SEPTIEMBRE 2024

DIRECTORAS
Ana Haydée Di Iorio
Marisa Repetto

INVESTIGADORES
Mario Adaro
Lucía Algieri
Pablo Cistoldi
Bruno Constanzo
Fernanda Díaz
Bibiana Luz Clara
Fernanda Rosales
Santiago Trigo

GUÍA DE ACTUACIÓN PARA LA ADQUISICIÓN, PRESERVACIÓN Y PRESENTACIÓN DE LA PRUEBA DIGITAL

INSTITUTO DE CIENCIAS FORENSES
UNIVERSIDAD FASTA
InFo-Lab
UNIVERSIDAD FASTA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
FACULTAD DE INGENIERÍA
IFITEJ
JUSLAB
UCH
UNIVERSIDAD CHAMPAGNAT

GUÍA DE ACTUACIÓN PARA LA ADQUISICIÓN, PRESERVACIÓN Y PRESENTACIÓN DE LA PRUEBA DIGITAL

Septiembre 2024

Guía de actuación para la adquisición, preservación y presentación de la prueba digital / Ana Haydée Di Iorio ... [et al.] ; Editado por Ana Haydée Di Iorio ; Mario Adaro. - 2a ed - Mar del Plata : Universidad FASTA ; Mendoza : Universidad Champagnat , 2024.
Libro digital, PDF

Archivo Digital: descarga y online
ISBN 978-631-90546-6-8

1. Seguridad Informática. 2. Derecho Procesal. 3. Derecho Informático. I. Di Iorio, Ana Haydée, ed. II. Adaro, Mario, ed.

CDD 347.064

AUTORES

DIRECTORA

Esp. Ing. Ana Haydée Di Iorio Facultad de Ingeniería de la Universidad FASTA

CODIRECTORA

Esp. Abg. Lic. Marisa Repetto Facultad de Derecho de la Universidad CHAMPAGNAT

INVESTIGADORES

Esp. Ing. Ana Haydée Di Iorio (FI UFASTA)

Ing. Santiago Trigo (FI-UFASTA),

Esp. Abg. Pablo Cistoldi (FCJyS-UFASTA, FI-UFASTA),

Ing. Bruno Constanzo (FI-UFASTA).

Lic. Lucía Algieri (FCJyS-UFASTA, FI-UFASTA)

Dra. Bibiana Luz Clara (FCJyS-UFASTA)

Esp. Ing. Fernanda Rosales (FI-UFASTA)

Facultad de Ingeniería de la Universidad FASTA - Facultad de Ciencias Jurídicas y Sociales de la Universidad FASTA

Abg. Mgter. María Fernanda Díaz (FD-UCHAMP)

Abg. Marisa Repetto (FD-UCHAMP)

Abg. Mgter Mario Adaro (FD-UCHAMP)

Facultad de Derecho de la Universidad CHAMPAGNAT

GUÍA DE ACTUACIÓN PARA LA ADQUISICIÓN, PRESERVACIÓN Y PRESENTACIÓN DE LA PRUEBA DIGITAL

A. Conceptos generales.

B. Aspectos jurídico-legales.

C. Procedimiento.

Consideraciones y problemáticas:

D. Casos de uso. Ejemplos.

Caso de uso: Exportar Contacto

Caso de Uso: WhatsApp

Caso de Uso: Telegram

5.3 Guía y Recomendaciones para el aseguramiento de información en Redes Sociales.

A. Conceptos generales.

B. Aspectos jurídico-legales.

C. Procedimiento.

Preservación de la prueba que se encuentra en un perfil público o en un contacto de la cuenta del usuario

Preservación de la prueba que se encuentra en el perfil de usuario del usuario

D. Casos de uso. Ejemplos.

Caso de Uso: Facebook

5.4 Recomendaciones para el aseguramiento de información de Sitios Web.

A. Conceptos generales.

B. Aspectos jurídico-legales.

C. Procedimientos

D. Casos de uso. Ejemplos.

Caso de uso: Preservación de un Sitio Web

Caso de Uso: Preservación de un Contenido obrante en YouTube

Caso de uso: Constatación de información de sitios web inexistentes o actualizados

5.5 Recomendaciones generales para el aseguramiento de cualquier tipo de archivos cualquiera sea su formato

6. Conclusiones y a futuro.

1. Introducción

Acerca de esta Guía de Actuación

Este trabajo es producto del Proyecto de Investigación "Desarrollo de una Guía de Recomendaciones para la Implementación de Protocolos de Actuación para la Adquisición, Preservación y Presentación de la Prueba Digital - PAFE-CCyLF", elaborado en forma conjunta entre investigadores de la Facultad de Ingeniería y de Ciencias Jurídicas y Sociales de la Universidad FASTA -integrantes del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense - InFo-Lab, e investigadores de la Facultad de Derecho de la Universidad Champagnat. En el ámbito de la Universidad FASTA el proyecto radica en la Línea de Investigación Ciencias Forenses.

La Suprema Corte de Justicia de la provincia de Mendoza y la Junta Federal de Cortes y Superiores Tribunales de las Provincias Argentinas y Ciudad Autónoma de Buenos Aires (JUFEJUS) se constituyen como instituciones adoptantes de los productos resultantes del proyecto.

Integrantes del Proyecto de investigación

El equipo técnico que desarrolló esta Guía está formado por el Grupo de Investigación en Informática Forense de la Facultad de Ingeniería (FI-UFASTA) y la Facultad de Ciencias Jurídicas y Sociales (FCJyS-UFASTA) de la Universidad FASTA e integrantes de la Facultad de Derecho de la Universidad Champagnat (FD-UCHAMP). Estuvo dirigido por la Esp. Ing. Ana Haydée Di Iorio (Facultad de Ingeniería UFASTA) y codirigido hasta marzo 2023 por la Mg. Abg. Barbara Peñaloza (FD-UCHAMP), continuando con la codirección la Esp. Abg. Marisa Repetto (FD-UCHAMP), en colaboración y diálogo directo con el Dr. Mario D, Adaro, Presidente del Instituto de Innovación, Tecnología y Justicia (IFITEJ-JUFEJUS) y Ministro de la Suprema Corte de Justicia de Mendoza.

Participaron los siguientes investigadores que son todo/as autores de la presente guía: Pablo Adrián Cistoldi (FI-UFASTA), Lucia Algieri (FCJyS-UFASTA/FI-UFASTA), Bruno Constanzo (FI-UFASTA / FCJyS-UFASTA), Santiago Trigo (FI-UFASTA), Bibiana Luz

Clara (FCJyS-UFASTA), María Fernanda Rosales (FI-UFASTA), María Fernanda Díaz (FD-UCHAMP).

Proceso de validación

Finalizada la redacción de la primera versión de la Guía, el equipo de investigación decide iniciar un proceso de validación para garantizar la calidad, la eficacia, la legitimidad y la legalidad de los procedimientos desarrollados.

Esta validación tuvo el objetivo de constatar que los procedimientos formulados fueran adecuados y contribuyeran a los fines previstos. Por otro lado, permitiría identificar los ítems que debían mejorarse o aclararse con mayor precisión o mejor calidad de ejemplos.

El proceso de validación comenzó en el mes de noviembre de 2023. Inicialmente se realizó una convocatoria abierta a través de redes sociales a abogados, escribanos, magistrados, funcionarios, operadores judiciales, peritos informáticos y demás profesionales relacionados a la actividad probatoria en procesos judiciales. También se invitó a participar a instituciones nacionales vinculadas con la temática.

Como resultado de la convocatoria se postularon más de cien profesionales para validar la guía. Además, todas aquellas instituciones que fueron invitadas y aceptaron, fueron parte del proceso de validación.

En el criterio de selección de validadores se consideraron los siguientes puntos: que la profesión sea pertinente, que hubiese distintos tipos de profesiones representadas y que hubiese diversidad de provincias en la actuación con el fin de garantizar un alcance federal. Cabe aclarar que si bien estos profesionales e instituciones validadoras no serán los únicos destinatarios finales, directos e inmediatos de la Guía, era fundamental en esta etapa contar con una visión integral, multidisciplinaria e interdisciplinaria de la Guía.

Validar la Guía, sin dudas, ha sido un proceso vital, lo que permite generar confianza sobre el producto final que será publicado, y lograr su legitimidad y adopción por parte de la comunidad.

Metodología:

Cada profesional que cumpliera con los estándares de la convocatoria podía elegir inscribirse en la cantidad de secciones de la Guía que fueran de su interés específico y/o en la que quisiera participar.

Así, a cada validador se le envió la sección de la guía a revisar según su interés al momento de la inscripción. A ello se adjuntó un formulario que debía completarse en base a su experiencia en la ejecución del procedimiento respectivo.

En el caso de las instituciones, además, se les solicitó una devolución detallada y cualitativa de la experiencia, que debía ser entregada en papel membretado y firmada por autoridades de la institución y las personas que participaron en la validación.

Resultados obtenidos:

- Participantes: promedio de 40 validadores por procedimiento.
- Representación federal: de las 24 jurisdicciones de nuestro país, 18 de ellas tuvieron representación en esta etapa (no participaron validadores de las provincias de Corrientes, San Juan, San Luis, Santa Cruz, Santiago del Estero y Tierra del Fuego).
- Perfiles: El 60% de quienes respondieron son de profesión abogado y el 40% restante se divide entre peritos informáticos e informáticos en general.
- Utilidad de la guía: según el 70% de los participantes las instrucciones que se indican en los procedimientos fueron muy útiles, para un 25% útiles y un 5% se reparte en algo útiles o nada útiles.
- Observaciones: las devoluciones de mejoras de la guía hicieron referencia principalmente al procedimiento relacionado con el sellado de tiempo, y al uso de herramientas de terceros.

Equipo de validadores:

Validadores individuales

Sergio H. Aleksinko

Alejandro Arenas

Elizabeth Armoa

Verónica Eugenia Arrueta

Damian Bes E.

Alejandro Ariel Bongiorno

Gianina Bravi

Javier Esteban Bura Peralta

Marisa Cerezoli

Lucía Victoria Contartese

Antonela D´Onofrio

Bruno Del Frari

Joaquín Del Torchio

Brenda Eldrid

Claudia Carina Espin

Guillermo Figueredo

Rene Aprile

Gaston Bielli

Marcos Fabian Galvan

Kheyla González

Nahuel Fernando Griffa Zima

Juan Heguiabehere

Maximiliano Andres Hermosilla Quiroga

Rodrigo Iglesias

Marcos Guillermo Irusta de Melo

Aimé Azul Juliá

Vanesa Krausse

Sabrina Lamperti

Romina Daniela López

Veronica Noemi Lopez Uriburu

Maximiliano Macedo

Pablo Enrique Molina

Nicolás Montefusco

Ezequiel Moreyra

Patricia Moyata

Ana Laura Nuñez

Edam Olivares

René Alejandro Parra Almirón

Natalia Poblete

Claudio Pocogsnich

Dario Alejandro Pokora

María Sol Puey

Hernan Quadri

Sabrina Andrea Quinteros

José Luis Ramón

Aldo Dario Ramos

Julieta Micaela Ríos

Agustina Romain

Marcelo Darío Rubio

Gustavo Sain

Julia Salomón

Juan Carlos Rubén Sanchez

Gaston Miguel Semprini

Miguel Angel Alfredo Traverso

Aldo Wayar

Marcela Andrea Yaverovsky

Alejandro Zen

Sergio Appendino

Fredi Aprile

Ezequiel Moreyra

René Parra

Beatriz P. de Gallo

Equipo de Seguridad TIC de la Fundación Sadosky.

Alejandro Arenas

Juan Heguiabehere

Marcela Pallero

Observatorio de Cibercrimen y Evidencia Digital en Investigaciones Criminales - OCEDIC-

Daniela Dupuy

Matias Fernandez Noguera

Agustina Débora Palencia

Diego Stratiotis

Instituciones validadoras

COPROCIER - Consejo de profesionales de ciencias informáticas de Entre Ríos

Silvia Mónica Aranguren

Cecilia Raquel Bressan

Walter Ricardo Elías

Federico Luis Losco

Hugo Daniel Orega

Waldemar Alejandro Poeti

DigiLab - UCASAL

Equipo de Comunicación, Difusión y Corrección de Estilo:

Lic. María Belén Alvarez Cestona

Lic. María Victoria Martinez Palacios

Importancia de los Protocolos, Guías y Recomendaciones

Los protocolos, guías y recomendaciones que se desarrollan en el presente documento tienen por objetivo unificar los criterios en relación a los procedimientos de adquisición, preservación y presentación de la prueba electrónica y/o digital, y se encuentran principalmente orientados a la justicia Civil, Comercial, de Familia, Laboral y Administrativo (procesos no penales).

La aparición de este tipo de pruebas en los procesos judiciales ha requerido una especial intervención de especialistas en informática para su tratamiento e investigación, con la finalidad de preservar los elementos probatorios esencialmente volátiles de manera adecuada, incorporando nuevas prácticas y herramientas a las tareas forenses.

Los protocolos, guías y recomendaciones, generalmente están compuestos de fases, actividades y tareas que procuran validar los principios forenses básicos: a) método, b) reproducibilidad del procedimiento y c) prevenir la contaminación de la prueba. Su seguimiento y/ o cumplimiento proporcionará buenas prácticas a las/los operadores del sistema de justicia con la finalidad de garantizar la validez de la metodología y del procedimiento para la obtención y manejo del material probatorio.

Es importante distinguir, a los fines didácticos de esta Guía, los conceptos de protocolo, guía y recomendación. Los protocolos son un conjunto organizado de instrucciones con un método científico, y resultan de aplicación a cuestiones que poseen cierto grado de certeza científica, o similar. Sin embargo, ciertos cambios tecnológicos más o menos disruptivos pueden desactualizarlos rápidamente o dejarlos obsoletos. La prueba adquirida, preservada y presentada observando correctamente un protocolo dotará de seguridad, explicabilidad, trazabilidad y rigor científico tanto al procedimiento como al resultado obtenido. Las guías, en cambio, son un conjunto de buenas prácticas con menor rigor científico, y desarrolladas para un contexto variable. Sin perjuicio de ello, la observancia de una guía favorecerá con un grado deseable de seguridad, trazabilidad y explicabilidad el procedimiento y el resultado obtenido en el marco de un contexto determinado. Por su parte, las recomendaciones u orientaciones son pautas, principios y valores aún más flexibles y útiles frente a los cambios tecnológicos, y resultan de utilidad para los casos más complejos, cuando ninguna “receta” resulta de ayuda.

Por último, resulta necesario aclarar que esta Guía, como un conjunto de buenas prácticas y recomendaciones, ha sido escrita, pensada y dirigida a un destinatario específico, la persona justiciable, y/o a los profesionales interdisciplinarios que la asistan según el caso, y que eventualmente acudirán al servicio de administración de justicia en pos de resolver sus conflictos. Es decir, la persona podrá -o no- contar con asesoramiento de un profesional (de la abogacía, de la informática, notarial, etc.), según sus posibilidades económicas, geográficas, tecnológicas, culturales, sociales, etarias, etc. Por tal motivo la Guía ha sido redactada en un lenguaje claro, sencillo y no estrictamente técnico (en la medida de lo posible), pues en la mayoría de los casos las personas destinatarias no son expertas en el uso y manejo de las nuevas tecnologías. Además, el término "eventualmente" no es antojadizo, sino que responde a un escenario temporal en el que esa persona necesitará adquirir y preservar prueba digital volátil que será luego presentada -o no- en un proceso judicial no penal. Es decir, al momento de la adquisición y preservación de la prueba digital no existe un juicio aún, y podrá nunca llegar a existir.

