**). En dicha metodología, denominada **ForenseUDE,** se definen y describen las etapas y actividades comunes aplicables a cualquier fuente de evidencia digital.

A partir de **ForenseUDE** se especifican las tareas propias a considerar en las bases de datos relacionales (**ForenseDB**).

El **ForenseUDE** se sustenta de ideas y conceptos del **modelo PURI** (Proceso Unificado de Recuperación de Información) y del **modelo EDRM** ("Electronic Discovery Reference Model"), como también, en la **norma ISO/IEC 27.037**.

Se puede visualizar el gráfico en le Figura 7 con las etapas de la metodología de **ForenseDB**, las cuales son coincidentes con **ForenseUDE**.

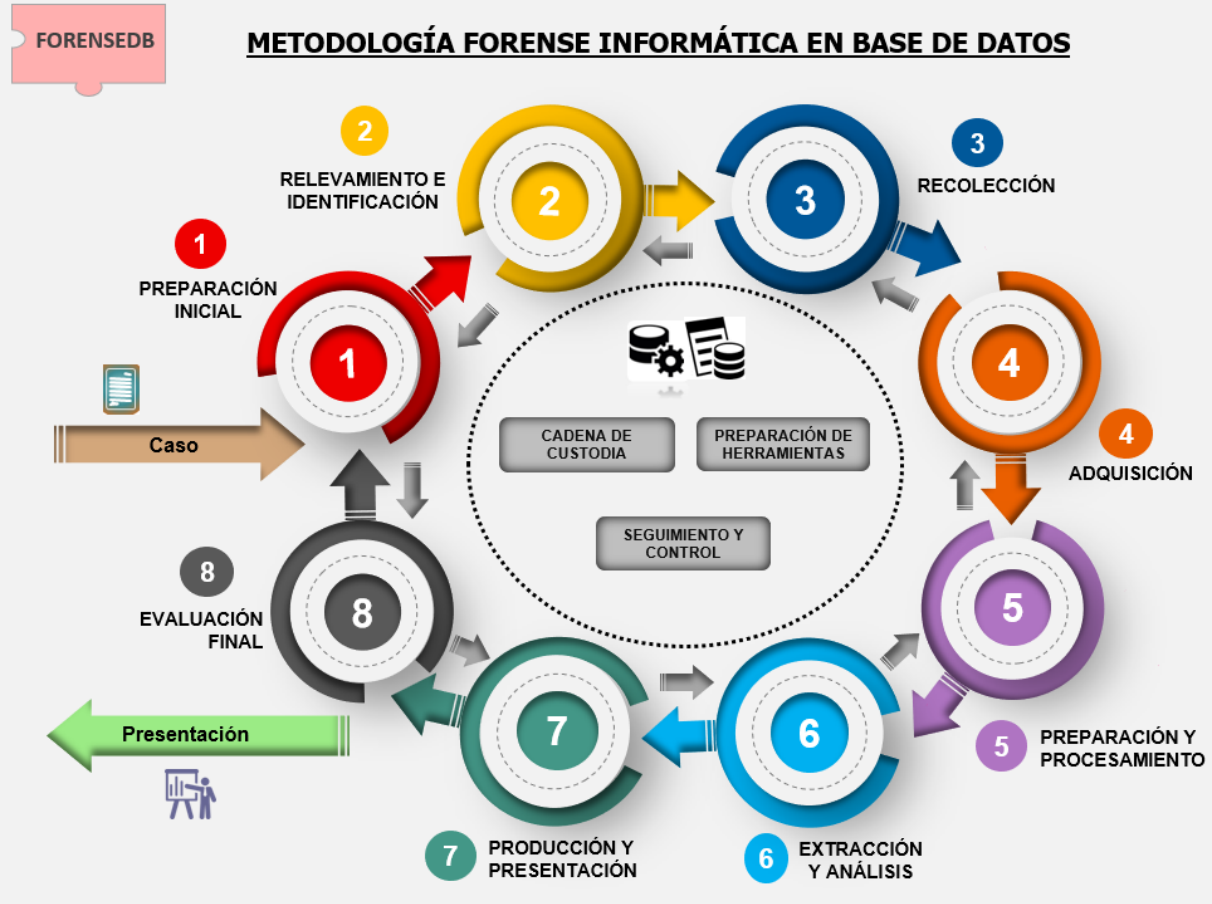

Figura 7: Metodología ForenseDB

La metodología de análisis forense informático para la obtención de evidencia digital en base de datos relacionales se plantea conforme a la **legislación de delitos informáticos** de la República Argentina. Asimismo, en lo referido a la protección de datos personales, a la **Ley Nacional 25.326**, y en ciertos requerimientos del **Reglamento General de Protección de Datos (RGPD) 2016/679 de la comunidad europea**.

Básicamente en la solución propuesta, los resultados de la implementación de auditorías de datos basadas en **AUDB**, proporcionan evidencia digital relevante para la investigación forense de casos que requieran la actuación de peritos en informática. Del mismo modo el resultado de las investigaciones y análisis forense de **ForenseDB** realimentan a las auditorías de datos y sus configuraciones. Se plantea de esta manera dos modelos complementarios que se retroalimentan entre sí, conformando una **metodología de análisis forense informática integral AUDBForense** que actúa de manera preventiva, reactiva y proactiva en pos del resguardo de la confidencialidad, integridad y disponibilidad de los datos sensibles.

De todas formas se plantea como parte de la aplicación de **ForenseDB** la posibilidad también de aplicar dicha metodología de forma independiente a AUDB.

A continuación, en la Figura 8 se visualiza el gráfico general de la solución propuesta:

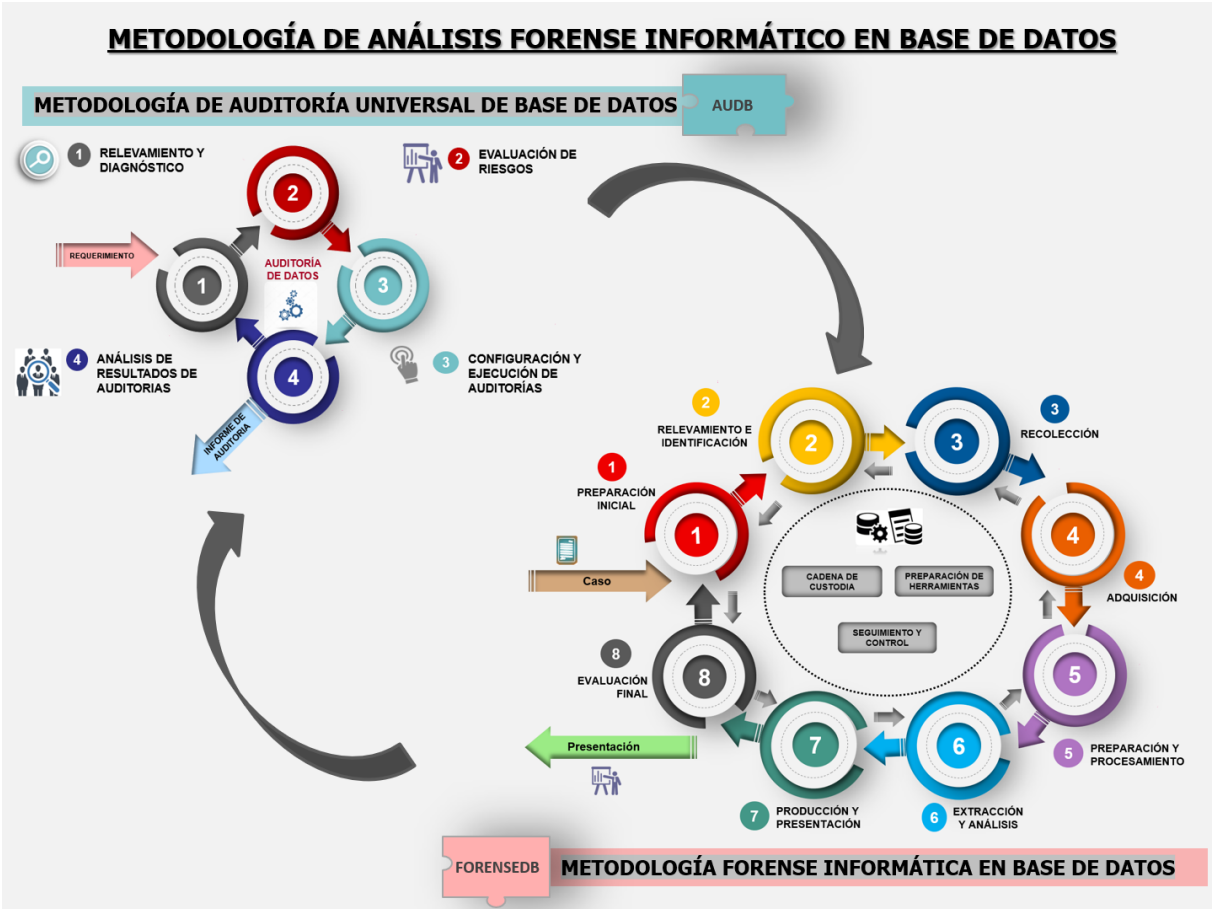

Figura 8: Metodología de Análisis Forense Informático en Base de Datos (AUDBForense)

Previo a detallar la solución, cabe aclarar la diferencia entre los términos **datos** e **información**. Los "datos" es un término que se refiere a hechos, eventos, transacciones, etc., que han sido registrados en las bases de datos. Son la entrada sin procesar de la cual se produce la información. Un dato por sí mismo no constituye información. La "información" se refiere a los datos que han sido procesados, analizados y comunicados de tal manera que pueden ser entendidos e interpretados por el receptor. Por lo que, en la solución propuesta, se hace referencia a "datos" sobre los cuales se aplican las auditorías. Según el caso, se hace mención al término "información auditada" cuando se hace referencia a resultados de auditorías analizados y/o procesados o al término "datos auditados" cuando se refiere solo a resultados registrados sin analizar o procesar. También se hace mención a "información" a la que se encuentra almacenada en las bases de datos y que tiene significado y relevancia para la organización, siendo esenciales para la consecución de los objetivos y continuidad de las mismas.

4.2 Metodología de Auditoría Universal de Base de Datos (AUDB)

La **Metodología de Auditoría Universal de Base de Datos (AUDB)** se basa principalmente en los principios de la **auditoría forense preventiva**, la cual posibilita prevenir y predecir situaciones indebidas, dudosas o maliciosas que podrían estar relacionadas con potenciales delitos definidos, como también la detección de la ocurrencia de los mismos.

La auditoría forense en base de datos planteada mantiene un **enfoque de auditoría legal** que permite obtener evidencia digital confiable y un programa de aseguramiento constante del riesgo de ataques o incidentes de seguridad sugiriendo medidas de control. La misma tiene como objeto de estudio los posibles ilícitos relacionados con los datos de las bases de datos de la organización de forma preventiva, aunque también reactiva.

Se basa en la configuración de **auditorías forenses**, en base a potenciales riesgos evaluados, donde la ejecución de las mismas se lleva a cabo aun cuando

no existe una declaración o aviso de delito, o incluso cuando no existe ningún fallo en controles que sugieran que un ilícito podría estar ocurriendo.

El **auditor forense** diseña estrategias para responder a los riesgos y obtener evidencia digital de las operaciones críticas como también para proveer de un marco de un plan de investigación.

A continuación, en la Figura 9 se visualiza el proceso general planteado por la metodología AUDB:

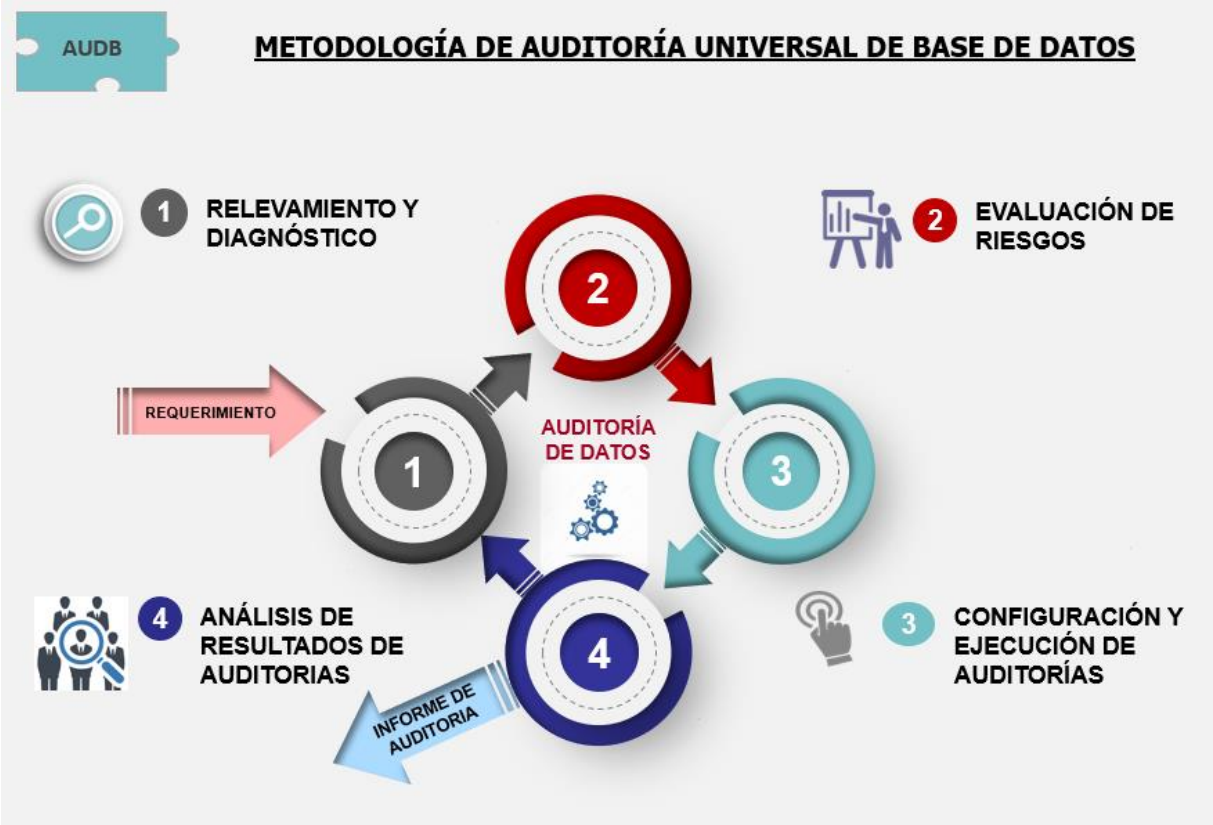

Figura 9: Metodología AUDB

4.2.1 Descripción de la Metodología de Auditoría Universal de Base de Datos

AUDB se basa en la configuración y ejecución de **Auditorías de Datos Universales**. La palabra **auditoría** alude a la revisión y verificación de una determinada actividad, y en este caso particular, a las **auditorías de datos** sobre la información almacenada en base de datos.

Las principales características de la **Auditoría Universal** descriptas se sintetizan en la siguiente Figura 10:

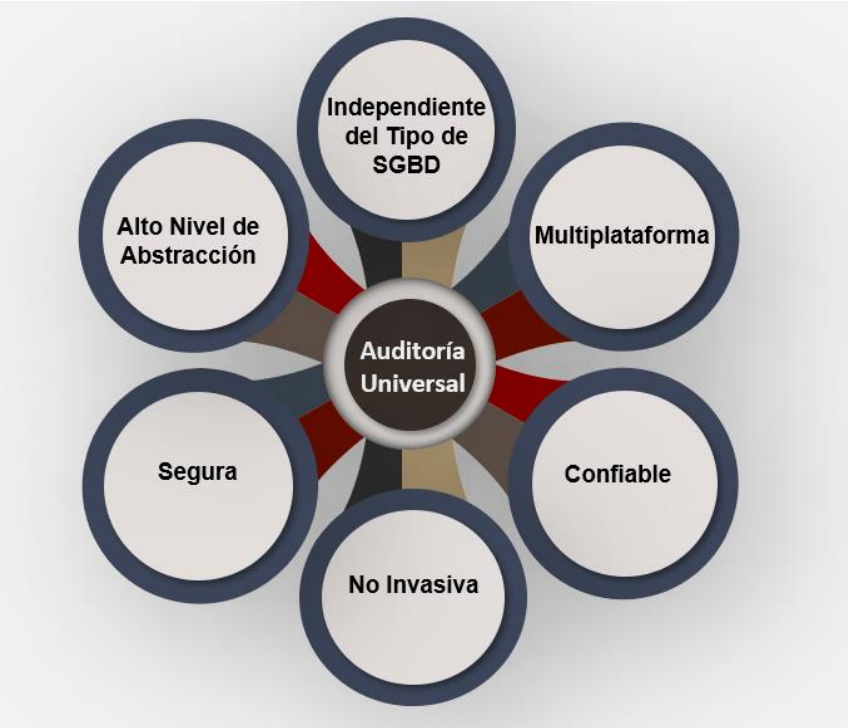

Figura 10: Características de la Auditoría Universal

El término "**universales**" se refiere a que corresponden a auditorías de datos que pueden ser aplicables **sobre cualquier motor de bases de datos relacional (SGBD), independientemente de la plataforma o sistema operativo** y con **alto nivel de abstracción** conceptual, funcional y técnico.

Se consideran **datos sensibles**, aquellos datos **críticos** o de gran importancia para la organización y su operatoria, o los relacionados a **datos personales de terceros**. Los datos sensibles son aquellos donde la confidencialidad, la integridad y las disponibilidad de los mismos son críticos a la operatoria de la organización o que por ley deben ser objeto de privacidad.

Las auditorías de datos universales se caracterizan por ser **no invasivas**, es decir, que su ejecución no afecta a la disponibilidad o funcionamiento de los sistemas. Se debe evitar que por temas de disponibilidad o rendimiento no se ejecuten o se interrumpan la ejecución de las mismas.

Las auditorías de datos universales son **confiables**, basadas a partir de auditorías sobre las bases de datos y con la aplicación de mecanismos de **seguridad** apropiados que garantizan también la integridad, confidencialidad y el no repudio de los datos auditados, como la protección de los mismos.

Las **auditorías de datos posibilitan obtener la evidencia digital** de las operaciones y actividades que los usuarios, procesos o aplicaciones realizan sobre los datos que se consideran sensibles. Con el resultado de las auditorías se puede analizar, revisar y aplicar controles sobre las actividades críticas o dudosas y detectar o prevenir futuras acciones maliciosas o delictivas que pueden afectar la confidencialidad, integridad o disponibilidad de la información. De esta manera se realimentan la configuración y ejecución de las auditorías de datos como parte de un **proceso iterativo incremental de mejora continua**.

Las auditorías de datos deben basarse y estar alineadas con **las políticas de seguridad de la información de la organización y basadas principalmente en riesgos detectados**.

Previamente a configurar las auditorías de datos, se deben evaluar los riesgos potenciales sobre los datos sensibles y configurar las auditorías basadas en las amenazas e impacto de las mismas, de manera de mantener **el equilibrio adecuado entre la necesidad de resguardar la seguridad y trazabilidad de los datos y la operatoria de los sistemas.**

Los usuarios que acceden y gestionan la información de las bases de datos pueden conectarse directamente a las bases, a través de procedimientos propios del motor de base de datos, desde cualquier tipo de aplicaciones que posean o logren acceso a la misma, sean internas o externas a la organización (como ser sitios web, servicios web, etc.). Incluso los datos pueden ser manipulados por procesos en ejecución, sin intervención directa de un usuario.

La **ejecución continua** (ininterrumpida) de las auditorías de datos retroalimenta a la estrategia de seguridad y de auditoría aplicada al motor de base de datos, al detectar riesgos potenciales, por ejemplo, a los que se expone ante el otorgamiento de determinados permisos a usuarios o aplicaciones o actividades dudosas en determinados días y horarios. La ejecución de las mismas, en el

tiempo, facilita la **trazabilidad y la obtención de la evidencia digital** asociada a acciones a investigar.

La metodología de auditoría universal de datos sirve de **apoyo a la prevención y detección de intrusiones y al control de la confidencialidad, la integridad y la disponibilidad de los datos a partir de los riesgos detectados**, basándose en la validación de políticas de seguridad sobre los datos auditados. Posibilita alertar, en tiempo y forma, la existencia de modificaciones que comprometan la integridad de los datos, como de lecturas que comprometan su confidencialidad.

La metodología AUDB plantea la posibilidad de ejecutar **alertas tempranas basadas en políticas**, lo cual no solo ayuda a acelerar, focalizar y asegurar las investigaciones forenses sino a respetar las leyes nacionales e internacionales vinculadas a protección de datos.

Por otro lado, registrar y notificar los desvíos e incidentes posibilita aplicar un **proceso de mejora continua** a la hora de definir las políticas de seguridad a validar y al **establecer listas de escalamiento**, y así a reducir la probabilidad de ocurrencia de riesgos potenciales de acciones maliciosas o perjudiciales.

En la siguiente Figura 11, se muestra las **principales características de las Auditorías de Datos**, sobre las que se basa la metodología AUDB.

Figura 11: Características de las Auditorías de Datos

4.2.2 Objetivos de la Metodología de Auditoría Universal de Base de Datos

Los objetivos de la Metodología de Auditoría Universal de Datos son:

1. Disponer de técnicas eficientes de auditoría de datos que permitan incrementar la protección y seguridad de la información almacenada y manipulada en las base de datos.
2. Aplicar auditorías de datos en base a análisis de riesgos y políticas de seguridad de la información, para prevenir y detectar intrusiones a partir de la detección de la ejecución o intento de ejecución de operaciones críticas, maliciosas, dudosas e indebidas sobre datos sensibles o personales.
3. Brindar facilidades de trazabilidad y análisis histórico de las operaciones realizada sobre los datos para la detección de fraudes, potenciales hechos delictivos o maliciosos, posibilitando el seguimiento y control de las acciones sobre datos sensibles.
4. Contar con los mecanismos adecuados para la evaluación del cumplimiento de las leyes de Protección de Datos Personales nacionales e internaciones, permitiendo conocer y analizar el detalle de los accesos de lecturas y modificaciones sobre los datos personales y sensibles, tanto para personal técnico como para auditores que no posean un alto nivel de conocimiento de cada uno de los diferentes motores de bases de datos y las plataformas donde se implementen.
5. Contar con los mecanismos adecuados para la evaluación del cumplimiento de las leyes y reglamentaciones que afecten a los datos y su tratamiento aplicables según la naturaleza de la organización.
6. Establecer notificación de alertas tempranas, con escalamiento de mensajes a los responsables de seguridad y/o auditoría, para posibilitar la prevención y la respuesta temprana, incluso desatendida (es decir autoprotección), ante un intento de ataque informático o acciones maliciosas o dudosas, logrando así el aumento de la seguridad objetiva de los sistemas de información.
7. Brindar soporte al cumplimiento de requerimientos de la norma de seguridad IRAM-ISO/IEC 27.001 (Sistemas de Gestión de la Seguridad de la Información

– Requerimientos) aplicables a la auditoría de datos sobre motores de base de datos.

8. Facilitar la gestión y detección de los riesgos de la seguridad de la información en base de datos relacionales dando soporte a la aplicación de una metodología de administración de riesgos (en referencia a la norma ISO/IEC 27.005:2011).
9. Facilitar el proceso de evaluación de la eficacia del Sistema de Gestión de la Seguridad de la Información (SGSI) sobre la seguridad de los datos almacenados en motores de base de datos relacionales (en referencia a la norma ISO/IEC 27.006).

En la siguiente Figura 12, se visualizan los puntos claves en los que se basa la metodología AUDB:

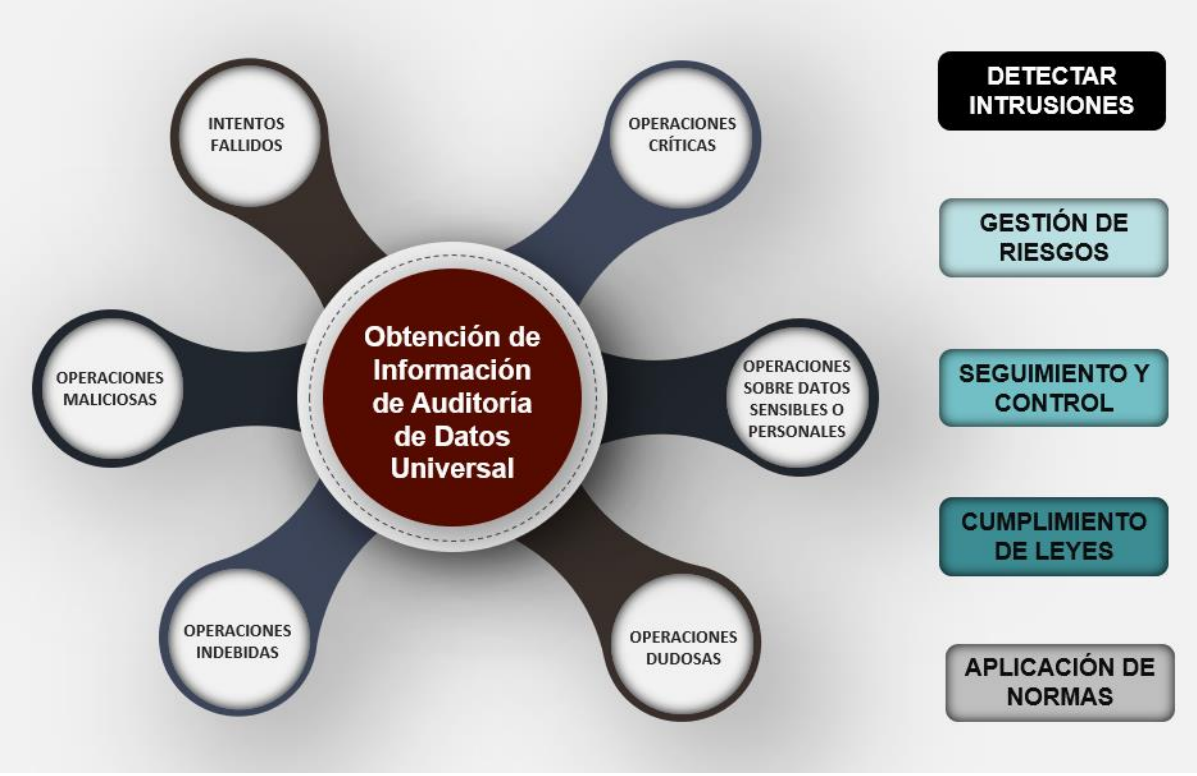

Figura 12: Puntos claves de AUDB

4.2.3 Fases de la Metodología de Auditoría Universal de Base de Datos

La metodología AUDB se basa en un **proceso iterativo e incremental** que consta de cuatro fases principales, como se puede visualizar en la Figura 13: 1) Relevamiento y diagnóstico; 2) Evaluación de riesgos; 3) Configuración y ejecución de Auditorías; 4) Análisis de resultados de auditorías.

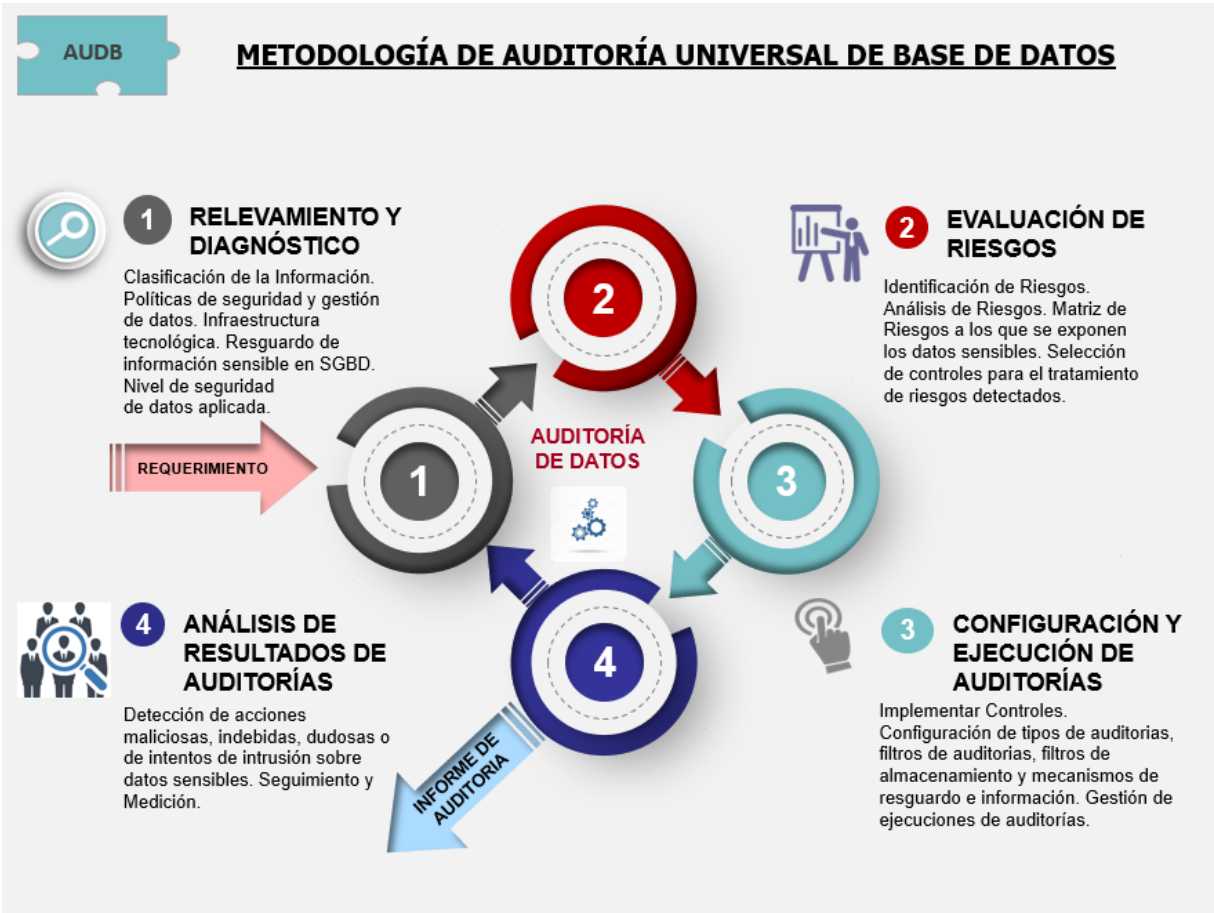

Figura 13: Fases de AUDB

A continuación, se describen cada una de las fases del proceso y sus actividades principales:

1. Relevamiento y Diagnóstico

Previo a la configuración de las auditorías de datos es importante realizar el relevamiento de la infraestructura tecnológica, para conocer no solo donde se resguarda o se accede a la información sensible, sino el contexto operacional, tecnológico y de seguridad de la misma.

Si bien la metodología se enfoca en las auditorías de datos, propiamente en motores de base de datos relacionales, se entiende que cualquier estrategia de seguridad debe poseer una visión integral, de manera de reducir al máximo posible los riesgos derivados del entorno. Por tal motivo es importante obtener el conocimiento de cómo se accede o manipula la misma, más allá de los límites del propio motor de base de datos.

La fase de relevamiento se enfoca también en investigar y analizar la administración de seguridad de los datos, para poder diagnosticar qué información es más vulnerable en el contexto de la organización y así, poder enfocar y reforzar aún más las auditorías de datos asociadas a las mismas en los datos y escenarios de mayor riesgo.

Las actividades generales de la fase de relevamiento son:

1) Conocer la naturaleza de la organización y obtener una visión general de los datos sensibles de la misma. Esto implica conocer la información relevante para la organización y la que por ley debe ser objeto de privacidad, disponibilidad e integridad.
2) Determinar el alcance de los datos personales almacenados, es decir si corresponden a datos personales en el ámbito nacional o internacional, para determinar las leyes de datos personales que aplican.
3) Clasificar la información que se considera crítica o sensible a la organización.
4) Disponer y conocer las políticas y procedimientos de seguridad existentes.
5) Relevar cómo se accede, actualiza, almacena y visualiza la información crítica o sensible, considerando tanto usuarios, procesos y sistemas que interaccionan con la misma a través de las bases de datos.
6) Relevar la infraestructura tecnológica general y de seguridad en los servidores y en las base de datos (donde se almacenan los datos a auditar) y su

contexto.

- Obtener información de configuración de los servidores y bases de datos que contienen los datos sensibles: relevar tipos servidores existentes, virtualización de servidores, servidores en la nube, tipo de motores de base de datos, versiones de softwares, formas de acceso o conexión a las mismas, sistemas o aplicaciones que las utilizan y con qué roles se conectan, transferencia de datos entre base de datos, entre otros aspectos que puedan ser relevantes según las características técnicas de cada contexto.
- Relevar y analizar la estrategia de seguridad general implantada en la infraestructura tecnológica.
- Relevar y analizar la estrategia de seguridad implantada en los motores de base de datos involucrados y en las bases de datos en si (qué usuarios pueden acceder, leer, actualizar, insertar o borrar datos, con qué roles, privilegios, permisos y de qué forma).
- Analizar políticas de resguardo y planes de contingencia de información implementados y cómo se llevan técnicamente a la práctica.

7) Obtener información de las base de datos y tablas que contengan los datos sensibles a auditar:
   - Determinar qué base de datos almacenan la información sensible.
   - A partir de la información clasificada como crítica o sensible, relacionar las tablas y campos asociados.
   - Determinar frente a qué acciones, usuarios, aplicaciones, horarios o cualquier variable de entorno o contenido de datos se consideran sensibles los campos y tablas.
   - Analizar las tablas con datos sensibles y sus relaciones con otras tablas de la misma base de datos u otra.
   - Investigar si existen algún tipo de replicación total o parcial de la información crítica a auditar, ya sea a otras tablas, archivos, servicios y la finalidad de la replicación.
   - Determinar claramente qué usuarios y sistemas acceden y manipulan la información sensible, de qué forman gestionan el acceso a la misma, tipos de conexión, información que se visualiza o modifica a través de

los diferentes sistemas y computadoras, horarios habituales de acceso, entre otras variables de entorno relevantes para el diagnóstico de criticidad.

- Relevar, si existiese, una estrategia de auditorías implementada y analizar las características de las mismas en cuanto a qué se audita, cuándo, de qué forma, la continuidad de la ejecución de los mismos y el control y seguimiento aplicado sobre las mismas.
- Incluir en el análisis las restauraciones de bases de datos y las bases de datos utilizadas para migraciones de datos.
- Investigar si existe información cifrada en las bases de datos y la estrategia de implementación asociada.
- Investigar el contenido de las bases de datos disponibles en ambientes de desarrollo, prueba y preproducción (y los que existiese). Conocer la política de seguridad de datos asociada a la generación, disponibilidad y acceso de datos en dichos ambientes (por ejemplo, verificar que en las mismas no se disponga de información de datos personales, que pudieran estar al alcance de un desarrollador de software, etc.).

8) Diagnosticar el nivel de la seguridad de datos aplicada por la organización, a partir de la evaluación de las medidas de protección de la privacidad digital que se aplican para evitar el acceso no autorizado a los datos y como se protege a los datos de una posible corrupción. Incluso considerar qué acciones o medidas toma la organización ante ataques a los datos sensibles.
9) Documentar la información de la etapa de relevamiento en un documento que formará parte de la justificación de la estrategia de auditoría a implementar.

2. Evaluación de Riesgos de la Información

El relevamiento y diagnóstico de la información posibilita armar una **matriz de riesgos potenciales**, donde se determina el nivel de los riesgos a los que se expone los datos a partir de la clasificación de criticidad los mismos en relación con la naturaleza de los datos, la infraestructura en general implantada, la seguridad de la información en el SGSI y la seguridad de los datos en particular.

Disponer de la matriz de riesgos a los que se expone la información es la base para el diseño de la estrategia de auditoría de datos a implementar.

Es importante como parte del análisis de riesgos clasificar la información en cuanto a su criticidad para la organización y sus propietarios.

La auditoría de datos es un proceso implementado por los auditores de sistemas (o administradores) con el fin de auditar los accesos a los datos, por lo general siguiendo una metodología basada en una lista de comprobación que contempla los puntos que se quieren auditar y que surgieron mediante la evaluación de riesgos potenciales volcada en la matriz de riesgos correspondientes.

3. Configuración y Ejecución de Auditorías

La configuración de auditoría de datos se basa en una combinación de selección de los tipos de auditorías de datos a utilizar, los filtros de auditorías a aplicar, los filtros de almacenamiento de la información auditada, la elección del mecanismo de almacenamiento seguro de la información auditada y la elección del nivel de protección de visualización de la información auditada (estos puntos se explicarán en detalle en la sección 4.2.4).

Al momento de configurar las auditorías se indican las operaciones o campos que se van a auditar en las tablas que contienen la información sensible.

La metodología incorpora la posibilidad de configurar diferentes tipos de auditorías de datos, según los cuales se puede decidir auditar los datos a partir de la ejecución de determinadas operaciones sobre las tablas o sobre determinados campos específicos, en base a valores de los datos, operaciones sobre estructura de datos de la tabla, operaciones de lecturas o incluso en base a información de contexto de las acciones con la finalidad de auditar a determinados usuarios, orígenes de conexiones o acciones en determinados horarios, entre otros. También es posible auditar los intentos fallidos de operaciones sobre datos sensibles.

En la configuración de los distintos tipos de auditorías se puede indicar, por ejemplo, si se necesitan auditar todos los campos de una tabla o solo algunos.

Esto es gracias a que la metodología considera disponer de filtros de auditoría para lograr que se audite específicamente lo que se considera sensible de auditar.

Como resultado de las auditorías se puede configurar almacenar todos los datos del registro auditado, los valores de ciertos campos o incluso solo las operaciones. Los filtros de almacenamiento permiten configurar los datos auditados que se necesita almacenar de manera de no resguardar información que no es necesaria, tanto por volumen como por suficiencia. Es importante aclarar que, en el caso de decidir solo registrar los cambios al campo sensible, se deberán también resguardar por defecto los campos claves o identificatorios que sirven para identificar a qué registro correspondía.

Las auditorías activas deben controlarse en su ejecución, de manera de garantizar la continuidad de los mismas, alertando cualquier anormalidad que pudiera afectar o estar impidiendo las ejecuciones de las mismas.

4. Análisis de Información Auditada

A partir de la evidencia digital recolectada por las auditorías de datos se puede conocer, analizar y controlar las actividades de los usuarios para detectar acciones maliciosas, dudosas o indebidas que pudieran involucrar potenciales hechos delictivos o que puedan afectar la confidencialidad, integridad o disponibilidad de la información. El análisis de los resultados obtenidos es una importante fuente de información para prevenir inconvenientes a futuro. Además, las ejecuciones de las auditorías de datos retroalimentan a la estrategia de seguridad aplicada al motor de base de datos al detectar riesgos potenciales. De esta manera se plantea un proceso iterativo, que retroalimenta las auditorías de datos configuradas como parte de un proceso de mejora continua.

Considerando que los resultados de las auditorías se pueden visualizar tanto en módulos del propio sistema de auditoría que se implemente como en reportes emitidos por el mismo, se establecen niveles de protección de visualización basados en la autorización de visualización, visualización con enmascaramiento y/o con enriquecimiento.

Las diferentes fases forman parte de un proceso iterativo que se retroalimenta con la finalidad de mejorar la estrategia de auditoria implementada a partir de los resultados obtenidos. Estas mejoras o ajustes pueden surgir con la finalidad de mejorar la calidad de las auditorias configuradas o por el surgimiento de nuevos hechos o riesgos detectados. Es importante considerar que las bases de datos no son estáticas, además de crecer en volumen continuamente, pueden sufrir diversas modificaciones (sean por mejoras o ajustes en las aplicaciones vinculadas, por cambios de políticas de acceso a las mismas, etc.) lo cual implica ajustar la estrategia de auditoría.

4.2.4 Configuración de Auditorías de Datos

Existen diferentes características para tener en cuenta al momento de configurar las auditorías de datos, de las cuales existe una categorización y clasificación clara.

A continuación, en la Figura 14, se presenta el flujo de actividades que involucran la configuración de auditorías de datos:

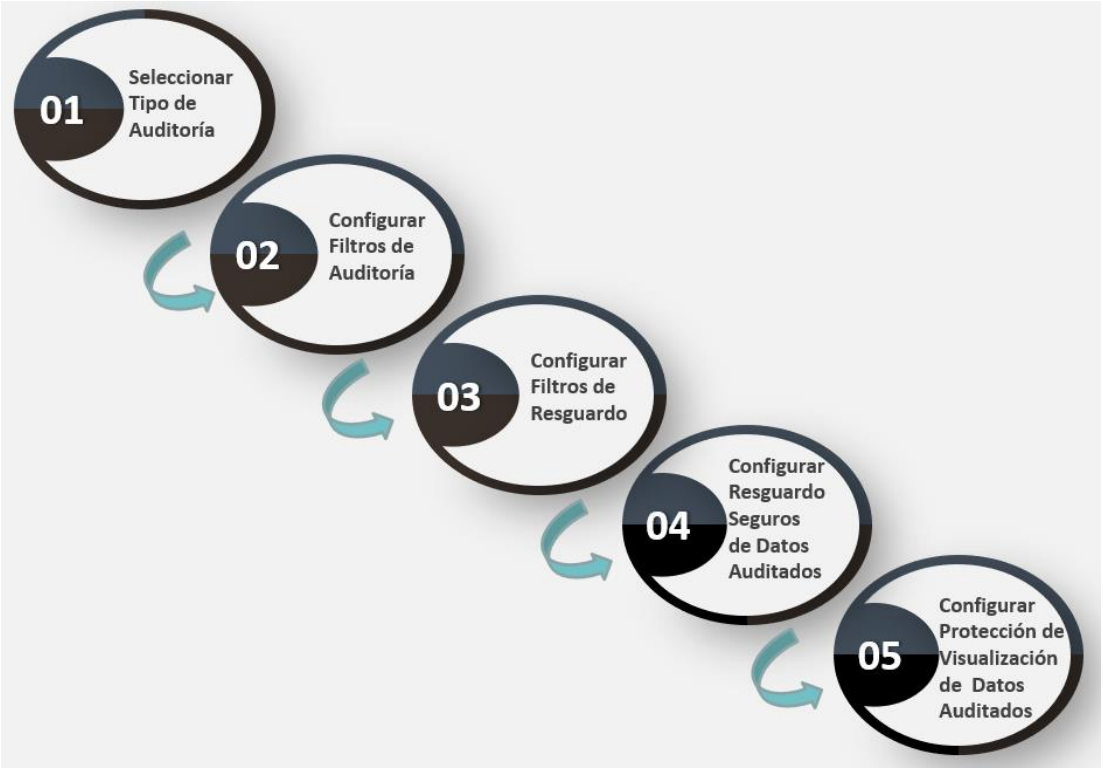

Figura 14: Configuración de Auditorías de Datos en AUDB

A. Tipos de Auditorías

En la Figura 15 se visualizan los diferentes **tipos de auditorías** propuestos en la metodología para la configuración de auditoría de datos.

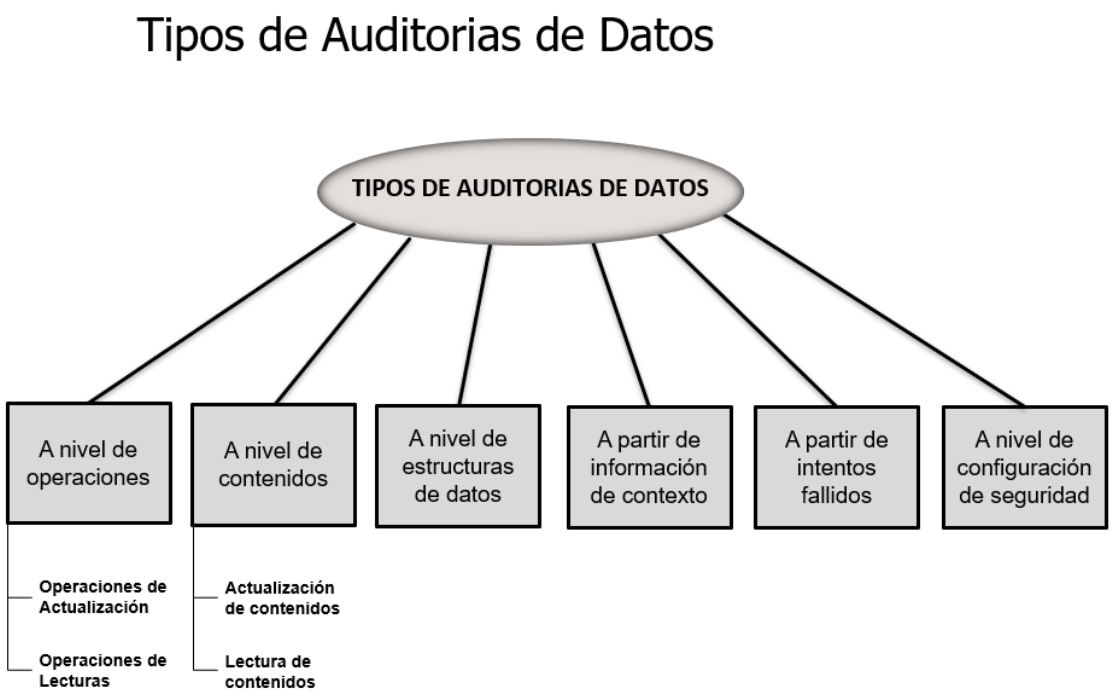

Figura 15: Tipos de Auditorías de Datos en AUDB

a) Auditoría a nivel de operaciones de actualización

Auditar las diferentes operaciones de actualización de datos sobre una tabla, sea inserción, modificación y/o eliminación de registros. Auditar las operaciones a nivel de sentencias, sin llegar al nivel de contenidos de los registros. Incluye auditar la ejecución de objetos que efectúen las operaciones (como procedimientos almacenados, etc.).

- Operaciones DML (Lenguaje de Manipulación de Datos o en sus siglas en inglés "Data Manipulation Language") de INSERT, UPDATE y DELETE.

b) Auditoría a nivel de operaciones de lectura de datos

Auditar operaciones de lecturas en determinadas tablas o columnas, sin alcanzar el nivel de datos por registro, es decir, se almacena solo la consulta de lectura asociada. Incluye auditar la ejecución de objetos que efectúen las operaciones (como vistas, procedimientos almacenados, etc.).

- Operaciones DML de SELECT.

c) Auditoría a nivel de actualización de contenido

Auditar los cambios a nivel de contenidos a partir de las operaciones de actualización de datos de registros. Se audita el contenido afectado. La auditoría registra la evolución de los datos en la tabla auditando los registros nuevos, eliminados y modificados, manteniendo un historial de cambios sobre todos o algunos de los campos de la tabla, según la configuración de auditoria basada en la criticidad de los mismos. Esta auditoría incluye la auditoría a nivel de operaciones de actualización (a).

- Operaciones DML de INSERT, UPDATE y DELETE y los datos afectados.

d) Auditoría a nivel de lectura de contenidos

Auditar los datos leídos en determinadas tablas o columnas junto con la operación de lectura realizada. Seleccionar los datos a auditar para evitar gran volumen de datos auditados, filtrando las lecturas en base a condiciones de registros, campos específicos, rangos de horarios, valores, usuarios, orígenes, entre otras características. Esta auditoría incluye la auditoría a nivel de lectura de datos (b).

- Operaciones DML de SELECT y los datos leídos.

e) Auditoría a nivel de estructuras de datos

Auditar los cambios de estructuras que afecten al formato de las tablas con información sensible (sea agregar, modificar o eliminar campos, nombres de campos, tipos de campos, tamaño de campos, índices, claves primarias, claves foráneas, restricciones y toda característica estructural de la misma). Estos cambios podrían causar una alteración directa o indirecta del

contenido de las tablas o incluso ser un posible intento de alteración de reglas (restricciones de tablas) para una posterior inserción, modificación o eliminación de los datos. Incluso pueden afectar a la ejecución de las propias auditorías de datos, alterando campos asociados a la configuración de las mismas.

- Operaciones DDL (Lenguaje de Definición de Datos o en sus siglas en inglés "Data Definition Language") de CREATE, ALTER, DROP.

f) Auditoría a nivel de configuración de seguridad

Auditar los cambios en los permisos de acceso, lectura y modificación otorgados sobre las tablas sensibles.

- Operaciones DCL (Lenguaje de Control de Datos o en sus siglas en inglés Data Control Language) de GRANT, REVOKE, DENY.

g) Auditoría a partir de información de contexto de la operación

Auditar la información de contexto de las operaciones realizadas sobre las tablas: el usuario de base de datos y/o del sistema operativo que ejecutó la operación, datos del origen de la conexión desde la cual se disparó la acción (dominio, nombre de la PC, aplicación, servicio o proceso, etc.), duración de la transacción, fecha y hora de inicio y fin de la misma o datos de la aplicación de donde se realizó la operación.

- Asociadas a operaciones DML, DDL y DCL.

h) Auditoría de intentos fallidos de operaciones

Auditar los intentos fallidos de operaciones de lecturas o modificaciones de datos, estructuras de tablas o configuraciones de seguridad por falta de permisos. Este tipo de auditoría dependerá de las capacidades de cada motor. El objetivo es detectar intentos de escalamiento de permisos o de usuarios que intentan acceder sin permisos, lo cual evidencia un comportamiento que debiera ser observada y tratada según la política de seguridad.

- Asociadas a operaciones DML, DDL y DCL.

Se aclara que en el caso de **auditorías a nivel de actualización de contenidos**, los datos a auditar variarán según el tipo de operación asociada:

- En sentencias de inserción de datos, se auditan los valores nuevos de los campos auditar.
- En sentencias de actualización, se auditan los valores anteriores y nuevos de todos los campos a auditar.
- En el caso de sentencias de eliminación, se auditan los valores de los campos a auditar en la tabla al momento de eliminarlos.
- Aclaración: con que una operación afecte a uno de los campos seleccionados a ser auditados, se resguardará como resultado de la auditoría por defecto todos los valores de los campos a auditar del registro, para mantener el historial de los campos en cada momento.

Si bien existe una **auditoría a nivel de estructuras de datos** específica a seleccionar, se configura por defecto una auditoría **implícita** de este tipo asociada al resto de las auditorías a nivel de operaciones o actualizaciones de tablas. De esta manera ante la detección de un cambio de estructura de datos de cualquier campo de la tabla auditada se alertará del mismo y se detallará la criticidad. Según el caso se puede seguir auditando o se afecta la disponibilidad de la auditoría. En los casos que, por ejemplo, se agreguen, modifiquen o eliminen campos no asociados directamente a la configuración de auditoría, se sigue auditando, se genera una alerta y se registra el cambio de metadatos de la tabla auditada. En los casos que la modificación sea de tipo de dato a otro compatible con igual tamaño mínimo, se intenta seguir auditando y se genera una alerta. En casos donde se elimine el campo, modifique el nombre del campo o el tipo de datos sea incompatible, entre otros, la auditoría de datos se ve afectada y se debe no solo a alertar sino, por ejemplo, a aplicar reglas de autoprotección para evitar que se realicen determinadas acciones sobre los datos hasta garantizar la disponibilidad de la auditoría.

Todos los tipos de auditorías están planteadas a aplicar principalmente sobre los datos almacenados en las base de datos, sin descartar **recuperar datos volátiles** que pudieran completar la trazabilidad o detectar acciones que en la operatoria normal no dejarían evidencia.

B. Filtros de Auditoría

La auditoría de datos, en especial la asociada a la lecturas de datos, puede producir cantidades copiosas de datos. Se debe buscar un compromiso entre auditar demasiados datos que resulten onerosos de clasificar y agoten los recursos del sistema o auditar pocos datos causando la pérdida de eventos importantes. Algunos eventos son tan sensibles y ocurren tan raramente que sería factible auditar todos los casos. Pero hay otros casos que ocurren muy frecuentemente y la información generada sería incontrolable.

La metodología define la configuración de filtros de auditorías que permiten focalizar las auditorías en acciones que se consideran críticas sobre los datos sensibles, según el contexto y los riesgos a los que están expuestos. Los diferentes filtros detallados pueden combinarse según la necesidad de auditorías a aplicar en las tablas con datos sensibles.

A continuación se detallan los tipos de filtros de auditorías para focalizar la obtención de evidencia digital a partir determinadas operaciones, datos, usuarios o información de contexto de las acciones sobre datos críticos.

a) Filtros a nivel de operaciones de actualización

Para configurar auditar operaciones de inserción, modificación y/o de eliminación sobre tablas sensibles o determinados campos. Incluye auditar la ejecución de objetos que efectúen las operaciones (como triggers, procedimientos almacenados, etc.).

b) Filtros a nivel de operaciones de lecturas

Para configurar auditar operaciones de lecturas sobre tablas sensibles o determinados campos. Incluye auditar la ejecución de objetos que efectúen las operaciones (como vistas, procedimientos almacenados, etc.).

c) Filtros a nivel de registros de datos

Para configurar auditar el contenido de los registros de tablas sensibles que cumplan con ciertos criterios de selección sobre los valores de uno o varios

campos sensibles (tanto sobre los valores actuales y/o anteriores según el tipo de operación).

d) Filtros a nivel de columnas de datos

Para configurar si se auditan todas las columnas de la tabla o determinadas columnas según se cumpla una condición sobre las mismas u otras columnas asociadas (tanto sobre los valores actuales y/o anteriores). En general los criterios de selección sobre los campos sensibles se basan en los campos claves, índices o críticos. También pueden configurarse filtros a nivel de columnas, seleccionando las columnas a auditar, independientemente de su contenido.

e) Filtros a nivel de cambios de estructuras

Para configurar auditar determinadas operaciones de cambios de estructuras sobre tablas sensibles. Se considera poder auditar determinadas operaciones de cambios de estructuras si afectan a ciertos campos sensibles o cumplen con algunas condiciones fijadas.

f) Filtros a nivel de configuración de seguridad

Para configurar auditar determinadas operaciones de cambios de permisos si afectan a ciertos campos o cumplen con algunas condiciones de filtro configuradas sobre la tabla.

g) Filtros a nivel de Información de Contexto de las Operaciones

Para configurar auditorías a partir de la información de contexto de las operaciones a auditar. Se pueden aplicar filtros a nivel de usuarios (para auditar acciones de determinados usuarios o grupo de usuarios de la base de datos y/o del sistema operativo), a nivel de información de orígenes de conexiones (dominio, computadoras, aplicaciones, procesos, servicios, etc.) o basados en un rango de días, horarios, fechas y/o duración de transacciones. Las condiciones de configuración de estos filtros pueden basarse en la realización de determinadas operaciones desde orígenes dudosos, a través de aplicaciones no autorizadas, ejecución de operaciones repetitivas o de aplicación masiva, operaciones sobre campos críticos u operaciones en fechas u horarios no habituales a la operatoria de la organización, entre otros.

h) Filtros a nivel de intentos fallidos de operaciones

Para configurar auditar los intentos fallidos de operaciones de lecturas o modificaciones de datos, estructuras de tablas o configuraciones de seguridad por falta de permisos. Se considera poder auditar determinadas intentos fallidos de operaciones si afectan a ciertos campos sensibles o cumplen con algunas condiciones fijadas.

Los diferentes filtros detallados pueden combinarse según la necesidad de auditoria a aplicar en las tablas con datos sensibles. Por ejemplo, se puede auditar operaciones de inserción de una tabla que realice determinado usuario en un rango horario determinado o auditar operaciones de modificación de registros si la modificación involucra a determinado campo.

Más allá de la configuración manual de los filtros a nivel de cambios de estructuras, se debe controlar siempre las estructuras de las tablas y los cambios sobre las mismas, para alertar sobre riesgos sobre las auditorias configuradas y en ejecución. Por ejemplo, si se modifica el tipo de dato de una columna que está siendo auditada, dicho cambio puede afectar la ejecución de la auditoría y los datos almacenados. Las estructuras de las tablas deben almacenarse de forma completa e histórica siempre para disponer de los distintos formatos en el tiempo para la lectura y procesamiento de transacciones basadas en los formatos actuales o anteriores y acceder y visualizar a la información auditada según las estructuras de las tablas en cada momento. Se debe considerar almacenar como parte de la estructura de la tabla las restricciones de la tabla, índices y claves foráneas.

C. Filtros de Almacenamiento de Información Auditada

Se pueden aplicar filtros aplicados al nivel de almacenamiento de la información auditada, de manera de configurar el grado de la información a almacenar, y así evitar resguardar registros completos de datos que sean innecesarios a fines de las auditorias en sí, almacenando solo aquellos campos identificatorios del registro y los campos sensibles a auditar o incluso solo las

operaciones asociadas. De esta manera se pueden almacenar los contenidos de los campos y/o de las operaciones que se requiere evidencia y trazabilidad, más allá de los usados para los criterios de auditoría.

De esta manera se plantean tres niveles de almacenamiento:

a) Primer Nivel de Almacenamiento (Nivel Operación):
Almacenamiento solo de la operación sin datos involucrados.

b) Segundo Nivel de Almacenamiento (Nivel Columna):
Almacenamiento de los datos de algunas columnas de los registros auditados. El almacenamiento a nivel de columna se divide en dos:

- Almacenamiento del valor de determinadas columnas sin condición.
- Almacenamiento del valor de determinadas columnas que cumplan cierta condición de almacenamiento.

En este nivel si ninguna columna es seleccionada a almacenar como resultado de los filtros de almacenamiento, como mínimo siempre se almacenará el valor de la clave identificadora del registro en la cabecera de la operación.

c) Tercer Nivel de Almacenamiento (Nivel Registro):
Almacenamiento de todo el registro auditado.

D. Almacenamiento Seguro de la Información Auditada

Es importante establecer el tipo y nivel de protección a aplicar a la información auditada en el almacenamiento de la misma, considerando que la información es sensible tanto en su almacenamiento original, como también en el resguardo de los registros de auditorías en sí.

La protección de los datos permite cumplir con normativas y regulaciones relacionadas con la privacidad de los datos y con regulaciones específicas de determinados sectores (financiero, salud, telecomunicaciones, etc.) o datos críticos para la organización en la propia solución. En los casos de información muy sensible o crítica, donde se requiera un nivel de protección adicional sobre el

almacenamiento universal de datos, se pueden implementar los siguientes métodos:

a) Enmascaramiento

Brinda la posibilidad de indicar que un determinado dato auditado se almacene con enmascaramiento por defecto, es decir, aplicando ocultación o modificación del valor original. Esta opción altera permanentemente los datos. Se permite configurar el tipo de enmascaramiento a aplicar al campo.

- Enmascaramiento estático: Técnicas de enmascaramiento aplicando caracteres especiales a elección, como por ejemplo ***, sobre todo o parte del contenido sensible. Por ejemplo, a aplicar en parte de los números de tarjetas de crédito.

- Enmascaramiento dinámico. Técnicas de enmascaramiento en tiempo real y basado en contenidos. Permite reemplazar los datos confidenciales enmascarando el contenido en base a reglas aplicar según el contenido. Por ejemplo, si se refiere a detalles o nombres de enfermedades que posea un paciente.

b) Cifrado de Datos

Es posible cifrar los datos sensibles auditados en el almacenamiento universal o los archivos de reportes de auditoría utilizando los algoritmos de cifrados más seguros. Se debe brindar la posibilidad de elegir entre diferentes algoritmos de cifrados (simétricos y asimétricos) y asegurar el resguardo de las claves. En este caso los valores originales se obtendrán aplicando el algoritmo de cifrado con la correspondiente clave de descifrado. Se considera la aplicación de mecanismos de almacenamiento seguro de claves.

c) Firma Digital de Reportes de Auditorías

Posibilita aplicar procesos de firma digital a los reportes de auditorías, a las notificaciones que se envíen por mail o se resguarden como archivos, para garantizar la autenticidad, autoría (no repudio) e integridad de los mensajes de mail y de los documentos electrónicos generados.

De esta manera se plantean cuatro niveles de almacenamiento seguro:

a) Primer Nivel de Almacenamiento Seguro (Nivel Operación):

Cifrado o enmascaramiento de la operación auditada (no incluye los datos).

b) Segundo Nivel de Almacenamiento Seguro (Nivel Columna):

Cifrado o enmascaramiento de los datos de algunas columnas de los registros auditados. El cifrado o enmascaramiento a nivel de columna se divide en dos:

- A aplicar al valor de determinadas columnas sin condición.
- A aplicar al valor de determinadas columnas que cumplan cierta condición de almacenamiento.

c) Tercer Nivel de Almacenamiento Seguro (Nivel Registro):

Cifrado o enmascaramiento del contenido de todo el registro auditado.

d) Cuarto Nivel de Almacenamiento Seguro (Nivel Reporte o Archivo):

- Cifrado o firma digital sobre determinados archivos o reportes de auditorías que se almacenen o se envíen.

Es limitante considerar que las variantes de almacenamiento seguro que alteren permanentemente los datos, sin posibilidad de recuperar el valor original, están alterando el valor del mismo, lo cual puede afectar a la admisibilidad de los resultados auditados como evidencia digital probatoria.

E. Protección de Visualización de la Información Auditada

Considerando que los resultados de las auditorias se pueden visualizar tanto en módulos del sistema como en reportes emitidos por el mismo, se pueden aplicar distintos niveles de protección de visualización.

El objetivo de esta protección es autorizar, enmascarar, reemplazar, transformar, ordenar o incluso aclarar los datos que se visualicen o se vuelquen en reportes, pero garantizando que los datos originales almacenados permanezcan intactos y sin cambios.

a) Autorización de Visualización

Permite configurar si determinada información auditada se visualizará o no en el sistema de auditoria y/o en los reportes por defecto o solo se visualizará para determinados usuarios o perfiles que se indiquen de forma explícita o según el nivel de privilegios de los usuarios.

b) Visualización con Enmascaramiento

Brinda la posibilidad de indicar que un determinado dato auditado se visualice con enmascaramiento por defecto y que solo sea visible en texto claro para determinados usuarios o perfiles que así lo requieran o según el nivel de privilegios de los usuarios. Se permite configurar el tipo de enmascaramiento a aplicar al campo.

- Enmascaramiento estático: Técnicas de enmascaramiento aplicando caracteres especiales a elección, como por ejemplo ***, sobre todo o parte del contenido sensible.

- Enmascaramiento dinámico. Técnicas de enmascaramiento en tiempo real basado en roles y contenidos. Permite reemplazar los datos confidenciales enmascarando el contenido en base a reglas aplicar según el usuario y/o el contenido.

c) Visualización con Enriquecimiento

Los diferentes nombres de campos de las tablas auditadas pueden ser visualizados con una **descripción que clarifique el contenido del campo**. También pueden aplicarse **reglas de transformación de visualización** al contenido de los datos en tiempo real ya sea con finalidades de protección, como de esclarecimiento del contenido. De la misma manera se pueden visualizar los campos aplicando un **reordenamiento lógico** de los mismos para facilitar su visualización y entendimiento. Asimismo, se brinda la posibilidad de adicionar **columnas virtuales**, que se agregan en tiempo real y no existen en la estructura de la tabla física, para almacenar campos calculados o que se completan a partir de valores de otros campos (ejemplo, fecha de nacimiento y la columna virtual de edad).

Cabe aclarar que estas técnicas de enmascaramiento o enriquecimiento, donde se altera en la visualización el contenido real, no son aplicables si lo que se busca es emitir reportes u obtener capturas de pantallas que luego sirvan como evidencia digital en un proceso judicial. La finalidad es que sean aplicadas como parte del análisis de resultados de auditoría con la finalidad de proteger o enriquecer los datos auditados en los sistemas o reportes en donde se visualicen o vuelquen los mismos.

4.2.5 Configuración de Reglas de Validación y Autoprotección de Datos en Tiempo Real

Otra de las actividades relacionadas con la configuración de auditorías se relaciona con la detección de acciones que involucren riesgos que puedan atentar contra la confidencialidad, disponibilidad e integridad de la información basadas en las políticas de seguridad de la información.

Se establecen **reglas de validación**, con la posibilidad de realizar **notificaciones** con la suficiente flexibilidad tanto a la hora de definir la regla como a la hora de establecer **listas de escalamiento** para la notificación de las mismas. Se establece la posibilidad de ejecución de **reglas de autoprotección** ante una potencial violación de una política crítica (por ejemplo, deshabilitar un usuario ante una actividad sospechosa).

El objetivo es permitir implementar reglas a partir como ser: “no se puede acceder a cambiar un saldo de cliente fuera del horario laboral del oficina”, o “deben notificarse inmediatamente los cambios realizados por fuera de la aplicación”, etc.

Tanto las reglas de validación como las de autoprotección se establecen a partir de la aplicación de los filtros similares a los auditorías, los cuales pueden basarse en determinadas operaciones desde orígenes dudosos, desde aplicaciones no autorizadas o desconocidas, intentos fallidos, operaciones repetitivas que incluso pueden estar siendo denegadas, operaciones de aplicación masiva, determinadas operaciones sobre campos críticos, operaciones de

determinados usuarios, operaciones desde determinados orígenes o en fechas u horarios no habituales a la operatoria de la organización, entre otros.

Estas **condiciones son categorizadas por niveles de criticidad** y al materializarse alguna de las acciones que cumplan con las condiciones se ejecutan las acciones configuradas. En general se configuran **notificaciones a enviar a los auditores y/o responsables de seguridad asignados y según el caso podrían aplicarse reglas de autoprotección** para evitar, por ejemplo, el acceso a los datos hasta que se analice si realmente hubo o se intentó ejecutar una acción maliciosa sobre los datos.

Las **reglas de autoprotección** podrían involucrar desde el bloqueo automático de determinados usuarios u orígenes de datos, bloqueo automático de acceso a determinadas tablas, bloqueo automático de determinadas operaciones, bloqueo automático de acceso a las tablas de una base de datos, entre otras acciones. Estas reglas deben ser analizadas por parte de los administradores de seguridad de las base de datos, en base a la criticidad de las acciones, la factibilidad técnica-operacional de implementar las mismas, la naturaleza de la organización y la infraestructura tecnológica disponible. Una aplicación práctica de estos filtros es ante la repetición de determinadas acciones o patrones de comportamiento que se consideren dudosos (dependiendo el tipo de auditoria).

Los **niveles de criticidad establecidos** son:

- **Severas**: Notificación de acciones que implican riesgos reales críticos y aplicación de reglas de autoprotección.
- **Críticas**: Notificación de acciones que implican riesgos reales críticos.
- **Advertencias**: Notificación de acciones que implican riesgos reales no críticos o potenciales.

4.2.6 Ejecución de Auditorías

A. Acciones de Ejecución de Auditorías

La manera más simple es la activación o desactivación de las **auditorías a demanda**, indicando el inicio o fin de ejecución de las mismas **de forma manual**.

De la misma manera se considera poder **planificar la activación de las auditorías** en determinados horarios, días o rangos de fechas, de manera de que se activen y focalicen cuando se consideren de riesgo ciertas acciones, obteniendo así **auditorías planificadas**.

La metodología AUDB valora la posibilidad de aplicar auditorías de datos no solo desde el momento que se configuran, sino en rango de fechas, días u horarios previos, pudiendo aplicar **auditorías históricas**. Esta característica será dependiente de la capacidad y configuración de cada motor de base de datos tanto sobre estructuras volátiles como persistentes.

Cualesquiera sean las formas de inicio de las auditorías, se debe registrar el inicio o fin de ejecución de las mismas, incluso los inconvenientes durante su ejecución, a fin de que sea **auditable y traceable la ejecución de las mismas**, quedando registro de qué momentos se auditó y de cuáles no. Al momento de iniciar una auditoría se debe validar que la misma pueda iniciarse sin inconvenientes, en caso contrario también se registra el problema.

Una auditoría configurada puede estar **activa** (en ejecución) o **inactiva** (no iniciada o frenada).

B. Estados de Ejecución de Auditorías

Para el seguimiento y control de las auditorías en ejecución o activas se definen los siguientes **estados de auditorías activas** visualizados en la Figura 16, que de alguna manera identifican la “salud” de la auditoría, es decir el funcionamiento de las auditorías de datos y la gravedad ante inconvenientes en su ejecución:

Figura 16: Estados de Auditorías de Datos activas en AUDB

- **Ejecución exitosa**: La auditoría de datos se está ejecutando sin dificultades.
- **Ejecución crítica**: La auditoría de datos no puede ejecutarse. El dato no puede auditarse (por errores propios de la auditoría, cambios de formatos que impiden la ejecución de la auditoría, problemas de acceso, problemas técnicos, etc.).
- **Ejecución con errores**: La auditoría se está ejecutando, pero existen ciertos problemas a observar que podrían implicar un futuro inconveniente crítico en la ejecución de la misma (sea por obtención de gran cantidad de datos auditados, cambios de formato imprevistos que no impiden la ejecución de la auditoría pero involucran una alerta, etc.).
- **Ejecución con advertencias**: La auditoría se está ejecutando, aunque se detectan ciertas advertencias a observar (sea lentitud en acceso, lentitud en resguardo de datos auditados, etc.).

4.2.7 Historial de Configuraciones, Formatos y Estados de Auditorías

Se almacenan de forma histórica los cambios en las estructuras de las tablas, en las configuraciones de auditorías, en las reglas de validación y autoprotección de datos, en las configuraciones de ejecución de las auditorías como también en los estados de las auditorías en cada momento. Esta información permite luego reconstruir los hechos en base a la trazabilidad de configuraciones, formatos y estados en el tiempo.

4.2.8 Requisitos de la Metodología de Auditoría Universal de Base de Datos

Toda solución que requiera basarse en la metodología detallada debe considerar una serie de requisitos principales establecidos por AUDB:

1) Garantizar la auditoria universal a nivel de datos y operaciones en la diversidad de plataformas y SGBD relacionales empleados en las organizaciones.
   - Aplicar un nivel de abstracción al tratamiento de las auditorías más allá de los aspectos técnicos de cada base de datos.
   - Configurar las auditorías de forma independiente del tipo de base de datos relacional, de forma tal que le permita al auditor configurar las mismas sin necesidad de poseer conocimientos técnicos de un SGBD particular.
   - Resguardar la información auditada de forma independiente a los tipos de motores de base de datos o plataformas a auditar.
   - Implementar una solución que no dependa de aplicaciones las cuales puedan ser eludidas por usuarios que se conecten vía otras aplicaciones o a través de herramientas nativas del propio SGBD.
2) Aplicar los filtros necesarios de auditorías de datos para enfocar sobre los datos, acciones y contextos en el que se quiere aplicar las auditorías.
3) Garantizar que las ejecuciones de auditorías de datos detecten toda acción sobre los datos sensibles independientemente de cómo y dónde se ejecuten las acciones.
   - Posibilitar la ejecución de auditorías de actualización y lecturas de datos permitiendo salvaguardar la integridad, confidencialidad y disponibilidad de información sensible o se requiera por ley.
   - Registrar como parte del resultado de las auditorías de datos la información de contexto referida a quién, cuándo, desde dónde y cómo se efectuó la operación.
   - Auditar a tiempo la información volátil que se pierde en la operatoria normal de la base de datos y que puede ser crucial para las investigaciones.
   - Garantizar la auditoría de datos en base a soluciones que además de los datos persistentes, audite datos volátiles, no volátiles y temporales.

4) Minimizar los cambios e impactos en las bases de datos al aplicar las auditorías de datos, aplicando soluciones lo menos invasivas posibles.
   - No aplicar soluciones invasivas con alto consumo de recursos por el uso de métodos inadecuados.
   - Asegurar que no se vean afectadas o interrumpidas las operaciones normales, es decir, proteger la disponibilidad, rendimiento y la continuidad de las bases auditadas.
   - Evitar la detención parcial o total de cualquiera de los procesos informatizados o sistemas vinculados a las base de datos (de manera de evitar afectar a la disponibilidad de los base de datos y los sistemas o procesos asociados).
5) Brindar facilidades de acceso a los resultados de las auditorías de datos.
   - Incluir módulos de reportes y generación de archivos de resultados.
   - Simplificar la lectura y comprensión de la información resultante aplicando un nivel de abstracción para que los auditores puedan enfocarse en los datos en sí y no en la representación técnica del motor de base de datos que los resguarda.
   - Facilitar la realización de análisis del resultado de las auditorías para la detección de fraudes, potenciales hechos delictivos, actividades maliciosas, dudosas o indebidas.
   - Brindar facilidades de análisis históricos de la información auditada.
   - Proporcionar diferentes niveles de protección sobre la información auditada resultante, tanto a nivel de la visualización como en su almacenamiento.
6) Permitir un seguimiento y alertas tempranas basada en políticas de seguridad.
   - Suministrar diversos mecanismos de protección ante la detección de potenciales acciones maliciosas, dudosas e indebidas, basados en políticas de seguridad de la información y análisis de riesgos.
   - Disponer de diversos mecanismos de notificación de alertas tempranas a los responsables de seguridad y/o auditoría, basados en listas de escalamientos, ante la detección de potenciales acciones maliciosas, dudosas e indebidas, basados en políticas de seguridad de la información y análisis de riesgos.