Más allá de lo expuesto, es probable y deseable que esta guía también sea una herramienta útil, para aquellos que trabajan en el sistema de administración de justicia, cualquiera sea su rol en los procesos judiciales no penales.

Mecanismos para uniformar y homogeneizar.

El creciente empleo en los procesos judiciales de variadas fuentes de prueba digital y/o electrónica exige la generación de consensos mínimos acerca de las mejores prácticas de obtención, preservación, presentación, interpretación y valoración de dichos elementos. La necesidad de procedimientos fiables y de criterios que brinden seguridad jurídica resulta, entonces, apremiante.

La búsqueda de estos consensos exige la adopción de un lenguaje común entre abogados y expertos en informática forense. Algunos conceptos y definiciones generales vertidos en esta Guía no buscan profundizar discusiones doctrinales ni puramente teóricas, sino que apuntan a lograr ese lenguaje común.

La adaptación a estas novedosas formas de prueba requiere, además, reforzar el pleno respeto de los principios básicos que regulan el servicio de justicia: la independencia y la imparcialidad del tribunal, el acceso a justicia en condiciones igualitarias, la eficaz

aproximación a la verdad, una prudente perspectiva de vulnerabilidad[1], la economía de tiempos y costos del proceso.

Por otra parte, es necesario tener en cuenta que las exigencias propias de la prueba digital, como sucede con cualquier otra clase de prueba, son altamente sensibles al tipo de caso, al rol del operador jurídico, a la regulación procesal aplicable, a los elementos de prueba disponibles, y a los recursos, urgencias y niveles de vulnerabilidad de las partes.

Por ello, el cumplimiento de los protocolos, guías y recomendaciones no asegurará un resultado infalible en todos los casos, y deberá ser analizado en el contexto concreto de cada caso.

De igual modo, la imposibilidad y/o la omisión de cumplir con algunas recomendaciones -o pasos- no siempre tendrá como consecuencia inevitable la inutilidad o ineficacia de la prueba digital obtenida. Su seguimiento, aunque sea parcial, mejorará considerablemente, y en la gran mayoría de los casos, las posibilidades de producir eficazmente la prueba digital en el proceso judicial no penal.

Es importante aclarar también que no siempre la prueba digital debe ser acompañada con un dictamen pericial informático. Poder distinguir cuándo es necesario, y cuándo no, es un desafío adicional.

En la actualidad, las fronteras entre ciencia, técnica y conocimiento ordinario son muchas veces engañosas, y cambian constantemente a través del tiempo. A ello se suman las brechas en la alfabetización digital, que merecen ser adecuadamente consideradas desde la perspectiva del acceso igualitario a la justicia. Materializar el derecho a producir y controlar prueba digital es esencial para que esa igualdad se concrete en las respuestas judiciales.

2. Fases de la Prueba Digital en el Proceso Judicial

El proceso de búsqueda, empleo y valoración de fuentes de prueba digital debe ser guiado por previsiones y criterios razonables en función del caso. Estas orientaciones generales son útiles para trabajar con cualquier fuente de prueba y para obtener una visión de conjunto sobre la totalidad del material probatorio. Por ello, permiten analizar el empleo de la

[1] 100 REGLAS DE BRASILIA SOBRE ACCESO A LA JUSTICIA DE LAS PERSONAS EN CONDICIÓN DE VULNERABILIDAD, XIV Cumbre Judicial Iberoamericana Brasilia, 2008, disponible en https://www.acnur.org/fileadmin/Documentos/BDL/2009/7037.pdf

prueba digital no sólo en sí misma, sino también como una pieza más dentro de la estrategia probatoria en cada caso concreto.

Para contribuir a organizar y agilizar esta labor, se ha elaborado una tabla que contiene tres columnas: la fase en la cual se encuentra el caso, los protagonistas que actúan y los requisitos o criterios que debe cumplir la prueba.

Las fases hacen alusión a una temporalidad del proceso en que se encuentra, adquiere, preserva, ofrece, admite, produce y valora la prueba digital.

Los sujetos o protagonistas que intervienen en esas diferentes fases cumplen roles específicos y asumen cargas diversas respecto de cada requisito de prueba y en las distintas fases del caso.

Finalmente, se propone un conjunto de requisitos que debería cumplir una prueba para ser considerada valiosa y útil en los procesos judiciales no penales, y que a un tiempo permita la búsqueda (y hallazgo) de la mejor evidencia posible dentro un contexto real y concreto de acceso a justicia.

Mediante el cuadro que a continuación se acompaña, se pretende proporcionar una ayuda rápida, de fácil lectura, para orientar el trabajo profesional. Se espera que contribuya a la identificación de problemas y exigencias propias y ajenas, y a efectuar un *check-list* rápido de los requerimientos que se consideran cumplidos o pendientes. La mayor o menor utilidad de la tabla es eminentemente práctica, y será puesta en juego al emplearla en la labor cotidiana.

Conviene tener presente que el cumplimiento de cada requisito no necesariamente se debe ponderar con la misma escala. Por ejemplo, la valoración de la licitud de una fuente de prueba es básicamente binaria, mientras que su confiabilidad admite grados o matices.

Es también importante recordar que la ponderación de los requisitos debe adecuarse a las cargas y estándares probatorios propios de cada tipo de procedimiento judicial.

Es imprescindible, además, completar la información con las especificaciones que se efectúan a lo largo de esta Guía respecto de cada tipo de fuente de prueba digital (correos electrónicos, información de redes sociales, páginas web, etc.). Si bien existen criterios técnicos comunes, los procedimientos a seguir presentan marcadas diferencias.

Fase	Protagonistas	Requisitos principales
Búsqueda	Justiciable Abogada/o Procurador/a Actuario Informático Forense	A. Admisibilidad de la fuente B. Admisibilidad del proceso de búsqueda C. Pertinencia potencial D. Suficiencia potencial E. Confiabilidad potencial F. Temporaneidad (urgencias, análisis de riesgos) G. Costos y accesibilidad H. Ventajas comparativas
Aseguramiento material (Recolección, Adquisición, Preservación)	Justiciable Abogada/o Procurador/a Escribana/o Informático Forense	A. Admisibilidad de los procesos de recolección y adquisición B. Confiabilidad del proceso de aseguramiento C. Temporaneidad D. Pertinencia E. Costos y accesibilidad F. Análisis de ventajas comparativas
Ofrecimiento y admisión	Abogado/a Juez/a	A. Admisibilidad B. Pertinencia C. Suficiencia D. Confiabilidad de la prueba, de su aseguramiento y de los medios legales para su presentación E. Temporaneidad F. Costos y accesibilidad G. Análisis de ventajas comparativas H. Análisis de la prueba de la/s otra/s parte/s I. Gestión de acuerdos conciliatorios, simplificación y/o estipulaciones probatorias
Presentación y/o Producción	Justiciable Abogado/a Experto/Perito Entidad externa Testigo Juez/Jueza	A. Revisión de los requisitos propios de la fase de ofrecimiento B. Confiabilidad (incluyendo el énfasis y la claridad adecuados) C. Control y análisis de la producción de la prueba contraria y/o de todas las partes
Alegación	Abogado/a	A. Análisis final del cumplimiento de todos los requisitos, y análisis crítico de la prueba contraria. Esto incluye: B. Elaboración y refutación de prueba indiciaria y presuncional; integración sistemática de la prueba compleja; C. Vinculación consistente entre hechos invocados, prueba invocada y consecuencias legales solicitadas. D. Ponderación acorde con los estándares probatorios vigentes.

		E. Énfasis y claridad adecuados como atributos del requisito de confiabilidad.
Valoración	Juez/a Abogado/a Tribunal	A. Análisis de la prueba producida a la luz de sus requisitos y de los estándares aplicables. B. Análisis de la prueba indiciaria y de la sistematización de prueba compleja propuestas por las partes, a la luz de sus requisitos y de los estándares aplicables. C. Determinación y fundamentación de los hechos que se consideran probados, a la luz de sus requisitos y de los estándares aplicables.

Fuente: elaboración propia

Observaciones y sugerencias

A continuación, se analizan brevemente los requisitos de la prueba propios de cada fase. Excede al alcance de esta Guía detallar los roles de cada protagonista. En resumen, es posible indicar:

a) El justiciable generalmente posee conocimiento sobre fuentes de prueba que pueden ser importantes para el caso, aunque no siempre las tiene presentes ni sabe distinguir cuáles son aptas y cuáles no.
b) El abogado tiene a su cargo proponer y desplegar una estrategia procesal. Es importante que interrogue adecuadamente al justiciable y evalúe otras pistas y posibles fuentes de información para diseñar un abordaje y una teoría del caso sólidos.
c) El experto aporta sus conocimientos y habilidades relativos a una determinada clase de fuente de información (en el caso, evidencia digital), para acceder a ella, facilitar su comprensión y/o contribuir a la apreciación probatoria. Nunca debe suplir la alegación de las partes ni la valoración judicial de la prueba.
d) El juez o tribunal tiene a su cargo, básicamente, admitir o denegar la prueba, dirigir su producción y valorarla al momento de dictar un pronunciamiento que así lo exija. Asimismo, los ordenamientos procesales suelen facultar al tribunal a ordenar por propia decisión producir prueba no ofrecida por las partes. Escapa al propósito de esta guía la discusión sobre los fundamentos, alcances, condiciones y límites de esta facultad.

Fase de Búsqueda

La finalidad básica de esta fase es la de acceder a toda la información valiosa para averiguar y/o probar determinados hechos o circunstancias, y descartar la que carece de ese valor. Esas pautas de apertura (a la información potencialmente valiosa) y de descarte (de la información potencialmente inútil o perjudicial) se aplican de forma flexible a lo largo del tiempo, en función de la mayor o menor solidez que vaya alcanzando una hipótesis sobre los hechos.

En las fases iniciales, frecuentemente se desconocen detalles importantes acerca de los hechos potencialmente controvertidos, y se ignora la postura de la parte contraria frente a cada cuestión de hecho o de prueba. Por esta razón, es importante comenzar con una búsqueda amplia (no sólo de las fuentes de prueba digital) e ir elaborando una teoría del caso, que se irá adecuando a los hallazgos y la estrategia que vaya mostrando la parte contraria. Este marco de análisis permite ir seleccionando la "mejor evidencia" para cada punto litigioso, junto con las posibles pruebas complementarias y subsidiarias.

Para ayudar en esta tarea, puede ser útil diversificar y sistematizar los interrogantes a responder. No es lo mismo decir: ¿qué necesito saber y/o probar?, que preguntarse ¿con cuáles fuentes de información podemos contar?, ¿para qué puede servir esto? o ¿cómo acceder a esa información? Es también relevante distinguir e integrar la labor de las partes, sus abogados, y eventualmente peritos y/u otros intervinientes (ej. escribanos, autoridades, etc.).

A) y B) Admisibilidad: la fuente de prueba y el procedimiento de búsqueda deben ser jurídicamente aptos para ingresar en un proceso judicial y ser valorados de modo favorable. Por razones prácticas, se otorga un sentido amplio al requisito de admisibilidad, incluyendo la licitud, la validez, la admisibilidad en sentido estricto y la eventual oponibilidad de la prueba.

C) Pertinencia: este requisito ayuda a analizar y filtrar desde la situación inicial todo aquello que no está vinculado con los hechos litigiosos. Para ir definiendo cuál fuente de prueba resulta o puede resultar pertinente, es importante lograr una interacción efectiva entre justiciable y abogado y, eventualmente, peritos, asesores técnicos y escribanos.

D) Suficiencia: como en un rompecabezas, las piezas deben encajar entre sí, sin dejar espacios en blanco. Las hipótesis sobre los hechos y circunstancias que se invocarán en un

proceso judicial deben tener un sustento probatorio. Para ir completando ese rompecabezas, es necesario precisar los alcances y límites de cada pieza o fuente de información (cuáles hechos o circunstancias concretos contribuye a averiguar o probar y cuáles no), y su vinculación con otras piezas. Es importante tener en cuenta este requisito y su utilidad para detectar cuáles elementos probatorios podrían ser superabundantes.

E) Confiabilidad: aun teniendo completo nuestro rompecabezas, puede haber piezas probatorias convincentes y otras poco creíbles. En la fase de búsqueda, el análisis de confiabilidad nos ayuda a prever el valor que podría tener la fuente digital de información: i) en sí misma; ii) en conjunto con otras pruebas; iii) en relación con la prueba que podría presentar la parte contraria y iv) en el marco de los estándares probatorios, cargas probatorias y presunciones legales aplicables según la ley. Esta evaluación es netamente anticipatoria, y podrá ir siendo reajustada de acuerdo con la evolución de las siguientes fases del proceso.

F) Temporaneidad: nos hace analizar si la prueba podrá obtenerse y/o preservarse para el momento necesario. Ello está en función de tres variables principales: i) el riesgo de eliminación o alteración de la prueba; ii) la necesidad concreta de esa prueba y iii) la urgencia de uso para el justiciable. Los niveles de urgencia de uso están relacionados con la finalidad asignada a esa prueba (averiguación, negociación, interrupción de prescripción, cumplimiento de plazos procesales, obtención de medidas cautelares, aseguramiento de prueba, sentencia definitiva). En algunos casos, si se trata de prueba imprescindible, se requerirá pasar sin demora a su aseguramiento, ya sea a través de la recolección directa de dispositivos y la adquisición y preservación de las evidencias contenidas en ellos, o mediante la solicitud de producción de prueba anticipada en un proceso judicial específico.

G) Costos previsibles y accesibilidad real de la información: junto con la temporaneidad, estas pautas permiten contextualizar la búsqueda de pruebas en el marco de la condición de cada justiciable (existencia de barreras o disparidades económicas, culturales, tecnológicas y otros factores de vulnerabilidad o desigualdad). En casos de prueba compleja y/o costosa es importante ir más allá de las pautas abstractas que suelen utilizarse, por ejemplo, para otorgar un beneficio de litigar sin gastos. Debe tenerse presente que la igualdad procesal no es sólo una garantía formal, y para que pueda hablarse de igualdad de trato, se requiere un análisis profundo y concreto de las posibles brechas y condiciones de vulnerabilidad. En lo que hace al procedimiento probatorio, la participación igualitaria en la

producción y el control de la prueba son, también, exigencias epistémicas para la determinación de los hechos probados.

H) Análisis de ventajas comparativas: se efectúa en el caso concreto, frente a otras posibles pruebas que puedan buscarse.

Dada la volatilidad que es propia de la prueba digital, esta primera fase es una de las más importantes, pues afectará la calidad de la prueba en todas las fases posteriores. Esta fase está compuesta por un conjunto de medidas destinadas a garantizar que la información digital que se pretende obtener conservará sus propiedades probatorias al momento de ser producida ante el tribunal.

Fase de Aseguramiento material (Tareas de Recolección, Adquisición, Preservación)

La fase de aseguramiento material de las fuentes de prueba y la fase de ofrecimiento no son necesariamente secuenciales ya que, en ocasiones, para acceder a la disponibilidad de esa prueba será necesario contar con una orden judicial.