- Validar políticas de seguridad de la información, en lo posible en tiempo real en los casos que se violen políticas muy críticas o que involucren grandes riesgos para la organización.
- Ejecución de reglas de autoprotección ante una potencial violación de una política de seguridad de la información o actividad maliciosa (por ejemplo, deshabilitar un usuario o acceso desde una determinada dirección).
- Facilitar el análisis de impacto, priorización, diagnóstico y resolución de incidentes detectados, para reducir al mínimo el tiempo y el coste de resolución de la incidencia de seguridad.

7) Garantizar la protección de los datos auditados y la solución en general.
   - Diseñar y realizar una recolección segura de los datos auditados, de manera de no ser vulnerables a ataques durante la recolección, transmisión o en el mismo almacenamiento.
   - Diseñar políticas de acceso y autorización a la información auditada y a las configuraciones de auditoría.
   - Garantizar la disponibilidad de las auditorías de datos.
   - Proponer soluciones tolerantes a fallas que garanticen la continuidad de las auditorías de datos.
   - Diseñar y planificar planes de contingencia ante problemas de ejecución de las auditorías de datos.
   - Permitir generar y almacenar los datos auditados en un servidor distinto a donde reside la base de datos, de manera de asegurar la disponibilidad de los mismos ante ataques al servidor.
   - Evitar que por la falta de disponibilidad de auditorías sea posible atacar al sistema.
8) Disponer de mecanismos de administración, seguimiento y control de las auditorías.
   - Administrar y controlar el estado de las auditorías de datos.
   - Aplicar diversos mecanismos de notificación de alertas a los responsables de seguridad y/o auditoría, basado en listas de escalamientos, ante la detección de acciones o problemas que afecten la ejecución de las auditorías de datos.
   - Ejecutar reglas de autoprotección ante una actividad maliciosa o dudosa

sobre las auditorías de datos.

- Ofrecer mecanismos de seguimiento de ejecuciones de auditorías de datos.
- Garantizar la ejecución de las auditorías de datos.

9) Disponer de mecanismos de auditoría y trazabilidad propia, donde se resguarde el historial de configuraciones de auditorías de datos y ejecuciones de la mismas.
   - Registrar información de contexto de cambios y accesos a las configuraciones de auditorías (quién, cuándo, desde dónde y cómo se realizaron los cambios).
   - Registrar información de contexto de acciones de ejecución sobre auditorías (quién, cuándo, desde dónde y cómo se iniciaron o frenaron las ejecuciones de las mismas).

4.2.9. Beneficios de AUDB

En la siguiente Figura 17 se sintetizan los **principales beneficios** al implementar una estrategia de auditoria de datos en base a AUDB:

Figura 17: Principales beneficios de AUDB

a. Detectar intrusiones
b. Prevenir intrusiones
c. Detectar fraudes
d. Disponer de evidencia digital y trazabilidad
e. Generar alertas tempranas o en tiempo real ante operaciones críticas
f. Brindar soporte al cumplimiento de leyes, políticas y normas

4.3. Metodología Forense Informática en Base de Datos (ForenseDB)

A partir de la denuncia o detección de un caso potencialmente delictivo vinculado con el uso de la tecnología de base de datos, como medio o fin del mismo, surge la necesidad de aplicar la ciencia de Informática Forense a las mismas, procurando respetar los principios forenses para lograr recuperar evidencia digital en base de datos para su uso en el ámbito judicial. Ante esta necesidad surge **ForenseDB, una metodología forense informática en base de datos**, cuya aplicación asegura una actuación metódica basada en un orden lógico de actividades a realizar, evitando contaminar las bases de datos y manteniendo la debida cadena de custodia, de manera de preservar la información recolectada como potencial prueba.

4.3.1. ForenseUDE y ForenseDB

Como parte de la solución y como base de la metodología **ForenseDB** se plantea el diseño propio de una metodología informática forense aplicable a cualquier tipo de evidencia digital, es decir, a evidencia digital universal (**UDE**, **Universal Digital Evidence**). En dicha metodología, denominada **ForenseUDE,** se definen y describen las etapas y actividades comunes aplicables a cualquier fuente de evidencia digital. A partir de **ForenseUDE** se especifican las tareas propias a considerar en las bases de datos relacionales (**ForenseDB**).

De este modo, **ForenseDB se basa tanto en actividades de la informática forense en general como en las específicas de base de datos relacionales**,

garantizando la confiabilidad de las diversas tareas a realizar por parte del investigador y/o perito informático forense y de la admisibilidad de la evidencia digital obtenida.

ForenseUDE se sustenta de ideas y conceptos del **modelo PURI** (Proceso Unificado de Recuperación de Información) y del **modelo EDRM** ("Electronic Discovery Reference Model"), como también de la **norma ISO/IEC 27.037**. Además, comprende fases y actividades distintivas y propias en base a la experiencia profesional personal en la actuación forense informática en casos judicializados como privados, como también en gestión de proyectos.

En primer lugar, con **ForenseUDE se desarrolla un proceso general de tratamiento de la evidencia digital**. Esto se debe a que como parte de la solución, surgió la necesidad de desarrollar un modelo más integral, amplio y detallado para la actuación pericial informática. Algunos modelos hacían énfasis solo en determinadas etapas, o el nivel de detalle de los mismos no era lo suficientemente completo como para tomarlos como referencia única para su aplicación en base de datos. En consecuencia, a partir de los modelos existentes se definieron fases, actividades y tareas aplicables en casos generales de informática forense.

En base al concepto de **proceso y esquema planteado por el modelo PURI**, la **metodología ForenseUDE** se basa en un proceso dividido en un conjunto de **fases**, que permiten focalizar los objetivos de cada fase, facilitan su comprensión y tratamiento y la interconexión de las mismas como un todo. El proceso se entiende como una serie de fases a seguir, las cuales podrían variar de acuerdo con el objeto origen, es decir, puede ser abordado en diferentes fases de acuerdo con el caso origen a resolver y a las características del objeto sobre el que se va a realizar las tareas forenses. En cada una de las **fases** se describen **actividades**, las cuales a la vez agrupan **tareas específicas**.

La **metodología ForenseUDE** se focaliza en la obtención de **cualquier evidencia digital admisible en un proceso judicial,** por lo tanto garantiza las características de **relevancia, confiabilidad, la suficiencia y validez legal** de la misma tratada durante el proceso. El proceso se plantea **justificable, auditable, repetible y reproducible** cumpliendo con los requisitos de confiabilidad.

ForenseUDE garantiza y facilita metodológicamente el registro de la debida cadena de custodia para asegurar la **confiabilidad** de la información recolectada y registrar la **trazabilidad** exacta de la misma, es decir, saber en todo momento, en qué lugar está la evidencia, bajo **responsabilidad** de quién, desde su identificación, hasta su presentación final. Las evidencias digitales a obtener en las bases de datos pueden cumplir **dos funciones, orientadora o probatoria**.

La metodología **ForenseDB** plantea actividades forenses en base de datos en forma general, **sin puntualizar en ningun tipo de motor de base de datos en concreto,** y se centra en la obtención de evidencia digital basada en cualquier dato o registro de información procesado electrónicamente y almacenada en base de datos relacionales o artefactos vinculados, como ser registros de log u archivos vinculados, pudiendo ser de valor para casos judicializados como en investigaciones solicitadas por particulares u organizaciones.

La metodología ForenseDB divide la evidencia digital en base de datos conceptualmente en las siguientes categorías:

1. Datos asociados a registros almacenados en tablas de las bases de datos (persistentes y confirmados en la tablas) .
2. Datos asociados a registros de auditorías de AUDB almacenados en tablas de base de datos (persistentes y confirmados en las tablas de auditoría).
3. Datos asociados a archivos físicos de datos, de registro de transacciones, de parámetros y de control.
4. Datos volatiles de memoria, caché, sesiones, sentencias ejecutadas recientemente y procesos varios asociados al SGBD, entre otros.
5. Datos generados a partir de procesos varios de auditorías, control y logueo que pueden estar almacenados tanto en tablas, archivos o eventos del sistema operativo (registros de auditorias, registros de eventos, registros de logs). Estos datos podrían ser volátiles, no volátiles, transitorios o temporales.
6. Datos asociados a vistas parciales de datos, consultas en base de datos, exportación de datos.
7. Datos en archivos de backups.

Disponer de la configuración y ejecución de **auditorías forenses en base de datos basadas en AUDB**, previo a la aplicación de ForenseDB, posibilitará

recolectar mayor cantidad y calidad de evidencia digital relevante y precisa referida al caso a investigar, como también retroalimentar a la estrategia de AUDB implementada.

Se plantea un proceso integral, describiendo diferentes tipos de actividades que agrupan tareas en función de un objetivo común. Las actividades de cada una de las fases agrupan tanto tareas generales como específicas para poder enmarcar y contextualizar el trabajo específico sobre base de datos relaciones.

- **Actividades generales** o comunes aplicables al tratamiento de cualquier tipo de evidencia digital, que son necesarias de aplicar como parte del proceso **(ForenseUDE).**
- **Actividades específicas aplicables al tratamiento de evidencia digital en base de datos relacionales (ForenseDB).** Estas actividades se especifican en casos donde se necesite particularizar o detallar tareas sobre **base de datos relacionales (BDR)**. Incluso se hace referencia de la interacción a partir de los resultados obtenidos de la aplicación de la metodología AUDB, como también las actividades de retroalimentación entre metodologías.

Las actividades se encuentran vinculadas de tal forma que sugieren un orden en el que podrían ser llevadas a cabo en las diferentes fases, orientando los **procedimientos** a llevar a cabo, estableciendo directrices de **preservación y recolección de la evidencia digital**, asegurando **no contaminar la evidencia digital**, priorizando la recolección según orden de **volatilidad** y manteniendo la debida **cadena de custodia**, como también el **seguimiento de intercambio de evidencias digitales entre intervinientes**.

Las **actividades detallan las tareas necesarias y suficientes** para que los expertos en informática forense recolecten, aseguren y preserven elementos materiales probatorios sobre base de datos relacionales, los cuales podrán ser revisados y analizados por terceros interesados.

Cada una de las actividades y las tareas que agrupan pueden realizarse o no, según el escenario a investigar o periciar.

En general, gran parte de los escenarios que se plantean en la realidad al analizar una base de datos, pertenecen a organizaciones donde la **disponibilidad de las mismas es crucial,** y donde se deben analizar alternativas factibles para evitar desconectar el servidor donde se aloja el motor de base de datos o los servicios vinculados, de manera de **no afectar la operatoria del negocio.**

4.3.2. Fases

Las fases generales de **ForenseDB** son las mismas que **ForenseUDE**.

En la Figura 18 se grafican las fases de **ForenseDB**:

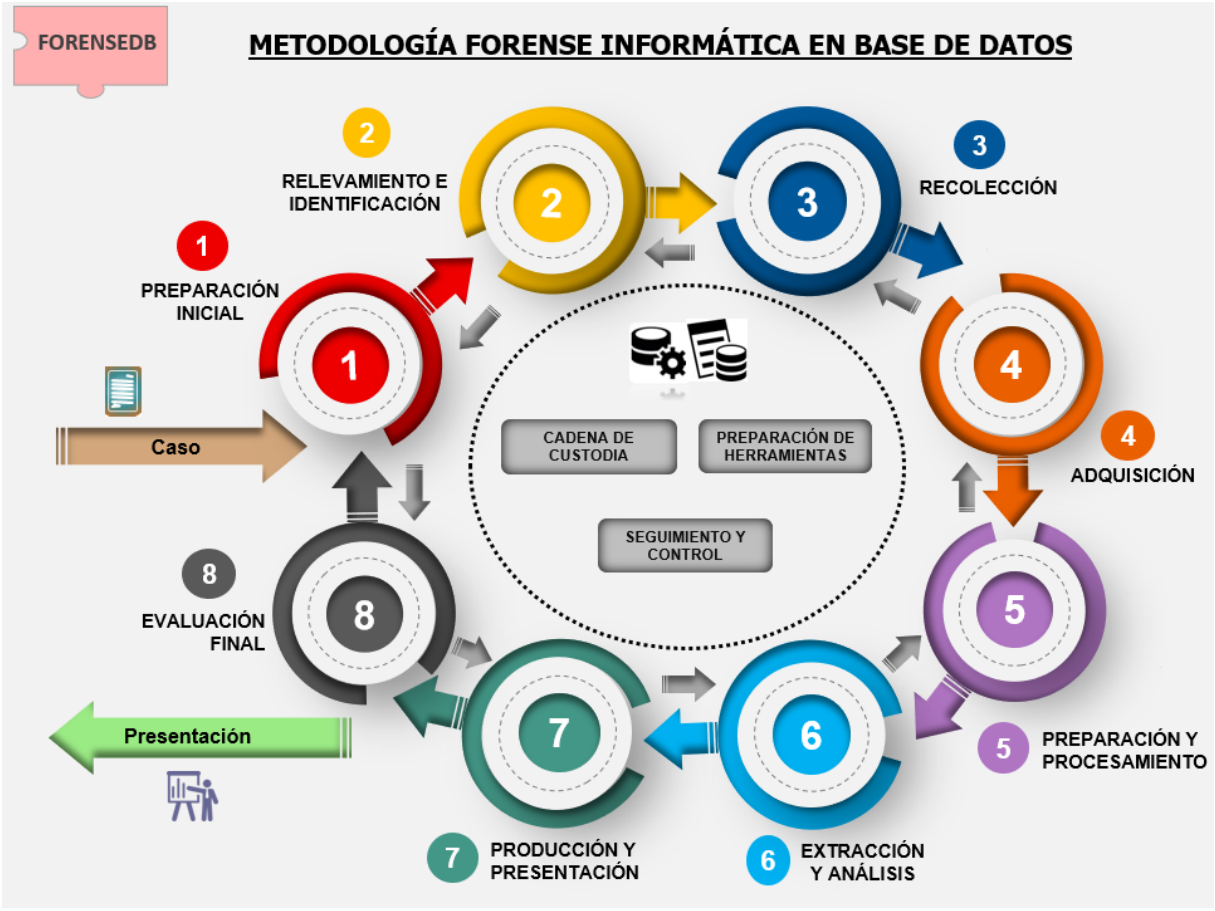

Figura 18: Fases de ForenseDB

Se plantean 8 fases principales:

1) **Preparación Inicial**
2) **Relevamiento e Identificación**
3) **Recolección**
4) **Adquisición**
5) **Preparación y Procesamiento**
6) **Extracción y Análisis**
7) **Producción y Presentación**
8) **Evaluación Final**

En cada una de las fases se detallan las actividades generales y también las específicas para casos de base de datos relacionales. Cada una de las actividades de las fases se aplicarán o no según los escenarios presentados, incluso podrían variar en su orden o solaparse.

Las fases se presentan en un **modelo iterativo con retroalimentación general** y donde **cada una de las fases también puede retroalimentar a las fases previas** y el final de cada iteración retroalimenta al inicio nuevamente.

Mientras se avanza en la investigación se pueden encontrar nuevas fuentes de evidencia que no se recolectaron al inicio o nuevas personas involucradas, lo cual involucra una retroalimentación del proceso que puede originar, por ejemplo, nuevos allanamientos o artefactos a recolectar o analizar. De esta manera se podría repetir el proceso completo varias veces, conduciendo a un conjunto más preciso de resultados o se podría también pasar nuevamente sobre las fases anteriores, refinando el enfoque para una mejor comprensión de los datos que surgen. El proceso permite iterar cuantas veces sea necesario hasta que se llegue algún tipo de decisión por parte del jurado o los interesados.

Además de estas fases, se adiciones tres actividades transversales:

a. **Cadena de Custodia**
b. **Preparación de Herramientas**
c. **Seguimiento y Control**

Las actividades transversales agrupan tareas que deben ser aplicadas en las actividades de las diferentes fases y son obligatorias. Por tal motivo se describen de forma separada para poder aplicarla en cada fase, según el contexto y el caso.

4.3.3. Roles Actuantes

A continuación, se detallan los roles actuantes (o niveles de actuación) en las diferentes fases. El rol actuante establece un conjunto de expectativas asociadas con la función, independientemente de la persona o el puesto que ocupa en el organismo o entidad al que pertenece.

Se establecen roles actuantes generales y específicos para casos de base de datos.

Roles Actuantes Generales (ForenseUDE):

- **Director Informática Forense (DIF):** Director de la Investigación Informática Forense o del Servicio Informático Forense. Es una persona con la capacidad de planificar la estrategia general y realizar el seguimiento y control de la ejecución de las diferentes fases. Coordina las actividades de las diferentes fases. Es responsable de la evaluación final del trabajo y de llevar adelante los procesos de retroalimentación y mejora continua.
- **Responsable de Identificación (RI):** Es una persona idónea para las tareas de identificación y la responsabilidad sobre las mismas. Puede estar a cargo de un investigador judicial debidamente capacitado en la materia o personal auxiliar de un Laboratorio de Informática Forense.
- **Especialista en Identificación (EI):** Es una persona especialista en informática idónea para las tareas de identificación vinculadas a tecnologías que requieran de un profesional entrenado y calificado.
- **Especialista en Recolección (ER):** Es una persona autorizada, entrenada y calificada para recolectar objetos físicos pasibles de tener evidencia digital. Puede necesitar el auxilio de un Especialista en Adquisición.
- **Especialista en Adquisición (EA):** Es una persona autorizada, entrenada y calificada para adquirir evidencia digital, como ser imágenes forenses de discos, volcados de memoria o red, entre otros tipos de evidencia digital.
- **Especialista en Evidencia Digital (EED):** Es una persona experta que puede realizar las tareas de un especialista de adquisición y además tiene conocimientos específicos, habilidades y aptitudes que le permiten manejar un

amplio rango de situaciones técnicas, tales como la realización de una pericia informática.

Roles Actuantes Específicos para Base de Datos (ForenseDB):

- **Especialista Forense en Base de Datos (EFBD)**: Es una persona especialista en tecnologías de base de datos. El mismo puede asesorar o actuar en las diferentes fases de la metodología.
- **Especialista Auditor Forense en Base de Datos (EAFBD)**: Es una persona especialista en tecnologías de base de datos, en especial en auditorías de datos y en la metodología AUDB. El mismo puede asesorar o actuar en las diferentes fases de la metodología donde la actuación forense se base en AUDB.

Los roles actuantes de responsable de identificación (RI), especialista en recolección (ER), especialista en adquisición (EA) y especialista en evidencia digital (EED) son análogos a los que plantea el modelo PURI como niveles de actuación. A diferencia del modelo PURI, se adicionan los roles actuantes generales de director en informática forense (DIR) y especialista en identificación (EI), como también los roles actuantes específicos de base de datos, el especialista forense en base de datos (EFBD) y el especialista auditor forense en base de datos (EAFBD).

Más allá de la división conceptual de los roles actuantes, **una misma persona puede cumplir distintos roles en un mismo caso o en distintos casos**.

Dependiendo de las tecnologías involucradas y de las características de cada escenario se define el nivel de conocimientos y habilidades requeridas. Los roles actuantes no siempre actúan en todos los casos, ya que según el caso pueden ejecutarse distintas fases o actividades.

Disponer de recursos humanos **capacitados**, **calificados** y con **disponibilidad** para la tarea pericial es un desafío interesante. Es importante la **capacitación** continua del perito. Se trabaja con información almacenada de manera electrónica, lo que implica que está almacenada en dispositivos que día a día van cambiando, evolucionando en rapidez, poder de procesamiento y volumen de información.

Es esencial **trabajar en equipo** considerando la necesidad de **multidisciplinariedad**, ya que una pericia informática muchas veces requiere de una serie de roles y habilidades donde muchas veces no es suficiente con disponer de grandes técnicos cuando se necesitan habilidades de carácter investigativo.

4.3.4. Fase de Preparación Inicial

Descripción General

Recepción del caso o requerimiento de análisis forense informático. Validación y revisión de las capacidades de tiempo, equipos y recursos humanos para dar respuesta al requerimiento de análisis forense. Definición del alcance general del requerimiento para luego establecer y diseñar un plan de acción acorde.

Objetivo

Analizar la factibilidad de resolución del requerimiento de análisis forense informático y planificar la estrategia asociada acorde a la disponibilidad y capacidades de los recursos necesarios para su trabajo.

Roles Actuantes

- Director Informática Forense (DIF).
- Puede tener colaboración de Responsable de Identificación (RI).
- Para casos de base de datos Especialista Forense en Base de Datos (EFBD) y Especialista Auditor Forense en Base de Datos (EAFBD).

Aplica a

- Labores de planificación de tareas y recursos para una investigación judicial.
- Labores de análisis de factibilidad, planificación de tareas y recursos para un caso asociado a servicio forense particular.

Consideraciones

Esta fase constituye se plantea previa al contacto con la evidencia digital y antes de dirigirse al lugar del hecho o del allanamiento, con la finalidad de evitar

imprevistos, problemas u obstáculos por falta de capacidad o recursos a la hora de la recolección o adquisición de cierto tipo de evidencia digital. La ejecución de esta fase de preparación inicial dependerá de la urgencia del caso involucrado y la naturaleza del mismo.

Frente a la infinidad de tecnologías existentes (Microsoft, IBM, SAP, Unix, Linux, etc.) es primordial realizar un análisis inicial de la capacidad y los equipamientos básicos para atender a los requerimientos. En este sentido, prever lo que se puede afrontar en la escena del hecho o en una actuación pericial posibilta planificar las actividades y asegurar las disponibilidad de los equipos, herramientas y recursos humanos necesarios.

Es importante diferenciar los casos que involucran secuestro de equipos, adquisición en el lugar, adquisiciones de imágenes forenses o los casos donde ya se dispone desde el inicio las imágenes o copias forenses y/o equipos a periciar.

La actividad de análisis de factibilidad en servicios forenses particulares es determinante para la aceptación e inicio del trabajo.

Planificar la estrategia de resolución del requerimiento implica plantear un esquema de trabajo conforme a los recursos de tiempo, técnicos y humanos disponibles.

No llevar a cabo una preparación inicial implica preparar e identificar todo en el lugar del hecho o del allanamiento o una vez iniciada la actuación pericial, es decir, tomar decisiones casi al mismo momento que se tiene que recolectar y/o aquirir la evidencia digital, donde se asume el riesgo de no disponer de equipos, herramientas o expertos necesarios para afrontar las tareas, con la consecuente afectación de los resultados que se podrían alcanzar.

Principales Actividades

Fase de Preparación Inicial			
Actividades Generales (ForenseUDE)		**Actividades Específicas (ForenseDB)**	
1	Recepción del Requerimiento	1.1	Recepción del Requerimiento de Análisis de BDR
2	Revisión de Capacidades	2.1	Ídem (aplicable a BDR)
3	Revisión de Equipamiento Necesario	3.1	Ídem (aplicable a BDR)
4	Análisis de Factibilidad	4.1	Ídem (aplicable a BDR)
5	Definición del Alcance	5.1	Ídem (aplicable a BDR)
6	Planificación y Diseño de Estrategia	6.1	Ídem (aplicable a BDR)
7	Análisis de Riesgos	7.1	Análisis de Riesgos de Análisis en BDR
8	Preparación de los equipos y herramientas para las tareas a realizar	8.1	Preparación de equipos y herramientas para las tareas en BDR

Tabla 1: Fase de Preparación Inicial

Detalle de Actividades Generales

1. Recepción del Requerimiento
   - Recepcionar el oficio o el pedido de un cliente.
   - Analizar criticidad del requerimiento.
   - Analizar de forma general el requerimiento, la naturaleza del mismo y las tecnologías que se conocen o se estiman involucradas.
2. Revisión de Capacidades
   - Revisar las capacidades de tiempo y recursos para dar respuesta al requerimiento.
   - Revisar la disponibilidad de recursos humanos capacitados y calificados para la tarea pericial.
3. Revisión de Equipamiento básico necesario
   - Evaluar si se cuenta con el equipamiento básico.
4. Análisis de Factibilidad
   - Determinar la factibilidad de atención y resolución del requerimiento, a partir del alcance inicial del mismo y de la revisión de capacidades y equipamiento disponible.

5. Definición del alcance
   - Definir un alcance acorde a las necesidades del requerimiento y las tecnologías que se conocen o estiman involucradas.
6. Planificación y Diseño de Estrategia
   - Planificar y diseñar la estrategia a implementar para la resolución del requerimiento.
   - Delinear los escenarios posibles.
   - Especificar la lista de actividades preliminares de las próximas fases (desde pedidos de allanamiento, actividades a realizar en el lugar del hecho, tipo de adquisiciones a realizar, preparación de ambientes específicos o la disponibilidad de equipos o expertos necesarios, etc.)
   - Resaltar las actividades críticas o relevantes.
   - Asignar recursos humanos a las actividades, según disponibilidad de tiempo, perfil y capacitación.
   - Asignar recursos técnicos a las actividades, según capacidad y disponibilidad.
7. Análisis de Riesgo
   - Analizar los riesgos sobre la estrategia planteada.
   - Detectar riesgos que pudieran modificar, alterar o eliminar la evidencia digital original; como también riesgos vinculados a la gestión del trabajo, como ser desvíos de tiempos o falta de capacidad de recursos.
   - Calificar los distintos riesgos asociados a las actividades y establecer las acciones para prevenir o mitigar los mismos.
   - Diseñar planes de contingencia.
8. Preparación de los equipos y herramientas para las tareas a realizar
   - Asociada a la Actividad Transversal “Preparación de equipos y herramientas”.
   - Preparar y validar herramientas de software y hardware necesarias para afrontar las tareas forenses, mínimamente para la próxima Fase de Relevamiento e Identificación.

Detalle de Actividades Específicas en casos de Base de Datos Relacionales

Según los escenarios, considerar servidores de base de datos como también servidores donde se migren o repliquen las base de datos (sean ambientes de producción, contingencia, preproducción, prueba, etc.). En caso de que existan auditorías de datos configuradas a través de AUDB, incluir siempre a las base de datos de configuración, metadatos y resultados de AUDB para el posterior análisis e interpretación de los datos de auditoría.

1.1. Recepción del Requerimiento de Análisis de Base de Datos Relacionales

- Recepcionar requerimientos de oficio o de un cliente relacionados a BDR.
- Analizar la tecnología de base de datos involucrada, sistema operativo, volumen de datos. Incluso observar la naturaleza de la organización para deducir criticidad de los datos, los servidores y alguna legislación particular asociada.
- Analizar el nivel de especificación del requerimiento. Por ejemplo:
    - Si es un requerimiento general que involucra a una investigación en base de datos o un requerimiento técnico.
    - Si incluye reclamos de empleados, clientes, usuarios por contenido o tratamiento de datos en las base de datos.
    - Si incluye resultados de mecanismos de control o incluso reportes de AUDB con detalle de potenciales acciones maliciosas, indebidas o dudosas.

7.1. Análisis de Riesgos de Análisis en Base de Datos Relacionales

- Detectar riesgos que pudieran modificar, alterar o eliminar la evidencia digital de base datos, según, se pueda deducir que el trabajo implique realizar análisis o adquisiciones en vivo, criticidad de la base de datos en la operatoria de la organización, naturaleza de la organización, volumen de datos, posición del propietario de la base de datos en relación con el caso (sospechoso o víctima), tecnologías involucradas, cantidad de usuarios, naturaleza de los datos afectados, tipo de sospechosos (empleados, ex-empleados, clientes, etc.), etc.

8.1. Preparación de los equipos y herramientas para las tareas en BDR

- Asociada a la Actividad Transversal “Preparación de equipos y herramientas”, ítem específico para base de datos relacionales.

4.3.5. Fase de Relevamiento e Identificación

Descripción General

La fase de relevamiento e identificación abarca la investigación que se realiza para conocer en detalle el caso e identificar los objetos de interés y potenciales fuentes de información útiles o de evidencia digital, como también el relevamiento de los recursos humanos como de las tecnologías de software y hardware.

Objetivo

Desarrollar y ejecutar estrategias fundamentales y críticas para el relevamiento, identificación y validación de las potenciales fuentes de evidencia digital de forma previa al contacto con la misma.

Aplica a

- Labores investigativas y de identificación de una investigación judicial.
- Labores de reconocimiento, exploración e identificación para un caso asociado a un servicio forense particular.

Roles Actuantes

- Responsable de Identificación (RI) y Especialista en Identificación (EI)
- Para casos de base de datos: Especialista Forense en Base de Datos (EFBD) y Especialista Auditor Forense en Base de Datos (EAFBD)

Consideraciones

La fase de relevamiento e identificación puede llevarse en forma conjunta con la fase de preparación inicial. Al igual que la fase de preparación inicial, esta fase se plantea previa al contacto con la evidencia digital, e idealmente antes de dirigirse al lugar del hecho o del allanamiento.

La fase de relevamiento e identificación puede ser llevada a cabo “in situ” en casos urgentes o que por alguna razón sea necesario realizarla en el lugar del hecho o del allanamiento.

El tipo de actividades de relevamiento e identificación a realizar dependen de la urgencia, la naturaleza del caso y si corresponde a un caso judicializado o no. Se plantean diferentes escenarios según el requerimiento implique asistir al domicilio de la víctima, del sospechoso o de la organización, o si se refiere a equipos aportados por la víctima, testigos o algún involucrado directa o indirectamente al caso, etc.

En esta fase se requiere, según los casos y posibilidad, determinado contacto con el cliente o miembros de la organización donde se realizará el trabajo para poder efectuar tareas de relevamiento.

Abarca actividades de identificación de documentación legal y técnica, como de identificación de infraestructura tecnológica. También la identificación de fuentes de información útiles y relevantes para el caso de investigación y la determinación de su alcance, amplitud y profundidad.

Las actividades de esta fase posibilitan categorizar y clasificar la evidencia digital según la volatilidad de los datos y el interés sobre cada uno.

La información relevada también sirve para ajustar la planificación y la estrategia planteada en la fase anterior (si no existiese, se puede definir en esta fase) y para la toma de decisiones sobre el caso (por ejemplo, gestión de pedidos de allanamientos, solicitud de disponibilidad de expertos en determinadas tecnologías, etc.).

En el caso de investigaciones judiciales, esta fase es llevada a cabo por responsables de identificación, pudiendo pedir el asesoramiento o asistencia a peritos informáticos especialistas en identificación o en tecnologías específicas.

Si bien pueden surgir escenarios no previstos en las fases siguientes, ejecutar una fase de relevamiento e identificación adecuada reduce el universo de posibilidades de situaciones inesperadas o inmanejables que puedan acontecer.

Principales Actividades

Fase de Relevamiento e Identificación			
Actividades Generales (ForenseUDE)		**Actividades Específicas (ForenseDB)**	
1	Relevamiento e Identificación de la documentación legal y administrativa	1.1	Ídem (aplicable a BDR)
2	Relevamiento e Identificación de la documentación técnica	2.1	Ídem (aplicable a BDR)
3	Relevamiento e Identificación de Infraestructura de IT	3.1	Relevamiento e Identificación de Infraestructura de BDR
4	Identificación y validación de potenciales fuentes de evidencia digital	4.1	Ídem (aplicable a BDR)
5	Identificación de las características de la Evidencia Digital	5.1	Identificación de las características de la Evidencia Digital en BDR
6	Clasificación de la Evidencia Digital	6.1	Categorización de la Evidencia Digital en BDR
7	Ajuste de Planificación y Diseño de Estrategia	7.1	Ídem (aplicable a BDR)
8	Gestión de pedidos de allanamientos	8.1	Ídem (aplicable a BDR)
9	Preparación de los equipos y herramientas para las tareas a realizar	9.1	Preparación de los equipos y herramientas para las tareas en BDR
10	Detallar Requisitos de Recolección y Adquisición	10.1	Ídem (aplicable a BDR)

Tabla 2: Fase de Relevamiento e Identificación

Detalle de Actividades Generales

1. Relevamiento e Identificación de la documentación legal y administrativa
   - Relevar e identificar toda la documentación legal y administrativa relacionada al requerimiento (por pedido de oficio, exploración en internet, aportes de involucrados, entre otros medios).
   - Identificar, para casos de investigaciones judiciales, los documentos de las denuncias y los informes que la acompañen.

- Relevar, para casos asociados a organizaciones, el marco legal asociado a la naturaleza de la misma. Conocer también la información relevante para la organización y la que por ley debe ser objeto de privacidad, disponibilidad e integridad.

2. Relevamiento e Identificación de la documentación técnica
   - Relevar e identificar la documentación técnica de infraestructura tecnológica, hardware, software, políticas y procedimientos de seguridad lógica y física, manuales de diseño o de ayuda de aplicaciones o cualquier otra documentación relevante para conocer el caso en profundidad y poder tomar las decisiones adecuadas (por pedido de oficio, exploración en internet, aportes de involucrados, entre otros medios).
3. Relevamiento e Identificación de Infraestructura de IT
   - Relevar e identificar la Infraestructura de IT (por pedido de oficio, exploración en internet, aportes de involucrados, entre otros medios).
     - Relevar e identificar la estructura de red y/o hardware sobre la cual se va a trabajar (sea un hogar con computadoras personales o una organización con servidores virtualizados o en la nube, etc.).
     - Identificar servidores internos y externos, usuarios, equipos o todo tipo de dispositivos vinculados al caso (o de los usuarios afectados) y el estado de los mismos (encendidos, apagados, rotos, u otros posibles estados).
     - Identificar el tipo de asignaciones IP (direcciones estáticas o asignación dinámica), ya que esto brinda una gran pauta de identificación de cada uno de los dispositivos a partir de la dirección IP.
   - Identificar sistemas vinculados al caso a investigar y las particularidades de los mismos (programas específicos, herramientas de trabajo, sitios web, bases de datos, etc.) y, según el caso, la cantidad y detalle de los usuarios que administran o acceden a los mismos con determinados permisos.
4. Identificación y validación de potenciales fuentes de evidencia digital
   - Identificar y validar las potenciales fuentes de información o elementos de prueba (físicos y el lógicos) de interés para la investigación.

5. Identificación de las características de la Evidencia Digital
   - Identificar toda característica relevante según la naturaleza de la evidencia digital, el caso y los escenarios posibles.
     - Determinar quiénes son los custodios o responsables de la evidencia digital.
     - Identificar cuál es la naturaleza de la evidencia digital.
       - Sistemas Operativos Linux, Windows, etc. Servidores locales o en la nube. Servidores físicos o virtualizados. Servidores de Base de datos (Oracle, MS SQL Server, etc.). Servidores de correo electrónico (Exchange, Lotus, etc.) con alojamiento local o externo. Computadoras. Dispositivos Móviles. Cámaras de Seguridad, etc.
       - Formato de la evidencia digital (archivos, mails, registros en el sistema operativo, registros en base de datos, etc.).
     - Identificar la criticidad de la información asociada a la evidencia digital en la organización.
     - Relevar dónde está ubicada y almacenada la evidencia digital.
       - Almacenada de forma local o en la nube.
       - Evidencia digital en la nube físicamente en el país o en el exterior.
       - Evidencia local en servidor físico o virtual.
     - Estimar volumen de la evidencia digital. Relevar si el trabajo pericial involucra gran cantidad de dispositivos de almacenamiento, gran volumen de datos o de capacidades altas. Evaluar si es necesario hacer un clonado de todos y cada uno de ellos.
     - Identificar la posibilidad de que la evidencia digital se encuentre cifrada o no accesible fácilmente.
     - Identificar los escenarios de adquisición de la evidencia digital según su volatilidad y relevancia.
     - Evaluar la disponibilidad o la posibilidad de obtener acceso a la información de las claves de acceso de manera voluntaria (de parte de administradores, usuarios, etc.).

  - Identificar otras características relevantes según el tipo de evidencia digital.