A), B), C) La Admisibilidad, la confiabilidad y temporaneidad de la fase de aseguramiento están directamente relacionadas con su necesidad y eficacia para fases futuras (producción, alegación y valoración). Aquí deben ponderarse variables jurídicas y técnicas:

- a quién/es pertenece la información;
- qué tipo de información se pretende asegurar, desde el punto de vista jurídico (ej.: datos públicos, datos personales) y técnico (archivos multimedia, textos, logs, datos en memoria volátil, software, etc.)
- en cuáles dispositivos o espacios está alojada (tipo de dispositivo, alojamiento en la nube, réplicas en poder de terceros, etc.)
- cuáles son los riesgos que se pueden derivar de una demora (pérdida o alteración de elementos probatorios; obstáculos para la obtención o continuidad de medidas cautelares, etc.). De acuerdo con el tipo de caso y las cargas probatorias propias de cada régimen procesal, puede ser necesario evaluar la posibilidad de solicitar la producción de prueba anticipada.

Para que los procesos de recolección de dispositivos y de adquisición u obtención de la información digital sean confiables, se deben cumplir no sólo ciertos requisitos generales, sino también métodos adecuados para cada clase de fuente de prueba digital (ej.: correos electrónicos, intercambios en redes sociales, páginas web, filmaciones de cámaras de monitoreo, etc.), teniendo en cuenta además las características del producto o servicio que ofrece la plataforma de cada empresa proveedora del servicio en cuestión (ej.: Telegram, WhatsApp, YouTube, etc.).

En el cuerpo principal de la Guía se detallan los procedimientos recomendados para asegurar la información digital de varias de estas fuentes. Se debe tener presente que, dados el incesante dinamismo del mundo digital (mejoras y modificaciones en aplicaciones y plataformas, nuevos dispositivos y productos de software, cambios en las regulaciones legales), es imprescindible contar con información actualizada para adaptar los procedimientos en la medida que fuere necesario.

En cuanto a la confiabilidad de la preservación o aseguramiento, los recaudos específicos que se adoptan en otros tipos de procesos judiciales deben ser contemplados con una perspectiva amplia. En los casos penales, cuando se busca preservar el estado de un contenedor de información, se aplican procedimientos de cadena de custodia. Esos procedimientos deben ser adaptados a las vulnerabilidades propias de los soportes digitales (ej.: protección contra interferencias electromagnéticas, sellado de puertos del dispositivo, etc.). Otros procedimientos técnicos utilizados de forma debidamente documentada son la clonación bit a bit de dispositivos de almacenamiento, la obtención del valor hash de las copias forenses, y la creación de copias de respaldo. Las exigencias de preservación se trasladan aquí a las copias forenses. Pero cuando lo que se pretende asegurar es la información contenida en un conjunto limitado de archivos (como sucede frecuentemente en procesos no penales), los procedimientos eficaces presentan algunas diferencias. No se trata tanto de conservar las condiciones del contenedor digital, sino de asegurar la integridad y/o autenticidad de un contenido. Esto lleva a hablar de una noción orientadora más amplia, que es la de la trazabilidad de la información probatoria. Dependiendo del tipo de información cuya calidad probatoria se desea preservar, de los dispositivos en los cuales está alojada, de los recursos disponibles y del nivel de urgencia, surgirá una gama de opciones: actas de constatación de contenidos perceptibles, presencia de testigos, empleo de terceros de

confianza, intervención de peritos, añadido de fotos o impresiones de pantalla, resguardo de ejemplares idénticos recibidos o emitidos por terceros, etc.

Como opciones a explorar, empleadas en otros países, se encuentran el empleo de terceros de confianza, certificaciones en línea, intervención de letrados de la administración de justicia u otros funcionarios estatales fedatarios. Más allá de que la actuación de fedatarios judiciales o estatales presenta limitaciones técnicas similares a las de la intervención de un escribano, ha de tenerse en cuenta que su carácter gratuito reduce las barreras y brechas de acceso a la justicia. En esta línea, podrían establecerse políticas de capacitación a dichos funcionarios para realizar comprobaciones y labores que requieren cierto grado de idoneidad, pero no exigen necesariamente la intervención de peritos.

D) y E) Los parámetros de pertinencia, y especialmente de costos, ayudan a delimitar el material probatorio al momento de hallarlo (ej.: cantidad de dispositivos a recolectar, espacio de almacenamiento para copias forenses, costos y requerimientos de preservación, etc.). Ello se hará previendo el desarrollo de las siguientes fases del proceso y en el marco de la estrategia y la teoría del caso de cada una de las partes. En cuanto a los costos, es importante que los abogados hagan un cálculo realista y evalúen la eventual necesidad de solicitar el beneficio de litigar sin gastos. Si consideran necesario requerir el beneficio, deberán brindar de forma concreta y convincente las razones que lo habilitan. Del mismo modo, el Tribunal ha de evitar acudir a criterios genéricos o abstractos que impidan un efectivo acceso a la justicia.

Fase de Ofrecimiento y Admisión

En rigor de verdad, el ofrecimiento y la admisión de pruebas son dos actividades diferenciables, en función de los responsables de llevarlas a cabo. Las partes ofrecen prueba, y el tribunal las admite o deniega[2]. Sin embargo, preferimos tratarlas conjuntamente porque dichas actividades están enlazadas entre sí, ya que los ofrecimientos y objeciones de las partes son un insumo imprescindible para la decisión judicial. Por otra parte, generalmente la prueba digital documental se presentará con la demanda para su agregación, y las restantes

[2] Se agradece la observación efectuada por el Observatorio de Cibercrimen y Evidencia Digital en Investigaciones Criminales -OCEDIC- de la Universidad Austral.

pruebas digitales se ofrecerán para su posterior producción. Teniendo en cuenta los fines prácticos de esta guía y sus principales destinatarios, no se profundizará en estas distinciones.

En el momento de ofrecer la prueba se deben volver a analizar y justificar ante el Tribunal (en la medida requerida en esta etapa) el cumplimiento de todos sus requisitos. También es una ocasión propicia para analizar y, en su caso, objetar la prueba de las demás partes.

Según los casos, la prueba digital tendrá características predominantemente documentales (por ejemplo, documentos digitales o electrónicos), en otros, tendrá características más afines con la evidencia material, e incluso podemos encontrarnos ante una prueba compleja que contendrá componentes documentales y componentes de evidencia digital material. En cuanto a su presentación en juicio, también las posibilidades y combinaciones serán variadas, por ejemplo, a través de su presentación directa (documental o efectos materiales), a través de peritos, constataciones, informes, etc.

En la práctica, la prueba digital se suele ofrecer y producir habitualmente como prueba documental. No obstante, los distintos códigos procesales contienen regulaciones disímiles. Frente a la irrupción de las fuentes de prueba digitales, ya hay ordenamientos que prevén su incorporación como medios de prueba autónomos[3]. Por otro lado, en casi todos los códigos se contempla la posibilidad de introducir prueba por medios no previstos expresamente, aplicando analógicamente la regulación de los medios similares, o si esto no fuera posible, en la forma que establezca el tribunal.

En este contexto, la tarea de abogados y jueces es fundamental para lograr, en cada caso, la mejor manera de incorporar y producir la prueba digital. La forma en que la prueba sea ofrecida en el proceso, especialmente si la prueba es documental, y el cumplimiento de la normativa procesal local en cuanto a los momentos en que debe producirse esa prueba, impactarán en su eventual admisión o no por parte del juez.

Además, gran parte del material probatorio sobre prueba electrónica a incorporarse al proceso va a encontrarse bajo la órbita de la prueba preconstituida. Esto significa que tales elementos de prueba han sido generados con anterioridad al inicio del juicio y sin participación de la parte contraria o el juez. Ello deberá ser considerado por los profesionales

[3] Ver, por ejemplo, el art. 47 de la ley 15.057 de procedimiento laboral bonaerense, o el art. 299 de la Ley de Enjuiciamiento Civil española

de la abogacía para entender mejor la naturaleza y el manejo de estas pruebas, y por los jueces, para valorarlas adecuadamente.

A) Una de las diferencias entre la prueba judicial y las pruebas históricas es que la primera posee un conjunto de filtros normativos. En esta fase, las diferencias entre una y otra comienzan a advertirse con mayor nitidez. Aquí no sólo se ha de evitar ofrecer prueba ilícita. Deben respetarse, también, los plazos, formas y demás cargas y límites legales, para asegurar que la prueba sea admitida y no existan impedimentos legales para su valoración a favor de quien la propone. Asimismo, en la etapa de ofrecimiento y admisión comienza para los abogados, la tarea de controlar y/o impugnar la admisibilidad de la prueba que ofrece la contraparte.

Corresponde a los jueces equilibrar la observancia de estos filtros legales con la garantía de acceso igualitario a la justicia, especialmente para quienes se ven afectados por una o más condiciones de vulnerabilidad (género, discapacidad, edad, situación socioeconómica, etc.).

B) Dependiendo del tipo de proceso, la pertinencia puede verse afectada por la postura de la contraparte (ej.: reconocimiento de ciertos hechos, impugnación de determinadas pruebas, etc.). Para los abogados, una posible estrategia para hacer frente a esta incertidumbre puede consistir en proponer acuerdos probatorios y ofrecer prueba principal (para los hechos previsiblemente controvertidos) y prueba subsidiaria (para el caso de que la contraparte niegue otros hechos o impugne ciertas pruebas). Jueces y abogados deben prestar atención a este requisito, ya que no sólo existe el riesgo de pérdida de prueba necesaria. Un criterio muy amplio o laxo puede generar mayores costos y demoras en el proceso. La prueba no pertinente y sobreabundante, además, puede producir ambigüedad y generar error judicial.

C) El análisis de suficiencia puede llevar a buscar pruebas complementarias relativas al punto o puntos que se desea probar mediante la prueba digital.

D) El análisis de confiabilidad debe abarcar la confiabilidad: 1) de la fuente probatoria, 2) de su aseguramiento, 3) del medio o medios legales escogidos para presentarla (documental, informativa, pericial y/o testimonial, etc..) y 4) del proceso de producción de la misma. Todo ello se ha de evaluar en el marco de las fortalezas o debilidades probatorias propias y de la contraparte, de las regulaciones procesales específicas y de los estándares de prueba aplicables.

Por ejemplo, puede ser necesario o no designar un perito de parte con determinado nivel de experticia o con conocimientos especiales en un área de la informática. La elección y redacción de los puntos periciales, la coordinación con los peritos, la preparación de interrogatorios de testigos y los pedidos de informes a proveedores de servicios de internet, la presentación adicional de impresiones de pantalla, actas notariales o testigos, entre otras alternativas, pueden tener efectos determinantes sobre la confiabilidad de la prueba.

F) Deben estimarse con mayor precisión los costos y preverse la posibilidad real de asumirlos o de obtener su exención.

G) Puede ser conveniente volver a analizar las ventajas y desventajas comparativas de cada fuente de prueba, al momento de decidir su ofrecimiento -por ejemplo, presentando prueba principal y subsidiaria-, y al sostenerlo o modificarlo si la ley procesal prevé la realización de audiencia preliminar.

H) Los abogados/abogadas deben analizar las pruebas ofrecidas por la parte contraria, para prever sus fortalezas y debilidades (análisis FODA de la teoría del caso). Por su parte, el tribunal analizará los ofrecimientos de prueba de todas las partes para precisar la que será admisible y, en su caso, proponer acercamientos, acuerdos probatorios y formas de simplificación procesal. Un punto no menor es la elección judicial (consensuada con las partes y/o según la normativa procesal local lo disponga) de los expertos/peritos que sean idóneos para el caso concreto y la selección del material probatorio a presentar y/o examinar.

I) Las pruebas ofrecidas por las partes dan ocasión a conversaciones y previsiones más realistas sobre el resultado futuro del litigio. Esto posibilita la búsqueda de acuerdos conciliatorios o transaccionales, la simplificación probatoria y/o las estipulaciones sobre determinados hechos. El tribunal, por su lado, tiene oportunidad de depurar las cuestiones controvertidas, simplificar y agilizar el procedimiento, y sostener las condiciones de igualdad de las partes.

Fase de Presentación y/o Producción

La fase de presentación y producción puede tener distintas modalidades y subfases. Por ejemplo: producción de dictámenes, presentación pericial en audiencia, reconocimiento de evidencias por testigos, etc.

A) Los requisitos de la prueba deben cumplirse en el momento de su presentación y/o producción, de lo contrario, todos los esfuerzos anteriores carecerán de sentido.

B) El proceso de producción de prueba debe ser confiable, y transparentar el grado de confiabilidad de las fuentes de información probatoria. Los abogados tienen a su cargo la organización y vigilancia de la producción de su propia prueba. Deben actuar de forma coordinada con los peritos o consultores y estar atentos a las circunstancias que sobrevengan en la fase de producción de la prueba, para mantener un margen de acción frente a situaciones imprevistas. Han de lograr, asimismo, captar la plena atención del tribunal sobre las cuestiones más importantes, y despejar cualquier ambigüedad o dificultad que presente la percepción, comprensión e interpretación de la prueba.

C) Cada abogado debe ejercer el control de la prueba producida por la parte contraria, en el momento de leer informes escritos o durante las presentaciones orales de testigos y peritos. La calidad de esta interacción pone al Tribunal en mejores condiciones para ponderar la calidad de la prueba. Por su parte, el Tribunal debe controlar todo el proceso de producción de prueba, como asimismo registrar e interpretar fielmente la prueba que va produciéndose, tanto en lo que hace a su contenido como a su peso probatorio.

Fase de Alegación

El alegato es un borrador o un esquema de sentencia, que cada parte propone al tribunal de acuerdo con su teoría del caso.

A) Se debe justificar en qué medida la prueba producida cumplió con los requisitos de una prueba eficaz, asumiendo en caso de ser necesario sus puntos débiles. Del mismo modo, se debe efectuar una crítica razonada de la eficacia de la prueba contraria, asumiendo, eventualmente, sus puntos irrefutables.

B) La elaboración de prueba indiciaria a través de hechos secundarios comprobados debe ser sólida. En cuanto a lo que indican los distintos elementos de prueba digital, parece necesario un desarrollo de máximas de la experiencia consistentes y fiables. Ello se ha de complementar con la identificación e invocación de las presunciones que pudieran ser aplicables al caso. Asimismo, aquellos puntos que han requerido la producción de prueba

compleja exigen una integración lógica y sistemática de la información presentada a través de distintos medios de prueba.

C) El énfasis en las cuestiones más importantes ayuda al tribunal a darles la relevancia que merecen y no pasarlas por alto. La claridad del análisis de la prueba y de su vinculación con la pretensión es clave para que dicha prueba sea adecuadamente comprendida por el tribunal.

Fase de Valoración

Los requisitos y los estándares legales se aplican en cada subfase de la valoración de la prueba (pronunciamiento de grado, recursos, sentencias revisoras)

A) Se aplican a todos los hechos primarios (los que son objeto de los relatos de las partes y tienen consecuencias jurídicas), y a los hechos secundarios (que sirven como base para la prueba indiciaria, o que sirven para fortalecer la prueba de los hechos directos).

B) A partir de los hechos secundarios (utilizados para elaborar prueba indiciaria) que estén debidamente probados y sean pertinentes, se debe examinar la prueba indiciaria propuesta por las partes, a fin de determinar su eficacia. En este punto, es importante ir delimitando el grado de certeza empírica de las máximas de la experiencia que sugieren las partes. Del mismo modo, se debe ponderar la fuerza probatoria de los conjuntos de pruebas complejas. La fundamentación del pronunciamiento debe ser efectuada de modo tal que pueda resistir la eventual actividad recursiva de las partes.

C) El resultado del análisis de los puntos anteriores debe estar volcado en el pronunciamiento del Tribunal. En cuanto a la labor recursiva, la crítica razonada del fallo debe ser acompañada de la solución propuesta y de su fundamento probatorio. Dependiendo de la instancia revisora y del tipo de recurso, será suficiente el control del razonamiento probatorio desplegado por el tribunal de grado o se requerirá también la valoración de la prueba producida.

3.Principios Generales de la Prueba Digital

¿Qué es la prueba?

Palabras como “prueba”, “evidencia”, “documento” o “instrumento” suelen tener distintos significados según el contexto y el ámbito en que se las utiliza. En esta Guía no se busca proponer un sentido “correcto” para estos términos, sino que se procura emplearlos de un modo que facilite la comprensión y la ejecución de las tareas de adquisición, preservación y presentación de los elementos probatorios digitales, que eventualmente serán aportados a un proceso judicial no penal.

Lo que en lenguaje coloquial entendemos como “prueba” o “pruebas” de algo, no es lo mismo que el concepto de prueba judicial. En la vida cotidiana, “descubrimos” o alguien “presenta” una prueba que nos convence acerca de algo. En un litigio judicial, en cambio, el sentido de la palabra prueba va a depender del contexto en el que se la utilice.

“La noción de prueba está presente en todas las manifestaciones de la vida humana. De ahí que exista una noción ordinaria o vulgar de la prueba, al lado de una noción técnica, y que ésta varíe según la clase de actividad o de ciencia a que se aplique. Pero es en las ciencias y actividades reconstructivas donde la noción de la prueba adquiere un sentido preciso y especial, que en sustancia es el mismo que tiene en el derecho. El jurista reconstruye el pasado, para conocer quién tiene la razón en el presente y también para regular con más acierto las conductas futuras de los asociados en nuevas leyes; el historiador, el arqueólogo, el lingüista, etcétera, lo hacen no sólo para informar y valorar los hechos pasados sino para comprender mejor los actuales y calcular los futuros”.[4]

Etimológicamente, el vocablo prueba deriva de la voz latina *probus*, que significa bueno, honrado; ergo lo que resulta probado es bueno, es correcto, es auténtico[5].

La Real Academia Española define a la prueba como la razón, argumento, instrumento u otro medio con que se pretende mostrar y hacer patente la verdad o falsedad de algo. Indicio, señal o muestra que se da de algo[6].

[4] DEVIS ECHANDIA, H., 2000, Compendio de la Prueba Judicial, Rubinzal Culzoni, Buenos Aires, p. 13/14.
[5] ARAZI, R., 2008, La prueba en el proceso civil, Rubinzal-Culzoni. Santa Fe.. p. 18
[6] Real Academia Española, Prueba, disponible en: https://dle.rae.es/prueba

Para Palacio, “la expresión prueba denota esa peculiar actividad que corresponde desplegar durante el transcurso del proceso y que tiende a la finalidad mencionada. Pero también abarca, por un lado, el conjunto de modos u operaciones (medios de prueba) del que se extraen, a raíz de la fuente que proporcionan, el motivo o motivos generadores de la convicción judicial (argumentos de prueba), y, por otro lado, el hecho mismo de esa convicción, o sea el resultado de la actividad probatoria. En ánimo de formular un concepto comprensivo de todas esas significaciones puede decirse que la prueba es la actividad procesal, realizada con el auxilio de los medios establecidos por la ley, y tendiente a crear la convicción judicial sobre la existencia o inexistencia de los hechos afirmados por las partes como fundamento de sus pretensiones o defensas”.[7]

Couture desarrolla el concepto en su dinámica procesal. Explica que, en tanto objeto de la prueba, los hechos y los actos jurídicos son objeto de afirmación o negación en el proceso. El juez es normalmente ajeno a esos hechos sobre los cuales debe pronunciarse, por lo que no puede pasar por las simples manifestaciones de las partes, y debe disponer de medios para verificar la exactitud de esas proposiciones con el objeto de formarse convicción a su respecto. Dice Couture: “... tomada en su sentido procesal la prueba es, en consecuencia, un medio de verificación de las proposiciones que los litigantes formulan en el juicio”.[8]

Según Devis Echandía, “entendemos por pruebas judiciales el conjunto de reglas que regulan la admisión, producción, asunción y valoración de los diversos medios que pueden emplearse para llevar al juez la convicción sobre los hechos que interesan al proceso”.[9]

La evidencia y la prueba.

Por influencia de la voz inglesa *evidence*, cada vez es más frecuente el uso del vocablo evidencia como sinónimo de prueba.

Si bien no es aconsejable el uso de la palabra evidencia como sinónimo de prueba -en sentido estricto-, en esta guía eventualmente utilizaremos el término evidencia como prueba en un sentido amplio, especialmente al tratar las fases de búsqueda y aseguramiento.

[7] PALACIOS, L. E., 2000, Manual de Derecho Procesal civil, Abeledo Perrot, Buenos Aires, p. 392.
[8] COUTURE, E, 1958, “Fundamentos del derecho procesal civil. Depalma, Buenos Aires, p. 217.
[9] DEVIS ECHANDIA, H., 2000, Compendio de la Prueba Judicial, Rubinzal Culzoni, Buenos Aires, p. 13/14.

La tecnología en los procesos judiciales.

Desde siempre el proceso probatorio ha estado vinculado estrechamente con la tecnología. Un claro ejemplo es el impacto que tuvo la incorporación de la fotografía como medio de prueba a finales del Siglo XIX, o cuando Vucetich logró en 1891 las primeras fichas dactilares del mundo con las huellas de 23 procesados, para luego concluir que en las impresiones digitales se hallaba la única solución integral a la problemática de la identificación humana[10].

En los últimos años la tecnología trajo a la vida en general, y a los procesos judiciales en particular, cambios y avances radicales con nuevas dificultades y desafíos.

Con mayor o menor profundidad, las nuevas tecnologías de la información y la comunicación (NTIC) atraviesan esta época, y esta realidad también se manifiesta en los procesos judiciales. De la mano de las NTIC, aparecen no sólo clases y formas de conflictos que hace unas pocas décadas no existían, sino también nuevas posibilidades y desafíos en materia probatoria.

¿Qué es la prueba digital?

Según la Guía de obtención, preservación y tratamiento de la evidencia digital [11], la evidencia digital es el conjunto de datos e información, relevantes para una investigación, que se encuentra almacenada en o es transmitida por una computadora o dispositivo electrónico.

Al poner el foco en las distintas y múltiples formas en las que lo digital se manifiesta en el ámbito de la prueba judicial, aparece la necesidad de encontrar un nombre que las abarque. Para ello, para la redacción de esta guía se ha escogido el término prueba digital.

La convención prueba digital permitirá saber de qué se está hablando, sin necesidad -al menos por un tiempo- de salir a buscar nuevos nombres en un campo donde constantemente aparecen novedades. Tal vez este rótulo pueda parecer vago o difuso, y está bien que así sea, ya que las fronteras de las NTIC están en constante expansión.

[10] GARCIA FERRARI . M., 2016,El gabinete de Juan Vucetich: un laboratorio de experimentación. La Plata, Argentina: 1891-1901". E.I.A.L., Vol. 27 – No 2.

[11] La "Guía de obtención, preservación y tratamiento de la evidencia digital" fue aprobada por Resolución de la Procuración General de la Nación N° 756/2016, con el fin de recomendar a todos/as los/as magistrados/as del Ministerio Público Fiscal que ajusten su proceder a los lineamientos de este documento en todos los casos en que resulte aplicable, disponible en https://www.mpf.gob.ar/ufeci/enlaces/protocolos-y-guias-de-actuacion/.

Se trata de eludir la tentación de teorizar en la búsqueda de definiciones precisas. Esto podría llevar a discusiones interminables que no son objeto de esta guía. También se procura no atarse a las particularidades que pueda presentar un determinado fuero o un ordenamiento procesal específico, porque eso llevaría a tener tantos conceptos como fueros y códigos existan.

Del mismo modo, buscamos un término que pueda ser medianamente aceptable tanto para quienes ejercen la abogacía como para especialistas del área informática, y que de este modo nos ayude a construir un lenguaje común.

La sociedad, las y los justiciables y quienes trabajan en el sistema de justicia necesitamos respuestas frente a los crecientes desafíos que las NTIC presentan en materia de prueba.

Por eso, buscamos que el término y el concepto de prueba digital sean prácticos, sencillos y útiles. Aclaramos también que la elección del término prueba digital no invalida el empleo de otros como "prueba electrónica" o "prueba informática", tratándose simplemente de la opción escogida por consenso del equipo.

Prueba Digital. Conceptos y Alcances

Digital es un adjetivo referido a un dispositivo o sistema que crea, presenta, transporta o almacena información mediante la combinación de bits (cf. Diccionario de la Lengua Española, ed. 2022).

Mediante el concepto de prueba digital pretendemos abarcar las diversas modalidades en las que "lo digital" aparece en el ámbito probatorio, ya sea como fuente de prueba, o como componente de distintas formas de producción o presentación de pruebas.

En efecto:

1. En muchos casos, tendrá características predominantemente documentales (por ejemplo, documentos digitales o electrónicos), aunque en otros tendrá rasgos más afines con la evidencia material, e incluso podemos encontrarnos ante una prueba compleja que contendrá componentes documentales y componentes de evidencia digital material. En cuanto a su presentación en juicio, también las posibilidades y combinaciones serán variadas,

por ejemplo, a través de su presentación directa (documental o efectos materiales), a través de peritos, constataciones, informes, etc.

2. Los dispositivos y sistemas digitales pueden también integrar complejos procesos de producción de prueba, por ejemplo, la prueba pericial. Y también es posible pensar en herramientas de inteligencia artificial para la producción de pruebas estadísticas o predictivas.

3. El uso de tecnologías digitales también permite optimizar la presentación de otras pruebas. Por ejemplo, las técnicas de mejora de imagen, audio o video procesan información preexistente para adecuarlas a las capacidades y límites de la percepción humana. Las imágenes 360 y las reconstrucciones virtuales son otras formas de facilitar la representación mental de una escena y/o secuencia. La graficación e interrelación visual de grandes volúmenes de datos son medios que pueden tener enorme utilidad para permitir la comprensión sintética y/o intuitiva de fenómenos complejos. Lo que unifica este conjunto heterogéneo de fuentes de prueba, componentes de producción de prueba y herramientas de presentación de pruebas es, precisamente lo digital.

Desde lo conceptual, cada una de estas modalidades presenta desafíos prácticos y jurídicos diferenciados, pero en la realidad del trabajo cotidiano, la prueba digital muchas veces aparece combinando características de más de una categoría. Sin embargo, este tipo de procedimientos suele requerir del auxilio de expertos. Tanto las oportunidades que ofrecen como los requisitos y técnicas requeridos para su presentación exceden los objetivos específicos de esta guía.

Características de la prueba digital.

Una de las características principales de la evidencia digital, y que la torna compleja en sí misma, es su volatilidad. Ello conlleva a que, por su propia naturaleza, sea frágil, fácil de alterar y dañar o directamente de destruir.

Si la evidencia digital puede ser contaminada, adulterada o eliminada muy fácilmente, la metodología que utilicemos para la identificación, recolección, obtención y preservación de la información será crucial para que la evidencia digital pueda ser utilizada con eficacia en el proceso judicial (prueba en sentido estricto).

Con esta finalidad se han elaborado una serie de principios forenses que deberemos considerar (InfoLab. 2022: 1m53s):

● Evitar la contaminación: Significa que la evidencia se mantiene inalterable, desde el momento en el que fue producida y recolectada.

● Integridad de la prueba: Si bien en los procesos judiciales no penales no podemos hablar técnicamente de cadena de custodia, será importante controlar y cumplir -en la medida de lo posible- las recomendaciones en el procedimiento desde que la prueba es recolectada hasta que llega a su destino final, y así garantizar una suerte de "cadena de valor probatorio": la mejor prueba posible para el caso concreto.

● Actuar metódicamente: En todo momento debe actuarse por medio de un método o proceso para poder reconstruir el camino. Tiene que haber un método para la recolección, conservación y posterior análisis de esa prueba.

A más de lo expuesto, "de acuerdo con la ISO/IEC 27037:2012 la evidencia digital es gobernada por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital, bien ésta sea utilizada para que sea admisible en corte o no.

- La relevancia es una condición técnicamente jurídica, que hace referencia a aquellos elementos que son significativos 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.
- La confiabilidad busca que en el proceso aplicado para obtener evidencia digital se puedan validar la repetibilidad y auditabilidad, es decir, que la evidencia que se obtiene es lo que debería ser y que, si un tercero sigue el mismo proceso, deberá obtener los mismos resultados verificables y comprobables.
- La suficiencia, está relacionada con la completitud de la evidencia digital, es decir que, con las evidencias que se recolectaron y analizaron se tiene suficientes

elementos para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada" [12]

Si bien puede haber otros elementos que ayuden en el gobierno de la evidencia digital, ISO ha determinado que estos tres 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 y sometidos a contradicción según el ordenamiento jurídico donde se encuentren[13].

Especialistas en informática forense asimilan la evidencia digital a la evidencia de ADN o de los rastros papilares, por ser un tipo de prueba latente.

Esta evidencia en su estado natural, no nos deja entrever qué información contiene en su interior. Resultará ineludible examinarla a través de instrumentos y procesos forenses específicos. En este sentido resulta importante distinguir el continente digital de su contenido perceptible o cognoscible (por ej. la evidencia + valor de registro; evidencia + valor documental; etc.). Es así que la producción de la prueba consistirá en hacer perceptible, comprensible y convincente la información contenida en formato digital.

[12] ROSALES, María Fernanda, 2021, "Guía de recomendaciones para la preservación de la prueba sobre el uso y acceso a los Sistemas de Información en un entorno corporativo, UFASTA-Facultad de Ingeniería, trabajo final Especialización en Informática forense.

[13] La "Guía de obtención, preservación y tratamiento de la evidencia digital" fue aprobada por Resolución de la Procuración General de la Nación N° 756/2016, disponible en https://www.mpf.gob.ar/ufeci/enlaces/protocolos-y-guias-de-actuacion/.

4. Recomendaciones generales para el aseguramiento material de la Prueba Digital.

Es importante considerar que los aspectos técnicos de estas recomendaciones deben ser revisados periódicamente y en un corto plazo, dado que este documento, consistente en un paso a paso, está previsto de acuerdo a las características y funcionalidades de las aplicaciones más populares en la actualidad.

Actuación Metodológica

La actuación sobre la prueba digital, tal como se plantea en la Tabla de Fases del punto 2, es posible dividirla en dos momentos claves.