6. Clasificación de la Evidencia Digital según la volatilidad y relevancia
   - Clasificar la evidencia digital según:
     - La volatilidad de la misma.
     - La relevancia para el caso.
     - Sea física (como dispositivos móviles, computadoras, discos rígidos, etc.) o lógica (o intangibles como archivos, programas, base de datos, etc.).
     - Según existan legislaciones por cumplir en el acceso, tratamiento y traslado de la misma, como ser la Ley de datos personales o leyes internacionales en el caso de evidencia digital en la nube.
   - Establecer y aplicar las clasificaciones que sean necesarias según la naturaleza de la evidencia digital y el caso asociado.
7. Ajuste de Planificación y Diseño de Estrategia
   - A partir del relevamiento e identificación realizado, ajustar la planificación y la estrategia diseñada, como también el análisis de riesgos, establecidos en la fase anterior.
   - Si por diversos motivos no existiese una planificación, una estrategia o un análisis de riesgos previamente, especificar los mismos en esta etapa.
8. Gestión de pedidos de allanamientos
   - Gestionar pedidos de allanamientos, en los casos que se requiera, para secuestrar equipos o las medidas que se consideren necesarias.
   - Detallar el tipo de material a secuestrar y las medidas a realizar, ya que lo que no se encuentre especificado en la orden de allanamiento, no podrá llevarse a cabo (como ser volcados de memoria principal, la necesidad de enumeración de dispositivos informáticos en la red y la utilización de herramientas informáticas para tal fin, etc.).
   - Estimar los elementos, dispositivos de resguardo, equipos, etc. que se deben llevar para realizar los allanamientos.
9. Preparación de los equipos y herramientas para las tareas a realizar
   - Asociada a la Actividad Transversal “Preparación de equipos y herramientas”.

- Preparar y validar herramientas de software y hardware necesarias para afrontar las tareas forenses, mínimamente para las próximas Fases de Recolección y/o Adquisición.

10. Detallar Requisitos de la Recolección y Adquisición
    - Identificar y detallar los requisitos de recolección y adquisición.
    - En el caso de evidencia digital que posea datos personales, datos sensibles o bajo protección intelectual, es indispensable trabajar con la debida autorización judicial o de la organización y aplicar niveles de protección adicionales, como ser cifrado de la información, para garantizar la confidencialidad de los datos.
    - Se recomienda solicitar autorización por escrito para efectuar la recolección de evidencias en las empresas que contraten los servicios periciales, ya que en ocasiones se pueden manejar datos confidenciales o que incluso la disponibilidad de los servicios puede quedar afectada. Además, a menos que haya indicios suficientes y fundamentados no se deben recopilar datos de fuentes o lugares a los que no se accede normalmente o sin permiso, como por ejemplo ficheros con datos personales.

Detalle de Actividades Específicas en casos de Base de Datos Relacionales

Según los escenarios, considerar servidores de base de datos como también servidores donde se migren o repliquen las base de datos (sean ambientes de producción, contingencia, preproducción, prueba, etc.). En caso de que existan auditorías de datos configuradas a través de AUDB, incluir siempre a las base de datos de configuración, metadatos y resultados de AUDB para el posterior análisis e interpretación de los datos de auditoría.

La metodología presta especial atención al tratamiento de los datos personales y la propiedad industrial, de manera de garantizar que tanto el acceso a información de carácter privado o información de una organización sea bajo el consentimiento previo del responsable de dichos datos o mediante autorización judicial.

3.1. Relevamiento e Identificación de Infraestructura de Base de Datos Relacionales

- Identificar los servidores y bases de datos vinculados al caso y la arquitectura implantada.
- Relevar si en las bases de datos identificadas existen configuradas auditorias forenses preventivas a través de la metodología AUDB. De ser así gran parte de la información de este punto podría estar disponible en la documentación de relevamiento y estrategia propia de AUDB.
- Obtener información de configuración y acceso en los servidores y bases de datos identificados: tipo de servidores, virtualización de servidores, servidores en la nube, tipo y versiones de motores de base de datos, formas de acceso o conexión a las mismas, sistemas o aplicaciones que las utilizan y con qué roles se conectan, transferencia de datos entre base de datos, auditorías de datos, entre otros aspectos que puedan ser relevantes según las características técnicas de cada contexto.
- Relevar la implementación física y lógica del motor de base de datos.
- Relevar y analizar la estrategia de seguridad general implantada en los servidores de base de datos relacionados al caso.
- Relevar y analizar la estrategia de seguridad implantada en los propios motores de base de datos involucrados y en las bases de datos en si (qué usuarios pueden acceder, leer, actualizar, insertar o borrar datos, con qué roles y de qué forma) y como se relacionan con la seguridad de los servidores (seguridad integrada o no).
- Analizar políticas de resguardo y planes de contingencia de información implementados y cómo se llevan técnicamente a la práctica.
- Analizar tipos y disponibilidad de resguardos (archivos de backups).
- En el caso que exista aplicación de AUDB, determinar en qué servidor se encuentran alojadas las base de datos de configuración de AUDB y la de almacenamiento de resultados AUDB asociada. Relevar las configuraciones de auditorías de AUDB (tipos de auditorías, filtros, almacenamiento seguro, protección de visualización, reglas de autoprotección) y las planificaciones de ejecución de auditorías.

- Investigar el contenido de las bases de datos disponibles en ambientes de desarrollo, prueba y preproducción (y los que existiesen). Conocer cómo es la política de seguridad de datos asociada a la generación, disponibilidad y acceso de datos en dichos ambientes. Por ejemplo, si existen mecanismos de ofuscación u ocultamiento de información sensible o si existe alguna política de accesos según el tipo de usuarios a cada uno de los ambientes (sean programadores internos o por consultora, entre otros).
- Identificar servicios de integración, servicios de análisis, servicios de reportes, y toda aplicación que interactúan con las bases de datos involucradas.

5.1. Identificación de las características de la Evidencia Digital en Base de Datos Relacionales

- Relevar información general de las base de datos, tablas y campos que contengan los datos relacionados al caso, como también sus relaciones con otras tablas de la misma base de datos u otra base de datos.
- Determinar claramente qué usuarios y sistemas acceden y manipulan la información, de qué forman gestionan el acceso a la misma, tipos de conexión, información que se visualiza o modifica a través de los diferentes sistemas y computadoras, horarios habituales de acceso, entre otras variables de entorno relevantes para el diagnóstico de criticidad.
- Investigar si existe algún tipo de replicación total o parcial de las tablas, ya sea a otras tablas, archivos, servicios y la finalidad de la replicación.
- Investigar si existe información cifrada en la base de datos y la estrategia de implementación asociada.
- Relevar, si existiese, mecanismos de auditorías implementada general o con AUDB y, de existir, analizar las características de las mismas en cuanto a qué se audita, cuándo, de qué forma, la continuidad de la ejecución de los mismos y el control y seguimiento aplicado sobre las mismas.
- Incluir en el análisis restauraciones de bases de datos y bases de datos utilizadas para migraciones de datos.
- Considerar archivos de configuraciones, de datos, de transacciones, de control, de reportes, de trazas, etc., vinculados a los datos.

6.1. Categorización de la Evidencia Digital en Base de Datos Relacionales

- Categorizar la Evidencia Digital según la volatilidad y relevancia en Base de Datos.
- Determinar el alcance de los datos personales involucrados en el caso, es decir si corresponden a datos personales en el ámbito nacional o internacional, para determinar las leyes de datos personales que aplican.
- Gestionar las autorizaciones judiciales necesarios para el tratamiento de datos personales.
- Incluir archivos, resultados de auditorías de datos generales o de AUDB asociadas a los datos a analizar.

9.1. Preparación de los equipos y herramientas para las tareas en BDR

- Asociada a la Actividad Transversal "Preparación de equipos y herramientas", ítem específico para base de datos relacionales.

4.3.6. Fase de Recolección

Descripción General

Etapa en la que se lleva a cabo la recolección de la evidencia digital potencialmente relevante identificada en la fase anterior. Abarca las acciones y medidas necesarias para obtener y preservar los equipos físicos y/o posibles fuentes de evidencia digital sobre los que se deberá trabajar posteriormente. Se aplican acciones de aislamiento de la evidencia digital para protegerla de cualquier contaminación.

Objetivo

Preservar la evidencia digital original aplicando procedimientos forenses adecuados para evitar contaminarla y que sea admisible en un proceso judicial, de forma que sea luego legalmente defendible, razonable, amplia, pero a medida, auditable y repetible.

Aplica a

- Acceso a posible fuentes de evidencia digital en una investigación judicial, a partir del secuestro de elementos (mediante orden de allanamiento autorizada)

o ante la presentación espontánea de las mismas en el caso por parte de involucrados.

- Acceso a posibles fuentes de evidencia digital en un servicio forense particular.

Roles Actuantes

- Especialista en Recolección (ER) y Especialista en Adquisición (EA)
- Para casos de base de datos Especialista Forense en Base de Datos (EFBD) y Especialista Auditor Forense en Base de Datos (EAFBD).

Consideraciones

Esta fase involucra aplicar procedimientos adecuados de preservación asegurando no contaminar la evidencia digital. Registrar cada acción sobre la evidencia digital, responsables y custodios involucrados, de manera de aplicar procesos auditables y repetibles, brindando trazabilidad al proceso a través de la aplicación de la debida cadena de custodia.

No todos los casos involucran un procedimiento de allanamiento o trabajar en el lugar del hecho, pueden incluso surgir de aportes de evidencia de clientes, organizaciones, víctimas o involucrados directa o indirectamente al caso. De todas maneras, en todos los casos se aplica la fase de recolección para preservar la evidencia digital del caso, garantizando además la debida cadena de custodia.

Se refiere a la recolección también de documentación, anotaciones u otras evidencias físicas relacionadas relevantes al caso.

Es indispensable en ciertos escenarios la manipulación por parte de un experto específico para manipular la evidencia digital en la escena del hecho.

Se debe recolectar según el orden de volatibilidad de la evidencia digital y en base a la categorización planteada en la fase anterior.

La fase de Recolección y la fase de Extracción y Análisis pueden estar muy distantes en el tiempo, por lo que se deben tomar las medidas necesarias para garantizar el correcto resguardo de toda la evidencia secuestrada, así como su persistencia.

Principales Actividades

Fase de Recolección			
Actividades Generales (ForenseUDE)		**Actividades Específicas (ForenseDB)**	
1	Preparación de los equipos y herramientas para las tareas de Recolección	1.1	Preparación de los equipos y herramientas para las tareas de Recolección en BDR
2	Preparación de los elementos necesarios para la recolección y/o traslado de la evidencia digital	2.1	Preparación de los elementos necesarios para la recolección y/o traslado de la evidencia digital en BDR
3	Inspección de Infraestructura de IT	3.1	Inspección de Infraestructura relacionada a BDR
4	Adquisición de datos volátiles o de sistemas encendidos	4.1	Adquisición de datos volátiles o de sistemas encendidos a BDR
5	Aplicar algoritmos de Hash para garantizar integridad de la evidencia digital	5.1	Ídem (aplicable a BDR)
6	Desconectar los equipos o dispositivos a recolectar	6.1	Ídem (aplicable a BDR)
7	Recolección, Secuestro, aislamiento, embalaje y transporte de objetos	7.1	Ídem (aplicable a BDR)
8	Fotografiar y/o filmar	8.1	Ídem (aplicable a BDR)
9	Acta de allanamiento	9.1	Ídem (aplicable a BDR)
10	Formulario de cadena de custodia	10.1	Cadena de Custodia de Evidencia Digital en BDR

Tabla 3: Fase de Recolección

Detalle de Actividades Generales

1. Preparación de los equipos y herramientas para las tareas de Recolección
   - Asociada a la Actividad Transversal “Preparación de equipos y herramientas”.
   - Preparar y validar herramientas de software y hardware necesarias para afrontar las tareas forenses de recolección y/o adquisición.

- Disponer de variedad de herramientas para enfrentar los diferentes desafíos y escenarios que se pueden presentar en el lugar.
- Garantizar que las herramientas que se utilicen y de la forma que se apliquen, no impliquen una intrusión a los equipos, la red, los servidores, las bases de datos, los correos electrónicas, etc. y que se usen con finalidad meramente informativa acorde y dentro del alcance de la inspección necesaria a realizar.

2. Preparación de los elementos necesarios para la recolección y/o traslado de la evidencia digital
   - Según el tipo de evidencia digital, preparar los elementos adecuados para la recolección y/o traslado de la misma, para garantizar que no se deteriore, rompa o pueda violarse su confidencialidad, integridad o disponibilidad.
3. Inspección y detección de Infraestructura de IT
   - Esta actividad aplica en el caso de recolecciones en el lugar del hecho o del allanamiento.
   - Inspeccionar para detectar todos los objetos de interés para la investigación o actuación pericial.
     - Estas inspecciones pueden ser oculares como también a partir del uso de técnicas y herramientas específicas.
     - En el caso de allanamientos, es importante que previamente en el pedido del mismo, se indiquen las medidas a llevar a cabo para que estén autorizadas judicialmente.
     - Detectar servidores internos y externos, dispositivos de usuarios (ejemplo, equipos PC, USB, SD, SIM, CD, dispositivos móviles, etc.), incluso routers, escáneres, impresoras y diseñar una topología general con los equipos involucrados.
     - Así mismo, se deben tomar los datos de la persona responsable del equipo y del usuario o los usuarios que trabajen en él, y cualquier otra información que se considere que puede resultar relevante.
     - Observar la seguridad física de los objetos (si están en una sala aislada, al alcance de cualquier persona, etc.).

- Categorizar la evidencia digital encontrada según orden volatilidad y relevancia.
- Separar los equipos a recolectar o secuestrar.
- Justificar los motivo por el que se van a recolectar, secuestrar o adquirir las evidencias.

4. Adquisición de datos volátiles o de sistemas encendidos
   - Actividad detallada en la siguiente Fase de “Adquisición”.
   - Identificar a los equipos sobre los que se necesita realizar adquisición de datos volátiles o en vivo.
   - Adquisición en vivo de los equipos de los cuales se quiera preservar datos volátiles, o que por su naturaleza o criticidad para la organización no es posible apagarlos o secuestrarlos y se necesite realizar una adquisición en vivo de la imagen forense o incluso un análisis en el lugar.
   - En el caso de adquisición de datos volátiles corresponde a la adquisición del volcado de la memoria principal, archivo de paginación e hibernación de sistemas encendidos, entre otros artefactos.
   - Realizar este trabajo siempre en presencia de testigos y en casos judicializados, con la debida autorización judicial. Es recomendable fotografiar y filmar las acciones.
5. Aplicar algoritmos de Hash para garantizar integridad de la evidencia digital
   - Aplicar algoritmos de Hash para garantizar la integridad de la evidencia digital adquirida “in situ”.
   - Aplicar algoritmos de Hash sobre cada uno de los archivos que formen parte de las actividades de la fase de recolección.
6. Desconectar los equipos o dispositivos a recolectar
   - Desconectar los equipos a recolectar de la alimentación eléctrica. Considerar que al desconectar el equipo de la alimentación eléctrica se puede evitar que un proceso siga alterando o eliminando datos, como también correr el riesgo de provocar, por ejemplo, un borrado de datos si existe una tarea planificada en caso de desconexión o del cifrado de información.

- Desconectar los equipos a recolectar de la red, en especial, si existen riesgos de que un hecho siga realizándose, como ser una descarga no autorizada de datos o el borrado remoto de datos.

7. Recolección, secuestro, aislamiento, embalaje y transporte de objetos
   - Respetar los protocolos de levantamiento de evidencia digital aplicables, de manera de evitar cualquier alteración inapropiada o destrucción de la evidencia digital o fuentes de la misma.
   - Identificar, separar, etiquetar y fotografiar cada elemento a recolectar con un número o identificación. Identificar marca, modelo y número de serie de cada uno de los equipos. Registrar el propietario del elemento y en qué lugar fue recolectado, y fecha y hora del evento.
   - Documentar y justificar todos los pasos seguidos.
   - Preservar lógicamente la evidencia digital aplicando adecuados métodos de aislamiento de la información contenida en los dispositivos. Aislar los dispositivos de manera que se preserve la integridad de los mismos y de la evidencia digital.
   - La preservación física y lógica debe realizarse con los elementos de embalajes y consideraciones adecuadas en función de la naturaleza de los equipos a recolectar (según deban protegerse, por ejemplo, contra estática o sean más o menos sensible a la manipulación, etc.) para evitar que se dañe físicamente la misma en el transporte y con etiquetas informativas para facilitar su identificación sin tener que desembalarla. Utilizar materiales especiales para el resguardo y transporte de los equipos, dispositivos o medios de almacenamiento (entre otros) con la finalidad de evitar golpes, roturas, deterioros a causa de un mal embalaje.
   - En el caso de evidencia digital que posea datos personales, datos sensibles o bajo protección intelectual, es indispensable que a las imágenes forenses asociadas adquiridas se le aplique cifrado de datos para asegurar la confidencialidad de los datos (leyes de protección de datos personales, derechos fundamentales de los individuos involucrados).

- Proteger los bienes para el transporte desde el lugar de los hechos hasta el laboratorio con los medios necesarios para evitar golpes o protegerlos de caídas fortuitas.

8. Fotografiar y/o filmar
   - Fotografiar o filmar la escena del hecho al llegar al allanamiento, para tener registro de cómo se encontraba inicialmente (estado original de la escena).
   - Fotografiar o filmar la escena del hecho al final y durante todo el proceso.
   - Fotografiar o filmar las fuentes de evidencias digitales de forma previa a la recolección y en especial en la adquisición en vivo.
   - Fotografiar o filmar el proceso de embalaje de las evidencias digitales y el estado de las mismas previo al transporte.
   - Aplicar algoritmos de hash a los archivos de fotos y videos.
9. Acta de allanamiento
   - En los casos de allanamientos, completar la correspondiente acta de allanamiento con los datos identificatorios de cada uno de los equipos y dispositivos a secuestrar, como también el nombre y tamaño de los archivos de las imágenes de volcado de memoria u otros archivos, con sus correspondientes valores de hash.
   - Constar en el acta de allanamiento todas y cada una de las operaciones realizadas, así como el detalle de lo secuestrado, incluyendo las imágenes o copias forenses y el correcto inicio de la cadena de custodia, siempre en presencia de testigos. Describir todas las operaciones y objetos involucrados lo más detalladamente posible.
10. Formulario de cadena de custodia
    - Asociada a la Actividad Transversal “Cadena de Custodia”.
    - En esta fase se debe efectuar el correcto inicio de la cadena de custodia, siempre en presencia de testigos para realizar el seguimiento de la evidencia digital mediante el formulario de Cadena de Custodia con el inventariado de los elementos recolectados.
    - Se conforma un formulario por cada elemento recolectado.

Detalle de Actividades Específicas en casos de Base de Datos Relacionales

Según los escenarios, considerar servidores de base de datos como también servidores donde se migren o repliquen las base de datos (sean ambientes de producción, contingencia, preproducción, prueba, etc.). En caso de que existan auditorías de datos configuradas a través de AUDB, incluir siempre a las base de datos de configuración, metadatos y resultados de AUDB para el posterior análisis e interpretación de los datos de auditoría.

1.1. Preparación de los equipos y herramientas para las tareas de Recolección en Base de Datos Relacionales

- Disponer de variedad de herramientas para enfrentar los diferentes desafíos y escenarios que se pueden presentar en el lugar para recolectar BDR.

2.1. Preparación de los elementos necesarios para la recolección y/o traslado de la evidencia digital en Base de Datos Relacionales

- La evidencia digital en BDR podrá ser recolectada o analizada “in situ” dependiendo del volumen y naturaleza de la organización.
- En general, no será factible secuestrar o desconectar servidores de SGBD o detener los servicios de base de datos dada la criticidad de los mismos.
- Se pueden requerir discos de almacenamiento de gran capacidad para resguardar las imágenes forenses adquiridas en vivo, adquisición de datos volátiles o en vivo o el resultado de análisis en el lugar del hecho.
- En el caso de recolectar backups, analizar si se dispone de los mismos (según el último backup disponible y los previos realizados) o se necesita hacer un nuevo backup en línea. Si es necesario realizar un backup de la base de datos, determinar el almacenamiento para realizar backup.

3.1. Tareas de Inspección de Infraestructura relacionada a Base de Datos Relacionales

- Aplicar las tareas de inspección de la actividad general en base de datos.
- En el caso que exista aplicación de AUDB, determinar en qué servidor se encuentran alojadas las base de datos de configuración de AUDB y la de almacenamiento de resultados AUDB asociada.
- Importante observar en el lugar la disponibilidad de acceso a Backups en los casos de imposibilidad de secuestro de datos de las Base de datos en línea.

- Observar impresiones de datos sensibles en la impresora o a alcance de cualquier persona, anotaciones de claves a la vista, etc.
- En los casos que sea posible y necesario y respetando la voluntad de los mismos, relevar a usuarios y administradores para conocer detalles de la infraestructura (de forma complementaria al relevamiento de la fase anterior).

4.1. Adquisición de datos volátiles o de sistemas encendidos a BDR

- Actividad detallada en la siguiente Fase de "Adquisición".

10.1. Cadena de Custodia de Evidencia Digital en Base de Datos Relacionales

- Es muy importante identificar el nombre del servidor, la base de datos, tablas, campos sobre las que se recolecta información.
- Agregar en la cadena de custodia datos sobre la arquitectura general donde estaba inserta la base de datos, como parte de la descripción del contexto.
- En el caso de recolecciones a partir de resultados de análisis, adjuntar como anexo los scripts de SQL ejecutados y/o el detalle de las aplicaciones utilizadas.
- Indicar el nombre, tamaño y extensión de los archivos resultantes, como también el tipo de contenido de los mismos y el valor de hash.

4.3.7. Fase de Adquisición

Descripción General

La fase de adquisición involucra las actividades en la que se obtiene el contenido a analizar de la evidencia digital relevante al caso, abarcando todas las tareas necesarios para la obtención de la imagen o copias forense del contenido.

Objetivo

Adquirir la evidencia digital basada en el orden de volatilidad y relevancia para su posterior análisis.

Aplica a

- Realizarse "in situ" en el lugar del hecho o durante un allanamiento (en este caso se solapa con la Fase de Recolección).

- Realizarse en un laboratorio forense luego de haber sido recolectado los objetos.

Roles Actuantes

- Especialista en Adquisición (EA)
- Para casos de base de datos Especialista Forense en Base de Datos (EFBD) y Especialista Auditor Forense en Base de Datos (EAFBD).

Consideraciones

La fase de adquisición hace énfasis en la aplicación de metodologías precisas de adquisición de evidencia digital, basadas en el orden de volatilidad, con el acompañamiento de la correspondiente documentación detallada de todo el proceso y del resguardo de la evidencia digital original, evitando o reduciendo al mínimo los cambios en la evidencia digital original que se está recolectando.

La adquisición se basa en una serie de pasos y pautas a seguir procurando ser lo menos intrusivo posible con el fin de preservar el sistema en su estado original, aplicando procedimientos forenses adecuados de tal forma que la evidencia digital obtenida pueda ser admisible como prueba en un proceso judicial.

Esta fase puede realizar “in situ” en el lugar del hecho o durante un allanamiento, o bien, en un laboratorio forense luego de haber recolectado los objetos.

Las actividades de esta fase abarcan tanto la adquisición de datos persistentes, datos volátiles, paquetes de red y medios de almacenamiento extraíbles, entre otros.

En esta fase se requiere de la intervención de un especialista en adquisición, incluso especialista en tecnologías particulares, con la experiencia no solo de discernir los escenarios de adquisición a partir de los puntos de pericia, sino con la capacidad de reacción ante eventos sensibles y/o inesperados que pueden suceder durante la adquisición.

Principales Actividades

Fase de Adquisición			
Actividades Generales (ForenseUDE)		**Actividades Específicas (ForenseDB)**	
1	Identificar y clasificar los dispositivos a adquirir	1.1	Ídem (aplicable a BDR)
2	Preparación de los equipos y herramientas para las tareas de Adquisición	2.1	Ídem (aplicable a BDR)
3	Preparación de los dispositivos de almacenamiento de imágenes forenses	3.1	Ídem (aplicable a BDR)
4	Definir la estrategia de adquisición	4.1	Ídem (aplicable a BDR)
5	Adquisición de datos volátiles o en vivo	5.1	Adquisición de datos volátiles o en vivo BDR
6	Adquisición y análisis de datos específicos (volátiles y persistentes) en vivo	6.1	Adquisición y análisis de datos específicos (volátiles y persistentes) en vivo en BDR
7	Adquisición de datos de medios de almacenamiento persistentes	7.1	Adquisición de datos de medios de almacenamiento persistentes en BDR
8	Otras adquisiciones	8.1	Ídem (aplicable a BDR)
9	Validación y resguardo	9.1	Ídem (aplicable a BDR)
10	Acta pericial	10.1	Ídem (aplicable a BDR)
11	Formulario de cadena de custodia	11.1	Ídem (aplicable a BDR)
12	Transporte con requisitos de protección adicionales	12.1	Ídem (aplicable a BDR)

Tabla 4: Fase de Adquisición

Detalle de Actividades Generales

1. Identificar y clasificar los dispositivos a adquirir.
   - Identificar y clasificar los equipos o dispositivos a adquirir según el orden de volatilidad y la naturaleza de los mismos.
   - En los casos de trabajo de adquisición en el laboratorio forense:

- Recibir e identificar los equipos y dispositivos a peritar.
- Validar y fotografiar el estado de cómo se reciben los elementos a peritar y enumerarlos.
- Constatar los datos y estados validados con respecto a los datos registrados en el formulario de cadena de custodia y acta de allanamiento (si existiese).
- Buscar medios de almacenamiento persistentes (discos rígidos, SSD, etc.), identificarlos y enumerarlos con número, marca, modelo, número de serie y capacidad de almacenamiento.
- Identificar como mínimo marca, modelo, y número de serie de cada uno de los equipos en el acta pericial.

2. Preparación de los equipos y herramientas para las tareas de Adquisición
   - Asociada a la Actividad Transversal "Preparación de equipos y herramientas".
   - Preparar y validar herramientas de software y hardware necesarias para afrontar las tareas forenses de adquisición, considerando las versiones de los sistemas operativos (Windows, Linux, etc.) y de los programas.
   - Preparar de forma adecuada la estación de trabajo forense y su configuración.
3. Preparación de los dispositivos de almacenamiento de imágenes forenses
   - Sanitización de los dispositivos de almacenamiento. Cada dispositivo que se destine para alojar una imagen o copia forense debe haber pasado por un proceso de borrado seguro ("wipeado") para evitar la contaminación cruzada de información que pudiera contener previamente asociada a otros casos. Considerar que la contaminación cruzada se produce ante la recuperación de información eliminada en discos sin previo borrado seguro.
   - Disponer de varios dispositivos de almacenamiento para poder realizar copias por duplicado de las imágenes forenses y así poder trabajar luego sobre las copias y no con las imágenes originales. Incluso, en los casos que sea factible, realizar dos copias mínimas para disponer de una copia adicional en el caso de roturas.

- Validar tamaño de los dispositivos de almacenamiento para que sean de igual o mayor tamaño al original.
- Disponer de los adaptadores para conectar cada tipo de dispositivo de almacenamiento.

4. Definir la estrategia de adquisición
   - Conocer los puntos de pericia para adquirir contenidos acorde a los mismos.
   - Evitar adquirir información por encima de lo pedido y de lo que compete acceder o manipular. No excederse en la recolección (por ejemplo, si solo se solicitan determinados tipo de archivos, no es necesario realizar la adquisición del dispositivo completo). Según el alcance, preparar la adquisición de un equipo, de los medios de almacenamientos o adquisiciones lógicas (de "File System").
   - Se debe realizar el acto con todas las partes notificadas y presentes (o que asistan).
5. Adquisición de datos volátiles o en vivo
   - La adquisición en vivo se realiza sobre:
     - Equipos o dispositivos de los cuales se quiera preservar datos volátiles y luego se realizará el apagado del equipo para realizar el resto de la adquisición con el equipo apagado.
     - Equipos que por su naturaleza o criticidad para la organización no es posible apagarlos o secuestrarlos, y se necesite realizar una adquisición en vivo de la imagen forense completa.
   - Lo primero que se debe obtener es la fecha y hora del sistema para poder establecer una línea temporal de recopilación de evidencias, duración del proceso, etc. (validar la fecha y hora que sea correcta).
   - Aplicar procedimientos para la adquisición de datos volátiles de dispositivos encendidos (por hardware o software).
     - Obtener datos de volcado de la memoria principal (RAM) y caché (del microprocesador) en un archivo.
     - Descargar también el archivo de paginación o memoria virtual (no es necesario obtener el archivo de paginación si se va a realizar un volcado de disco en vivo a posteriori).

  - Obtener archivos hibernación de la computadora el cual contiene la imagen exacta del ordenador justo antes de que hiberne.
  - Adquirir datos volátiles del router obteniendo volcado de las tablas de ruteo (con información de la ruta de los paquetes de red), etc.
  - Almacenar la imagen con el volcado de datos volátiles a través de herramientas portables disponibles en un medio de almacenamiento externos.
- Aplicar procedimientos de adquisición en vivo de imágenes forenses de medios de almacenamientos de equipos encendidos, que no pueden ser apagados. Por ejemplo, en los casos donde se estima que si se apaga el equipo se podría cifrar la información del mismo y perder la posibilidad de acceder a la información plana. Incluso, casos donde por la criticidad del equipo en la organización no puede ser apagado o secuestrado como ser en hospitales, aeropuertos, etc. En estos casos, se debe realizar una imagen forense de los discos con el equipo encendido.
- Recomendaciones:
  - No apagar el ordenador hasta que se haya recopilado toda la información volátil.
  - No confiar en la información proporcionada por los programas del sistema ya que pueden haberse visto comprometidos. Se debe recopilar la información mediante programas desde un medio protegido (disco externo, pendrive, CD-ROM, etc.),
  - No ejecutar programas que modifiquen la fecha y hora de acceso de todos los ficheros del sistema.
  - Fotografiar o filmar el procedimiento completo.
  - Es esencial realizar este trabajo siempre en presencia de testigos y en casos judicializados, con la debida autorización judicial.
  - Considerar que la manipulación del equipo encendido va a generar cambios o modificaciones controladas, las cuales deben estar autorizadas y debidamente justificadas, documentadas y detalladas en la cadena de custodia.

6. Adquisición y análisis de datos específicos (volátiles y persistentes) en vivo
   - Habitualmente se suele volcar la memoria o el disco completo, y a partir de ahí se trabaja sobre diferentes copias para obtener el resto de las evidencias. Pero en ocasiones se puede obtener concretamente diferentes evidencias, ya que, dependiendo del caso, puede no ser necesario o posible realizar u obtener un volcado completo de la información, sino que será suficiente con realizar un análisis específico.
   - Los análisis de datos volátiles específicos en el lugar en general comprende: obtener la lista de procesos en ejecución, servicios en ejecución, usuarios que han iniciado sesión y listado de cuentas de usuario, información de red (estado de las conexiones activas, puertos UDP y TCP abiertos), FTP y otros servicios similares, registros del sistema operativo, dispositivos USB conectados, listado de redes WIFI a las que se ha conectado un equipo, configuración de seguridad del sistema operativo (ejemplo, Windows Security Center), configuración del firewall, programas que se ejecutan al iniciar el sistema operativo, extensiones de ficheros y programas asociados para abrirlos, listado de aplicaciones y archivos utilizados recientemente, programas instalados, contraseñas almacenadas en el equipo de diferentes servicios (en navegadores, de red, de correo, etc.), información cacheada en los navegadores (direcciones, historial de descargas), árbol de directorios y ficheros, histórico de intérpretes de comandos, capturas de pantalla, información del portapapeles, historial de internet, últimas búsquedas, cookies, volúmenes cifrados, unidades mapeadas, carpetas compartidas, grabaciones pendientes de CD, etc.
   - Los análisis de datos persistentes específicos en el lugar en general comprenden: información del sistema, tareas programadas, archivos impresos, variables de entornos, logs del sistema (como log de eventos de Windows, logs de actualizaciones del sistema, logs de firewalls, logs de FTP, logs de servicios de mensajería, etc.), archivos de copias locales de correo electrónico (como archivos con extensión “.pst” u “.ost”), programas que se abren habitualmente, papelera de reciclaje, archivos de URL accedidas (archivos de hosts), archivos ejecutables que no estén firmados, archivos de accesos directos, etc.

- Recomendaciones:
    - La recopilación de claves es recomendable siempre y cuando se haya obtenido previamente una autorización expresa, y se traten de acuerdo con la legislación vigente sobre protección de datos.
    - Fotografiar o filmar el procedimiento completo.
    - Es esencial realizar este trabajo siempre en presencia de testigos y en casos judicializados, con la debida autorización judicial.
    - Estas actividades de análisis deben estar autorizadas y debidamente justificadas, documentadas y detalladas en la cadena de custodia.

7. Adquisición de datos de medios de almacenamiento persistentes
    - Aplicar procedimientos para la adquisición tradicional sobre equipos apagados o medios de almacenamiento extraídos o extraíbles y efectuar una imagen física del medio.
    - Hoy en día el volumen de los discos es muy amplio por lo que el proceso puede resultar costoso en cuanto a tiempo y a recursos. Se pueden realizar tres tipos de volcados (por hardware o software):
        - Clonado de disco a archivo de imagen forense (copia exacta bit a bit).
        - Clonado de disco a disco (copia exacta bit a bit).
        - Copia forense de ciertas carpetas o archivos (corresponde a la copia a nivel del sistema de archivos y en general corresponde a la copia de evidencia lógica resultante del análisis del punto anterior).
    - En el caso de equipos apagados lo ideal es previamente extraer físicamente los medios de almacenamiento y luego realizar la adquisición.
    - En los casos que no pueden extraerse los dispositivos de almacenamiento involucrados (como puede ser el caso de determinadas notebooks) se debe evaluar conectar el dispositivo de almacenamiento destino al equipo a peritar, o incluso ejecutar un clonado a través de la red según los escenarios presentados.
    - Previo al clonado, bloquear el medio de almacenamiento (por hardware o software), garantizando no modificar los datos contenidos en el mismo tanto en la adquisición como en el montado del mismo.

- Detectar y acceder a zonas protegidas configuradas en el medio de almacenamiento.
- Identificar los datos identificatorios de número, marca, modelo, número de serie y capacidad de almacenamiento.

8. Otras adquisiciones
   - Adquirir un volcado del contenido del tráfico de la red (captura y filtrado) mediante la técnica de "sniffing" (técnica utilizada para capturar todo el tráfico generado en una red local), generalmente en el lugar del hecho, como medida de investigación, con autorización judicial y con frecuencia en diferentes momentos del tiempo.
   - Adquirir tarjetas inteligentes (por ejemplo, SIM, tarjetas de crédito, pasaportes inteligentes, etc.), los cuales requieren el conocimiento específico de formatos, normas o protocolos, lo cual requiere además de hardware específico.
9. Validación y resguardo
   - Validar la integridad de la imagen forense obtenida, aplicando algoritmos de hash MD5, SHA-256, SHA-512 (con el uso del hash MD5 pueden surgir colisiones, por lo que es recomendable evitarlo de ser posible).
     - Obtener hashes asociados a los archivos (códigos alfanuméricos que representan unívocamente al archivo de la imagen forense).
     - Generar hash en original y copia. En el caso de adquisiciones de memoria que pudieron involucrar modificaciones controladas, generar múltiples hashes por regiones.
     - Comparar hashes de original y copia.
   - Detallar tamaño y nombre del archivo de la imagen resultante o de los archivos adquiridos y el valor del hash obtenido sobre los mismos, a fin de dejar constancia por escrito de estos datos del resultado obtenido en el formulario de cadena de custodia y el acta pericial (como también en el acta de allanamiento según el caso).
10. Acta pericial
    - Detallar en el acta pericial todas las acciones realizadas.
    - Indicar el nombre de todas los archivos obtenidos, indicando tipo de archivo, equipo o dispositivo asociado, tamaño, fecha y valores de hash.

- Completar los datos identificatorios de número, marca, modelo, número de serie y capacidad de almacenamiento de cada equipo y dispositivo.

11. Formulario de cadena de custodia
    - Asociada a la Actividad Transversal “Cadena de Custodia”.
    - Debe constar en el formulario de cadena de custodia la información de cada una de las operaciones realizadas y la información de los equipos y dispositivos involucrados. Como también la información de las copias o imágenes forenses obtenidas con detalle similar a la que se indica en el acta pericial.
    - Esta actividad debe realizarse desde el inicio de la fase.
12. Transporte con requisitos de protección adicionales
    - Aplicar técnicas de almacenamiento seguro mediante cifrado (por hardware o software) previo al transporte.
    - En el caso de evidencia digital que contenga datos personales, sensibles o bajo protección intelectual, es indispensable que a las imágenes forenses asociadas se les aplique mecanismos de cifrado del medio de almacenamiento para asegurar la confidencialidad de los datos, de manera de garantizar no vulnerar la ley y los derechos fundamentales de los individuos involucrados.