Un primer momento que abarca desde la fase de aseguramiento hasta la fase de ofrecimiento y admisión, denominada etapa **de aseguramiento pre-judicial** y un segundo momento, desde el ofrecimiento y admisión hasta la producción y/o presentación ante el juez, denominada **etapa de aseguramiento judicial**

- **Etapa de aseguramiento PRE-JUDICIAL:** Desde la adquisición de la prueba hasta el ofrecimiento y admisión de la prueba en la causa (para más detalle ver la Tabla de Fases en Punto 2):

  Recomendaciones **<u>previas a la adquisición</u>**:

  - En la medida de lo posible no usar el dispositivo que tiene alojada la evidencia digital a preservar.
  - Pese a no ser un camino explorado, podría evaluarse como medida previa extrajudicial -o eventualmente judicial- en caso de que la prueba digital esté alojada en los servidores de un tercero, enviar un requerimiento de preservación en calidad de depositario o hacer saber que es un documento que podrá ser utilizado como prueba en un proceso judicial (arts. 255 y 294 del Código Penal, en su caso, art 9 Ley 25.326 Datos Personales).
  - Evitar demoras en la extracción.
  - Realizar un backup de la información para evitar pérdidas, priorizando los casos donde la información está en un único dispositivo y/o cuenta.
  - **Se sugiere no modificar el formato original de la prueba a presentar.**

- En caso de ser posible, al elegir el formato en el cual realizar la descarga de la prueba digital se debe procurar seleccionar un formato universal.
- De no ser posible seleccionar el formato en el cual realizar la descarga, efectuarla en el formato previsto, documentando detalladamente el nombre de la aplicación de ORIGEN del cual se realiza la descarga y su n° de versión.
- Según las posibilidades y necesidades del usuario, podrá convocar a un escribano o funcionario fedatario durante el proceso de adquisición de la prueba digital, y/o a un especialista informático forense *(ver apartado especial de actas notariales, y sobre intervención del informático)*.

Recomendaciones posteriores a la adquisición:

- En caso de ser posible, realizar al menos 2 (dos) copias y almacenar cada una de estas de manera independiente en diferentes lugares físicos. Por ej: una en manos de la parte y otra en poder del profesional (ej. abogado, informático).
- Resguardar en un documento adjunto a la copia en el mismo medio de preservación: Nombre y número de versión de la aplicación ORIGEN desde la cual se realizó la extracción, Función Hash utilizada (SHA1, MD5, etc.), Valor Hash resultante, Fecha y hora.
- Según las posibilidades y necesidades del usuario, podrá convocar a un escribano o funcionario fedatario durante el proceso de adquisición de la prueba digital, y/o a un especialista informático *(ver apartado especial de actas notariales, y sobre intervención del informático)*.
- Cabe recordar que la prueba digital recolectada, por su característica, debe viajar por un soporte acorde a la misma. No tiene sentido imprimir las evidencias y plasmarlas en un papel. Pueden ser útiles a modo de ejemplo, pero no es la forma adecuada para su presentación.

- **Etapa de Aseguramiento Judicial** -Desde el ofrecimiento y admisión hasta la producción y/o presentación ante el juez:
  - Para la acreditación de su integridad y autenticidad, es determinante presentar la prueba digital de manera completa con su respectivo respaldo y la descripción de los elementos que permiten realizar esta verificación.

- Entregar la prueba digital por el medio más adecuado, y respetando las normas de procedimiento junto a documento que acredite dicha entrega.
- Informar al Juzgado o Tribunal, y ofrecer colaboración para la presentación de la prueba digital, en caso de tratarse de un formato específico no universal, que pudiera no tener a disposición el organismo.
- Proponer y poner a disposición los softwares alternativos compatibles que permitan reproducir la prueba digital en el formato presentado.

Para todo ello, podemos utilizar la metodología utilizada por el Ministerio Público Fiscal de la Provincia de Buenos Aires, la cual consta de 5 fases primordiales como muestra la siguiente figura:

Pasos metodológicos sin herramientas forenses

Fuente: elaboración propia

Es importante destacar que la información digital que se desea preservar es muy variada, y por ello es necesario contar con pasos metodológicos que puedan contemplar este tipo de información tan disímil. A continuación, se explicará brevemente en qué consiste cada una de las fases propuestas:

- **Análisis de escenario:** básicamente refiere al estudio necesario que se debe llevar a cabo para contemplar las diferentes posibilidades de extracción de información digital con las que se cuenta. Durante el desarrollo de la presente guía, se irán mencionando las formas en las cuales se puede presentar este tipo de información y su posibilidad de extracción.

- **Descarga de información:** una vez que se sabe la forma más adecuada de extracción, se procede a realizar la descarga y almacenamiento de la información digital. También y durante el desarrollo de la presente guía, se mencionan las técnicas más adecuadas de extracción dependiendo el caso.

- **Compresión:** Es la utilización de un software para comprimir toda la información digital que se obtuvo en la fase de "Descarga de Información". De esta forma, se

genera un único archivo que contiene toda la información resguardada y, por otro lado, hace más sencillo el procedimiento de la siguiente fase. Se recomienda utilizar el programa 7zip. Este programa de libre desarrollo sirve para comprimir archivos o carpetas. De lo contrario, si no se realiza esta compresión, habría que realizar el proceso de la siguiente vez por cada archivo con el que se cuente.

- **Hash:** es el proceso por el cual se calcula el valor de hash por cada uno de los archivos que se desean resguardar para el proceso y el cual es detallado en el acta o informe (fase siguiente). Mediante esta técnica se puede garantizar la integridad de los archivos preservados. Esta fase también podría contener el sellado de tiempo. Si durante el proceso, alguno de los archivos preservados, presentara una alteración en su valor de hash, significa que dicho archivo sufrió una modificación y no es el mismo que se obtuvo el día de la preservación del mismo. Algunas aplicaciones que se pueden utilizar para generar códigos hash son:

    - **HashMyFiles:** Es un programa portable que permite la generación de hashes en forma masiva. Permite seleccionar más de un archivo a la vez, generando los hashes para cada uno. Soporta los algoritmos SHA (todas sus variantes) y CRC32. Es compatible con Windows a partir de la versión 2000. (En línea: https://www.nirsoft.net/utils/hash_my_files.html).

    - **QuickHash:** Es un programa de código abierto multiplataforma (disponible para Windows, Mac y Linux). Es muy completo. Soporta los algoritmos populares como por ejemplo MD5 y SHA2-256. (En línea: https://www.quickhash-gui.org/).

- **El informe:** es el documento que detalla todas las actividades y evidencias recolectadas en este proceso de adquisición y preservación. Decimos informe y no acta porque este documento será elaborado, en la mayoría de los casos, en forma previa a la eventual existencia de un proceso judicial. El objetivo de elaborar un informe es generar un documento complementario y accesorio a la recolección de la prueba digital, en el que quede una constancia (o, mejor dicho, un recordatorio) de los pasos realizados por el usuario, y que eventualmente será presentado en un proceso judicial. En ese informe el usuario, o bien el profesional que lo asista, describe si se cumplió -o no- todos los pasos que se encuentran sugeridos en esta guía según cada

uno de los procedimientos, de manera tal de dotar de explicabilidad al proceso de recolección y preservación realizado. Se enumeran a continuación los datos que debería contener el informe, cualquiera sea la evidencia a resguardar:

a) Fecha y hora de la recolección de la evidencia digital
b) Datos personales del aportante de la evidencia digital: Nombre y apellido, DNI, domicilio, localidad, provincia, número de teléfono, mail.
c) Todas las actividades llevadas a cabo explicadas de la forma más minuciosa posible. Para ello se recomienda al usuario consultar la guía de pasos que se encuentran en el procedimiento que va a realizar, y describir cuáles ha podido cumplir y cuáles no (en este último caso, los motivos de su no cumplimiento).
d) Listado de todos los archivos que se preservan con su correspondiente hash. El valor hash siempre debe ser incorporado en este informe, impreso en papel o firmado digitalmente, nunca enviarse como archivo de texto por el mismo medio en que es transportado el archivo de mensaje de correo propiamente dicho.
e) Medio en el que se almacenan los archivos.

En cada uno de los procedimientos en particular, se indicará qué información deberá adicionarse al informe.

Algunas aclaraciones sobre la prueba digital y la intervención del Informático Forense

Esta Guía fue desarrollada para que un usuario sin conocimientos informáticos forenses pueda preservar información en caso de urgencia y/o necesidad.

En caso de que las siguientes recomendaciones no puedan llevarse a cabo o bien se requieran de conocimientos específicos propios de la actividad informática forense debido a la complejidad del caso, será preciso recurrir a un especialista en la materia.

Algunas aclaraciones sobre la prueba digital y las actas notariales.

En la práctica tribunalicia a menudo observamos que la información vinculada a la prueba digital no sólo está plasmada en un documento o informe, sino en ciertos y determinados tipos de documentos: las actas de constatación o comprobación.

La parte interesada en la adquisición, preservación, obtención y posterior presentación de la evidencia digital en un juicio, en ocasiones contrata a un/a escribano/a para intervenir en alguna de estas etapas, o en todas ellas, a fin de que confeccione un acta de constatación o comprobación de las tareas realizadas.

Es evidente que las actas notariales sobre prueba digital o electrónica, realizadas con la intervención de un notario público, requieren un grado de especificidad que esta guía no abarca completamente, debido a la complejidad y amplitud del derecho notarial.

Los aspectos técnicos de las actas notariales relacionadas con la prueba electrónica justifican la necesidad de elaborar una guía separada y específica para el notariado argentino. Esto permitirá abordar de manera más detallada y precisa las particularidades de estas actas, asegurando así su correcta aplicación y validez jurídica.

Claro está que las actas notariales sobre prueba digital o electrónica generadas bajo intervención de un notario público requieren una especificidad que puede no ser cubierta adecuadamente en esta guía, debido a la amplitud y complejidad del derecho notarial.

Los requisitos técnicos de las actas notariales sobre prueba electrónica justifican la creación de una guía separada y específica para el notariado argentino a fin de que pueda ser correctamente adoptada. Esto permitirá abordar con mayor profundidad y precisión las particularidades de este tipo de actas, garantizando una correcta aplicación y validez jurídica.

Capturas de pantalla o videograbación de pantalla.

Si bien las capturas de pantalla han tenido una recepción favorable tanto en la jurisprudencia como en la doctrina, desde un punto de vista técnico informático-forense este tipo de evidencia presenta muchas debilidades.

En primer lugar, es difícil establecer la autenticidad de una captura de pantalla. Existen muchos programas de edición de imágenes que podrían utilizarse para modificar una captura de pantalla y lograr que muestre algo distinto de la realidad, incluso hay aplicaciones que están especializadas en crear capturas de pantalla falsas (por ejemplo, de WhatsApp u otras aplicaciones de mensajería). En algunas situaciones se podrían plantear medios técnicos para la validación del origen de un archivo de imagen, pero estos métodos no son infalibles, y a lo sumo mejoran ligeramente el valor probatorio de una evidencia que es muy débil.

Por otra parte, a veces ni siquiera es necesario alterar la imagen de la captura de pantalla. Por ejemplo, es posible utilizar cualquier navegador web para alterar el contenido de un sitio que se cargó en el mismo de manera local. De esta manera, se podría obtener una captura de pantalla "legítima", en cuanto que no se ha modificado el archivo, y su obtención fue realizada por medios propios del sistema operativo, que sin embargo no es real. Este tipo de modificaciones de contenido tampoco son exclusivas del contenido web o accesible por internet.

Entonces, por más que se arbitren medios técnicos para verificar la integridad de una captura de pantalla, en principio no podemos confiar en ellas como método único de adquisición y preservación de la prueba digital.

Además, para la gran mayoría de las fuentes de evidencia digital de las cuales podrían tomarse capturas de pantalla, existen medios técnicos con garantías forenses que permiten adquirir la evidencia digital, y sus metadatos, con mayor confiabilidad y robustez. El uso de estos medios permitirá entonces sostener esta evidencia ante cuestionamientos y análisis exhaustivos de las otras partes involucradas en un eventual proceso judicial.

Por estas razones, las capturas de pantalla no pueden ser recomendadas como un medio confiable y suficiente para adquirir y preservar la evidencia digital.

Ante la situación de que las capturas de pantalla hayan sido adquiridas con anterioridad a la elaboración y difusión de la presente guía, y ya no pueda accederse al contenido que estas representan, por cuestiones de volatilidad o disponibilidad, quedará a buen criterio del juez o jueza su admisión en los procesos judiciales, aunque teniendo en cuenta que su valor probatorio por sí mismo es débil.

Sin perjuicio de lo expuesto, en algunos casos (por ej. mensajería instantánea) es posible encontrar situaciones en las que esas capturas son complementarias y necesarias a la

extracción de la prueba, pues agrega contexto y además facilita la lectura, comprensión e interpretación de la potencial evidencia digital.

Además de las capturas de pantalla, o en su reemplazo, es posible grabar la pantalla o videograbar con otro dispositivo, el procedimiento de extracción y preservación de la prueba.

Dispositivos de Almacenamiento.

Un dispositivo de almacenamiento es el medio de almacenamiento físico que se utiliza para almacenar datos de manera permanente o temporal. Se utilizará algún dispositivo de almacenamiento para guardar la evidencia digital obtenida en la fase de adquisición y que podrá ser utilizada en la fase de presentación.

Existen diferentes tipos de dispositivos de almacenamiento.

I. Dispositivos de almacenamiento magnético:
   A. *Discos duros (HDD):* Son los que frecuentemente se encuentran instalados en las computadoras personales (ya sea PC o Notebook). Poseen gran capacidad de almacenamiento. Suelen estar disponibles como discos rígidos externos, lo que los hace una posibilidad para almacenar información fuera de la computadora. Con las configuraciones estándar de este tipo de dispositivos, lo que se almacena en los discos se puede editar y/o eliminar.
   B. *Dispositivos de almacenamiento ópticos:* Este tipo de almacenamiento se basa en el guardado de la información en discos ópticos. Con el correr de los años han ido evolucionando en su capacidad de almacenamiento:
      i. *CD (Compact Disc):* Utilizados para almacenar datos, música o videos con capacidades típicas de 700 MB a 1.4 GB.
      ii. *DVD (Digital Versatile Disc):* Tienen mayor capacidad de almacenamiento que los CDs y se usan para almacenar películas, programas de televisión y datos, con capacidades típicas de 4.7 GB a 9 GB.
      iii. *Blu-ray Disc:* Tienen aún más capacidad de almacenamiento que los DVDs y se utilizan para almacenar videos de alta definición y datos, con capacidades típicas de 25 GB a 128 GB.

II. Dispositivos de almacenamiento flash (memoria estado sólido): Son dispositivos de almacenamiento electrónicos, de acceso mucho más rápido que los discos magnéticos. Su aparición masiva en el mercado aparece como memorias para los celulares y pendrives para luego convertirse en una opción para discos de almacenamiento para computadoras personales o notebooks. Existen también discos rígidos externos con esta tecnología. Debido a su alto costo, las capacidades de almacenamiento de estos discos en los equipos, generalmente es menor que el de los discos magnéticos. La información que se almacena en estos discos puede eliminarse y/o modificarse.

A. *Unidades flash USB (pendrives):* Son pequeñas, portátiles y se utilizan para transferir y almacenar datos de manera rápida. Son cómodos para transportar y de un costo relativamente bajo.
B. *Tarjetas de memoria:* Se utilizan en cámaras digitales, teléfonos inteligentes, tabletas y otros dispositivos portátiles para almacenar fotos, videos y otros datos.
C. *Discos de Estado Sólido - SSD (Solid State Drive):* Son similares a los discos duros magnéticos, pero no tienen partes móviles, lo que los hace más rápidos y resistentes a los golpes.

III. Dispositivos de almacenamiento en la nube: Son servicios de almacenamiento en servidores que se encuentran en Internet. Ejemplos de este tipo son Google Drive, Dropbox, iCloud, etc., que permiten almacenar datos de forma remota en servidores de esas empresas a los que se accede a través de Internet. El contenido almacenado en la nube puede ser modificado y/o eliminado por aquellos usuarios que tengan permiso de editor sobre ese contenido. La información que se encuentre alojada en la nube se puede compartir con otros usuarios y descargarse en un equipo.

¿En qué dispositivo guardamos la evidencia adquirida para luego presentarla?

Desde que se incorpora la evidencia digital a los procesos judiciales surge el requerimiento de tener un medio de almacenamiento para esa evidencia, desde que el momento en que debe ser almacenada para luego ser presentada y entregada.

De aquí surgen dos temas a tener en cuenta, ¿dónde se almacena? y ¿cómo lo acepta el juzgado?

Hasta hace algunos años la mecánica de trabajo consistía en almacenar la evidencia en una unidad de almacenamiento óptico (CD/DVD) que se entregaba junto con el expediente. La gran ventaja que tenía este tipo almacenamiento es que no se podía modificar su contenido y que el costo de los discos era económico.

El problema empezó a surgir cuando los equipos informáticos comenzaron a no tener unidades de lectura de almacenamiento óptico por defecto, lo que comenzó a complejizar el proceso de grabación y de lectura de estos dispositivos.

Por otro lado, el almacenamiento de los discos ópticos generaba problemas si se rayaban, deterioraban o rompían.

Asimismo, los juzgados, al migrar al expediente digital, comenzaron a implementar la opción de que se lleve la evidencia en algún tipo de almacenamiento portátil (disco externo, pendrive) de manera de facilitar el traspaso para el almacenamiento de esta evidencia en sus propios servidores y/o nube. Incluso, hay juzgados que permiten que se les envíe un link para proceder a la descarga de la evidencia y su respectivo almacenamiento.

5. Guías y Recomendaciones

Las guías que se presentan a continuación constituyen un conjunto de buenas prácticas desarrolladas para un contexto variable que favorecerá con un grado deseable de seguridad, trazabilidad y explicabilidad el procedimiento y el resultado obtenido. Cada una de estas guías contiene además un conjunto de recomendaciones que conforman pautas, orientaciones, principios y valores flexibles y útiles que resultan beneficiosos.

Las herramientas y sistemas operativos en los cuales se ejemplifican los procedimientos mencionados, se realizan en base a los sistemas operativos, aplicaciones y redes más utilizados, dejando a la propia investigación del lector o ejecutor de dicho procedimiento como realizar dicha actividad en una herramienta o sistema operativo no mencionado en la presente guía.

El cumplimiento de las guías y recomendaciones no implica ni asegura un resultado infalible en todos los casos, sino una manera ordenada y validada para hacer las tareas. Siempre se recomienda analizar el contexto concreto de cada caso.

5.1 Guía y recomendaciones para el aseguramiento de correos electrónicos.

A. Conceptos generales:

Para Calvinho «el e-mail integra -junto al intercambio electrónico de datos, el telegrama el télex o el telefax, entre otros- la categoría genérica mensajes de datos, cuyos integrantes tienen por denominador común el hecho de que en ellos la información es originada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares» [14]

Bender concibe al correo electrónico como un medio de comunicación que permite el envío de documentos electrónicos que pueden instrumentar actos jurídicos y hechos jurídicos. Asimismo, indica que estos documentos satisfacen el requerimiento legal de escritura, conforme el art. 6 de la Ley de Firma Digital N° 25.506. [15]

[14] CALVINHO, Gustavo. (2010). «La prueba de los correos electrónicos'. Disponible en la Revista Jurídica Argentina La Ley /Número: 2010 E (Revista).

[15] BENDER, Agustín. (2019). «El correo electrónico como prueba en la jurisprudencia y en el proyecto de Código Civil y Comercial de la Nación». Pág. 33. Dossier Especial «El desafío de la prueba electrónica en el proceso judicial». Ed. Thomson Reuters.

Para Fernández Delpech el correo electrónico es uno de los elementos de Internet que mayores beneficios ha traído, y cuya utilización se ha extendido notablemente en los últimos años. Ha reemplazado al correo tradicional, generando numerosas consecuencias y nuevas situaciones en las que se debe tener presente la intimidad de las personas y su derecho a la privacidad… el correo tradicional, prácticamente ha desaparecido y el 90% de las comunicaciones entre las personas se efectúa mediante la remisión de mensajes electrónicos, fundamentalmente mediante correos electrónicos, muchos de ellos a través de los cuales se contraen obligaciones o al menos se desarrolló en las etapas previas al contrato y las posteriores al mismo, así como los reclamos y todas las incidencias que se pueden producir ante el incumplimiento de los contratos. [16]

Hoy en día es importante mencionar que el correo electrónico podría asimilarse a una aplicación de **mensajería instantánea**.

Los mensajes de correo llegan casi al instante, pero tienen una gran diferencia con la mayoría de las aplicaciones de mensajería instantánea que existen hoy en día: una vez que el mensaje es enviado, llegará a su destino (siempre y cuando exista la cuenta destino), sin la posibilidad de que el emisor pueda detener o eliminar el mensaje remotamente en la casilla destino de su receptor.

Por ejemplo, varias aplicaciones de mensajería instantánea, permiten eliminar el mensaje en ambos lados: tanto del lado del emisor como del receptor. Con el correo electrónico esto no puede hacerse, y ello es debido a cómo funciona. Razón por la cual, es una evidencia que perdura en el tiempo, excepto que el propietario de la cuenta de correo electrónico borre intencionalmente dicho mensaje de correo. Es decir, que todo mensaje que quiera ser aportado como prueba, no debe eliminarse de la cuenta o casilla de correo de quien lo quiera aportar.

Ahora bien, el correo electrónico también tiene una desventaja con respecto a las aplicaciones más modernas. En algunas ocasiones, es más complejo poder determinar su autenticidad si no se siguen ciertas consideraciones, ya que utiliza un protocolo bastante antiguo, pero no por eso obsoleto o ineficiente. A medida que ha pasado el tiempo, se han

[16] FERNANDEZ DELPECH, Horacio. (2016). «Manual de derecho informático». Pág. 373. Editorial Abeledo Perrot. Ciudad Autónoma de Buenos Aires.

implementado ciertas medidas de seguridad al correo electrónico para verificar su autenticidad.

B. Aspectos jurídico-legales.

1. Constitución Nacional [17]

   Artículo 18.- Ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso, ni juzgado por comisiones especiales, o sacado de los jueces designados por la ley antes del hecho de la causa. Nadie puede ser obligado a declarar contra sí mismo; ni arrestado sino en virtud de orden escrita de autoridad competente. Es inviolable la defensa en juicio de la persona y de los derechos. El domicilio es inviolable, como también **la correspondencia epistolar y los papeles privados**; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación. Quedan abolidos para siempre la pena de muerte por causas políticas, toda especie de tormento y los azotes. Las cárceles de la Nación serán sanas y limpias, para seguridad y no para castigo de los reos detenidos en ellas, y toda medida que a pretexto de precaución conduzca a mortificarlos más allá de lo que aquélla exija, hará responsable al juez que la autorice.

   Artículo 19.- Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe.

2. Código Civil y Comercial de la Nación (CCYCN).

   Art. 284 Libertad de formas: Si la ley no designa una forma determinada para la exteriorización de la voluntad, las partes pueden utilizar la que estimen conveniente. Las partes pueden convenir una forma más exigente que la impuesta por la ley.

   Art. 285 Forma impuesta: El acto que no se otorga en la forma exigida por la ley no queda concluido como tal mientras no se haya otorgado el instrumento previsto, pero vale como acto en el que las partes se han obligado a cumplir con la expresada formalidad, excepto que ella se exija bajo sanción de nulidad.

[17] http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

Art. 286 Expresión escrita: La expresión escrita puede tener lugar por instrumentos públicos, o por instrumentos particulares firmados o no firmados, excepto en los casos en que determinada instrumentación sea impuesta. Puede hacerse constar en cualquier soporte, siempre que su contenido sea representado con texto inteligible, aunque su lectura exija medios técnicos.

Art. 287 Instrumentos privados y particulares no firmados: Los instrumentos particulares pueden estar firmados o no. Si lo están, se llaman instrumentos privados. Si no lo están, se los denomina instrumentos particulares no firmados; esta categoría comprende todo escrito no firmado, entre otros, los impresos, los registros visuales o auditivos de cosas o hechos y, cualquiera que sea el medio empleado, los registros de la palabra y de información.

El CCYCN regula en la Sección Sexta del Título IV la forma y requisitos de los instrumentos particulares firmados y no firmados.

Art. 318: La correspondencia, cualquiera sea el medio empleado para crearla o transmitirla, puede presentarse como prueba por el destinatario, pero la que es confidencial no puede ser utilizada sin consentimiento del remitente. Los terceros no pueden valerse de la correspondencia sin asentimiento del destinatario, y del remitente si es confidencial.

3. Código Penal de la Nación. [18]

Sin perjuicio de que la presente guía ha sido diseñada para los procesos no penales, debemos remitirnos a algunas normas de Derecho Penal que son de aplicación también a los procesos no penales, por ejemplo, porque definen normativamente un bien jurídicamente protegido por la norma penal.

ART. 77.- Para la inteligencia del texto de este código se tendrán presente las siguientes reglas:

…El término “documento” comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

[18] http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm

Los términos “firma” y “suscripción” comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

Los términos “instrumento privado” y “certificado” comprenden el documento digital firmado digitalmente…

ART. 153. - Será reprimido … el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será …, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

ART.153 BIS. - Será reprimido … el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será …cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

ART. 154. - Será reprimido … el empleado de correos o telégrafos que, abusando de su empleo, se apoderare de una carta, de un pliego, de un telegrama o de otra pieza de correspondencia, se impusiere de su contenido, la entregare o comunicare a otro que no sea el destinatario, la suprimiere, la ocultare o cambiare su texto.

ART. 155. - Será reprimido …el que, hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

ART. 156. - Será reprimido … el que, teniendo noticia, por razón de su estado, oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa.

ART. 157. - Será reprimido … el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

ART. 157 bis. -Será reprimido …el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

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

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

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial …

4. Ley Nacional N° 25.506 Firma digital (BO 14/12/2001)

Art. 2 Firma Digital: Se entiende por firma digital 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. Los procedimientos de firma y

verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

Art. 5 Firma electrónica: Se entiende por firma electrónica al 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. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez

Art. 6º Documento digital: Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura y lo que es un documento digital.

Art. 7 Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

Art. 13 Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

C. Procedimiento.

A continuación, se brindará una serie recomendaciones y buenas prácticas para la obtención de este tipo de evidencias dependiendo el caso, siempre tomando como referencia Los Pasos Metodológicos. *-ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses-* Para cada una de las actividades y pasos propuestos, se detallará a la fase que pertenece de dichos pasos. No se recomienda realizar este procedimiento en un dispositivo móvil ya que le resultará muy difícil de resolver.

Con respecto a las capturas de pantalla nos remitimos a lo expuesto en el apartado general. *- ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital. - Captura de pantalla -*

1. *Descargar el correo electrónico*

En primer lugar, se debe descargar el mensaje original completo. Esto es fundamental, dado que el mensaje completo contiene todos los datos de interés: direcciones IP de servidores, dominios de servidor involucrados, registros de seguridad, asunto, emisor, destinatarios, cuerpo del mensaje, entre otros.

Dependiendo la aplicación que se utilice como cliente de correo electrónico esta opción puede variar de nombre, pero generalmente podemos encontrarla como “Ver mensaje original” o similar.

Al descargar este mensaje, simplemente, se genera un archivo de texto (".eml" o similar) conteniendo todas estas características. Esto significa que, el archivo generado y descargado, podrá abrirse con un editor de texto (bloc de notas, por ejemplo).

El nombre con el que se almacena este archivo se sugiere que sea descriptivo.

La descarga del correo electrónico se corresponde con las fases de análisis de escenario y descarga de información de los pasos metodológicos. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Análisis de escenario y Descarga de información -*

2. Descargar los archivos adjuntos

Si el mensaje de correo tuviere adjuntos, se deben descargar estos archivos con nombres descriptivos para incorporar en el procedimiento. Se recomienda no abrir estos adjuntos en el equipo en dónde se alojará la descarga.

Es recomendable que, por cada mensaje de correo electrónico que se descargue, se generen una carpeta o directorio contenedor diferente para cada uno de ellos.

Este proceso puede realizarse de dos formas, siempre dependiendo del cliente de correo electrónico:

1. Al acceder a la opción de "Ver Original", por lo general, existe la opción de descargar el mensaje. En ese momento, se descargará el archivo (.eml) en el dispositivo que esté realizando el procedimiento;
2. Al ver el mensaje original, se puede copiar ese texto y copiarlo en un bloc de notas o editor de texto. Luego, guardarlo con un nombre descriptivo.

Esta tarea se corresponde con la fase de descarga de información de los pasos metodológicos. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Descarga de información -*

3. *Generar archivo comprimido y generar hash*

Una vez descargados el correo electrónico original y los archivos adjuntos -si los hubiera- se deben comprimir estos en un único archivo y calcular la función de hash sobre el archivo comprimido para garantizar la integridad del mismo. Esta tarea se corresponde con la fase de compresión y hash. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Hash -*

4. *Dejar constancia*

Dejar una constancia escrita o realizar un informe - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - El informe -*

Esta tarea se corresponde con las fases de acta o informe.

5. *Preservar y aportar*

Preservar el archivo comprimido, generado en el punto precedente, que se aportará en el medio de almacenamiento que se considere pertinente.

Esta tarea se corresponde con las fases de informe de los *Pasos metodológicos* (desarrollado en Recomendaciones generales para el aseguramiento de Prueba Digital). - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - El informe -*

D. Consideraciones para verificar la autenticidad de un correo electrónico

- La autenticidad de un correo electrónico puede verificarse bajo ciertas condiciones y será efectiva en el único caso de que el mensaje de correo sea aportado por la cuenta receptora. Si desea aportar un mensaje de correo desde la cuenta emisora, algunos de estos parámetros no podrán ser visualizados.

- El remitente real de un mensaje puede ocultarse. Este enmascaramiento podría pasar inadvertido si sólo se observa la vista convencional de un correo electrónico y no la vista completa del mensaje original.

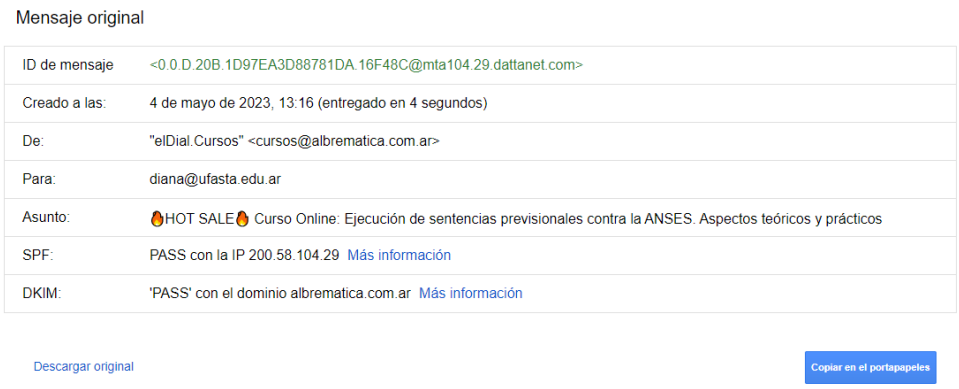
Mediante todas estas consideraciones, será posible no sólo incorporar un mensaje de correo electrónico a un proceso judicial, sino también verificar la autenticidad del mismo.