Detalle de Actividades Específicas en casos de Base de Datos Relacionales

Según los escenarios, considerar servidores de base de datos como también servidores donde se migren o repliquen las base de datos (sean ambientes de producción, contingencia, preproducción, prueba, etc.). En caso de que existan auditorías de datos configuradas a través de AUDB, incluir siempre a las base de datos de configuración, metadatos y resultados de AUDB para el posterior análisis e interpretación de los datos de auditoría.

5.1. Adquisición de datos volátiles o en vivo en Base de Datos Relacionales
    - Aplicar herramientas para la adquisición de datos volátiles relacionados a las base de datos, como ser datos volátiles del caché (datos, diccionarios de datos, sentencias de SQL recientemente ejecutadas, datos del log de transacciones en memoria), páginas de los índices, compilación de

sentencias de SQL, estado del servidor, procesos en memoria (a nivel de servidor, base de datos o usuarios), sesiones de base de datos, etc.

- Aplicar herramientas para la recolección de imágenes forenses en vivo de servidores o medios de almacenamiento en los casos que sea necesario y factible por volumen y naturaleza de los datos (ejemplo, si se necesita la historia clínica de un paciente, no es necesario llevarse la base de datos con todas las historias clínicas).
- En el caso de adquisición o análisis de datos personales (además de gestionar previa autorización judicial en casos judicializados y actuar acorde a la legislación), se deben considerar mecanismos de cifrado o de protección adicionales en los archivos resultantes.
- En el caso de aplicación de AUDB, incluir en la adquisición las configuraciones y resultados de auditorías de AUDB.

6.1. Adquisición y análisis de datos específicos (volátiles y persistentes) en vivo en Base de Datos Relacionales

- Aplicar herramientas para adquirir datos persistentes en vivo como ser: archivos de datos, archivos de control, archivos de log, archivos de configuración, archivos de alertas, archivos de trazas, archivos temporales, información del registro en el sistema operativo relacionado con base de datos, archivos preexistentes de consultas o de resultados sobre los datos investigados, capturas de pantalla de resultados, configuraciones de base de datos, configuraciones de seguridad a nivel de servidor y base de datos, archivos de auditoría y de logs, etc. De cada uno de estos archivos considerar tanto los activos u online, como los archivados o resguardados.
- Emplear estrategias para la recolección de estructuras y datos que no alteren su integridad y características.
- Exportar la base de datos o parte de la misma aplicando procesos de exportación o generando scripts de exportación de estructuras de datos y de scripts de inserción de contenidos.
- En el caso de recolectar tablas específicas, evaluar si se debe recolectar la tabla completa o alcanza con copiar determinados campos según el alcance del caso.

- En el caso de aplicación de AUDB, incluir en la adquisición y análisis las configuraciones y resultados de auditorías de AUDB, como también el servidor y base de datos de almacenamiento de los mismos.
- Realizar análisis en vivo, por ejemplo, obtener resultados ejecutando scripts de SQL o exportando datos con alguna herramienta o comandos, como también buscar información específica sobre los elementos no volátiles indicados en el punto 5.1 de esta fase.

7.1. Adquisición de datos de medios de almacenamiento persistentes en BDR

- Aplicar procedimientos para la adquisición tradicional sobre equipos apagados o medios de almacenamiento extraídos o extraíbles y efectuar una imagen física del medio relacionados con los servidores de base de datos, servidores donde se migren o repliquen base de datos, medios de almacenamientos de resguardos (backups).
- En el caso de recolectar backups, adquirirlos desde backups disponibles o hacer un nuevo backup en línea.
- En el caso de aplicación de AUDB considerar los servidores de datos o base de datos donde se almacenen las configuraciones y resultados de AUDB.

4.3.8. Fase de Preparación y Procesamiento

Descripción General

Esta fase involucra las actividades técnicas de preparación del ambiente de trabajo del informático forense para las futuras tareas de extracción y análisis. Se llevan a cabo tareas de procesamiento inicial con la finalidad de normalizar los datos y reducir la cantidad de archivos duplicados o irrelevantes. Además, se plantea una planificación y diseño de estrategia preliminar de extracción y análisis.

Objetivo

Preparar el ambiente de trabajo del informático forense junto con la restauración de imágenes forenses y el procesamiento inicial de datos para realizar las futuras tareas de extracción y análisis de información.

Aplica a

- Realizarse en un laboratorio forense

Roles Actuantes

- Especialista en Evidencia Digital (EED).
- Para casos de base de datos Especialista Forense en Base de Datos (EFBD) y Especialista Auditor Forense en Base de Datos (EAFBD).

Consideraciones

Esta fase es fundamental para la correcta realización de las tareas análisis. Involucra las tareas de validación de las imágenes forenses y la virtualización de las mismas para las futuras tareas de extracción y análisis de información.

Es esencial identificar las tecnologías de la información en el objeto de análisis y preparar e instalar el conjunto de técnicas y herramientas necesarias para efectuar la extracción y el análisis según los puntos periciales o requerimientos del servicio forense solicitados.

Las tareas de procesamiento permiten reducir volumen de información a analizar y convertir la información, si es necesario, a formas más confortables para su posterior extracción y análisis.

Nunca se debe trabajar con datos originales y se debe respetar cada una de las leyes vigentes en la jurisdicción donde se lleva a cabo la investigación.

Se plantea de forma preliminar la planificación y diseño de estrategia de extracción. La misma se establece como guia inicial de trabajo de la próxima fase, en base a la preparación técnica obtenida y los puntos de pericias o requerimientos del servicio forense.

Principales actividades

Fase de Preparación y Procesamiento			
Actividades Generales (ForenseUDE)		**Actividades Específicas (ForenseDB)**	
1	Acondicionar lugar de almacenamiento	1.1	Ídem (aplicable a BDR)
2	Ensamblado y descompresión de imágenes forenses	2.1	Ídem (aplicable a BDR)
3	Validar la integridad de las imágenes forenses y archivos	3.1	Ídem (aplicable a BDR)
4	Identificación de tecnologías de información en los objetos de evidencia digital	4.1	Identificación de tecnologías de información en los objetos de evidencia digital en BDR
5	Preparación de extracción	5.1	Preparación de extracción en BDR
6	Preparación del ambiente	6.1	Preparación del ambiente en BDR
7	Procesamiento	7.1	Procesamiento en BDR
8	Planificación y Diseño de estrategia de Extracción y Análisis	7.1	Ídem (aplicable a BDR)

Tabla 5: Fase de Preparación y Procesamiento

Detalle de Actividades Generales

1. Acondicionar lugar de almacenamiento
   - Cuando se reciben los elementos a analizar, antes de dicha tarea puede pasar un período de tiempo, en el cual se requiere almacenar temporalmente los mismos.
   - Reunir en el lugar de almacenamiento de los elementos las condiciones mínimas de seguridad, no sólo de acceso físico a las evidencias, sino ambientales. No se podrán almacenar dispositivos electrónicos en lugares húmedos o con temperaturas extremas o con exceso de polvo o suciedad.
2. Ensamblado y descompresión de imágenes forenses
   - Preparar y asegurar el espacio de almacenamiento en disco necesario y el entorno de trabajo para descomprimir, recomponer y validar las imágenes

forenses (tantos de medios de almacenamiento, como de datos volátiles, etc.).

- Disponer (idealmente) de tres copias adicionales de las copias o imágenes forenses. Una de las copias es con la finalidad de preservar una copia intacta para presentar en el juicio (o para entregar en el juzgado). Las otras dos copias adicionales, son para analizar y de respaldo en el laboratorio respectivamente.
- Ensamblar y descomprimir las imágenes forenses.

3. Validar la integridad de las imágenes forenses y archivos
   - Validar el valor de hash de las copias de las imágenes forenses contra las de la evidencia original (por ejemplo, de los discos originales), para chequear que la evidencia recibida sea válida y no haya sido alterada de alguna manera o haya sufrido errores en la copia.
   - Validar valores de hash de archivos.
4. Preparación de extracción
   - Conocer el sistema operativo y la arquitectura asociada a las imágenes forenses. Mapear cada imagen a un dispositivo del sistema operativo.
   - Crear máquinas virtuales para emular los dispositivos a cómo se encontraban al momento antes de su adquisición.
   - Configurar máquinas virtuales. Las mismas deben poseer una conexión de red controlada y aislada del resto de la red del laboratorio forense, no deben tener conexión a Internet ni con las demás computadoras del laboratorio para evitar infectar a la red, si por ejemplo estuviera infectada con un "malware".
   - Virtualizar imágenes forenses adquiridas. Es importante realizar la virtualización en base a copias de la imagen forense y no con la imagen forense original, debido a que la máquina virtual escribe datos de acceso y demás datos en dicha imagen forense, por lo tanto, es modificada.
5. Identificación de tecnologías de información en los objetos de evidencia digital
   - Identificar la sistemas operativos, cantidad de discos, cantidad de particiones, tipos de sistemas de archivos, volúmenes RAID, etc.
   - Identificar medios de cifrado presentes y aplicar mecanismos para poder acceder al mismo si no se dispone de la clave para descifrar los datos.

- Identificar máquinas virtuales y el estado de las mismas.
- Identificar programas instalados.
- Documentar, por cada imagen forense, datos generales de la configuración que puedan ser de interés para las tareas de extracción o análisis.

6. Preparación del ambiente
   - Esta actividad está fuertemente relacionada con los puntos periciales o requerimientos del servicio forense.
   - Seleccionar y preparar el conjunto de técnicas y herramientas a utilizar en la fase de extracción y análisis.
   - Preparar los medios de almacenamiento que contengan el sistema operativo y las herramientas a utilizar para la extracción e instalar los programas necesarios.
   - Preparar los medios de almacenamiento que almacenarán toda la evidencia digital resultante (o procesada) que se obtenga en la fase de análisis y extracción.
7. Procesamiento
   - Esta actividad está fuertemente relacionada con los puntos periciales o requerimientos del servicio forense y aplica especialmente en casos que involucre un gran volumen de información.
   - Reducir volumen de información a analizar: eliminar información duplicada o irrelevante.
   - Normalizar formatos de la información proveniente de distintas fuentes.
   - Organizar la información a analizar en subconjuntos lógicos.
   - Clasificar los hallazgos identificados en función de los requerimientos planteados.
8. Planificación y Diseño de estrategia de Extracción y Análisis
   - Planificar el orden de las tareas de extracción y análisis.
   - Diseñar un plan estratégico de ejecución de las mismas, de manera de clarificar y asociar cada una de las herramientas o ambientes de trabajo preparados e instalados con los trabajos de extracción y análisis a realizar.

Detalle de Actividades Específicas en casos de Base de Datos Relacionales

Según los escenarios, considerar servidores de base de datos como también servidores donde se migren o repliquen las base de datos (sean ambientes de producción, contingencia, preproducción, prueba, etc.). En caso de que existan auditorías de datos configuradas a través de AUDB, incluir siempre a las base de datos de configuración, metadatos y resultados de AUDB para el posterior análisis e interpretación de los datos de auditoría.

4.1. Identificación de tecnologías de información en los objetos de evidencia digital

- Identificar la tecnología de base de datos involucradas (Oracle, MS SQL Server, etc.), las versiones y arquitectura de despliegue.
- Identificar si se tratan de imágenes forenses de servidores, de medios de almacenamientos, archivos de backups, exportación de base de datos, scripts de SQL de estructuras o de datos, archivos de datos, archivos de logs, trace, etc. Identificar formato de los mismos, sea formato propietario del SGBD o exportación a otro formato.
- Identificar si se trata de resultados obtenidos por consultas del investigador, hallados en computadoras, resultantes de auditorías, resultantes de la implementación de AUDB, etc.

5.1. Preparación de extracción en BDR

- Recrear un entorno inicial de la base de datos a analizar según se adquirido o recolectado la información:
    - Restaurar esquemas, usuarios, vistas, tablas, índices, procedimientos almacenados, etc. e importar los datos del ambientes de ejecución de la base de datos, junto con sus variables.
    - Restaurar backups.
    - Importar los archivos de base de datos (datos y estructuras, logs) o ejecutar los scripts de estructuras de datos y datos en sí.

6.1. Preparación del ambiente en BDR

- Preparar en el entorno de trabajo el conjunto de técnicas y herramientas necesarias para efectuar la extracción y el análisis en BDR.

- Preparar los medios de almacenamiento que contengan el sistema operativo y las herramientas a utilizar para la extracción e instalar los programas necesarios.
- Preparar las herramientas de consulta y análisis específicas de base de datos.
- Preparar las herramientas de consulta y análisis de AUDB.

7.1. Procesamiento en BDR

- Analizar los datos de las base de datos identificando las tablas y campos relevantes, de manera de descartar del análisis los datos irrelevantes.
- Analizar y procesar los resultados de las bases de datos en relación con las tablas y campos relevantes.
- Analizar las tablas duplicadas, tablas similares en parte, campos duplicados o relacionados entre tablas, datos calculados o deducidos a partir de otros, datos similares (pero con diferencias en sus tipos de datos o tamaño), etc.
- Analizar y procesar los archivos de resultados de consultas y de auditorías en relación con las tablas y campos relevantes.
- Analizar y procesar los resultados de AUDB en relación con las tablas y campos relevantes.

4.3.9. Fase de Extracción y Análisis

Descripción General

Extracción de la información de las imágenes forenses. Selección de la potencial evidencia digital. Análisis en relación con el caso y a los puntos periciales o requerimientos del servicio forense.

Objetivo

Extraer y analizar la información relevante en relación con los puntos de pericias o requerimientos del servicio forense.

Aplica a

- Realizarse en un laboratorio forense luego de haber preparado el ambiente de trabajo.

Roles Actuantes

- Especialista en Evidencia Digital (EED)
- Para casos de base de datos Especialista Forense en Base de Datos (EFBD) y Especialista Auditor Forense en Base de Datos (EAFBD).

Consideraciones

Se distingue la extracción del análisis, ya que son dos labores independientes aunque están íntimamente ligadas entre sí. Por un lado, está el proceso de extraer datos de las posibles fuentes de evidencia digital y, por otro lado, el análisis particular de acuerdo al caso que debe realizarse sobre los datos extraídos.

La extracción suele ser automatizada e integrada por actividades técnicas, mientras que el análisis implica un proceso de interpretación de los datos extraídos en el contexto de los puntos periciales y el interés de los investigadores.

Es indispensable las habilidades del forense para la asociación de los datos obtenidos que le permitan brindar una respuesta integral y objetiva de los puntos a peritar o analizar.

Los resultados que se obtengan de todo el proceso deben ser verificables y reproducibles.

Es importante mantener un esquema de comunicación y colaboración entre las partes involucradas en la investigación del hecho como para lograr mejores resultados.

La fase de análisis es crucial para tratar de determinar por ejemplo según los casos, qué o quién causó el incidente, cómo lo hizo, que afectaciones causó, cuándo, etc. Tiene que concluir con el máximo de información relevante para proceder luego a elaborar los informes finales.

Principales Actividades

Fase de Extracción y Análisis			
Actividades Generales (ForenseUDE)		**Actividades Específicas (ForenseDB)**	
1	Extracción	1.1	Extracción en BDR
2	Adquisiciones en ambientes virtualizados	2.1	Adquisiciones de BDR en ambientes virtualizados
3	Análisis de contenidos	3.1	Análisis de contenidos en BDR
4	Análisis de relaciones	4.1	Análisis de relaciones en BDR

Tabla 6: Fase de Extracción y Análisis

Detalle de Actividades Generales

1. Extracción
   - Extraer los datos en base a diferentes plataformas, incluyendo la rápida identificación de archivos o registros potencialmente relevantes o sensibles para el caso y aplicando filtros sobre los mismos en base a diferentes criterios (como ser palabras clave, rango de fechas, etc.).
   - Extraer datos a nivel de aplicación, a fin de lograr extraer información específica de aplicaciones.
     - Búsqueda y extracción de:
       - Archivos y aplicaciones recientes o frecuentes, archivos comprimidos, archivos de imágenes, archivos temporales, papelera de reciclaje, de ofimática, etc.
       - Navegadores e historiales de navegación web.
       - Redes sociales, mensajería instantánea, correo electrónico, aplicaciones de transferencia de archivos, juegos y otras aplicaciones particulares.
       - Almacenamiento en la nube.
       - Archivos o sectores de la imagen que contengan cierta cadena de caracteres.
       - Máquinas virtuales.

        - Entre otras.
    - Análisis de archivos de aplicaciones: de configuración, de datos y bases de datos, ejecutables y otros archivos relacionados.
    - Análisis de la aplicación en entorno controlado (emulador). De ser necesario y posible, desensamblar la aplicación aplicando ingeniería inversa.
    - Otros análisis dependiendo de la naturaleza del caso y escenario planteado.
- Extraer datos a nivel de plataforma, lo que incluye los sistemas operativos, sistemas de archivos y su configuración.
    - Analizar aplicaciones más utilizadas.
    - Recuperación y extracción de archivos eliminados.
    - Extracción de tipo de información a analizar por tipo de archivo.
    - Extracción de metadatos de archivos.
    - Detección y extracción de archivos protegidos con contraseña o cifrados. Aplicar técnicas de ataque por fuerza bruta u otras técnicas si no se dispone de las claves de protección o descifrado. Ejemplo: buscar las claves en la imagen de la memoria.
    - Búsqueda de información de configuración.
    - Búsqueda de información de procesos en memoria.
    - Búsqueda de servicios del sistema y el estado y configuración de los mismos.
    - Otras búsquedas dependiendo de la naturaleza del caso y escenario planteado.
- Extraer datos a bajo nivel (bloques/bytes), a través de tareas de recuperación de información lógica al nivel de bloque de datos puro.
    - Búsqueda y extracción de información a nivel de disco, en el área de paginado, en espacio no asignado (“file carving”), en particiones no formateadas.
    - Otras búsquedas dependiendo de la naturaleza del caso y escenario planteado.
- En cada escenario de extracción se requiere un conocimiento y experiencia determinada para el éxito de la extracción.

- Clasificar los hallazgos identificados en función de los requerimientos planteados.
- En general, utilizar nuevas tecnologías para agilizar las extracciones:
    - Búsqueda basada en conceptos.
    - Reconocimiento de patrones lingüísticos.
    - Búsqueda basada en entrenamiento de documentos relevantes e irrelevantes.
    - Utilización de expresiones regulares.
    - Correcta definición de palabras claves.
    - Firmas de archivo (encabezados de los archivos) para identificar los reales tipos de archivos, los cuales fueron renombrados en extensión con la finalidad de ocultarlos.

2. Adquisiciones en ambientes virtualizados
    - Efectuar tareas de adquisición, por ejemplo, de datos volátiles o de paquetes de red o medios de almacenamientos, dentro del espacio de trabajo de las máquinas virtuales adquiridas (es decir máquinas virtuales contenidas en las imágenes forenses).
    - Ejecutar las tareas de extracción mencionadas en el punto anterior dentro del espacio de trabajo de las máquinas virtuales adquiridas.
3. Análisis de contenidos
    - Analizar el contenido de la información propiamente dicha que se almacenan en los datos extraídos en las tareas anteriores.
        - Analizar artefactos forenses según el caso: historial de internet, usuarios, servicios de mensajería instalados, u otras herramientas.
        - Analizar a partir de palabras claves definidas.
        - Evaluar el contenido y contexto del mismo, incluyendo patrones clave, tópicos, personas y temas de discusión, entre otros.
        - Buscar información ofuscada u oculta en el contenido (por ejemplo, aplicación de técnicas de esteganografía que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia).

- Obtener una adecuada comprensión del contenido de la información recolectada, a través de la organización de los mismos en subconjuntos lógicos de una manera eficiente.
- Obtener elementos suficientes para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada.
- Establecer la línea de tiempo a analizar para poder conocer que se hizo en un determinado dispositivo en un período de tiempo e, incluso correlacionar hallazgos u eventos importantes determinados (reconstrucción de hechos sucedidos).
- En los casos que corresponda y exista evidencia, determinar qué procedimiento se llevó a cabo por parte del atacante e identificar el autor o autores de los hechos.

4. Análisis de relaciones
   - Analizar las relaciones entre los distintos elementos extraídos, el contenido recuperado y los elementos previos aportados, con el fin de encontrar su peso, relevancia y significancia en el caso.
   - Vincular la evidencia obtenida con otras investigaciones.

Detalle de Actividades Específicas en casos de Base de Datos Relacionales

1.1. Extracción en BDR

- Extraer datos y estructuras a nivel de base de datos y su motor:
  - Tablas:
    - Campos.
    - Claves primarias y forañas.
    - Índices.
    - Reglas y restricciones.
    - Relaciones entre las tablas.
    - Propietario.
  - Procedimientos SQL.
  - Triggers.
  - Vistas.
  - Usuarios, roles, privilegios y perfiles.
  - Configuraciones del servidor en relación a las base de datos.

- Configuración de la base de datos en general. Configuración de almacenamiento. Configuración de límites de recursos.
- Configuración de seguridad a nivel de base de datos y en el motor de base de datos.
- Backups. Replicaciones de base de datos.
- Registros de acciones en la base de datos: registros de logs de transacciones, ejecución de triggers, intentos de accesos, y accesos a la tabla maestra del log de transacciones, etc.
- Registros de autenticación y autorización.
- Auditorías en general.
- Procesos en memoria a nivel de usuario, base de datos o servidor.
- Caché en memoria (sentencias SQL recientemente ejecutadas, diccionarios de datos, búfer de datos, datos de sesiones, etc.).
- Procesos agendados.
- Archivos de datos, archivos de control, archivos de log, archivos de configuración, archivos de alertas, archivos de trazas, archivos temporales. De cada uno de estos archivos considerar tanto los activos u online, como los archivados o resguardados.
- Cifrado de datos.
- Transacciones no confirmadas.
- Propietarios, fecha de creación, fecha de modificación, etc. de cada uno de los objetos o artefactos mencionados (de los que se pueda o corresponda obtener dicha información).
- Implementación de AUDB:
    - Tipos de Auditorías: a nivel de operaciones, de contenidos y de estructuras de datos, en base a información de contexto de las operaciones, intentos fallidos o a nivel de configuración de seguridad.
    - Configuración de filtros de auditoría. Configuración de filtros de almacenamientos. Resguardo seguro de datos auditados (cifrado o enmascaramiento de datos). Configuración de protección de visualización de datos auditados.

- Configuración de reglas de validación y autoprotección de datos en tiempo real.
- Configuración de ejecución de auditorías de AUDB. Estados de ejecución de auditorías.
- Información auditada resultante de AUDB.

  - Entre otros, dependiendo de cada tipo de SGBD.

2.1. Adquisiciones de BDR en ambientes virtualizados

  - Aplicar proceso de análisis forense de base de datos contenidas dentro de máquinas virtuales.

3.1. Análisis de contenidos en BDR

- Analizar el contenido de la información en los datos extraídos:
  - Analizar información extraída a partir de palabras claves, nombres de objetos, nombres de usuarios, rango de fechas y horarios, etc.
  - Analizar comandos SQL exitosos y fallidas, comandos SQL sobre tablas sensibles, comandos SQL masivos, etc.
  - Revisar los planes de ejecución de sentencias SQL y sus variables.
  - Analizar según lo que esté disponible en los logs de transacciones y otros.
  - Analizar información de configuración y auditada por AUDB.
  - Evaluar el contenido y contexto del mismo, incluyendo patrones clave, tópicos, personas y temas de discusión, entre otros.
  - Buscar información ofuscada u oculta en el contenido de las base de datos (por ejemplo, imágenes embebidas en campos).
- Evidenciar y analizar eventos anormales:
  - Ocurrencia de una brecha de seguridad.
  - Ejecución de comandos de manipulación de datos (DML) o de definición de datos (DDL).
  - Transacciones sospechosas, incompletas o pendientes.
  - Eliminación o manipulación de datos o estructuras de datos indebidas o dudosas.
  - Recuperación o manipulación de estructuras o datos no autorizadas.

4.1. Análisis de relaciones en BDR

- Analizar las relaciones entre los distintos elementos de base de datos extraídos, el contenido recuperado y los elementos previos aportados, con el fin de encontrar su peso, relevancia y significancia en el caso.
- Vincular la evidencia obtenida con entre auditorías similares en el tiempo, por contenido o por usuarios.

4.3.10. Fase de Producción y Presentación

Descripción General

Fase destinada a producir de manera eficiente y en un formato útil los resultados de la investigación, cumpliendo en tiempo y forma con los plazos comprometidos. A partir de los resultados, esta fase también incluye actividades destinadas a presentar los resultados obtenidos. Comprende la preparación de la presentación del caso en un juicio o a los solicitantes.

Objetivo

Producir el dictamen y los resultados finales en tiempo y forma según los plazos comprometidos. Preparar las presentaciones que sean solicitadas, tanto a particulares como para presentar en el juicio.

Aplica a

- Realizarse en un laboratorio forense.

Roles Actuantes

- Director de Informática Forense (DIF) y Especialista en Evidencia Digital (EED)
- Para casos de base de datos Especialista Forense en Base de Datos (EFBD) y Especialista Auditor Forense en Base de Datos (EAFBD).

Consideraciones

Esta fase incluye principlamente el armado de un informe pericial claro, preciso y concreto incluyendo la documentación de todas las actividades y tareas

realizadas, como también las presentaciones ante una eventual exposición en un juicio o para quienes hayan solicitado el servicio forense.

Los informes sirven para documentar los antecedentos del caso, todo el trabajo realizado, el método seguido y las conclusiones. Como también en casos de servicios forenses privados analizar el impacto al que se ha derivado por el incidente.

Principales Actividades

Fase de Producción y Presentación			
Actividades Generales (ForenseUDE)		**Actividades Específicas (ForenseDB)**	
1	Armado y presentación de dictamen final y anexos necesarios	1.1	Armado y presentación de dictamen final y anexos necesarios en BDR
2	Armado y presentación de informes técnicos y anexos necesarios	2.1	Armado y presentación de informes técnicos y anexos necesarios en BDR
3	Exposición del caso en juicio o a los solicitantes.	3.1	Ídem (aplicable a BDR)

Tabla 7: Fase de Producción y Presentación

Detalle de Actividades Generales

1. Armado y presentación de dictamen final y anexos necesarios
   - Armar dictamen final: Documentar todas las actividades y tareas realizadas en un informe pericial claro, preciso, concreto y redactado en un lenguaje apropiado, es decir, técnico-científico comprensible para una autoridad judicial, incluyendo las conclusiones de la pericia.
   - Basar el armado de informes y anexos en modelos de trabajo.
   - Contemplar los plazos comprometidos.
   - Aclarar todos los conceptos técnicos de las actividades desarrolladas en cada fase, ya que serán leídos por personas que no tienen conocimientos técnicos.
   - Responder a los puntos solicitados con un nivel de detalle de operaciones tal que permita reproducir y replicar el proceso de análisis llevado a cabo por el cual se arriba a esa conclusión.

- Incluir la siguiente información de referencia:
    - Breve introducción del caso, partes intervinientes, número de causa y detalle del delito.
    - Explicar los conceptos técnicos de las actividades desarrolladas.
    - Detallar las fuentes de información con las que se contaron para la realización de la pericia informática.
    - Documentar y justificar por cada punto pericial cual fue la evidencia digital obtenida.
    - Detallar todos los pasos realizados, procesos y herramientas utilizadas para tratar y obtener la evidencia digital.
    - Presentación del resultado de la fase de análisis.
    - Si la evidencia digital es muy extensa se deben preparar anexos al informe con toda la evidencia digital referenciándolos en el informe principal. Los anexos se deben adjuntar en algún soporte detallando el valor de hash de los mismos en el informe pericial.
    - Conclusiones sobre la investigación.
- Preparar presentación del dictamen final y anexos necesarios para ser entregados como resultado del trabajo.

2. <u>Armado y presentación informes técnicos y anexos necesarios</u>
    - Armado de informes técnicos incluyendo todos los procesos, los programas utilizados, las técnicas, etc.
    - Preparar un resumen completo y comprensible de la totalidad de la investigación.
    - Los informes técnicos están orientados a público final técnico y con conocimientos en la materia, y en general se solicitan en servicios forenses a particulares.
3. <u>Exposición del caso en juicio o a los solicitantes</u>
    - Preparar la información y la evidencia digital hallada en el caso para una eventual presentación en juicio o a los solicitantes del servicio forense.
    - Armar, adicionalmente, presentaciones con muestras relevantes y contundentes extraídas de la información recolectada en las primeras etapas, con el fin de visualizar más detalles y/o validar los hechos.

- Adaptar el contenido de las presentaciones al nivel o habilidades del público que las está recibiendo. Aplicar lenguaje coloquial o básico a usuario con pocos conocimientos técnicos, para que no se mal entienda el mensaje o realizar informes técnicos si el público final es técnico.

Detalle de Actividades Específicas en casos de Base de Datos Relacionales

1.1. Armado y presentación de dictamen final y anexos necesarios en BDR

- Adicionalmente a lo detallado en el punto general, incluir los conceptos técnicos de base de datos.
- Es muy importante identificar los datos del servidor donde se hospeda la base de datos, la base de datos, tablas, campos sobre las que se recolecta información, incluso detallar la arquitectura general donde estaba inserta la base de datos, como parte de la descripción del contexto.
- Detallar los datos del motor de base de datos de acuerdo con las especificaciones de su instalación, licencias y nivel de parches.
- Detallar la información volátil adquirida.
- Listado detallado de los objetos y estructuras de datos debidamente documentadas.
- Listado de los archivos de scripts de SQL ejecutados y los archivos de los resultados alcanzados en las diferentes fases, de forma detallada y fundamentada, indicando nombre de archivo, extensión, fecha, hora y valor de hash. En general, dada la extensión de los mismos, es aconsejable incluir el contenido de los mismos en Anexos.
- En el caso que se ejecuten herramientas específicas detallarlas y fundamentar su aplicación e impacto sobre la evidencia digital.
- Si la evidencia digital se basa en resultados de la aplicación de AUDB, se debe anexar la configuración asociada de AUDB y los resultados de auditorías que se plantean como evidencia digital. En este caso es importante incluir un apartado de la explicación técnica funcional de AUDB para justificar la admisibilidad de la evidencia digital en un proceso judicial.
- Presentación del resultado de la fase de extracción y análisis.
- Conclusiones sobre la investigación.

2.1. Armado y presentación de informes técnicos y anexos necesarios en BDR

- Armar un informe detallado técnico con el detalle de todas las operaciones realizadas y justificadas técnicamente a nivel de base de datos. Incluso si se basan en los resultados de la aplicación de AUDB detallar y justificar la misma.
- Detallar la arquitectura sobre la que se trabajó de forma más detallada que en el dictamen final.
- En los casos que aplique, por ejemplo, en un servicio forense particular, es una buena práctica incluir análisis de impacto y recomendaciones de seguridad y controles para evitar sucesos similares a futuro.

4.3.11. Fase de Evaluación Final

Descripción General

Fase destinada a realizar la evaluación final del trabajo como parte del proceso de calidad y mejora continua de la metodología aplicada.

En esta fase también se plantea la retroalimentación con AUDB, en los casos de base de datos relacionales que hayan aplicado previamente dicha metodología o pretendan aplicarla a futuro.

Objetivo

Evaluar los resultados del trabajo y proponer mejoras o buenas prácticas a las actividades, técnicas y procedimientos. Proponer mejoras, ajustes o nuevas auditorías de datos a partir de los resultados.

Aplica a

- Realizarse en un laboratorio forense.

Roles Actuantes

- Director de Informática Forense (DIF) y Especialista en Evidencia Digital (EED)
- Para casos de base de datos Especialista Forense en Base de Datos (EFBD) y Especialista Auditor Forense en Base de Datos (EAFBD).

Consideraciones

Esta fase evalúa el trabajo realizado, detectando posibilidades de mejoras y valorando la calidad del trabajo final, retroalimentando la metodología forense en general.

Para casos de base de datos relacionales, a partir de las acciones indebidas, maliciosas o dudosas detectadas en las mismas, se retroalimenta, de ser necesario, la estrategia de AUDB proponiendo ajustes y mejoras a las configuraciones de auditorías de datos.

Principales Actividades

Fase de Producción y Evaluación Final			
Actividades Generales (ForenseUDE)		**Actividades Específicas (ForenseDB)**	
1	Evaluación Final	1.1	Ídem (aplicable a BDR)
2	Informe de propuestas de mejoras	2.1	Informe de propuestas de ajustes y mejoras generales y en AUDB

Tabla 8: Fase de Evaluación Final

Detalle de Actividades Generales

1. Evaluación Final
   - Análisis de los resultados obtenidos.
   - Revisión y análisis de los procedimientos, actividades y tareas aplicadas.
   - Revisión y análisis de técnicas y herramientas aplicadas.
   - Revisión y análisis del desarrollo de las actividades y de los imprevistos o dificultades que pudieron surgir.
   - Revisión y análisis de la documentación.
   - Revisión y análisis de esquemas de comunicación entre los roles actuantes y los diferentes actores intervinientes.
2. Informes de propuestas de mejoras
   - Retroalimentar al proceso con informe de propuestas de mejoras de procedimientos, actividades, tareas, técnicas, herramientas, modelos de documentación, etc. a partir del análisis del punto anterior.

Detalle de Actividades Específicas en casos de Base de Datos Relacionales

2.1. Informe de propuestas de ajustes y mejoras generales y en AUDB

- A partir del análisis caso proponer mejoras en la configuración y estrategia de seguridad y auditoría general de las bases de datos.
- A partir de las acciones indebidas, maliciosas o dudosas detectadas y analizadas podrían surgir sugerencias de mejoras o ajustes en las configuraciones de auditorías de datos de AUDB para mejorar la calidad y detalle de las auditorías.
- Del mismo modo, de no existir previamente una metodología AUDB implementada (o cualquier configuración de auditoría de datos), este informe podría sentar las bases para planear una estrategia de auditoría de datos en base a acciones ocurridas o intentos de las mismas.

4.3.12. Actividades Transversales

Actividad Transversal: Cadena de Custodia

La cadena de custodia es un registro cronológico y minucioso de la manipulación controlada de todos los elementos incautados e identificados unívocamente en el lugar del hecho o detectados durante todo el proceso. Debe ser actualizado en todas las actividades y tareas del proceso pericial en las cuales se realicen acciones sobre la evidencia digital, incluso de custodia, desde el momento en que se encuentran en el lugar del hecho hasta en su análisis en el laboratorio.

Se debe iniciar un Formulario de Cadena de Custodia por cada elemento involucrado en el caso, incluso de las imágenes forenses y otros archivos como fotos o videos que se hayan tomado (nombre de archivos, tamaño y valores de hash),etc. También se deben registrar hallazgos como impresiones, anotaciones de valor para el caso.

Cada uno de los Formularios de Cadena de Custodia deben acompañar a la evidencia correspondiente durante todo el ciclo de la pericia.

Es fundamental una adecuada identificación de los elementos, indicar quién los ha manipulado, cómo lo ha realizado, porqué lo ha manipulado, para qué lo ha hecho y cuándo ha tenido lugar dicha manipulación, indicando siempre fecha y hora de las acciones.

En la recolección y adquisición es crítico registrar la fecha y hora de los equipos o dispositivos involucrados, las cuales no tienen por qué coincidir con la real, la cual también se tiene que registrar. Esto posibilita clarificar la investigación posterior y la realización de una línea temporal con todos los sucesos que han ocurrido, considerando el desfase de la fecha y hora del equipo y la fecha y hora real.

También se debe registrar todos los responsables de las acciones como también los custodios definitivos y transitorios de la misma en cada momento y lugar. Los responsables de esta actividad corresponden a los roles actuantes de cada una de las fases.

La cadena de custodia involucra también registrar todos los lugares donde ha pasado la evidencia y quién ha realizado su embalaje, transporte y acceso.

En el formulario de cadena de custodia se deben registrar y detallar también los datos de las actas y documentos anexos que se completen en cada fase.

Es esencial también documentar detalladamente y con fundamentos todos los procedimientos ejecutados, para luego poder reproducirlos con precisión aplicando los métodos usados.