Por otra parte, si lo que se quiere es preservar una cadena de correos electrónicos, es decir, mensajes y sus respuestas, se deberá realizar esta operación por cada uno de los mensajes. Por ejemplo, si se realiza la preservación del último mensaje de correo dentro de una cadena de mensajes, sólo se preservarán los datos de este último y no así de todos los anteriores.

Es importante tener especial atención en que los métodos aquí descriptos no están disponibles (hasta el momento) si se está utilizando el cliente nativo[19] de correo electrónico de Windows 10 o superior.

E. Caso de uso. Ejemplo.

1. En primer lugar, se debe descargar el mensaje original o completo.



Mensaje Original desde Cliente de correo Gmail

   a. Si el mensaje de correo tuviere adjuntos, se deben descargar y no ejecutar (abrir), para incorporar.

   b. Una vez descargados estos archivos, se debe comprimir estos archivos en un único archivo y ejecutar la función de hash sobre este archivo para garantizar

[19] Un cliente nativo de correo electrónico es un software que viene instalado en el equipo por defecto con la versión del Sistema Operativo y permite enviar, recibir y gestionar los correos.

la integridad del mismo. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Hash* -

c. Dejar constancia

Dejar una constancia escrita o realizar un informe. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - El Informe* -

d. Preservar y aportar

Adjuntar el archivo de texto conteniendo el mensaje completo original que se quiere aportar en el medio que se considere pertinente. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Dispositivos de Almacenamiento* -

Aportar los archivos de interés por el medio más adecuado, y respetando las normas de procedimiento.

5.2 Guía y Recomendaciones para el aseguramiento de información en Servicios de Mensajería.

A. Conceptos generales.

Desde el punto de vista jurídico el servicio de mensajería instantánea es asimilable a los correos electrónicos (ver Guía y Recomendaciones para el aseguramiento de Información en Correos Electrónicos, Conceptos generales). - *ver sección 5.1 Guía y recomendaciones para el aseguramiento de correos electrónicos - Conceptos generales* -

Conforme al art. 318 del Código Civil y Comercial “la correspondencia, cualquiera sea el medio empleado para crearla o transmitirla, puede presentarse como prueba por el destinatario, pero la que es **confidencial** no puede ser utilizada sin consentimiento del

remitente. Los terceros no pueden valerse de la correspondencia sin asentimiento del destinatario, y del remitente si es confidencial".

"Por su parte, los mensajes de correo llegan casi al instante, pero tienen una gran diferencia con la mayoría de las aplicaciones de mensajería instantánea que existen hoy en día: una vez que el mensaje es enviado, llegará a su destino (siempre y cuando exista la cuenta destino), sin la posibilidad de que el emisor pueda detener o eliminar el mensaje remotamente en la casilla destino de su receptor" [20].

Sin embargo, a diferencia de lo que ocurre con los correos electrónicos, algunas aplicaciones de mensajería instantánea permiten hoy eliminar el mensaje tanto del lado del emisor como del receptor.

Un tema que requerirá un abordaje interpretativo y valorativo particular será la "confidencialidad" de la información en los llamados "grupales" o grupos de mensajería instantánea. Tal es el caso de los grupos de WhatsApp, integrados por un gran número de usuarios, a veces más de un mil, que incluso no se conocen entre sí, para compraventa de servicios o bienes, o intercambio de información (ej. material de estudio), para comunicación entre vecinos de un mismo barrio o zona, cuyo funcionamiento interno se asimila a las redes sociales según los parámetros explícitos o tácitos de configuración de los mismos usuarios. Será una cuestión sujeta a valoración judicial, en el caso concreto.

B. Aspectos jurídico-legales.

En este punto ver *sección 5.1. Guía y Recomendaciones para el aseguramiento de Información en Correos Electrónicos - Aspectos jurídico-legales*.

C. Procedimiento.

A continuación, se brindará una serie de recomendaciones y buenas prácticas para la obtención de este tipo de evidencia. Dependiendo el caso, siempre tomando como referencia los *Pasos metodológicos* mencionados en el capítulo "3.2 - Actuación Metodológica". Para cada una de las actividades y pasos propuestos, se detalla a la fase que pertenece de dichos pasos. - *ver sección 4. Recomendaciones generales para el*

[20] BIELLI, G., 2020, Derecho Procesal Informático: E-mails, chats, WhatsApp, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías. Validez probatoria en el proceso civil, comercial , penal y laboral, dirigido por H. Granero, elDial.com, Buenos Aires, p. 75/81.

aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forense - Para preservar la información, se procederá a exportar (descargar y guardar) el historial (las conversaciones) del chat requerido.

La persona deberá seleccionar el chat en el dispositivo donde se encuentra instalado el programa de mensajería, o bien (según el caso) se necesitará el dispositivo para poder usar la versión desktop (en un equipo). De acuerdo a la necesidad del caso y las posibilidades del usuario, se recomienda realizarlo en la computadora del profesional interviniente.

Consideraciones y problemáticas:

1. Imágenes efímeras: Son fotos o videos que están diseñados para desaparecer después de un período de tiempo determinado o luego de ser vistas. Por esta razón cuando se quiera exportar el chat, estas imágenes o vídeos efímeros ya no estarán disponibles. Cuando se encuentre con una imagen o video de interés de este tipo, una vez abierta para visualizar no la cierre y utilice otro dispositivo para capturar la imagen o el video.

2. La exportación puede demorarse dependiendo de la cantidad de información que se va a descargar.

3. Si bien las capturas de pantalla no suelen aportar información por sobre los medios digitales - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital. - Captura de pantalla* -, en el caso de mensajería instantánea es posible encontrar situaciones en las que esas capturas pueden resultar complementarias. En particular la exportación de mensajes de WhatsApp realizada desde el teléfono no representa adecuadamente las reacciones a mensajes y las citas o respuestas, que sí se pueden ver claramente en una captura de pantalla. Para estos casos, la captura de pantalla es un complemento a la extracción que agrega contexto y además facilita la lectura, comprensión e interpretación de la potencial evidencia digital.

4. En algunos programas de mensajería sólo podrá exportarse el historial de conversación entre dos personas: A y B, siendo ésta la única información requerida.

5. En otros servicios de mensajería, deberán exportarse todas las conversaciones del usuario: comunicaciones, e interacciones de todo tipo que el usuario haya tenido con

otros usuarios de la red de mensajería. Para limitar la información que es relevante y pertinente habrá que desglosar el archivo que se obtenga y seleccionar las partes que se quieren adquirir y preservar.

6. Los casos de uso que se explican a continuación son con las herramientas que más frecuentemente se utilizan. Para el resto de los servicios de mensajería los procedimientos tendrán la misma finalidad: almacenar los datos que se encuentran en los chats, exportando las conversaciones, aunque los procedimientos pueden diferir de los aquí explicados.

7. Para cada uno de los casos de uso, la explicación se hace usando las versiones de la aplicación que existe en el momento de la redacción de esta guía.

8. Se sugiere exportar el contacto referido de la agenda si correspondiera, a fin de poder relacionar el número telefónico con el nombre una vez realizada la exportación del chat.

9. En el caso de archivos de audio o video, además de conservar el archivo original puede complementarse con la transcripción del mismo en formato texto.

Por todo lo explicado anteriormente, para el servicio de mensajería no existe un paso a paso único para todas las aplicaciones, por lo tanto, se explicará el procedimiento en los casos de Uso o Ejemplos.

D. Casos de uso. Ejemplos.

Caso de uso: Exportar Contacto

El procedimiento para exportar un contacto puede variar dependiendo la interfaz de usuario de los teléfonos (ya sea Android base, iOS, o interfaces propias de las empresas).

A continuación, se explicará el procedimiento con sistemas Android. En iPhone, podría variar la disposición de las opciones para realizarlo, pero la metodología es similar.

Para exportar un contacto desde Android (tener en cuenta que puede llegar a variar según la marca y/o modelo del celular):

- En su teléfono o tablet Android, abra la app de Contactos .

- Seleccione el contacto.
- En la parte inferior, presione Compartir y luego Archivo de presentación (VCF)
- Puede enviar el contacto por WhatsApp, por mail, subirlo a una nube, entre otras opciones. Seleccione la más conveniente.
- Descargue el archivo en una computadora

Calcular la función de Hash correspondiente - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Hash -*

En el caso de grupos (tanto de Telegram como WhatsApp), será necesario sacar capturas de pantalla (o grabar la pantalla) para preservar el listado de miembros, ya que no proveen un mecanismo para exportar los integrantes de los grupos. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital. - Captura de pantalla -*

Observación: es posible que por la configuración de cada grupo no se pueda visualizar la totalidad de los integrantes (Telegram).

Caso de Uso: WhatsApp

WhatsApp nos permitirá descargar el historial de conversaciones en forma independiente con cada uno de los usuarios que se requiera. Esto deberá realizarse siempre desde el dispositivo celular del usuario, donde se encuentra instalada la cuenta de WhatsApp de la que se desea preservar la información, ya que la aplicación WhatsApp desktop (o web) todavía no dispone de esta opción.

Se recuerda que este procedimiento debe llevarse a cabo con la autorización del usuario (el dueño del dispositivo donde se encuentra instalado el programa de mensajería).

Lo que se debe guardar son la o las conversaciones de WhatsApp con una determinada persona o con un grupo. Si son dos conversaciones diferentes, el proceso debe repetirse para cada una de las conversaciones.

Tenga en cuenta que guardar la base de datos de toda la cuenta de WhatsApp, que se encuentra almacenada en el dispositivo celular, o la copia de seguridad, que se almacena en Google Drive, no es la forma correcta de preservar la información. Para extraer la base de datos del celular requerirá de software específico y experticia. Las copias de seguridad

que se almacenan en Google Drive se sobrescriben, a medida que se van generando copias nuevas, según el usuario tenga configuradas las opciones de su cuenta. Por otro lado, esas copias pueden abrirse solamente desde el dispositivo celular donde se encuentra configurado el número de teléfono asociado a la copia de WhatsApp. Al levantar esa copia de seguridad en el celular, se reemplaza el contenido del WhatsApp actual con el de la copia de seguridad.

Las conversaciones de mensajería pueden contener texto, audios, imágenes y/o videos y contactos que se hayan enviado.

Importante: en el archivo de texto que se genera como resultado de extraer la conversación de WhatsApp, no se diferencia las respuestas a los mensajes ni las reacciones a los mismos. Por lo tanto, cuando exista una respuesta o una reacción en el archivo, se verá como un mensaje sin conexión con el que haga referencia. Para aclarar tal situación se aconseja acompañar de las imágenes de captura de pantalla - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital. - Captura de pantalla* -.

Procedimiento:

1. Registrar el número de teléfono que se asocia a la red de mensajería del usuario (Fase de “Análisis de Escenario”).

2. Registrar el número de teléfono y datos de contacto de la persona que interviene en la conversación. En caso de ser un grupo, realizarlo para cada uno de los integrantes del grupo. (Fase de “Análisis de Escenario”)

3. Abrir el chat individual o grupal.

4. Tocar el ícono de más opciones (los tres puntitos) - Más - Exportar chat.

5. Elegir si se quiere exportar el historial incluyendo los archivos multimedia (audios y videos) o no.

6. Seleccionar la forma en la que enviará la exportación. Puede ser enviada por mail, por WhatsApp, subirlo a Drive y alguna otra opción según las aplicaciones que tenga instalada el usuario en su celular. Se aconseja realizarlo vía mail ya que es un

procedimiento más conveniente, por tal razón se explicará ese procedimiento. En caso de haber seleccionado algún otro los pasos para la descarga son similares.

7. Seleccionar la opción de envío por correo electrónico. Si bien permite enviar la exportación por otros medios, Si seleccionó exportar sin archivos multimedia, se adjuntará automáticamente al mail un archivo de texto (.txt). Si en cambio, seleccionó incluir los archivos multimedia, se adjuntará al mail un archivo comprimido (.zip) que contendrá el archivo de texto correspondiente a la conversación y todos los archivos multimedia asociados. Para tener en cuenta: si se seleccionó exportar sin archivos, y dentro de los mensajes, había envíos de contactos, los mismos se agregarán a la descarga; por lo tanto, deberá proceder en el paso 7 como si hubiera extraído con archivos multimedia.

   Al respecto, WhatsApp hace algunas aclaraciones[21]:

   - Si se decide activar la opción Incluir archivos, se añadirán los archivos multimedia más recientes como adjuntos al correo electrónico.
   - Si se adjuntan los archivos, se podrán exportar los 10.000 mensajes más recientes. Si no se adjuntan, se podrán exportar 40.000 mensajes. Estas restricciones se deben al tamaño máximo del correo electrónico.

   Con respecto a estas limitaciones, tenga en cuenta que WhatsApp no mandará ningún mensaje de error avisando que no pudo exportar todo el contenido.

   A lo que aclara WhatsApp hay que agregarle el problema en los límites para adjuntar un archivo en un mail ya que también depende de la cuenta de correo electrónico que se utilice para enviar el tamaño máximo del archivo adjunto. Por ejemplo: Gmail permite adjuntar archivos de hasta 25 MB. Si su extracción supera este límite puede probar enviarlo por WhatsApp o por Drive, teniendo en cuenta que el tamaño total del archivo va a depender de las aclaraciones que hace WhatsApp con respecto a las limitaciones que se encuentran en los párrafos anteriores.

[21] https://faq.whatsapp.com/1180414079177245/?locale=es_LA&cms_platform=android

8. Una vez recibido el correo electrónico descargar el archivo (puede ser solo un archivo .txt o un .zip dependiendo de lo seleccionado) en la computadora. (Fase de "Descarga de Información" y "Compresión").

9. Generar el Hash correspondiente sobre el archivo descargado en el punto anterior (Fase de "Hash"). - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Hash -*

10. Frecuentemente cuando se exporta la información de una conversación de WhatsApp hay mucha información que es de índole privada o no es pertinente para el caso. Por tal motivo hay que realizar el análisis de los archivos:

    - Si sólo se envió el archivo de texto (.txt), abrir dicho archivo y copiar las partes que correspondan en un nuevo archivo de texto (no modificar ni eliminar contenido del archivo original). Esto lo puede hacer en la computadora desde el Bloc de Notas

    - Si eligió la opción que incluye archivos multimedia, deberá primero descomprimir el archivo comprimido (.zip) por ejemplo utilizando el programa 7zip. Una vez descomprimido, en la carpeta que se genera, encontrará el archivo de texto con la conversación y todos los archivos multimedia. Del archivo de texto si no necesita todo el contenido, proceda como se explica en el punto anterior. Con respecto a los archivos multimedia, cree una carpeta nueva en el equipo donde se encuentra trabajando, seleccione todos los archivos multimedia que sean necesarios y los pega en la carpeta anteriormente creada. Comprima la carpeta que contiene todos los archivos(con el programa 7zip) y genere el HASH correspondiente.

11. La extracción de información de este punto, según la necesidad y posibilidad de usuario, se recomienda que sea realizada por un profesional informático (debido a la posible dificultad en el entendimiento de los tipos de archivos) en presencia del usuario.

12. Dejar una constancia escrita o realizar un informe donde se especifiquen las partes intervinientes en el acto, las tareas realizadas, los nombres de los archivos que se

incorporan, la función de hash utilizada, el valor de hash resultado, tamaño del archivo, tanto del archivo de datos completo como de los que sean de interés. Agregar al informe sugerido los datos recolectados en los puntos 1 y 2 del procedimiento. .- *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - El Informe -*

13. Preservar y aportar: Almacenar los archivos descargados, incluyendo el o los archivos de contactos, en un dispositivo o en una nube. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Dispositivos de Almacenamiento -*

Caso de Uso: Telegram

Al momento de la redacción de esta Guía, Telegram no permite realizar la copia del historial de chats desde la aplicación del celular, por lo tanto se deberá usar Telegram Desktop, que es la versión Telegram para ser usada en la computadora y que se descarga del sitio oficial https://desktop.telegram.org/ Por lo mencionado anteriormente tener en cuenta que deberá estar instalada dicha aplicación en la computadora del estudio jurídico o pericial interviniente.