La debida cadena de custodia garantiza la autenticidad, trazabilidad y confiabilidad de la evidencia que se podrá utilizar como prueba dentro del proceso judicial, como también brinda transparencia a todo eventual cambio o alteración del material probatorio de forma controlada.

Aunque existan actas específicas o complementarias en algunas de las fases, como ser el acta de allanamiento, no se debe omitir incluir la información necesaria en el formulario de cadena de custodia, aunque se repita en ambos documentos. El formulario de cadena de custodia acompaña siempre a la evidencia desde el minuto cero de la pericia hasta que se termina y eventualmente se devuelvan los dispositivos o se le dé el destino que

corresponda; en cambio el resto de la documentación cumple otras funciones y pueden ser entregadas a diferentes responsables u áreas.

Actividad Transversal: Preparación de Equipos y Herramientas

Esta actividad establece las tareas y buenas prácticas comunes relacionadas a la preparación de los equipos y herramientas necesarias en las diferentes fases de la metodología. Los responsables de esta actividad corresponden a los roles actuantes de cada una de las fases.

1. Conocimiento y experiencia en los equipos y herramientas a utilizar
   - Conocer el potencial y alcance de cada uno de los equipos y de las herramientas.
   - Investigar módulos, las ventajas y desventajas de cada uno frente a escenarios posibles.
   - Conocer la forma de trabajo, cómo funcionan, cómo utilizarlas/os, cuáles y cuándo.
2. Validación de los equipos y herramientas a utilizar
   - Validar que los equipos y herramientas realizan funcionalmente lo que el fabricante dice que hacen.
   - Probar los equipos y herramientas previamente a utilizarlos en un caso real.
   - Verificar manuales y realizar pruebas de laboratorios (no con evidencia real).
3. Comprobación de la integridad de las herramientas a utilizar
   - Obtener y almacenar el hash de los ejecutables de las herramientas (para cada versión de las mismas) para verificar la integridad (la no adulteración) del archivo ejecutable de instalación o ejecución.
4. Verificación de licencias de los equipos y herramientas
   - Verificar que se posea una licencia válida en caso de que la herramienta no sea de código abierto.
   - Validar que las licencias estén actualizadas.
   - Verificar no solo las licencias de equipos o herramientas forenses, sino también las licencias del sistema operativo, procesadores de texto y de

cualquier software que se utilice en la resolución del caso para cualquiera de las actividades involucradas (excepto las open source). Esta tarea evita estar presentando a la justicia el producto de una investigación en un soporte ilegal, aunque el resto de las herramientas forenses tengan licencia legal.

5. Disponer de variedad de equipos y herramientas
   - Disponer y conocer variedad de equipos y herramientas para enfrentar los diferentes desafíos y escenarios que se pueden presentar (o incluso por si surgieran problemas o imprevistos con algunos de los equipos u herramientas).
   - Disponer de variantes de hardware y de software para la resolución de similares tareas.
   - Disponer de adaptadores para la variedad de tipos de medios de almacenamiento que pudieran tener que ser adquiridos.
6. Preparar estaciones forenses
   - En las estaciones forenses pueden llevarse a cabo tanto tareas de adquisición, como de extracción o análisis.
   - Configurar y/o validar configuraciones de las estaciones de trabajo:
     - Deshabilitar las actualizaciones automáticas (por ejemplo, en Windows podría causar un apagado sin previo aviso o afectar el funcionamiento de las aplicaciones).
     - Ajustar y chequear las configuraciones de energía para evitar que pasen a estado de suspensión en el medio de un procesamiento, bloqueando la ejecución de la aplicación en uso (por ejemplo, en el medio de una adquisición).
     - Configurar y verificar la zona horaria (dado que puede estar configurada en otra región o tiempo de trabajo, restándole o sumándole horas de trabajo a realizar).
     - Chequear la configuración de auto montaje de discos, de manera de evitar el auto montaje al conectar discos con evidencias digitales a la estación forense.
7. En el caso de Base de Datos
   - Disponer de variedad de herramientas para enfrentar los diferentes desafíos y escenarios que se pueden presentar en el lugar para recolectar BDR.

- Preparar un conjunto de herramientas de atención de incidentes en base de datos, tanto para adquisición de datos volátiles como persistentes. Ejemplo: adquirir datos volátiles del caché (Data Caché, Plan Caché, Caché Clock), páginas de los índices, compilación de sentencias de SQL, estado del servidor (procesos activos, conexiones de base de datos, sesiones de base de datos, sentencias SQL ejecutadas recientemente, datos del log de transacciones en memoria), como también datos persistentes de tablas, configuraciones de base de datos, configuraciones de seguridad a nivel de servidor y base de datos, archivos de auditoría y de logs, etc.
- A la fecha sólo se conocen herramientas propias de cada tipo de moto de base de datos, por lo cual es muy importante utilizarlas y conocer cómo funcionan, para brindar nivel de confiabilidad de las herramientas utilizadas.
- Preparar herramientas vinculadas a AUDB, para interpretar configuraciones y resultados de auditorías de AUDB, y conocer cómo funciona para fundamentar su utilización.
- Desarrollar scripts SQL (o de otros lenguajes como Python) generales y específicos al caso que permitan extraer información volátil y persistente requerida.
- Preparación de los elementos necesarios para la recolección y/o traslado de la evidencia digital en Base de Datos Relacionales.
- La evidencia digital en BDR podrá ser recolectada o analizada “in situ” dependiendo del volumen y naturaleza de la organización. En general, no será factible secuestrar, desconectar o apagar servidores de BDR, por lo que habitualmente se necesitan discos de almacenamiento de gran capacidad para resguardar las imágenes forenses adquiridas en vivo, adquisición de datos volátiles o el resultado de análisis en el lugar del hecho, incluso para recolectar imágenes forenses sobre backups.
- Preparar herramientas y equipos para restaurar imágenes forenses, backups o incluso base de datos exportadas a scripts.
- Preparar estación forense para conectividad remota con las máquinas o servidores comprometidos.

Actividad Transversal: Seguimiento y Control

Esta actividad involucra tareas de seguimiento y control sobre todas las fases y actividades de las mismas.

El responsable principal de esta actividad es el Director en Informática General (DIF), quien está a cargo de verificar la ejecución de la planificación y diseño de la estrategia general planteada en las fases iniciales, como también de la gestión de los desvíos sobre la misma.

El DIF puede ajustar la planificación y la estrategia diseñada acorde al avance de la investigación, siempre y cuando respete los plazos de entrega (sean casos judicializados o casos corporativos o particulares). Si el trabajo es excelente pero no se cumple los plazos se puede afectar la investigación.

Es crucial que todo los desvíos y ajustes a la planificación sean debidamente documentados y justificados, no solo como parte de las actividades de seguimiento y control, sino como base de experiencia para futuros casos y de mejora continua.

También debe gestionar y controlar los riesgos y la ejecución de actividades de prevención o mitigación necesarias a lo largo del proceso. El DIF es quien está a cargo de asegurar que se ejecuten los planes de contingencia establecidos cuando sean necesarios.

Si bien el rol del DIF no figura dentro de los roles actuantes de las diferentes fases, excepto en la fase de Preparación Inicial, es quien debe gestionar y controlar el trabajo general de todas las fases, incluso más allá del límite de cada una de las fases individuales.

Es importante mantener un esquema de comunicación y colaboración entre las partes involucradas en la investigación del hecho para lograr mejores resultados.

El DIF cumple el rol de facilitar y promover la comunicación entre los roles actuantes, como también de todos los intervinientes del proceso, sean expertos internos, externos, operadores de la justicia, peritos oficiales, fiscales, jueces, etc.

El DIF debe velar por facilitar la colaboración de los cuerpos de peritos, cuerpos de investigación, el poder judicial para el logro de resultados de calidad en tiempo y forma.

Capítulo 5 – Validación de la Solución

A continuación, se plantea un ataque informático a la base de datos y su análisis forense. En primer lugar, se describe el hecho sucedido y se plantea su investigación planteando dos escenarios posibles. En el primer escenario no se dispone de la aplicación de la metodología **AUDB** previo al hecho. En el segundo escenario existe una estrategia de auditoría de datos implementada a través de AUDB previa al hecho.

En el ejemplo se aplica **ForenseDB**, y se focaliza en el análisis forense sobre la base de datos en sí (y no sobre el servidor o las aplicaciones), en un contexto de aplicación de proceso de prueba pericial anticipada, que surge ante la necesidad de congelar la realidad de la información en un momento dado, considerando la volatilidad y la fragilidad de la evidencia digital, fácilmente destruible o alterable con el fin de asegurar su sobrevida durante el proceso y permitiendo a la empresa continuar luego con su operación normal.

Si bien se menciona en el ejemplo la asistencia de un Especialista en Evidencia Digital, e incluso de una pericia realizada sobre la PC de un empleado, la misma se explica de forma conceptual (no detallada), en base a la aplicación conceptual de **ForenseUDE**, a modo de complemento del análisis integral del caso específico sobre la base de datos.

Se aclara en forma general, que, en ambos escenarios, todas las tareas son filmadas y/o fotografiadas y también registradas debidamente en un Formulario de Cadena de Custodia que se inicia antes de estar en contacto con la evidencia digital y con la presencia como testigos del Administrador de Base de Datos y el Responsable de Seguridad de la empresa. Finalmente, la prueba es certificada por un escribano público.

5.1. Hecho Sucedido

Un empleado descontento que se desempeña como programador de sistemas en una empresa Distribuidora de Fertilizantes y Agroquímicos “DISTFA S.A.”, en enero del 2019 tiene la oportunidad de *vender* la información de los clientes a la competencia de la empresa. Además, como parte de su insatisfacción laboral, decide ejecutar una serie de acciones en pos de perjudicar a la empresa y su relación con los clientes.

El empleado, cuyo nombre es Ulises Prat, trabaja hace 9 años en la empresa, de lunes a viernes de 9 a 18 hs (aunque, por sus tareas específicas, suele trabajar fuera del horario laboral). Ulises Prat participa tanto en proyectos de desarrollo, como en las actividades de implementación de software. Por falta de proyección dentro de la empresa, en diciembre de 2018 decide buscar un nuevo trabajo.

En una de las implementaciones críticas del 22 de noviembre del 2018, realizadas fuera del horario laboral, a las 21:00 hs., surge una contingencia, por lo que el Administrador de Base de Datos, Ariel Gómez, pide colaboración a Ulises Prat. Ante la urgencia de la situación, le brinda un usuario y clave de acceso (usuario: “apower” pw: “NH4NO3_Nitrato”) a la base de datos “COMERCIAL”, la cual incluye datos de los clientes (nacionales e internacionales), ventas, facturación y stock disponible, entre otros.

Siendo enero del 2019, período vacacional para la mayoría de los empleados, Ulises Prat decide obtener la lista completa de clientes nacionales e internacionales, tanto activos como inactivos. El 14 de enero a las 08:00 hs. desde su PC “DESA05” conectado con su usuario de red “uprat”, se conecta a través de una aplicación cliente SQL a la Base de Datos “COMERCIAL” con el usuario de SQL “apower” y realiza una consulta SQL sobre la tabla de clientes completa “CLIENTES”, tanto activos como inactivos, obteniendo todos sus campos de contacto, información general y datos personales, como también la lista completa de precios por producto “PRODUCTOS_PRECIOS”. Además, a las 08:20 hs. de ese mismo día y conectado de la misma forma, ejecuta una vista de SQL “ESTRATEGIA_COMERCIAL” almacenada en la base de datos, la cual

devuelve la información estratégica asociada a los clientes, la cual es utilizada para la estrategia comercial de la propia empresa DISTFA S.A. Esta información se encuentra almacenada de forma cifrada en la tabla “PERFIL_CLIENTES” y sólo quienes tienen permisos de ejecución de la vista, logran acceder a la información resultante descifrada. Incluso, ese mismo día a las 08:20 hs. logra modificar a estado inactivo a algunos de los clientes activos de la tabla “CLIENTES” (algunos no los pudo modificar a inactivo por errores de restricción de base de datos). Todas las acciones mencionadas las ejecuta desde un script que prepara y almacena en una carpeta de su PC laboral en el directorio “C:\PERSONALES”, con el nombre “info_clientes.sql” y los resultados en un archivos “info_clientes.xls”.

Previamente, había investigado cuales eran los fertilizantes con mayor venta en enero y programó un script de SQL que aumentaba el stock disponible registrado en la base de datos de dichos fertilizantes en la tabla “STOCK”, difiriendo de la realidad; logrando que desde el área comercial se sobrevenda el producto sobre los stocks de “sulfato amónico” y “nitrato de calcio”. El script SQL lo almacenó en una carpeta de su PC laboral en el directorio “C:\PERSONALES”, con el nombre “ajuste_de_stock.sql”. Planificó el script para que se ejecute automáticamente el lunes 14 de enero a las 8:30 hs. y luego, el lunes 21 de enero a las 8:30 hs. (ambas ejecuciones en días y horarios previos al inicio de la actividad comercial), desde su PC “DESA05”, conectado con su usuario de red “uprat” y con el usuario de SQL “apower” a través de la aplicación cliente SQL.

El martes 22 de enero el empleado tiene planeado presentar su renuncia y a partir del 1 de febrero ya no asistiría a la empresa.

5.2. Escenario 1

Detección de la situación

La empresa DISTFA S.A. a fines de enero comienza a recibir reclamos de clientes por el retraso en las entregas de los productos DISTFA S.A. a causa de problemas con el stock disponible. El martes 5 de febrero de 2019, luego de un

análisis del área comercial y responsables del stock, detectan la diferencia del stock registrado en la base de datos, con respecto al real. No se pudo validar los movimientos de stock en relación con el stock disponible, observando una variación de stock anómala. Además, en el mismo período de tiempo, de forma aleatoria, se detectaron algunos clientes activos que pasaron erróneamente a estar inactivos, los cuales fueron reclamados por el área comercial.

En ese momento, deciden contratar un servicio informático forense de urgencia para poder investigar y analizar lo sucedido. Deciden paralizar las ventas de manera de seguir evitando vender sin conocer el detalle de lo que está sucediendo o sobre un valor de stock erróneo.

Fase de Preparación

Recepción del requerimiento informado por la empresa DISTFA S.A. el 6 de febrero de 2019.

Dada la urgencia del requerimiento y teniendo los recursos humanos y físicos disponibles, se decide realizar un trabajo “in situ” ese mismo día para poder investigar inicialmente la situación.

Se plantean como escenarios posibles, que haya sido un ataque informático interno o externo, como también un error en el funcionamiento o utilización de las aplicaciones que administran el stock y clientes.

Se conoce a priori que a nivel de Base de Datos la empresa trabaja con Oracle 19c, en servidores Windows y que manejan un volumen importante de datos.

Del análisis de riesgos se plantea la posibilidad que se sigan aconteciendo ataques u errores sino se detecta el origen rápidamente, por lo cual se asume el riesgo de iniciar todo el trabajo en vivo en el lugar lo antes posible.

Se preparan para llevar al lugar:

- Herramientas para la adquisición y análisis en un medio de almacenamiento externo. Para el caso de adquisición y análisis en vivo se dispone de:
- Equipos bloqueadores y duplicadores.
- Medios de almacenamiento de gran capacidad (para el caso que se pueda adquirir parte de información de la base de datos) y otros para adquisición de discos de alguna computadora específica.

- Estación forense para utilizar ante la necesidad de conectarse con una máquina potencialmente comprometida. Equipada con herramientas relacionadas a base de datos.

Fase de Relevamiento e Identificación

El Especialista Forense en Base de Datos y el Especialista en Evidencia Digital se dirigen al lugar del hecho.

Particularmente el Especialista Forense en Base de Datos realiza un relevamiento e identificación general:

- Revisión de las políticas y procedimientos de seguridad lógica y física vinculados al servidor y la base de datos involucrada.
- Documentación del modelo relacional de la Base de Datos "COMERCIAL" donde se gestiona el stock.
- Política de backups, replicación de base de datos en ambientes de desarrollo, prueba, etc.
- Lista de las aplicaciones y procesos que actualizan el Stock y los usuarios.

Luego del relevamiento general identifica la siguiente **información relevante al caso y detalle de objetos involucrados** (con colaboración del Administrador de Base de Datos y el Responsable de Seguridad Informática) previo al contacto con la evidencia:

- Datos del almacenamiento de los datos asociados. La base de datos involucrada es la denominada "COMERCIAL" y se encuentra en un servidor local con Oracle 19c, en un dominio lógico (virtualizado).
- Identificación de las tablas de "STOCK", sus relaciones y los procedimientos que interactúan con dicha tabla.
- Identificación de la tabla "HISTORIAL_STOCK". Esta tabla es actualizada mediante un trigger "TR_STOCK" asociado a la tabla STOCK donde se registran los movimientos de stock sobre cada producto con fecha y hora exacta y el usuario de la aplicación asociado al mismo. Los campos principales de la misma son: "Id_Producto", "Fecha_Movimiento", "Cantidad_Mov", "Cant_Parcial", "Tipo_Movimiento", "User_Id_App", "Nombre_PC", "IP".

- Análisis de la naturaleza de los clientes y los datos almacenados sobre los mismos en la tabla “CLIENTES”. Considerando que los clientes de la empresa son tantos nacionales como internacionales y que se resguardan los datos personales de los mismos, se identifica el riesgo de que hayan sucedido posibles ataques a la confidencialidad de datos personales. Se determina entonces que los casos donde determinados clientes pasaban a inactivos, pudieron haber sido parte del mismo ataque.
- En la tabla “CLIENTES” existen tres campos propios a “fecha_alta”, “fecha_mod” y “fecha_baja”. Cuando se inserta un registro de la tabla se actualiza el campo “fecha_alta” con la fecha y hora del alta, cuando se modifica un registro se actualiza el campo “fecha_mod” y cuando se elimina el campo “fecha_baja”. Esto se debe a que la tabla maneja las bajas lógicas de registros, asignando fecha y hora de baja al campo “fecha_baja” a través de un Trigger “TR_CLIENTES” asociado a la tabla (el cual cada operación de borrado, la transforma en una modificación del campo fecha_baja). Los clientes con información en fecha_baja se los considera inactivos. El trigger mencionado, también tiene la funcionalidad de actualizar los campos “fecha_alta” y “fecha_mod”.
- A partir de la revisión de la política de seguridad sobre base de datos, se detecta el uso de vistas específicas para el caso de acceso a datos sensibles cifrados en las tablas. Se identifica que existe la vista “ESTRATEGIA_COMERCIAL”, que permite consultar los datos de clientes e información confidencial como ser la estrategia comercial según el perfil del cliente. Los datos de la tabla “PERFIL_CLIENTES” se encuentran cifrados y accesibles en forma plana, a nivel de base de datos, mediante la vista mencionada.
- No existen mecanismos de auditorías implementados, excepto algunos Triggers específicos, como los mencionados, que auditan alguna información.
- En los ambientes de desarrollo, preproducción y test no existen datos productivos sensibles, ya que se utiliza una herramienta específica de transformación de datos para dichos ambientes que permite garantizar la confidencialidad e integridad de los datos.

A partir de las identificaciones realizadas se definen las próximas acciones y pasos a seguir y se gestiona la autorización de la empresa para realizarlas.

Fase de Recolección y Adquisición

En este caso, como se plantea trabajar en el lugar del hecho, se inician las tareas de Adquisición y parte de Análisis en vivo, siempre en presencia de los testigos mencionados y con el registro de la debida cadena de custodia. Se fija como período inicial de análisis desde el 1 de enero de 2019 hasta la fecha actual del 6 de febrero de 2019. Se plantea realizar una adquisición de datos volátiles y en vivo en el servidor de la base de datos COMERCIAL.

El Especialista Forense en Base de Datos conecta la estación forense a la red (cumpliendo los principios forenses para tal actividad) y, a través de un cliente de SQL, accede a la Base de Datos “COMERCIAL” con un usuario de solo lectura brindado por el Administrador de Base de Datos. Se registra la hora del servidor, con respecto a la hora real.

Adquisición en vivo de la tabla CLIENTES y objetos relacionados:

Se exporta los datos y estructura de la tabla “CLIENTES” y el código del trigger “TR_CLIENTES”. Los datos exportados se vuelcan en el archivo “CasoDF_datos_clientes.dat” y el script de exportación correspondiente en “CasoDF_BD_exportdatos_clientes.sql”. La estructura de la tabla clientes y vinculadas de interés, junto con el código del trigger de clientes se vuelcan en el archivo “CasoDF_BD_estructuras_clientes.sql”.

De cada uno de los archivos se obtiene el valor de hash correspondiente.

Adquisición en vivo de la tabla STOCK y objetos relacionados:

Se exporta los datos y estructura de la tabla “STOCK” y el código del trigger “TR_STOCK”. Se exporta los datos y estructura de la tabla “PRODUCTOS” y también del “HISTORIAL_STOCK” en el período de análisis fijado.

Los datos exportados se vuelcan en el archivo “CasoDF_BD_datos_stocks.dat” y el script de exportación correspondiente en “CasoDF_BD_exportdatos_stocks.sql”. La estructura de las tablas de stock,

productos e historial de stock y el código del trigger de stock se vuelcan en el archivo “CasoDF_BD_estructuras_stocks.sql”.

De cada uno de los archivos se obtiene el valor de hash correspondiente.

Adquisición en vivo de estructuras y objetos de base de datos:

Se decide obtener script de los objetos de base de datos, para analizar otros procedimientos o vistas que accedan a las tablas mencionadas y se almacena en el archivo “CasoDF_BD_estructuras_stocks.sql”. Del archivo se obtiene el valor de hash correspondiente.

Adquisición y Análisis en vivo en el servidor de la base de datos COMERCIAL:

Se realiza un análisis en vivo, dada la urgencia y riesgo sobre los datos, para detectar procesos maliciosos o actividades anómalas que impliquen un ataque a la base de datos “COMERCIAL” en general y su disponibilidad en ese instante, como también un análisis de red para detectar actuaciones remotas desde la red. Del resultado de dicho análisis no se encuentra ninguna otra evidencia o hallazgo. Se realiza el correspondiente informe y toma de evidencias en el documento “CasoDF_análisis_vivo_BDComercial.doc”.

Luego se realiza una adquisición de los datos volátiles para un posterior análisis “CasoDF_BD_MemoryDump.mem”, “CasoDF_BD_Pagefile.sys”, “CasoDF_BD_memcapture.ad1”. De cada uno de los archivos se obtiene el valor de hash correspondiente.

Fase de Extracción y Análisis

A partir de los archivos obtenidos en la fase anterior se realiza la extracción y análisis forense en la estación forense.

Análisis de la tabla CLIENTES y objetos relacionados:

Analiza el código del trigger “TR_CLIENTES” y determina que los campos “fecha_mod” y “fecha_baja”, donde se registran la fecha y hora de modificación y baja respectivamente, se pisan con la última acción asociada a la tabla.

De los datos obtenidos no se detectan clientes inactivos erróneamente, dado que se realizó días previos por parte del DBA un proceso de corrección de

estados de clientes ante los reclamos del área comercial. Por lo cual los clientes afectados tienen la fecha de baja vacia y la fecha de modificación correspondiente a la corrección.

Los resultados obtenidos del análisis forense de clientes se vuelcan en el archivo “CasoDF_BD_análisis_clientes.doc”. Del archivo se obtiene el valor de hash correspondiente.

Análisis de la tabla STOCK y objetos relacionados:

Luego, el especialista consulta la información de las tablas “HISTORIAL_STOCK”, “STOCK” y “PRODUCTOS” en el período de análisis fijado. Analiza también el código del trigger “TR_STOCK”.

En los resultados se observa que existen registros en la tabla “HISTORIAL_STOCK” asociados a los productos “sulfato amónico” y “nitrato de calcio”, en los cuales, a diferencia del resto de los productos, el campo “User_Id_App” se encuentra vacío y el “Nombre_PC” es diferente al resto

El nombre la PC de dichos registros corresponde a “DESA05”. En esta situación son cuatro registros, que reflejan dos movimientos del 14 de enero a las 8:30 hs. aumentando el stock en un 50% en cada producto y dos movimientos repitiendo la acción sobre los mismos productos el lunes 21 de enero a las 8:30 hs. (ambas ejecuciones en días y horarios previos al inicio de la actividad comercial). Los resultados obtenidos del análisis de stock se vuelcan en el archivo “CasoDF_BD_análisis_stock.doc”. Del archivo se obtiene el valor de hash correspondiente.

Detección de PC origen de las acciones:

El Responsable de Seguridad identifica que la PC “DESA05” es la asignada al empleado Ulises Prat. De esta manera se puede deducir que hubo una acción de la PC del empleado Ulises Prat. En ese momento, el Administrador de Base de Datos comenta que Ulises Part es un programador de sistemas que habitualmente participa en implementaciones y tiene conocimiento de accesos con permisos de administración. Sin embargo, informan que dicho empleado renunció y que desde el 1 de febrero ya no asiste a la empresa.

Resultados de análisis en la base de datos:

Se realiza una extracción y análisis del volcado de memoria y del script de los objetos de base de datos y no se detectan hallazgos relevantes al caso.

Se conforma el documento "CasoDF_BD_análisis_general.doc" con el resultado del análisis.

Antes de seguir analizando más en detalle a nivel de Base de Datos, se espera al resultado de las pericias sobre la PC del empleado mencionado.

Todos los archivos obtenidos y generados son registrados en el Formulario de Cadena de custodia, indicando sus respectivos nombres, fechas y valores de hash. Cada uno de los fundamentos e impacto de las acciones realizadas se volcaron también en el formulario. Se cifran los archivos conteniendo datos personales. Todo el proceso fue filmado y fotografiado y en presencia de los testigos.

Aplicación de Metodología Forense General sobre computadora "DESA05"

De esta manera, se replantea parte de la estrategia adicionando una nueva fuente de evidencia digital, sobre la que se aplica el proceso completo de informática forense general a través de la aplicación de **ForenseUDE**.

El Especialista en Evidencia Digital, se dirige a realizar la pericia sobre la PC del empleado Ulises Prat, para llevar adelante una adquisición en vivo del equipo. La PC "DESA05" aún permanece en el escritorio, no ha sido reutilizada por ningún otro empleado y se encuentra apagada. Por lo cual se realiza un adquisición de datos de medios de almacenamientos persistentes obteniendo una imagen forense sobre el mismo (y una copia adicional de la misma), sin poder adquirir datos volátiles.

Como parte de las actividades periciales sobre el equipo, se recuperan archivos eliminados. Se logra recuperar la carpeta "C:\PERSONALES", la cual contenía, entre otros archivos, los archivos de script SQL "ajuste_de stock.sql" e "info_clientes.sql" y el archivo con datos de clientes "info_clientes.xls".

Entre los hallazgos más relevantes se mencionan, el uso reciente y frecuente de los archivos mencionados y una herramienta cliente SQL. El acceso a la Base de Datos de producción estaba configurado por defecto con el usuario "apower".

Se evidencia que hubo un dispositivo USB conectado a la PC donde se copiaron dichos archivos.

Además, se detecta que se había configurado en la computadora la planificación del script “ajuste_de_stock.sql” de forma automática para que se ejecute el 14 de enero a las 8:30 hs y el lunes 21 de enero, en el mismo horario, conectándose con el usuario de SQL “apower”. Dichas configuraciones en la PC fueron realizadas por el usuario de red “uprat”, al igual que las ejecuciones planificadas.

Además, se verifica del análisis de los metadatos de los archivos recuperados de la PC “DESA05” todos fueron creados en dicha PC por el usuario “uprat” en la primer semana de enero.

Se registran en el Formulario de Cadena de custodia la identificación del disco de la PC del empleado, los nombres de las imágenes forenses adquiridas y los archivos resultantes de la extracción y análisis, con sus respectivos nombres, fechas y valores de hash. Se cifran los archivos conteniendo datos personales.

Todo el proceso fue filmado y fotografiado y en presencia de los testigos.

Se efectuó la debida preservación lógica y física y el embalaje del disco original y de los discos conteniendo las imágenes forenses y los resultados, para su posterior almacenamiento y traslado.

Fase de Extracción y Análisis (posterior a pericia de PC “DESA05”)

A partir de los archivos recuperados en la pericia de la PC se vuelve a ejecutar una fase de extracción y análisis vinculada al proceso forense en Base de Datos.

El Especialista Forense en Base de Datos, analiza y verifica que el archivo “ajuste_de_stock.sql” corresponde a un script SQL de actualización de stock, personalizado a aplicar sobre los productos “sulfato amónico” y “nitrato de calcio”, el cual utiliza para conectarse por defecto el usuario “apower”. Luego, determina que el archivo “info_clientes.sql” contiene scripts de SQL con una consulta del listado completo de clientes, una consulta de la vista de información confidencial de clientes, una consulta de lista de precios, incluso un script de modificación de estado de clientes específicos a estado inactivo (los clientes específicos coincidían con los informados por el área comercial en sus reclamos).

A partir del análisis del archivo de script “info_clientes.sql” y de los resultados asociados en el archivo “info_clientes.xls”, se detecta que se ejecutó la vista de SQL “ESTRATEGIA_COMERCIAL” la cual devuelve la información estratégica y confidencial asociada a los clientes y la estrategia comercial según el perfil del cliente desde la tabla “PERFIL_CLIENTES”. Los datos de la tabla “PERFIL_CLIENTES” se encuentran cifrados y accesibles en forma plana, a nivel de base de datos, mediante la vista mencionada. La estructura de la tabla de perfiles de clientes y el código de la vista estrategia comercial se pudieron analizar desde el script adquirido previamente “CasoDF_BD_estructuras_stocks.sql”.

Se actualiza el documento “CasoDF_BD_análisis_general.doc” con el resultado del análisis del cual se obtiene el valor de hash correspondiente.

Todos los archivos con los resultados del análisis en la base de datos son registrados en el Formulario de Cadena de custodia, con sus respectivos nombres, fechas y valores de hash. Se cifran los archivos conteniendo datos personales. Todo el proceso fue filmado y fotografiado y en presencia de los testigos.

El Director de Informática Forense, determina que no tiene sentido seguir investigando sobre el servidor de base de datos. Con los hallazgos logrados se puede pasar a realizar el dictamen final.

Fase de Producción y Presentación

Se escribe el dictamen final integral detallando todo el trabajo e incluyendo como anexos el contenido de los archivos encontrados y también los generados y utilizados por el especialista, es decir, todos los pasos y archivos involucrados en cada una de las actividades, con su correspondiente fundamentación. Luego se desarrolla un informe técnico específico de base de datos, detallando las tablas, el formato de las mismas, los triggers asociados, el análisis y las consultas realizadas por el Especialista Forense de Base de Datos y su fundamentación, como también las consultas y resultados hallados en la PC del empleado.

Se resalta el acceso indebido a información de datos personales por parte del empleado Ulises Prat, tanto Nacionales como Internaciones, dado que se viola la confidencialidad de los datos, protegidos bajo la Ley Nacional de Protección de

datos 25.326 como el Reglamento General de Protección de Datos (RGPD) 2016/679 de Europa. Resaltando la necesidad de efectuar las acciones consecuentes requeridas según la reglamentación.

Fase de Evaluación Final

Como parte de la evaluación final, se asesora a la empresa reforzar las políticas y procedimientos de seguridad en las base de datos como también implementar mecanismos de auditorías de datos. Se resalta la gravedad de difundir usuarios y claves genéricos. También se detecta la necesidad de revisión de las políticas de seguridad en cuanto a aplicativos instalados en las PC, permisos sobre conexiones en puertos USB, control de horarios de conexiones de los empleados (en especial a ciertas plataformas o aplicaciones), entre otros. Se resalta la necesidad de establecer procedimientos claros ante implementaciones en producción y planes de contingencia cuando durante las mismas surgen imprevistos.

5.3. Escenario 2

Detección de la situación

El lunes 14 de enero el Administrador de Base de Datos y el Responsable de Seguridad Informática, mientras estaban en camino a su trabajo, entre las 08:00 hs. y 08:35 hs. reciben, cada uno, una serie de alertas en su celular, que provenían de controles de acciones críticas desde la solución AUDB implementada en la base de datos “COMERCIAL”.

Las notificaciones de AUDB consistían en lo siguiente:

- Aviso de alerta de lectura completa de la lista de clientes, desde una aplicación cliente SQL con el usuario “apower”.
- Aviso de alerta ejecución de la vista “ESTRATEGIA_COMERCIAL” desde una aplicación cliente SQL con el usuario “apower”.

- Aviso de actualización de estado a inactivos de clientes desde una aplicación cliente SQL con el usuario “apower” (actualización que finaliza en parte con errores de restricción de datos).
- Modificación del STOCK por fuera de la aplicación.

Ante esta situación, al llegar a la empresa analizan lo sucedido y detectan el origen de las acciones y el supuesto responsable a través de la información brindada por AUDB y un análisis por parte del administrador de base de datos. Para lo cual, el área de recursos humanos se contacta con el empleado para que pueda explicar lo sucedido.

A la vez deciden contratar un servicio informático forense para investigar y analizar lo sucedido más a detalle y poder resguardar la evidencia digital que pueda ser admisible en un probable proceso judicial.

Fase de Preparación

Recepción del requerimiento informado por la empresa DISTFA S.A. el 15 de enero de 2019.

Dada la urgencia del requerimiento y teniendo los recursos humanos y físicos disponibles, se decide realizar un trabajo “in situ” ese mismo día para poder investigar inicialmente la situación.

El escenario por analizar es el ataque informático, supuestamente por parte del empleado de la compañía Ulises Prat. Adjunto con el requerimiento la empresa, se hace llegar el informe de las alertas recibidos por el Administrador de Base de Datos y el Responsable de Seguridad y los resultados relevantes del reporte que la empresa emitió desde AUDB.

Se conoce a priori que a nivel de Base de Datos la empresa trabaja con Oracle 19 c, sobre servidores Windows y que manejan un volumen importante de datos.

Del análisis de riesgos se plantea la posibilidad que, si bien se ha retirado al empleado de sus funciones, puede existir aún el riesgo que haya agendado en algún equipo la ejecución de algún otro proceso malicioso, por lo cual se asume el riesgo de iniciar el trabajo en vivo en el lugar lo antes posible.

Se preparan para llevar al lugar:

- Herramientas para la adquisición y análisis en un medio de almacenamiento externo. Para el caso de adquisición y análisis en vivo se dispone de:

- Equipos bloqueadores y duplicadores.
- Medios de almacenamiento de gran capacidad (para el caso que se pueda adquirir parte de información de la base de datos) y otros para adquisición de discos de alguna computadora específica.
- Estación forense para utilizar ante la necesidad de conectarse con una máquina potencialmente comprometida.
- Herramientas asociadas a AUDB.

Asistirá al lugar del hecho el Especialista Forense en Base de Datos (quien también cumplirá el rol de Especialista Auditor Forense en Base de Datos).

A diferencia del escenario anterior, dado el detalle del requerimiento se planea iniciar de forma paralela tanto la recolección y adquisición en las base de datos como la pericia en la PC "DESA05" del empleado Ulises Prat.

Aplicación de Metodología Forense General sobre computadora "DESA05"

Similar al escenario 1 anterior.

Fase de Relevamiento e Identificación

Como en este caso ya se recibe junto al requerimiento el detalle de las alertas, el relevamiento es mucho más ágil y conciso, enfocado a partir del contenido de los avisos de alertas y de los objetos involucrados. Dado el detalle del requerimiento se logra, ya desde la fase inicial, detectar que hubo una lectura indebida de información confidencial de clientes y ejecución la vista de estrategia comercial.

Particularmente el Especialista Forense en Base de Datos lo primero que hace es relevar a través del Administrador de Base de Datos y la documentación de AUDB, las auditorías de datos AUDB asociadas a las alertas, y así, deducir los objetos afectados y validar la configuración y ejecución de AUDB:

- Aviso de alerta de lectura completa de la lista de clientes, desde una aplicación cliente SQL con el usuario "apower".
    - Aviso asociado a la auditoría a nivel de operaciones de lectura de datos, para la detección de lecturas masivas sobre la tabla completa de "CLIENTES", incluyendo todos sus campos, desde un origen distinto a la

aplicación oficial de administración comercial y siendo aún más crítico el uso de un usuario genérico.

- Aviso de alerta ejecución de la vista “ESTRATEGIA_COMERCIAL” desde una aplicación cliente SQL con el usuario “apower”.
    - Aviso asociado a la auditoría a nivel de operaciones de lectura de datos, en base a auditar la ejecución de la vista crítica “ESTRATEGIA_COMERCIAL” (la cual consulta la información cifrada de la tabla “PERFIL_CLIENTES”), desde un origen distinto a la aplicación oficial de administración comercial y siendo aún más crítico el uso de usuario genérico.
- Aviso de actualización de estado a inactivos de clientes desde una aplicación cliente SQL con el usuario “apower” (actualización que finaliza en parte con errores de restricción de datos).
    - Aviso asociado a la auditoría a nivel de actualización de contenidos sobre campos críticos de la tabla de “CLIENTES” desde un origen distinto a la aplicación oficial de administración comercial y siendo aún más crítico el uso de un usuario genérico (la auditoría considera la acción del trigger de actualización “TR_CLIENTES” asociada a la tabla).
    - Aviso asociado a la auditoría de intento fallido de operaciones.
- Modificación del STOCK por fuera de la aplicación.
    - Asociado a la auditoría a nivel de actualización de contenidos sobre los campos críticos de la tabla de “STOCK”, desde un origen distinto a la aplicación oficial de administración comercial y siendo aún más crítico el uso de un usuario genérico (la auditoría considera la acción del trigger de actualización “TR_STOCK” asociada a la tabla).

Además, realiza un relevamiento de la arquitectura general las bases de datos y de la implementación de AUDB y sus configuraciones. Incluso releva la estrategia de almacenamiento y seguridad implantado en AUDB.

A partir de esta identificación, se obtiene mucho más rápido el detalle de los objetos involucrados.

Fase de Recolección y Adquisición

En este caso, se plantea trabajar en parte en el lugar del hecho, siempre en presencia de los testigos mencionados y con el registro de la debida cadena de

custodia. Se fija como período inicial de análisis desde el 1 de enero de 2019 hasta el 14 de enero de 2019.

Por un lado se plantea realizar una adquisición de datos volátiles y en vivo en el servidor de la base de datos COMERCIAL. Por otro lado, se plantea efectuar una adquisición en vivo de la imagen forense de AUDB.

El Especialista Forense en Base de Datos conecta la estación forense a la red (cumpliendo los principios forenses para tal actividad) y, a través de un cliente de SQL, accede a la Base de Datos "COMERCIAL" y de AUDB con un usuario de solo lectura brindado por el Administrador de Base de Datos. Se registra la hora del servidor, con respecto a la hora real.

En primer lugar se repiten las siguientes tareas de la fase de recolección y adquisición del escenario 1:

- Adquisición en vivo de la tabla CLIENTES y objetos relacionados.
- Adquisición en vivo de la tabla STOCK y objetos relacionados.
- Adquisición y análisis en vivo en servidor de la base de datos.

Se adicionan las siguientes tareas:

Adquisición en vivo de objetos relacionados a la estrategia de clientes:

Se exporta la estructura de la tabla "PERFIL_CLIENTES" y el código la vista "ESTRATEGIA_COMERCIAL" y el resultado de ejecución de la misma (invocada de de forma similar a la detectada por la auditoría). Los datos obtenidos se vuelcan en el archivo "CasoDF_BD_estrategia_clientes.dat". Dada la sensibilidad de la información se cifra el archivo y se obtiene el valor de hash correspondiente.

Adquisición en vivo de objetos de AUDB:

Se adquieren información y resultados asociados a las auditorías mencionadas en la etapa de relevamiento e identificación. Se exportan configuración de auditorías, estados de auditorías, resultados, historial, alertas y trazabilidad de las mismas en el período de análisis.

También se emiten reportes de la propia solución de AUDB. Los reportes de AUDB se obtienen con firma digital aplicada al contenido desde la solución, y en

el caso de los relacionados a datos sensibles de clientes, se le aplicó un cifrado para asegurar su confidencialidad.

El objetivo es adquirir no solo los resultados de auditorías, sino la evidencia de que las mismas hayan sido ejecutadas correctamente y no hayan sufrido modificaciones, errores o interrupciones que pudieran afectar los resultados.

Los datos exportados se vuelcan en el archivo "CasoDF_AUDB.dat" y las estructuras correspondientes en "CasoDF_AUDB_metadato". De cada uno de los archivos se obtiene el valor de hash correspondiente.

Adquisición y Análisis en vivo en el servidor de las bases de datos AUDB:

Se realiza un análisis en vivo, dada la urgencia y riesgo sobre los datos, para detectar procesos maliciosos o actividades anómalas que impliquen un ataque a las bases de datos AUDB de configuración y resultados, como también un análisis de red para detectar actuaciones remotas desde la red.

Del resultado de dicho análisis no se encuentra ninguna otra evidencia o hallazgo. Se realiza el correspondiente informe y toma de evidencias en el "CasoDF_AUDB_análisis_vivo.doc".

Luego se realiza una adquisición de los datos volátiles para un posterior análisis "CasoDF_AUDB_MemoryDump.mem", "CasoDF_AUDB_Pagefile.sys", "CasoDF_AUDB_memcapture.ad1". De cada uno de los archivos se obtiene el valor de hash correspondiente.

Fase de Extracción y Análisis

A partir de los archivos obtenidos en la fase anterior se realiza la extracción y análisis forense en la estación forense.

En primer lugar se repiten las siguientes tareas de la fase de extracción y análisis del escenario 1:

- Análisis en de la tabla CLIENTES y objetos relacionados.
- Análisis en de la tabla STOCK y objetos relacionados.

Análisis y validación de AUDB

Se realizan las siguientes tareas:

- Se valida la configuración de cada una de las auditorías relevadas.

- Se valida la información sobre la continuidad de las auditorías. Es decir, que no hayan surgido errores o modificaciones durante o después de las ejecuciones de auditorías y alertas emitidas asociadas al caso.
- Se valida los filtros de auditoría y almacenamiento involucrados en cada una de las auditorías. En el caso de las auditorías de lecturas de datos, las mismas están configuradas para almacenar solo la sentencia SQL de la operación. En auditorías de actualización se almacenan también los registros completos.
- Se analiza la información recolectada por cada una de las auditorías referida al caso y se compara la misma con respecto a las alertas emitidas. En este punto se tiene en cuenta el almacenamiento seguro de la información auditada, donde en el caso de clientes ciertos campos de clientes tienen aplicado cifrado de datos o enmascaramiento estático (almacenamiento seguro a nivel de columna).
- Se compara y analizan los resultados de auditoría en relación a los adquiridos y analizados de la base de datos COMERCIAL.

Los resultados obtenidos del análisis de stock se vuelcan en el archivo "CasoDF_AUDB_análisis.doc". Del archivo se obtiene el valor de hash correspondiente.

A diferencia del escenario anterior existe evidencia a nivel de base de datos de los siguientes puntos:

- Los cambios de estados a inactivos de los clientes específicos e incluso de los intentos fallidos, con fecha, hora, IP de origen, nombre_origen, aplicación de origen y usuario.
- En forma complementaria al log de historial de stock, la auditoría asociada a las actualizaciones de stock, identifican IP de origen, nombre_origen, aplicación de origen y usuario (no solo el nombre de la PC).
- Evidencia de la lectura de la tabla completa de clientes.
- Evidencia de la ejecución de la vista estratégica comercial.

Resultados de en las base de datos:

Se realiza una extracción y análisis del volcado de memoria de los servidores de bases de datos y no se detectan hallazgos relevantes al caso.

Se conforma el documento “CasoDF_análisis_general.doc” con el resultado del análisis.

Antes de seguir analizando más en detalle a nivel de Base de Datos, se espera al resultado de las pericias sobre la PC del empleado mencionado. Todos los archivos obtenidos y generados son registrados en el Formulario de Cadena de custodia, indicando sus respectivos nombres, fechas y valores de hash. Cada uno de los fundamentos e impacto de las acciones realizadas se volcaron también. Se cifran los archivos conteniendo datos personales. Todo el proceso fue filmado y fotografiado y en presencia de los testigos.

Fase de Extracción y Análisis (posterior a pericia de PC “DESA05”)

Similar a la misma Fase de Escenario 1.

Fase de Producción-Presentación y Fase de Evaluación Final

Similar al Escenario 1, adicionando todo lo relacionado a AUDB y la evidencia vinculada a la misma, y recomendaciones asociadas .

5.4. Comparativa de Escenarios

En el Escenario 1 el impacto del ataque es mayor porque afecta a los clientes de la empresa y la relación con la misma, ya que se advierte el problema recién dos semanas después. Por otro lado, en este escenario se debe iniciar una investigación desde cero, sin indicios reales, afectando la continuidad del negocio durante dicho análisis, en pos de seguir evitando nuevas afectaciones a los datos y servicios de la empresa.

En el Escenario 2 se logra una detección temprana del ataque, evitando afectar a los clientes de la empresa y pudiendo ajustar casi inmediatamente la acción maliciosa sobre el stock sin afectar la continuidad y la imagen del negocio. Incluso, se detecta al responsable desde el inicio y se evita que las acciones del empleado se reiteren. En este caso la investigación ya empieza más focalizada y con mayor evidencia registrada sobre el caso. Es evidente en la resolución del escenario 2, que la disponibilidad de AUDB simplifica y focaliza el trabajo de las diferentes fases, se obtiene mayor calidad, cantidad y exactitud de evidencia digital.

Capítulo 6 – Conclusiones y Futuras Investigaciones

6.1. Conclusiones

No existía, previo a este trabajo, ninguna metodología forense específica sobre la cual basar las investigaciones o actuaciones periciales en base de datos relacionales, como tampoco un marco único y detallado que sirviera como base general para la misma. El hecho que no exista ninguna guía oficial que detalle cada uno de los pasos relevantes u obligatorios que debe tener en cuenta un investigador o perito informático a lo largo de la investigación y análisis de un caso, provoca que cada profesional trabaje de diferentes formas y que cada uno aplique sus normas, procedimientos, experiencia y criterios de la mejor manera posible y según los recursos que disponga. Esta realidad se acrecienta más aún si se consideran casos relacionados con tecnologías específicas como Base de Datos Relacionales.

Por tal motivo, se diseñó una metodología informática forense general que aporta los pasos detallados a seguir para realizar un análisis forense de cualquier tipo de evidencia digital con garantías de confiabilidad y calidad, denominada **ForenseUDE** y luego, en base a la misma, se especificó la metodología forense para base de datos relacionales denominada **ForenseDB**.

En el presente trabajo se han estudiado diversas metodologías, procesos, guías, protocolos y normas, incluso varios documentos publicados por organismos públicos, que han sido de gran aporte y referencia como base general para el desarrollo de la metodología propuesta. Como resultado de la investigación se observó que no solo se manejan conceptos compartidos, sino que las etapas o fases que plantean para la práctica forense informática son bastante similares, con cierta variación de nombres, mayor o menor subdivisión, más o menos enfocadas en determinadas actividades, pero conceptualmente análogas. Se

plantean roles o perfiles específicos para cada etapa, apuntando principalmente a diferenciar el perfil investigativo del técnico.

La importancia de la estandarización de procesos y resultados facilita la colaboración no solo entre diferentes jurisdicciones e instituciones de nuestro país, sino entre países. Si bien cada jurisdicción, provincia o país se basa en sus propios protocolos, es esencial avanzar en la estandarización para promover el trabajo colaborativo y que se entiendan los resultados alcanzados o el proceso aplicado, evitando que, por desconocimiento o diferencias de criterios se invaliden evidencias digitales relevantes en los casos.

Como parte de la investigación también se ha realizado un análisis y repaso de la legislación nacional e internacional, considerando que las actividades de los investigadores o peritos informáticos forense, se encuentran totalmente ligadas a aspectos jurídico-legales, no solo en su actuación sino en los casos a analizar que puedan ser constitutivos de delitos. Conocer las leyes y los derechos fundamentales de los individuos permite dilucidar también los límites de las tareas de investigación y análisis, como también el tratamiento de la evidencia digital admisible como prueba en un proceso judicial.

La metodología **ForenseUDE** se plantea versátil y adaptable al máximo de situaciones posibles, incluyendo las actividades y tareas conceptuales comunes u obligatorios para tener en cuenta en la mayoría de los escenarios y tecnologías. De todas formas, considerando la gran variedad de situaciones y tecnologías, resulta imposible analizar todas los escenarios posibles, por lo cual se basó la solución en los escenarios más habituales, tanto para casos judicializados como privados. Asimismo, dicha metodología se plantea como base y marco de referencia para especificar metodologías en determinadas tecnologías, que, en el caso del presente trabajo, se aplicó a Base de Datos relacionales.

A través de la aplicación de la metodología **ForenseDB**, queda demostrado que se logra aplicar un proceso que brinda confiabilidad, trazabilidad, integridad y suficiencia al proceso de análisis forense en base de datos relacionales; evitando así errores u omisiones graves en el manejo de la evidencia digital, en la ejecución de procedimientos o en la aplicación de técnicas, que pueden poner en

riesgo toda una investigación o actuación pericial, brindando garantías en todo el proceso y asegurando la debida cadena de custodia.

Por otro lado, el diseño de la metodología de auditoria universal de base de datos, **AUDB**, posibilita configurar auditorías que permiten dejar rastros sobre acciones sensibles, dudosas o maliciosas, de las cuales no se podría recuperar información o el detalle necesario si no se dispusiera de las auditorías de datos.

De esta manera, **AUDB** actúa como base de generación de evidencia digital para la investigación forense y **ForenseDB** se nutre y realimenta a las auditorías forenses de **AUDB**. Ambas metodologías forman parte de la **metodología de análisis forense informático para la obtención de evidencia digital en base de datos relacionales (AUDBForense).**

Como se pudo validar, si la metodología **ForenseDB** se basa también en la recolección de resultados de auditorías preventivas de **AUDB** como evidencia digital admisible, posibilita no solo obtener información más valiosa del contexto de los hechos, sino reconstruir los sucesos en una línea trazable de tiempo.

La protección de datos se convirtió en un elemento esencial y clave en la configuración de los modelos de negocio, por tal motivo la auditoría de datos representa un gran desafío, ya que los sistemas de gestión de base de datos aumentan su complejidad con mayor rapidez que los procedimientos y tecnologías diseñadas para su control y auditoria eficaz.

Las auditorias de base de datos se convirtieron en un control necesario, cuya dificultad aumenta por la creciente variedad de nuevas tecnologías de bases de datos y volúmenes inmanejables de datos. Las amenazas de seguridad crecen exponencialmente, apareciendo nuevos riesgos e incrementándose los ya existentes. Estas circunstancias han motivado la necesidad de proponer una metodología de auditoria de datos general.

La aplicación de **AUDB** posibilita, facilita y da soporte seguro a la configuración, seguimiento y mantenimiento de auditorías de datos, permitiendo que las mismas sean llevadas a cabo de forma controladas y analizadas por usuarios que no necesitan ser expertos o especialistas en determinados gestores de base de datos. AUDB posibilita un nivel de abstracción necesario para

focalizarse en las auditorias de datos en sí y la prevención de intrusiones o riesgos potenciales sobre los mismos, sin conocer en detalle las características o necesidades técnicas de cada motor de base de datos y facilitando la puesta en práctica de los requisitos de las leyes de Protección de Datos Personales nacionales e internacionales. AUDB se basa en preservar los principios fundamentales de la información: confidencialidad, integridad y disponibilidad, permitiendo descubrir a través de un proceso continuo e incremental a qué riesgos están expuestos los datos, procurando evitar daños que afecten a los principios de la información.

AUDB además de cumplir su función principal de auditoría de datos, al complementarse e integrarse con la aplicación de **ForenseDB**, se logran poder obtener una **solución preventiva, probatoria y correctiva, en la que ambas metodologías se retroalimentan**.

En cada una de las fases (tanto de auditoría como de informática forense), la metodología integral de **AUDBForense**, enuncia y detalla las actividades obligatorias, críticas y habituales y una serie de recomendaciones para tener en cuenta.

Obviamente no todos los casos se producen ante hechos criminales o penales, y por lo tanto no todos involucran investigaciones judiciales. Puede requerirse la implementación de esta metodología con fines de auditoría y mejora continua ante incidentes, para la reparación de una base de datos dañada a partir de la reconstrucción de los hechos, para toma de decisiones para que no se reproduzcan ciertos incidentes o una investigación forense solicitada por la misma organización a un perito en forma privada, o una investigación como resultado de una denuncia. En cualquiera de los escenarios la metodología propuesta es aplicable y resulta beneficiosa.

6.2. Futuras Líneas de Investigación

A futuro se pretende extender el presente trabajo a una metodología de análisis forense informático para la obtención de evidencia digital en base de datos no relacionales y de gran escala como también almacenadas en la nube.

Es de gran importancia poder extender y adecuar la metodología de análisis forense informático para poder ser aplicada a bases de datos de datos de gran escala Big Data y poder realizar pericias sobre datos que vayan más allá de los datos estructurados típicos que pueden ser consultados por SGBD relacionales, en general, archivos sin estructuras, video digital, imágenes, datos de sensor y cualquier dato que no esté contenido en registros divididos por campos (en un modelo relacional).

La implementación de servicios de cómputo en la nube ofrece múltiples ventajas, sin embargo, una de las grandes dificultades que se presentan a la hora de realizar un análisis forense de estos servicios es de índole legal, más precisamente, cuando se transfieren datos personales de un país a otro para luego aplicarles un proceso informático. Es importante considerar los nuevos escenarios y problemática que se generan al abordar pericias en contextos de bases de datos en la nube, lo cual se centra en el debido conocimiento y control de la gestión en la nube, el cumplimiento contractual entre el prestador y el cliente, la disponibilidad del servicio en la nube y la confiabilidad, seguridad y confidencialidad sobre los servicios.

Actualmente, existe un vacío normativo en relación con el tratamiento de la evidencia digital en servidores externos que puede ser causa de que la evidencia no sea aceptada en una instancia judicial. Por lo tanto, al momento de iniciar un análisis forense de base de datos en la nube, es necesario considerar la normativa local, teniendo en cuenta también la legislación internacional y analizar las cláusulas relativas a la seguridad de la información, especialmente a la protección de los datos personales.

Las metodologías actuales no definen directivas asociadas a base de datos en la nube considerando aspectos técnico-periciales según los modelos de implementación posibles.

En términos de pericias en contextos de cómputo en la nube y Big Data, se plantean nuevos paradigmas, desafíos y escenarios que implican la necesidad del diseño de una metodología específica para manejar nuevos aspectos no solo técnicos sino legales en el tratamiento de grandes volúmenes de datos estructurados o no, almacenados en la nube, de manera de asegurar la admisibilidad de las pruebas.

Bibliografía

Aboso, G. E., & Zapata, M. E. (2006). *Cibercriminalidad y Derecho Penal.* Buenos Aires - Montevideo: B de F.

Airala, A. D., & Rapetti, O. H. (30 de Octubre de 2007). *A las puertas de una nueva especialización: La informática forense.* Recuperado el 15 de Junio de 2019, de: *https://blog.segu-info.com.ar/2007/10/las-puertas-de-una-nueva-especializacin.html*

Armendariz Perez, I. (2016). *Tésis Máster: Análisis de los principales sistemas de gestión de bases de datos ante ataques básicos.* Gatika, España: Universidad Internacional de la Rioja.

Arquillo Cruz, J. (2007). *Herramienta de Apoyo para el Análisis Forense de Computadoras.* Proyecto fin de carrera, Universidad de Jaén, Escuela Politécnica Superior de Jaén, Andalucía, España. Recuperado el 15 de Junio de 2019, de *https://issuu.com/eslibre.com/docs/herramienta_de_apoyo_para_el_an__li*

Cano, J. (2011). Computación Forense: Conceptos y reflexiones. (págs. Cano Martínez, Jeimy (2011) “Computación Forense: Conceptos y reflexiones”. 2011, de Information Systems Audit and Control Association (ISACA). Colombia.). Colombia: Information Systems Audit and Control Association (ISACA). Recuperado el 10 de Junio de 2019, de *http://sas-origin.onstreammedia.com/origin/isaca/LatinCACS/cacs-lat/forSystemUse/papers/I242.pdf*

Cano, J. (2016). *Computación Forense. Descubriendo los Rastros Informáticos.* (Segunda ed.). Bogotá, Buenos Aires, México: Alfaomega.

Casey , E. (2018). *Digital Evidence and Computer Crime: Forensic Science, Comp.* USA: Academic Press.

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Orlando, USA: Academic Press Inc.

Casey, E. (2014). *Digital Evidence and Computer Crime.* USA: Academic Press.

Cavagnaro, M. V., & Celiz, A. P. (2005). *La prueba ilegal en el proceso penal: alcances de la doctrina del fruto del árbol venenoso.* Recuperado el 19 de Mayo de 2019, de *www.saij.jus.gov.ar*

Committee IT/012. (2003). *HB:171 Guidelines for the Management of IT evidence.* Standards Australia International. Recuperado el 30 de Junio de 2019, de *https://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB171.PDF*

Darahuge, M. E., & Arellano González, L. (2011). *Manual de Informática Forense.* Buenos Aires, Argentina: Errepar.

Darahuge, M. E., & Arellano González, L. (2012). *Manual de Informática Forense II.* Buenos Aires, Argentina: Errepar.

Darahuge, M. E., & Arellano González, L. (2016). *Manual de Informática Forense III .* Buenos Aires, Argentina: Errepar.

Di Iorio, A. H. (2016). *Guía Integral de Empleo de la Informática Forense em el Proceso Penal (2da edición).* Universidad Fasta, Mar del Plata, Buenos Aires, Argentina. Recuperado el 15 de Junio de 2019, de *http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/1592/PAIF.pdf?sequence=1*

Di Iorio, A., Castellote, M., & Bruno , C. (2017). *El Rastro Digital del Delito.* Mar del Plata, Argentina: Universidad FASTA Ediciones.

Dominguez, F. L. (2015). *Introducción a la Informática Forense.* Buenos Aires, Argentina: Rama.

Dupuy, D., & Kiefer, M. (2017). *Cibercrimen. Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet.* Buenos Aires - Montevideo: B de F.

EDRM. (2014). *Modelo EDRM.* Recuperado el 15 de Junio de 2019, de *https://www.edrm.net/frameworks-and-standards/edrm-model/*

Ferreyra, E. (2017). *Evidencia Digital, Investigación de Cibercrimen y Garantías del Proceso Penal.* Asociación por los Derechos Civiles (ADC), Buenos Aires, Argentina. Recuperado el 30 de Mayo de 2019, de *https://adcdigital.org.ar/portfolio/evidencia-digital-investigacion-cibercrimen-garantias-del-proceso-penal/*

Ferreyra, E. (2018). *La Convención de Cibercrimen de Budapest y América Latina. Breve guía acerca de su impacto en los derechos y garantías de las personas.* Asociación por los Derechos Civiles (ADC), Buenos Aires, Argentina. Recuperado el 30 de Mayo de 2019, de *https://adcdigital.org.ar/wp-content/uploads/2018/03/Convencion-Budapest-y-America-Latina.pdf*

Ferreyra, E. (2018). *La investigación forense informática en América Latina.* Asociación por los Derechos Civiles (ADC), Buenos Aires, Argentina. Recuperado el 30 de Mayo de 2019, de *https://adcdigital.org.ar/wp-content/uploads/2018/04/Investigacion-forense-informatica-Latam.pdf*

Ferro Rodriguez, G. A., & Santiesteban, P. A. (2010). *Estado del arte de la aplicación de técnicas antiforenses en bases de datos Oracle. Conceptos y retos para los informáticos forenses.* Pontificia Universidad Javeriana, Facultad de Ingeniería, Bogotá. Colombia. Recuperado el 15 de Junio de 2019, de *https://repository.javeriana.edu.co/bitstream/handle/10554/7528/tesis355.pdf?sequence=1*

García Guilabert, N. (2017). *El Ciberacoso. Análisis de la victimización de menores en el ciberespacio desde la Teoría de las actividades cotidianas.* Madrid, Buenos Aires, Montevideo: B de F, Edisofer S.L. Libros Jurídicos.

Gioia, C. (2012). *Desarrollo de una Metodología de Auditoria Universal de Datos a Nivel de Registro (Tesis de Especialización en Criptografía y Seguridad Teleinformática).* Escuela Superior Técnica del Ejército Argentino (EST), Buenos Aires, Argentina.

Gioia, C., & Eterovic, J. (2017). CIBSI 2017. *Proposal of a non-invasive universal data audit methodology.* Buenos Aires, Argentina: IX Congreso Iberoamericano de Seguridad Informática, UBA. Recuperado el 15 de Junio de 2019, de http://cibsi2017.org/programa/Actas_cibsi2017_UBA.pdf, p.83-90

Gomez, L. (2014). Copitec 2014. *Calidad de servicio pericial mediante procedimientos operativos estandarizados.* Buenos Aires, Argentina: Congreso Argentino de Ingeniería Forense 2014. Recuperado el 15 de Junio de 2019, de *http://www.copitec.org.ar/comunicados/CAIF2014/calidadserviciopericial.pdf*

Gonzalez Allonca, J., Gioia, C., Eterovic, J., Krajnik, M., Ureta, W., Conde, S., . . . Igarza, S. (2019). Análisis del Marco Normativo de la Protección de los Datos Personales a Aplicarse en la Argentina en Proyectos de Cloud Computing Implementados en el Exterior del País. *Análisis del Marco Normativo de la Protección de los Datos Personales a Aplicarse en la*

Argentina en Proyectos de Cloud Computing Implementados en el Exterior del País, (pág. 12). Córdoba.

Goodman, M. (2015). *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It.* (Anchor, Ed.) New York, United State: Anchor Books.

Heredia, C. (2011). *La Evidencia Digital: un nuevo reto para el Fiscal.* Recuperado el 30 de Mayo de 2019, de Hipótesis Acusatoria: *http://hipotesis-acusatoria.blogia.com/2011/052601-la-evidencia-digital.php*

ISO/IEC 27037:2012. (2012). Information Technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence. Estados Unidos. Recuperado el 10 de Mayo de 2019, de *https://www.iso.org/standard/44381.html*

ISO/IEC 27040. (2015). Information technology - Security techniques - Storage security. Estados Unidos. Recuperado el 10 de Mayo de 2019, de *https://www.iso.org/standard/44404.html*

ISO/IEC 27041. (2015). "Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method. Estados Unidos. Recuperado el 30 de Junio de 2019, de *https://www.iso.org/standard/44405.html*

ISO/IEC 27042. (2015). Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence. Estados Unidos. Recuperado el 10 de Mayo de 2019, de *https://www.iso.org/standard/44405.html*

ISO/IEC 27043. (2015). Information technology - Security techniques - Incident investigation principles and processes. Estados Unidos. Recuperado el 10 de Mayo de 2019, de *https://www.iso.org/standard/44407.html*

ISO/IEC 27050. (2015). Information technology - Security techniques - Electronic discovery - Part 1: Overview and concepts. Estados Unidos. Recuperado el 10 de Mayo de 2019, de *https://www.iso.org/standard/66231.html*

IT-Insecurity. (2013). *Reflexiones sobre la norma ISO/IEC 27037:2012. Directrices para la identificación, recolección, adquisición y preservación de la evidencia digital.* Recuperado el 15 de Junio de 2019, de IT-Insecurity: *http://insecurityit.blogspot.com.ar/2013/09/reflexiones-sobre-la-norma-isoiec.html*

Jara, H., & Pacheco, F. (2012). *Ethical Hacking 2.0.* Buenos Aires, Argentina: RU.

López Delgado, M. (2007). *Análisis Forense Digital.* España: CriptoRed. Recuperado el 30 de Junio de 2019, de *https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf*

López Rivera, R. (2012). *Peritaje informático y tecnológico.* Madrid: Blanco y Negro.

Marqués Arpa, T., & Serra Ruiz, J. (2014). RECSI 2014. *Cadena de Custodia en el Análisis Forense. Implementación de un Marco de Gestión de la Evidencia Digital.* Alicante, España. Recuperado el 30 de Mayo de 2019, de *http://web.ua.es/en/recsi2014/documentos/papers/cadena-de-custodia-en-el-analisis-forense-implementacion-de-un-marco-de-gestion-de-la-evidencia-digital.pdf*

Márquez Arcila, R. H. (2018). *Auditoría forense.* (IMCP, Ed.) México.

Ministerio de Justicia y Derechos Humanos. (2018). *Protocolo unificado de los ministerios públicos de la República Argentina.* CABA, Argentina: Ediciones SAIJ. Recuperado el 15 de Junio de 2019, de *http://www.jus.gob.ar/media/3262247/Protocolo%20unificado.pdf*

Ministerio de Justicia y Derechos Humanos de la Nación. (s.f.). *InfoLEG, Información Legislativa y Documental*. (Ministerio de Justicia y Derechos Humanos. Presidencia de la Nación Argentina.) Recuperado el 15 de Mayo de 2019, de *http://www.infoleg.gob.ar/*

Pereyra, D., & Eterovic, J. E. (2014). WICC 2014. *Desarrollo de una Guía de Asistencia para el Análisis Forense Informático en un Ambiente Piloto.* Ushuaia, Tierra del Fuego, Argentina: XVI Workshop de Investigadores en Ciencias de la Computación. Recuperado el 30 de Junio de 2019, de *http://sedici.unlp.edu.ar/bitstream/handle/10915/43214/Documento_completo.pdf?sequence=1*

Presman, G. D. (s.f.). Copitec 2014. *ISO/IEC 27037 normalizando la practica forense informática.* 2014: Congreso Argentina de Ingeniería Forense 2014. Recuperado el 15 de Junio de 2019, de *http://www.copitec.org.ar/comunicados/CAIF2014/CAIF-Presman.pdf*

Presman, Gustavo; ADC Por los Derechos Civiles. (2018). *La investigación forense informática en América Latina.* ADC Digital. Recuperado el 15 de Junio de 2019, de *https://adcdigital.org.ar/portfolio/la-investigacion-forense-informatica-en-america-latina/*

Programa Nacional de Criminalística. (2018). *Protocolo Unificado de los Ministerios Públicos de la República Argentina.* CABA, Argentina: Ediciones SAIJ.

Sain, G. (2015). Cibercrimen: el delito en la sociedad de la información. En S. Eissa, *Políticas Públicas y seguridad ciudadana.* Buenos Aires, Argentina: Eudeba.

Sain, G., & Azzolin, H. (2017). *Delitos Informáticos. Investigación criminal marco legal y peritaje.* Buenos Aires - Montevideo: B de F.

Semprini, G. (2017). El Análisis integral de la evidencia digital. *XLIIICLEI-46 JAIIO.*

Sergi, N. (2018). *Análisis jurídico de la situación de la evidencia.* Buenos Aires, Argentina: Asociación por los Derechos Civiles. Recuperado el 30 de Mayo de 2019, de *https://adcdigital.org.ar/portfolio/analisis-juridico-de-la-situacion-de-la-evidencia-digital-en-el-proceso-penal-en-argentina/*

UFECI. (2016). *Guía de obtención, preservación y tratamiento de evidencia digital.* Recuperado el 30 de Junio de 2019, de *https://www.mpf.gob.ar/resoluciones/PGN/2016/PGN-0756-2016-001.pdf*

Ureta, W. (2013). *Marco de referencia para el análisis forense de dispositivos Android (Tesis de Maestría en Informática).* Universidad Nacional de la Matanza (UNLaM), Buenos Aires, Argentina.

Vila Avendaño, P. (2018). *Técnicas de Análisis Forense Informático para Peritos Judiciales Profesionales.* Madrid, España: ZeroxWord Computing.

Anexos

Anexo 1: Legislación Nacional en Delitos Informáticos

En primer lugar, el artículo 1 de la Ley 26.388 de Delitos Informáticos, incorporó al artículo 77 del Código Penal Argentino, nuevas definiciones adaptadas a las nuevas tecnologías. El término "**documento**"[1] comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. De esta manera la ley le da el valor jurídico probatorio al documento electrónico. Los términos "**firma**" y "**suscripción**" comprenden la **firma digital**[2]. Los términos "**instrumento privado**" y "**certificado**" comprenden el **documento digital firmado digitalmente**[3].

En relación con **delitos contra la integridad sexual**, en el artículo 2 de la Ley de Delitos Informáticos, se modificó el artículo 128 del Código Penal de la Nación

[1] En la Ciudad de Posadas, Provincia de Misiones, Argentina, en el año 2006 la Resolución DGCC N.º 175/06 del día 21 de diciembre, se definió al documento electrónico como: "El documento electrónico debe entenderse como toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos, con eficacia probatoria o cualquier otro tipo de relevancia jurídica. Técnicamente el documento electrónico es un conjunto de impulsos eléctricos que recaen en un soporte de computadora que, sometidos a un proceso, permiten su traducción a lenguaje natural a través de una pantalla o una impresora."

[2] La Ley 25.506 de "Firma Digital", sancionada y promulgada a fines de 2011, establece en sus artículos primero y segundo el valor jurídico probatorio y las definiciones de firma electrónica y firma digital. Reconociendo el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la Ley. Del mismo modo define a la Firma Digital como "al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma." Se diferencia la firma digital a la firma electrónica en que ésta última es un conjunto de "datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital." Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm.

[3] El artículo 11 de la Ley 25.506 establece que: "Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación".

que reprime el **delito de pornografía infantil**[1] por cualquier medio, sea Internet u otros medios como redes informáticas, DVD, fotos, revistas, etc. Inicialmente con esta modificación se contemplaba únicamente la sanción penal si había intención de compartir o comercializar el material de pornografía infantil, de lo contrario, poseerlo no era delito. De esta manera, la simple tenencia del material era considerada acción privada[2]. Este artículo fue nuevamente modificado bajo la sanción de la Ley 27.436 el 23 de abril de 2018 penando no solo la distribución sino la tenencia simple de material pornográfico infantil, sin importar si la posesión sea con intención de compartirlo o comercializarlo. De todas maneras, no se reprime con la misma pena a quien distribuya representaciones, como a quien las tenga en su poder con fines inequívocos de distribución o comercialización, ya que son ilícitos de diferente peligrosidad. También, junto con esta última modificación, todas las escalas penales previstas en la modificación inicial del artículo se elevaron en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años.

Asociado también a delitos contra la integridad sexual, en el año 2013, el 13 de noviembre se sancionó la Ley 26.904 incorporando al mencionado Código **el delito de Grooming**[3] (o acoso informático contra menores de edad), incorporando el Artículo 131. En el 2018 el Senado de la Nación aprobó la Ley 27.458 por el que se declara el 13 de noviembre como Día Nacional de la Lucha contra el Grooming.

En el artículo 3 de la Ley 26.388, en cuanto a los **delitos contra la libertad**, se modificó el título del capítulo III, incluyendo la **violación de secretos y de la privacidad** y modificó los artículos del C.P. relacionados a estos delitos en los

[1] Esta reforma se enrola dentro de los criterios generales establecidos en el Protocolo relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de los Niños en la Pornografía (ley 25.763, año 2003), complementarios de la Convención de las Naciones Unidas sobre los Derechos del Niño, y art. 9° Convención de Budapest.

[2] Ante un delito de acción privada, si bien existe un interés público en que sea penado, este interés se ajusta al del damnificado expresarlo en forma sostenida a lo largo de todo el proceso judicial, debido a que afectan una esfera muy íntima de bienes jurídicos. Solo se procede por querella del agraviado o de sus guardadores o representantes legales, no puede ser perseguido de oficio por los poderes públicos (Policía, Jueces de Instrucción o Ministerio Público Fiscal). En cualquier momento el damnificado puede desistir de la querella. Este delito está previsto en el artículo 73 del CP. La diferencia con los delitos dependientes de instancia privada es que, si bien tampoco se puede actuar de oficio, una vez hecha la denuncia, el denunciante no puede detener la acción penal una vez realizada la denuncia.

[3] Etimológicamente la palabra “Grooming” es un vocablo inglés derivado de “groom” que alude a conductas de preparación o acercamiento para un fin determinado. El delito de Grooming se refiere a cuando un adulto contacta a un menor de edad, a través de Internet u otros medios digitales, mediante la manipulación o el engaño y ocultando la condición de adulto, con una finalidad sexual, logrando que el niño o niña realicen acciones de índole sexual.

artículos 4, 5, 6, 7, y 8 de la ley de delitos informáticos. Se incorpora la "privacidad" como bien jurídico protegido teniendo en cuenta que las nuevas tecnologías aumentan los peligros para la protección de este derecho.

En artículo 4 de la misma ley, se sustituye el artículo 153 del C.P. para incluir **cuatros tipos de conducta a penalizar**: a) La violación o acceso indebido de una comunicación electrónica; b) El apoderamiento indebido de una comunicación electrónica; c) La supresión o desvío indebido de una comunicación electrónica; d) La interceptación o captación indebida de comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema privado o de carácter restringido.

Con la modificación del artículo 153 del C.P., además de los medios tradicionales de comunicación, se incorpora el término "comunicación electrónica" pudiendo considerarse como tipo de intercambio privado, sea un correo electrónico, chats, mensajes de texto, mensajes de voz, u otros que encuadren en dicha acepción (Di Iorio, Castellote & Bruno, 2017, p.110).

Previo a la sanción de la ley de delitos informáticos, el correo electrónico no se encontraba equiparado al correo postal por lo que todas las acciones que se planteaban judicialmente eran rechazadas por inexistencia de delitos, aun así, en ocasiones, se había intentado aplicar la analogía, olvidando que en el derecho penal la aplicación de la misma es improcedente, ya que según el principio de legalidad penal se prohíbe la analogía cuando se quiere usar para condenar o agravar la responsabilidad penal [1].

Se tipifica como delito también el **acceso indebido a sabiendas a un sistema o dato informático de acceso restringido por cualquier medio sin la debida autorización o excediendo la que posea**, en el articulo 5 de la Ley 26.388, modificatorio del artículo 153 bis del CP. Este delito supone vulnerar la confidencialidad de la información tanto en exclusividad como en intimidad a través de un acceso ilegítimo informático o de modo ilegal, a sabiendas, es decir, conociendo la situación en carácter previo a realizar la acción, accediendo a información que no estaba destinada a ser pública. Los bienes jurídicos

[1] A la prohibición de analogía, también se la conoce como "prohibición de la analogía in malam partem". Cabe aclarar que no se opone el uso de la analogía para excluir o atenuar la responsabilidad penal, "analogía in bonam parte".

protegidos son la reserva, confidencialidad, derecho a la privacidad del titular del sistema y del dato informático.

En relación con la acción típica, Pablo Palazzi[1] explica que “El texto legal hace referencia a ´sistema o dato informático de acceso restringido´, puesto que no se prohíbe acceder a sistemas o redes abiertas, o al contenido publicado en un sitio de internet de acceso público (como lo son la gran mayoría). Será de acceso restringido porque tiene alguna medida de seguridad que impida el libre ingreso. Para ello, deberá tener que sortearse esta protección; de lo contrario, si es un dato o sistema de libre acceso, no habrá delito”.

El término "a sabiendas" indica claramente que corresponde a una figura que únicamente acepta el dolo[2], desestimando la negligencia. Muchas veces el acceso ilegítimo a sistemas informáticos suele ser el paso previo para la comisión de otros delitos como la estafa, sustracción de datos personales, daño, etc. Del mismo modo, al referirse a "acceso restringido", se refiere a sistemas en los cuales el ingreso no sea libre o de acceso gratuito a través de Internet[3]. Si el sistema posee algun tipo de verificación de identidad, requiera autorización expresa, solicitud de usuario y/o contraseña o cualquier otra modalidad de autorizacion o autenticación que limite el acceso se considera restringido. Se excluye los casos donde se medie consentimiento expreso, cumplimiento de un deber o técnicas de pruebas de vulnerabilidades de seguridad informática, como testeos de penetración[4] o se aplique ingeniería reversa o inversa[1].

---

[1] Palazzi, P (2009). *Los Delitos Informáticos en el Código Penal. Análisis de la Ley 26.388*. Buenos Aires: Abeledo Perrot. p. 102-103.

[2] Según el aspecto subjetivo del tipo penal, si el delito por parte del autor es cometido con intención, se lo denomina doloso, caso contrario si no hubo voluntad del autor en cometer o querer producir el resultado del delito es culposo, sea por negligencia o imprudencia al momento de la acción. Con la incorporación de la palabra "indebido" se contempla únicamente la acción dolosa descartando la culpa.

[3] Dr. Hugo Sorbo (2013) en su artículo web “Delitos Informáticos - Aspectos para tener en cuenta de la Ley 26.388”. Protocolo A00376672921 de Utsupra. Enlace de acceso http://server1.utsupra.com/doctrina1?ID=articulos_utsupra_02A00376672921

[4] Las pruebas de penetración (también llamadas “pen testing”) son una práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar. Una vulnerabilidad (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

Para diferenciar los delitos dolosos o culposos es relevante tener en cuenta la voluntad del autor en cometer y querer producir el resultado del delito en particular, por ejemplo, la intención de estafar, o el querer dañar una cosa o a alguien. A diferencia de la culpa donde el resultado se produce sin intención, no planeada, sino por negligencia o imprudencia al momento de llevar a cabo la acción. Existe un caso particular que es el dolo eventual que se da cuando el autor del hecho se imagina que puede ocasionar un daño, pero actúa pensando que ese daño no va a acontecer (Di Iorio, Castellote & Bruno, 2017, p.93).

En su artículo 6 sustituye el artículo 155 del C.P. para incorporar la sanción bajo pena de multa al delito de "**publicación indebida de una comunicación electrónica que no esté destinada a ser pública y que puede causar perjuicios a terceros**", eximiendo de responsabilidad a quien lo hace en pos de la protección de un bien o interés público. Por "publicar" se entiende dar a conocer a terceros por cualquier forma, ya sea reenviando un correo electrónico, contándolo verbalmente, publicando el contenido en un sitio web, etc.

También, en su artículo 7 sustituye el artículo 157 del C.P. agregando como delito a "**la revelación de hechos, actuaciones, documentos y datos que por ley sean secretos**", en especial los que deben ser conservados y preservados por funcionarios públicos, cuyo acceso legítimo a la información en base de datos o archivos, no los habilita a revelarlos a terceros ajenos al secreto en sí. Se agrega el término "datos" para actualizar la figura y proteger penalmente los datos que están en poder de la Administración Pública y que por ser secretos no deben ser revelados a terceros[2]. La acción típica es "revelar" el secreto, y el sujeto activo debe ser un funcionario público que tenga la obligación de guardar el secreto.

Esta ley también sustituye el artículo 157 bis del C.P. en su artículo 8, reprimiendo con pena de prisión a quien "**acceda, proporcione, revele o inserte directa o indirectamente datos ilegítimamente a un banco de datos personales**".

[1] La ingeniería inversa es el proceso llevado a cabo con el objetivo de obtener información o un diseño a partir de un producto, con el fin de determinar cuáles son sus componentes y de qué manera interactúan entre sí y cuál fue el proceso de fabricación. No se relaciona con privacidad, pero si con la protección intelectual.

[2] Palazzi, P (2008). *Análisis de la ley 26,388 de reforma del Código Penal en materia de delitos informáticos*. Revista de Derecho Penal y Procesal Penal n° 7/2008.

Esta figura del delito está íntimamente relacionada con la Ley de Protección de Datos Personales establecidos en la Ley 25.326 en el año 2000, por la cual se incorporó al C.P. el artículo 117 bis, que preveía la falsedad en archivos de datos personales y suministro de información falsa y el artículo 157 bis, que incorporaba las figuras del acceso ilegítimo a un banco de datos y revelación ilegítima de información. Este último artículo fue modificado por la Ley 26.388 para intensificar la protección penal a los bancos de datos personales, donde además de reprimir a quien ingresa indebidamente, revela o proporcione la información personal resguardada, penaliza a quien modifica el contenido de dicha base de datos o archivo de datos personales, ya sea, agregando, modificando o eliminando el contenido de la información. Con este artículo se procura resguardar a la intimidad personal de toda intromisión ilícita de personas no autorizadas.

Es importante aclarar, en relación con el segundo inciso del artículo 157 bis, que “revelar” la información implica dar a conocer, mostrar o exponer a un tercero la información secreta; mientras que “proporcionar” implica poner a disposición una información, facilitándose de cualquier modo a quien la solicita (Di Iorio, Castellote & Bruno, 2017).

Según el Dr. Pablo Palazzi[1] "la norma no hace referencia a que los datos sean falsos sino a datos, por ende, poco importa que estos datos sean falsos o verdaderos. La protección que el legislador otorga al banco de datos podrá extenderse tanto al responsable de los datos como a su titular…" y continúa "…la norma se refiere a insertar datos, pero no aclara cuales pueden ser. El resultado típico requerirá que el archivo se modifique, ya sea agregándose nuevos asientos o borrando los existentes.".

En cuanto a los sujetos autores, el sujeto activo será toda persona que ingrese indebidamente sin autorización, y el sujeto pasivo será tanto el dueño o titular de la base de datos como quien tenga la responsabilidad de proteger y resguardar la base de datos personales.

[1] Cita del Dr. Pablo Palazzi realizada por el Dr. Hugo Sorbo (2013) en su artículo web “Delitos Informáticos - Aspectos a tener en cuenta de la Ley 26.388”. Protocolo A00376672921 de Utsupra http://server1.utsupra.com/doctrina1?ID=articulos_utsupra_02A00376672921. El Dr. Pablo Palazzi, es autor de la obra " Análisis de la ley Argentina 26.388/2008 de reforma del Código Penal en materia de delitos informáticos", revista brasilera de ciencias criminales, ISSN 1415-5400, Nº.75,2008, págs. 39-70, a la que se hace referencia en el artículo https://dialnet.unirioja.es/servlet/articulo?codigo=5232873.

En relación con **delitos contra la propiedad** en el Código Penal, previo a la reforma de la Ley de Delitos informáticos, en el año 2004, se había incorporado a través de la Ley 25.930 el inciso 15 al artículo 173 asociado a la **defraudación por uso ilícito de tarjeta de crédito o débito**. Luego la Ley 26.388 en su artículo 9, agrega al artículo 173 del C.P. el nuevo inciso 16, penalizando específicamente la **estafa informática**, donde se reprime al que defraude a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de los datos.

También vinculado con delitos contra la propiedad, la Ley 26.388 tipifica el delito de **daño informático** en sus artículos 10 y 11, los cuales incorporan un segundo párrafo al artículo 183 y sustituyen el artículo 184 del Código Penal, respectivamente. De esta manera el delito de daño no recae solo sobre cosas tangibles, sino también sobre bienes intangibles como lo son los datos, documentos o programas o sistemas informáticos. La reforma considera como delito la conducta de quien altere, destruya o inutilice los bienes intangibles mencionados, o incluso venda, distribuya o haga circular o introduzca en un sistema informático cualquier programa destinado a hacer daño, introduciendo con esto último la figura de "virus informático"[1] ya que por "programa destinado a causar daño" debe entenderse un programa malicioso con posibilidad de causar un perjuicio. Se plantean agravantes si el daño se produce en infraestructuras críticas, como ser datos, documentos o sistemas informáticos públicos, pertenecientes a entidades del Estado Nacional, Provincial o Municipal o sistemas informáticos destinados a la prestación de servicios de salud, comunicaciones, provisión o transporte de energía, de medios de transporte u otro servicio público.

En el contexto informático, "destruir" quiere decir borrar definitivamente sin posibilidad de recuperación. A su vez, el hecho que exista un sistema de resguardo en modo alguno altera el deleito de daño, pues a la restauración requiere un esfuerzo que ya implica reparar el daño causado[2]. A su vez, "alterar"

[1] Un virus es un software que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo.

[2] Palazzi, P (2008). *Análisis de la ley 26.388 de reforma del Código Penal en materia de delitos informáticos*. Revista de Derecho Penal y Procesal Penal n° 7/2008.

significa modificar provocando un daño sin destruirlo totalmente, igual que "inutilizar" que requiere que el archivo no funcione.

Asociado a **delitos contra la seguridad del tránsito y de los medios de transporte y de comunicación** (que atentan contra la seguridad pública), la Ley 26.388, en su artículo 12, modificó el artículo 197 del C.P. para tipificar los delitos de **interrupción o entorpecimiento de comunicación privada y pública** con la finalidad de proteger el normal funcionamiento de los servicios de telecomunicaciones y el intercambio de información por medios electrónicos o de otra naturaleza, debido a la interrupción o entorpecimiento de las mismos o ante la resistencia violenta al restablecimiento de dichos servicios. La figura no sólo ampara lo público sino además cualquier clase de comunicación, incluyendo las privadas como el correo electrónico, la voz a través de IP[1], o los mensajes de chat o de texto a través de celulares (SMS[2])[3].

El articulo 13 de la Ley 26.388, asociado a **delitos contra la administración pública**, tipifica el **delito de sustracción, alteración, ocultamiento, destrucción o inutilización en todo o en parte de objetos destinados a servir como prueba**, modificando el artículo 255 del C.P. Se procura la conservación o preservación de objetos que sirvan de prueba cuya custodia esté a cargo de un funcionario u otra persona en el interés del servicio público.

Si bien es cierto que la Ley 26.388 llenó un vacío legal, queda un largo camino por recorrer a nivel legislativo y procesal.

Los **delitos que pueden cometerse con herramientas informáticas** son en el Código Penal Argentino: calumnias e injurias (art. 109 y 110), divulgación de secretos (art. 156), defraudación (art. 172), amenazas (art. 149 bis y ter), comercialización y suministro de medicamentos sin autorización por internet (art. 208), instigación a cometer delitos (art. 209), instigaciones basadas en la ley antidiscriminatoria (23.592, arts. 1, 2 y 3), intimidación pública (art. 211-212),

[1] Voz sobre IP se refiere a la transmisión de tráfico de voz sobre redes basadas en internet. Es una tecnología que proporciona la comunicación de voz y sesiones multimedia (tales como vídeo) sobre Protocolo de Internet (IP).

[2] SMS, por las siglas en inglés, Short Message Service, mensaje corto de texto que se puede enviar entre teléfonos celulares.

[3] Palazzi, P (2008). *Análisis de la ley 26,388 de reforma del Código Penal en materia de delitos informáticos.* Revista de Derecho Penal y Procesal Penal n° 7/2008.

impedimento arbitrario del pleno ejercicio de los derechos y garantías fundamentales reconocidos en la Constitución Nacional (Ley 23.592, arts.1, 2 y 3).

El nuevo Código Procesal Penal Federal, sancionado por la Ley 27.063[1] contiene cambios que lo distinguen estructuralmente de su antecesor regulado en la Ley 23.984. Se resalta la incorporación del artículo 144 relativo al **secuestro de datos** y el artículo 150 sobre la **implementación de un sistema de cadena de custodia para preservación de evidencias incautadas**. En general establece que el juez puede ordenar el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación, rigiendo las mismas limitaciones dispuestas para el secuestro de documentos. Se establecerá una cadena de custodia para resguardar identidad, estado y conservación de los elementos de prueba y se debe identificar a todas las personas que hayan tomado contacto con esos elementos, siendo responsables los funcionarios públicos y particulares intervinientes.

Previamente a la sanción de la Ley 26.388 de delitos informáticos algunas leyes fueron sancionadas o actualizadas con la finalidad de protección en especial a sectores privados ante el auge de Internet y el comercio electrónico, como fueron las leyes de protección de secretos comerciales y propiedad intelectual.

La **Ley 24.766[2] de Secretos Comerciales, de 1996, tipificó la sustracción de secretos comerciales contenidos en soportes electrónicos**. Esta ley se refiere a confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos.

La **Ley de Propiedad Intelectual (Ley 11.723)[3]** establece el régimen legal de la propiedad intelectual, es decir, actúa sobre las obras científicas, literarias y

[1] Ley 27.063. Código Procesal Penal Federal (Denominación del Código sustituida por art. 1° de la Ley N° 27.482 B.O. 7/1/2019).

[2] Ley 24.766 de secretos comerciales disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41094/norma.htm.

[3] Ley 11.723 de Propiedad Intelectual disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm.

artísticas. La Ley 25.036[1] sancionada en el año 1998 modificó la Ley de Propiedad Intelectual 11.723 del año 1933, brindando protección penal a los derechos de autor sobre los programas de computación fuente y objeto, las compilaciones de datos o de otros materiales, incluyéndolos en varios artículos, enmarcando en la modalidad de estafa las infracciones a estos artículos. Con esta reforma se pena a quien realice una copia ilegítima de cualquier programa de software o base de datos informática.

En el año 2000 con la **Ley de Datos personales 25.326** se dictaron normativas relacionadas con la confidencialidad de los datos personales de los usuarios almacenados tanto en base de datos públicas como privadas. Mientras que en el 2001 se sanciona la **Ley de Firma Digital 25.506**[2] para la protección de la integridad y autenticidad de la información transmitida por Internet mediante el reconocimiento legal de la tecnología de firma digital. La Ley de Firma Digital reconoce y establece las condiciones para el empleo de la firma electrónica y de la firma digital y su eficacia jurídica y crea la Infraestructura de Firma Digital de la República Argentina.

Ley 24.769[3] **del régimen penal tributario**, sancionada en 1996, fue reformada por la **Ley 26.735**[4] **del año 2011**, que tipifica el delito de alteración dolosa de registros fiscales y sistemas informáticos o equipos electrónicos con el objetivo de penar conductas fraudulentas en busca de algún tipo de beneficio fiscal que no corresponde y darle protección a los sistemas de controladores fiscales o cualquier sistema y equipo que tenga por finalidad emitir facturas y controlar operaciones tributarias (Di Iorio, Castellote & Bruno , 2017, p.143-144).

Ley 25.520[5] **de Inteligencia Nacional** (del año 2001, modificada en 2015 por la Ley 27.126[6]) determinó la creación de la **agencia federal de inteligencia (AFI)** y la disolución de la secretaría de inteligencia (SIDE). La ley tiene por finalidad

[1] Ley 25.036 disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/50000-54999/54178/norma.htm.

[2] Ley de Firma Digital 25.506, disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm.

[3] Ley 24.769 disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41379/texact.htm.

[4] Ley 26.735, modificatoria de la Ley 24.769, disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/190000-194999/192148/norma.htm.

[5] Ley 25.520 disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm.

[6] Ley 27.126 modificatoria de la Ley 25.520 disponible en http://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=243821

establecer el marco jurídico en el que desarrollen las actividades los organismos de inteligencia conforme a la Constitución Nacional, los tratados de Derechos Humanos suscriptos y los que se suscriban con posterioridad a la sanción de la ley y a toda otra norma que establezca derechos y garantías. Se establece que las tareas principales de la AFI consisten en la obtención, reunión, sistematización y análisis de la información específica referida a hechos, riesgos y conflictos que afecten la seguridad de la Nación y sus habitantes. Establece que la AFI es el órgano superior a cargo de las tareas vinculadas con las escuchas que ordenen los jueces, transfiriendo a la Procuración del Ministerio Fiscal el Sistema de Observaciones Judiciales que hasta ese momento estaba en el ámbito del Poder Ejecutivo. De esta manera, todo juez o fiscal que necesite pedir una escucha, debe dirigirse al Ministerio de la Procuración Fiscal.

La ley 25.520 crea los bancos de protección de datos y archivos de inteligencia garantizando su reserva constitucional y legal, y determina que los datos de inteligencia almacenados que no sirvan para los fines establecidos sean destruidos. Además, garantiza que no se almacene información por razones de raza, fe religiosa, acciones privadas u opinión política o de adhesión o pertenencia a organizaciones partidarias, sociales, de derechos humanos, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales o cualquier otra actividad lícita. Establece que el ámbito de trabajo de la AFI es la defensa frente a ataques externos o frente a delitos complejos por su globalización, como la trata de personas, el narcotráfico, el ciberdelito o los delitos económicos.

En términos jurídicos, la aplicación de la ley penal Argentina se rige prioritariamente por el artículo 1° del C.P.: por los delitos cometidos o cuyos efectos se producen en el territorio nacional o lugares sometidos a la jurisdicción nacional. Se tiene jurisdicción si el hecho se concreta en el país o sus efectos se producen en nuestro territorio, aunque la acción haya sido iniciada fuera de las fronteras. Esto plantea un problema jurisdiccional al momento de investigar ciertos delitos, por ejemplo, en casos donde se emplea computación en la nube (“cloud computing”) que involucra almacenamiento de información en el ciberespacio con la posibilidad que los servidores estén alojados en el extranjero (Dupuy & Kiefer, 2017, p.18).

La reforma al Código Penal por la Ley 26.388 si bien es un gran avance, no fue exhaustiva y quedan muchas conductas por revisar, como ser por ejemplo el robo de identidad, ataques de denegación de servicios, entre otros (Sain & Azzolin, 2017, p46). Otro tema también a considerar es que la legislación penal no prevé la responsabilidad penal de las personas jurídicas en materia de criminalidad informática (Dupuy & Kiefer, 2017, p.18).

Anexo 2: Metodologías adicionales de informática forense

Además de los modelos de tratamiento de la evidencia digital descriptos en el Capítulo 2, a continuación se detallan otros modelos de uso común en la metodología de la práctica forense que sentaron la base conceptual para muchos de las metodologías presentadas en este campo.

RFC 3227, Recolección y manejo de evidencias

En el año 2002 la IETF[1] formuló la RFC 327, siendo uno de los primeras en ser adoptados por la comunidad de informática forense.

El RFC[2] 3227[3] denominada "Guía para recolectar y archivar evicencia" es un estándar referente que plasma las principales guías para la recolección y el almacenamiento de evidencias digitales desde un punto de vista teórico y bastante completo.

El RFC 3227 es un estándar de facto para la recopilación de información en incidentes de seguridad, considerando muy pocos aspectos legales, que naturalmente, son particulares del ordenamiento legal de cada país.

[1] El Grupo de Trabajo de Ingeniería de Internet, representado por las siglas IETF "Internet Engineering Task Force", es una organización internacional abierta de normalización que contribuye a la ingeniería y evolución de las tecnologías de Internet. Se creó en los Estados Unidos en 1986. Es mundialmente conocido porque se trata de la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC. Es una institución sin fines de lucro y abierta a la participación de cualquier persona. Para obtener más información acceder a www.ietf.org.

[2] Los RFC "Request For Comments" son documentos que recogen propuestas de expertos en una materia concreta, con el fin de establecer por ejemplo una serie de pautas para llevar a cabo un proceso, la creación de estándares o la implantación de algún protocolo.

[3] La guía RFC 3227 puede consultarse en el enlace https://www.ietf.org/rfc/rfc3227.txt.

El proceso de recolección de este estándar hace énfasis en la aplicación de metodologías precisas de adquisición de evidencia digital, basadas en el orden de volatilidad, con el acompañamiento de documentación detallada de todo el proceso y del resguardo de la evidencia digital original evitando o reduciendo al mínimo los cambios en la información que se está recolectando.

Plantea una serie de pasos y pautas a seguir en el proceso de recolección procurando ser lo menos intrusivo posible con el fin de preservar el sistema en su estado original.

La transparencia en el trabajo del profesional forense es fundamental, los métodos y procesos aplicados deben ser reproducibles y cada decisión tomada en la extracción y tratamiento de la evidencia digital debe estar fundamentada y documentada. Se debe completar toda la documentación necesaria para luego poder reproducir con precisión los métodos usados, y que dichos métodos hayan sido evaluados y verificados por expertos independientes.

Otro punto al que el estándar presta atención es a la privacidad de las personas y la propiedad industrial, de manera de garantizar que tanto el acceso a información de carácter privado o información de una empresa sea bajo el consentimiento previo del responsable de dichos datos o mediante autorización judicial.

Modelo de Eoghan Casey

El **modelo de Eoghan Casey** fue presentado en el año 2002 y luego evolucionado en dos publicaciones posteriores en los años 2014 (Casey, Digital Evidence and Computer Crime, 2014) y 2018 (Casey , Digital Evidence and Computer Crime: Forensic Science, Comp, 2018).

El modelo de Casey sirve como referencia para procesar y examinar evidencias digitales. Se basa en los siguientes pasos principales: (Arquillo Cruz, 2007)

- Autorización y preparación.
- Identificación.
- Documentación, adquisición y conservación.

- Extracción de información y análisis.
- La reconstrucción.
- Publicación de conclusiones.

El proceso puede verse en la siguiente Figura 19, donde cada flecha indica el flujo de información, de modo que la información que obtenemos en un etapa sirve para la siguiente y viceversa. En cualquier momento se puede volver a la etapa anterior y obtener más datos. Toda la información generada se guarda como documentación que sirve para la publicación final.

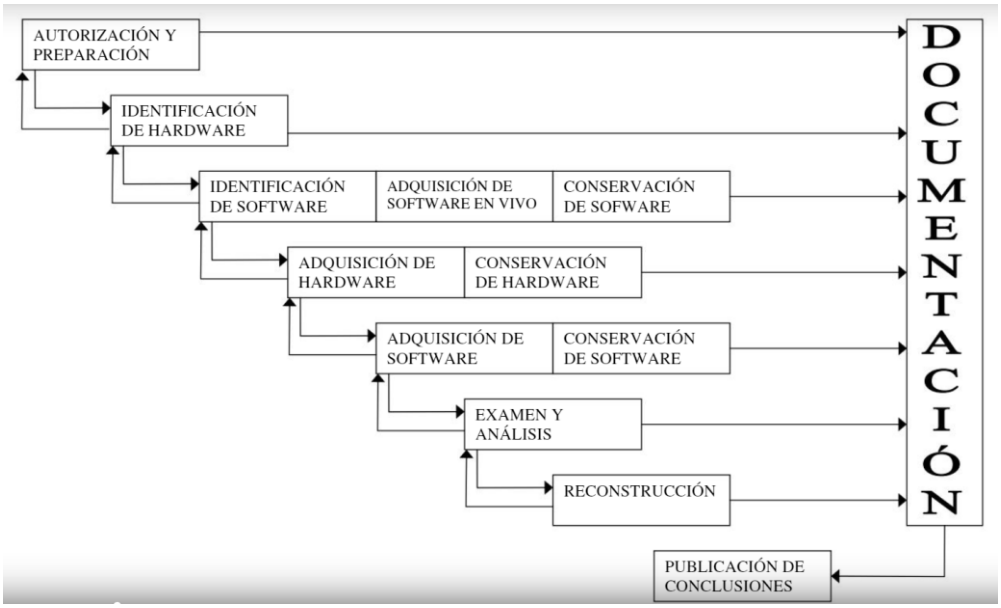

Figura 19: Modelo de Eoghan Casey

Casey señala que este proceso constituye un ciclo de procesamiento de prueba, porque al hacer la reconstrucción pueden hallarse pruebas adicionales que provoquen que el ciclo comience nuevamente. El modelo de Casey es general y se aplica exitosamente a diferentes escenarios y tecnología. (Arquillo Cruz, 2007)

Modelo del Departamento de Justicia de los Estados Unidos

El **modelo presentado por el Departamento de Justicia de los Estados Unidos en el 2001** es el más sencillo y se basa en cuatro elementos claves del

análisis forense en computadoras: Identificar, Preservar, Analizar y Presentar, como puede verse en la siguiente Figura 20: (Arquillo Cruz, 2007)

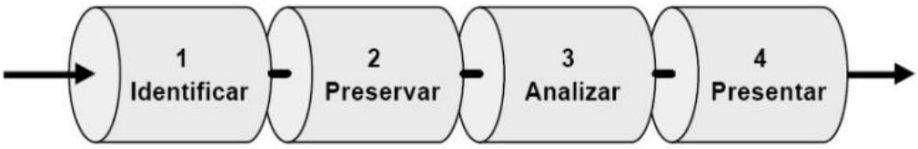

Figura 20: Modelo del Departamento de Justicia de EEUU

Modelo DFRWS

El **modelo DFRWS**[1] **("Digital Forensic Research Workshop")** del año 2001, representa los pasos del análisis forense digital en un modelo lineal, aunque se menciona la posibilidad de retroalimentación entre los pasos. Las etapas prinicipales son las marcadas en gris en la siguiente Figura 21. El modelo no se plantea como definitivo, sino como base para trabajos futuros, listando asuntos pendientes por cada uno de los pasos (Arquillo Cruz, 2007).

Identificación	Preservación	Recolección	Investigación	Análisis	Presentación	Decisión
Detección del Evento/Crimen	Gestión del caso	Preservación	Preservación	Preservación	Documentación	
Firma de resolución	Tecnologías de imágenes	Métodos Aprobados	Trazabilidad	Trazabilidad	Testimonio del experto	
Detección del perfil	Cadena de custodia	Software Aprobado	Técnicas de Validación	Estadísticas	Aclaración	
Detección de la anomalía	Sincronización del tiempo	Hardware Aprobado	Técnicas de Filtrado	Protocolos	Declaración del impacto de la Misión	
Quejas		Autoridad legal	Coincidencias de patrones	Minería de datos	Contra-medida Recomendada	
Monitoreo del Sistema		Comprensión sin pedidas	Descubrimiento de datos ocultos	Linea de tiempo	Interpretación de estadísticas	
Análisis de auditoria		Muestreo	Extracción de datos ocultos	Asociación		
Etc.		Reducción de datos		Espacial		
		Técnicas de Recuperación				

Figura 21: Modelo DFWRS

[1] Se puede consultar el modelo DFRS accediendo al enlace http://www.dfrws.org/

Anexo 3: Guías y Protocolos Nacionales

Guía de Obtención, Preservación y Tratamiento de la Evidencia Digital del Ministerio Público Fiscal (resolución PGN-0756/16)

La "Guía de obtención, preservación y tratamiento de evidencia digital" [1] es una guía aprobada bajo la resolución de la Procuración General de la Nación PGN-0756/16. La misma señala una serie de herramientas de investigación y recomendaciones utilizadas a nivel mundial como forma de reforzar la actividad del Ministerio Público Fiscal en los casos en que se cuente con evidencia digital. Concretamente, aborda el modo en el cual se debe obtener, conservar y tratar la evidencia digital para mejorar los niveles de eficiencia en materia de persecución penal, en tanto resulta ser un eje central de preocupación de la comunidad internacional para la investigación transfronteriza del delito (UFECI, 2016).

La guía compila documentación internacional sobre ciberdelincuencia y permite graficar la relevancia a nivel mundial del fenómeno de la cibercriminalidad, al tiempo que define qué es la evidencia digital, cómo debe ser obtenida, preservada y tratada para mejorar los niveles de eficiencia mínima en materia de persecución penal.

También aborda los aspectos a considerar al momento de analizar la evidencia digital obtenida, en función de cada delito que se investigue, en los que el medio informático puede resultar relevante.

Por otro lado, resalta la importancia de la auditoría y el registro fehaciente de todo el proceso relativo a la manipulación de la evidencia digital, precisando detalladamente las medidas y acciones llevadas a cabo.

La guía plantea una serie de conceptos fundamentales a tener en cuenta para la manipulación de la evidencia electrónica:

[1] La "Guía de obtención, preservación y tratamiento de evidencia digital" fue elaborada por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) a cargo del fiscal Horacio Azzolin. Se puede descargar del enlace https://www.mpf.gob.ar/resoluciones/PGN/2016/PGN-0756-2016-001.pdf.

- Principios de tratamiento de la evidencia digital con principal énfasis en evitar la contaminación de la evidencia digital.
- Tendencias del tratamiento de la cibercriminalidad a nivel mundial.
- Estandarización de procesos para enfrentar el delito trasnacional. Colaboración entre países para la resolución de esta problemática.
- Recolección y preservación de la evidencia digital, con el planteo de diversos escenarios posibles con dispositivos encendidos u apagados, computadoras en red y diversos dispositivos a tener en cuenta.
- Embalaje, traslado, resguardo, manipulación y copia de la evidencia digital.
- Manipulación idónea del hardware.
- Imagen o copia forense y uso de hash.
- Tipos de delitos y la evidencia relevante a recolectar para cada uno.

Protocolo Unificado de los Ministerios Públicos de la República Argentina

El Protocolo Unificado de los Ministerios Públicos de la República Argentina del año 2018[1] es una guía para el levantamiento y conservación de la evidencia. Constituye un conjunto de procedimientos de cómo recabar los elementos, rastros e indicios en el lugar de la escena del posible crimen y su tratamiento en el laboratorio forense (Ministerio de Justicia y Derechos Humanos, 2018).

Este protocolo fue elaborado en forma conjunta por el Programa Nacional de Criminalística del Ministerio de Justicia y Derechos Humanos, el Consejo de Procuradores, Fiscales, Defensores y Asesores Generales junto con el Consejo Federal de Política Criminal. Surge ante la diversidad de prácticas de levantamiento de la evidencia en la escena del hecho, con el objetivo de elaborar un instrumento consensuado y federal que incluyan los criterios necesarios para la recolección y tratamiento de la evidencia por parte de los laboratorios forenses.

[1] El Protocolo unificado de los ministerios públicos de la República Argentina se puede descargar desde el enlace http://www.jus.gob.ar/media/3262247/Protocolo%20unificado.pdf

Asimismo, explica minuciosamente cómo debe ejecutarse el levantamiento de la evidencia, cómo tratarla en el ámbito de los laboratorios y cómo hacerlo al momento de la autopsia. Contiene un detalle de los medios necesarios para recolectar los elementos sin contaminarlos, cómo embalarlos y luego, cómo debería estar estipulada una cadena de custodia. Debido a ello, tiene como destinatarios a quiénes deben realizar tareas en el lugar del hecho como también a quiénes deben controlar o coordinar su labor.

Resalta la importancia de la planificación previa al allanamiento con la finalidad de procurar obtener información de la infraestructura tecnológica y hardware en el lugar del hecho. Sugiere una investigación minuciosa con el objeto de identificar con precisión la ubicación y características técnicas generales de los elementos a secuestrar. Asimismo, diferencia las actividades operativas correspondientes al personal policial, siguiendo el protocolo; con respecto al profesional perito, cuya actuación principalmente es una actividad en el laboratorio y de asesoramiento científico al operador judicial responsable de la investigación penal.

Describe los principios generales para la recolección, preparación y embalaje de las evidencias digitales halladas en la escena del hecho y la debida cadena de custodia, tanto para los registros activos y volátiles, como para medios de almacenamiento masivos. Destaca la posibilidad de evitar el secuestro masivo de elementos informáticos, de manera de enviar a peritar únicamente si se tiene presunciones con un alto grado de verosimilitud de poseer la evidencia buscada.

Protocolo General de Actuación para las fuerzas policiales y de seguridad (Resolución Nro. 234/2016)

Mediante la Resolución Nro. 234/2016, el Ministerio de Seguridad de la Nación Argentina aprobó el Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos[1]. Su objetivo es establecer pautas para la recolección y el tratamiento de pruebas relativas a ciberdelitos en general. El Protocolo es de

[1] Protocolo del Ministerio de Seguridad de la Nación Argentina sobre la investigación y proceso de recolección de pruebas en Ciberdelito disponible en https://doc.segulupa.com/wp-content/uploads/resolucion-ciberdelito.pdf

aplicación obligatoria para el personal de Gendarmería Nacional Argentina, Prefectura Naval Argentina, Policía Federal Argentina y Policía de Seguridad Aeroportuaria.

El protocolo sienta los siguientes principios específicos de intervención: i) los procesos de tratamiento de la evidencia digital no podrán en ningún caso modificar el original, y antes de trabajar con una prueba original se deberá efectuar una copia forense; ii) la evidencia digital solo debe ser examinada por personal capacitado; iii) todo lo actuado en los diferentes procesos deberá estar documentado y disponible para su posterior examen (cadena de custodia); y iv) en relación con la prevención de los ciberdelitos, las fuerzas policiales y de seguridad podrán utilizar y solicitar las técnicas de investigación establecidas en los códigos y leyes especiales de la jurisdicción correspondiente, por ejemplo, para acceder a datos que tienen los proveedores de servicio de Internet, se requerirá de autorización judicial.

Adicionalmente, el protocolo instituye pautas de actuación para adecuar los procesos de denuncia, la preparación técnica previa a un allanamiento, los allanamientos en sí, el secuestro de dispositivos tecnológicos, el correcto embalaje y transporte y la extracción de pruebas a las necesidades específicas de la persecución de los ciberdelitos.

Protocolo de Actuación para Pericias Informáticasde Neuquén

El Protocolo de Actuación para Pericias Informáticas utilizado en el Poder Judicial de la Provincia del Neuquén tiene por objeto detallar la modalidad de trabajo interna para el envío de material tecnológico al laboratorio pericial. La adopción de estos lineamientos permite una correcta definición del alcance de los servicios profesionales de informática forense, contribuye a profundizar los resguardos en la cadena de custodia de la prueba, y explicita la modalidad de trabajo interno para una mejor adecuación de los requerimientos judiciales.

El protocolo detalla un procedimiento para pericias informáticas, una guía operativa para el secuestro de tecnología informática y también un instructivo para la utilización de etiquetas de seguridad sobre dispositivos informáticos.