Telegram permite descargar el historial de una sola conversación o bien la base de datos completa, que contendrá todas las conversaciones de mensajería y sus archivos correspondientes. Deberá descargarse todo el historial de todas las conversaciones o una en particular de acuerdo a los requerimientos.

El archivo donde se almacena la conversación de chat, es un archivo .html, lo va a poder visualizar como una página web. Por tal razón no podrá editarse (para extraer partes de interés) tan fácilmente como un archivo de texto. Para poder extraer alguna parte en particular de ese archivo, ya se requiere de un profesional que sepa modificar el contenido de dicho archivo.

En el caso de Telegram, sí podrá ver cuando un mensaje es respuesta o reacción a otro mensaje, ya sea a través de un texto o de un emoji. Le indicará que es una respuesta y un link que lo dirige al mensaje correspondiente.

Procedimiento:

1. Registrar el número de teléfono, siempre que sea posible, que se asocia a la red de mensajería del usuario (Fase de “Análisis de Escenario”). - *ver sección ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Análisis de escenario -*

2. Registrar el número de teléfono y datos de contacto de la persona que interviene en la conversación. En caso de ser un grupo, realizarlo para cada uno de los integrantes del grupo. (Fase de “Análisis de Escenario”) - *ver sección ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Análisis de escenario -*

3. Iniciar sesión en la cuenta de Telegram en la aplicación Telegram Desktop. Se necesitará del dispositivo móvil donde se encuentra la aplicación instalada para realizar la conexión correspondiente.

   Para realizar el resguardo de una conversación determinada (Fase de “Análisis de Escenario”): - *ver sección ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Análisis de escenario -*

   a. Acceder el chat correspondiente (de una sóla persona o un grupo)
   b. Seleccionar el botón con los tres puntitos de arriba a la derecha. Se abrirá un menú desplegable y seleccionar la opción exportar chat.
   c. En la ventana emergente seleccionar los ajustes de exportación:
      i. Tipo de archivos a descargar: fotos, videos, mensajes de voz, video mensajes, stickers, gif y archivos (con un límite máximo de 8 MB)
      ii. Seleccionar el formato del archivo de descarga (HTML o JSON). Se aconseja descargarla como HTML (todo el proceso que sigue a continuación se explica en base a ese formato).
      iii. Seleccionar la ruta de descarga (la carpeta de la computadora donde se descargarán los archivos)
      iv. Desde (por defecto lo más antiguo), hasta (por defecto el presente)

v. Presionar el botón exportar. La aplicación puede avisar que, por razones de seguridad, el proceso de descarga comienza en una determinada cantidad de horas.

vi. Pasado ese tiempo repetir la solicitud usando el mismo dispositivo para descargar los archivos. Dirigirse a la carpeta que se seleccionó en el punto c.iii, como ruta de descarga. Comprimir la carpeta. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Descarga de información - Compresión -*

d. Generar el Hash correspondiente sobre el archivo del punto anterior. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Hash -*

e. Dentro de la carpeta encontrará todas las carpetas y archivos pertenecientes a la descarga de la conversación.

i. un archivo messages.html, que contiene toda la conversación.

ii. por cada tipo de archivo que pidió descargar, como indica el punto c.i, tendrá una carpeta con el contenido. Si no requiere (porque no es pertinente) todos los archivos, puede crear una nueva carpeta y copiar en ella los archivos necesarios.

iii. En el caso que lo que se desee preservar sea un archivo de audio, proceder a la transcripción del mismo en formato texto.

iv. Comprimir la nueva carpeta y hashear.

<u>Para realizar el resguardo de toda la base de datos (Fase de "Descarga de Información"):</u>

f. Con la aplicación abierta, pulsar en las tres barras verticales que se encuentran en la parte superior izquierda.

g. En el menú lateral que aparece, seleccionar Ajustes, Avanzados.

h. Desplazar la ventana hasta el final donde se encuentra la opción Exportar datos de Telegram.

i. En la ventana emergente de Exportar tus datos, realizar la selección de opciones correspondiente:

i. Información de la cuenta (nombre visible elegido, nombre de usuario, número de teléfono y fotos de perfil)
ii. Lista de contactos
iii. Ajustes de exportación: chats personales, chats con bots, grupos privados (sólo los mensajes del usuario o todos), canales privados, grupos públicos, canales públicos.
iv. Ajustes de exportación multimedia: fotos, videos, mensajes de voz, video mensajes, stickers, GIF, archivos (límite de tamaño 8 MB).
v. Otros: Secciones activas en otros dispositivos, datos varios.
vi. Ubicación y formato: seleccionar la ruta de descarga (la carpeta de la computadora donde se descargarán los archivos), formato del archivo de descargar (HTML, JSON)
vii. Presionar el botón Exportar
viii. La aplicación puede avisar que, por razones de seguridad, el proceso de descarga comienza en una determinada cantidad de horas. Pasado ese tiempo debe repetir la solicitud usando el mismo dispositivo.
ix. Pasado ese tiempo, repetir la solicitud usando el mismo dispositivo para descargar los archivos. Dirigirse a la carpeta que se seleccionó en el punto c.iii, como ruta de descarga. Comprimir la carpeta. . - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Descarga de información - Compresión -*
x. Dirigirse a la carpeta de descarga elegida, buscar la carpeta que contiene la descarga. El nombre de la misma comenzará con "Data_export".

j. Comprimir la carpeta. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Compresión -*
k. Generar el Hash correspondiente a la carpeta comprimida ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital -

Actuación metodológica - Pasos metodológicos sin herramientas forenses - Hash.

l. Dentro de la carpeta “Data_export” se encuentra un archivo export_results.html que contiene toda la información sobre los resultados de la exportación, como cantidad de chats, contactos, etc. Probablemente al exportar toda la base de datos, no requiera del total de la información para presentar, ya que hay mucho contenido que es de índole privada o no es pertinente. Por tal motivo hay que realizar el análisis de los archivos:

   i. Encontrará dentro de la carpeta chats una sub carpeta por cada conversación, deberá buscar la que corresponda a la o las conversaciones de interés. Esa carpeta contiene toda la información: el archivo messages.html (que contiene la conversación) y todas las carpetas correspondientes a audios, fotos, stickers, etc.

   ii. Si no requiere (porque no es pertinente) todos los archivos, puede crear una nueva carpeta y copiar en ella los archivos necesarios.

   iii. En el caso que lo que se desee preservar sea un archivo de audio, proceder a la transcripción del mismo en formato texto.

   iv. Comprimir la nueva carpeta y hashear.

4. Dejar constancia

   Dejar una constancia escrita o realizar un informe. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - El Informe* -. Agregar al informe sugerido los datos recolectados en los puntos 1 y 2 del procedimiento.

5. Preservar y aportar

   Adjuntar el archivo de texto conteniendo el mensaje completo original que se quiere aportar en el medio que se considere pertinente. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Dispositivos de Almacenamiento* -

Aportar los archivos de interés por el medio más adecuado, y respetando las normas de procedimiento.

5.3 Guía y Recomendaciones para el aseguramiento de información en Redes Sociales.

A. Conceptos generales.

El concepto de medios sociales (social media) implica la producción de contenidos de manera descentralizada y sin el control editorial de los grandes grupos. Es decir, significa la producción de muchos para muchos.

Siguiendo a Fernando Tomeo[22], citado por G Bielli y C. Ordoñez[23] "las redes sociales pueden definirse como espacios digitales que brindan a los ciudadanos la oportunidad de compartir información personal de especial interés, bien sea mediante el intercambio de imágenes y videos que contengan vivencias personales, perfiles profesionales encaminados a explorar oportunidades laborales o simplemente el encuentro con amigos y familiares que, por la distancia, pueden encontrar en estos medios una ocasiones ideal para reunirse virtualmente."

Andreas Kaplan y Michael Haenlein definen los medios sociales como "un grupo de aplicaciones para Internet, desarrolladas sobre la base de los fundamentos ideológicos y tecnológicos de la Web 2.0, y que permiten la creación y el intercambio de contenido generado por el usuario (UCG, User Generated Content)"[24].

Las redes sociales tienen su origen a mediados de los años ´90 con el sitio *www. classmates.com* de Randy Conrads, que procuraba mantener contactos con compañeros que se hubieran educado juntos.

Las redes permiten agrupar y compartir gran cantidad de información personal de cada uno de sus usuarios en el espacio electrónico compartido con otras personas. También permiten la comunicación instantánea entre los usuarios.

[22] TOMEO F., 2010, Las redes sociales y su régimen de responsabilidad civil, L.L.2010-C-1025
[23] BIELLI G. y ORDOÑEZ C., 2021, Tratado de la prueba electrónica, Tomo 1 Cap. 4, Ed. Thomson Reuters. Bs.As., pág. 803
[24] KAPLAN, A. M. and HAENLEIN, M. ,2010, Users of the world, unite! The challenges and opportunities of Social Media, Business Horizons, p. 61, 59-68.

Los medios sociales pueden tener diferentes formatos como blogs, intercambio de fotos, videologs, scrapbooks, correo electrónico, mensajes instantáneos, intercambio de canciones, crowdsourcing, VoIP, entre otros.

Además, las personas pueden acceder a las redes sociales desde cualquier dispositivo móvil con conexión a Internet, y pueden compartir información con distintos formatos, como textos, fotografías, audio y video.

En los últimos años han aumentado en progresión geométrica la cantidad de usuarios, quienes muestran sus actividades diarias y compartiendo videos, fotos y todo tipo de información.

Los medios sociales o redes sociales presentan varias características que los diferencian fundamentalmente de los medios tradicionales.

Primeramente, dependen de la interacción entre personas, porque la discusión y la integración entre ellas construyen el contenido compartido, y utilizan la tecnología como conductor.

Segundo, los medios sociales no son finitos: no existe un número determinado de páginas u horas. El público puede participar en un medio social haciendo un comentario o incluso modificando las historias. Los contenidos de un medio social, en textos, gráficos, fotos, audios o vídeos, se pueden mezclar. Otros usuarios pueden crear mashups y recibir actualizaciones a través de lectores de feed.

Significa un amplio espectro de tópicos, con diferentes connotaciones. Cabe resaltar que la optimización en los medios sociales (SMO, Social Media Optimization) es el proceso de distribuir de una mejor manera, entre varias redes y medios sociales, el contenido creado por el público. Estas mejoras incluyen agregar vínculos a servicios como Digg, Reddit y Del.icio.us para que las páginas puedan guardarse y compartirse fácilmente.

El contenido vertido en las redes sociales es dinámico, creado por las acciones realizadas por el propio usuario y los intercambios con otros usuarios que la aplicación permite. Se constituyen de este modo en especiales instrumentos de comunicación que otorgan poder a quienes lo utilizan.

En cuanto a las redes sociales más conocidas, como Facebook, Instagram, TikTok, Twitter, LinkedIn, tienen la particularidad de que cada usuario y usuaria debe generar un espacio propio, una *cuenta*.

El problema es que "nada nos asegurará, en principio, que el espacio generado por el usuario coincida con los demás datos reales que hagan a su persona. Es decir, la existencia por ejemplo de una cuenta en Facebook a mi nombre no quiere decir, necesariamente, que haya sido yo mismo quien lo ha creado o que sea yo quien lo administre. Con todo, la información allí existente tendrá mayor eficacia probatoria si puede acreditarse la veracidad de los datos consignados en el perfil del autor."[25].

Algunas redes sociales han implementado sistemas de verificación de cuentas, con criterios más o menos estrictos (como demostrar que se trata de una figura pública, una marca reconocida o una empresa importante) para confirmar la autenticidad de una cuenta pública. Las cuentas verificadas se identifican por un icono de verificación azul al lado del nombre de la cuenta, y este icono puede indicar que la cuenta es auténtica y oficial en esa red social, aunque estas cuestiones varían por lo que hay que chequear las condiciones del servicio al momento de realizar la operación.

Otro elemento característico es que los usuarios pueden configurar su privacidad dentro de la red, y seleccionar/elegir con quién o quiénes quieren compartir su información (llamados amigos o seguidores), que estará vedada al resto de la comunidad. Por lo tanto, se requieren *permisos* para conocer determinada información. Esa autorización o habilitación, además, puede ser general, es decir, el usuario puede configurar su cuenta como *pública* y así decidir que cualquier persona pueda ver su información. O bien puede ser particular, cuando el usuario configura su cuenta como *privada* y autoriza en forma expresa a cada persona que pretenda acceder a ella. Pero incluso, el titular de la cuenta puede configurar supuestos especiales de privacidad de cierta y determinada información y establecer niveles de restricción o niveles de acceso, por ejemplo, los llamados "mejores amigos" en la red social Instagram.

Para Quadri, en el primero de estos casos (cuenta de configuración pública) "no habrá ningún tipo de inconveniente para la recolección probatoria en cuanto a la

[25] QUADRI, H, 2020, La prueba electrónica y los procesos de familia (WhatsApp, archivos multimedia y Facebook), en GRANERO, H, Derecho Procesal Informático: E-mails, chats, WhatsApp, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías. Validez probatoria en el proceso civil, comercial , penal y laboral. Ed. El Dial.com, Bs. As, p. 224.

información referente a otras personas; pero si se trata de recabar alguna información que no está accesible para el público en general, aquí se genera un problema" [26].

Respecto al marketing de medios sociales, el mismo abarca la creación de contenido memorable, único y con potencial para convertirse en noticia. En tal caso, se puede difundir este contenido por medio de su popularización, o hasta por la creación y propagación de vídeos "virales" en YouTube, por ejemplo, y cuando conquistaron el gusto de los usuarios, perfilan sus preferencias. Aquí aparece el valor de las redes sociales, que está determinado por la cantidad de usuarios que poseen en sus distintas categorías. [27]

B. Aspectos jurídico-legales.

Una primera hipótesis, sostenida por la jurisprudencia[28], indica que, salvo los mensajes cursados en forma privada en redes sociales, casi por definición, éstas implican la voluntad de comunicarse impersonalmente con una audiencia potencialmente infinita.

En consecuencia, la primera tarea será identificar si la publicación en la red social es de contenido de acceso público, o se trata de un mensaje privado.

En 2014, la Corte Suprema de Justicia de la Nación, adhiriendo al dictamen del Sr .Procurador Eduardo Casal, afirma que las cuentas de correo electrónico y de "Facebook" constituyen una "comunicación electrónica" o "dato informático de acceso restringido".[29]

En segundo lugar, la cantidad de información que se publica, procesa y distribuye en redes sociales derivará en la complejidad de la recolección y preservación de la prueba como en su autenticación.

Para Quadri, "habría que acudir a las reglas del Código Penal (art. 153,153 bis y 155) y a las del Código Civil y Comercial de la Nación vinculadas a la correspondencia como prueba en los procesos (art. 318); para la licitud o no"[30].

---

[26] QUADRI, H, 2020, La prueba electrónica y los procesos de familia (WhatsApp, archivos multimedia y Facebook), en GRANERO, H, Derecho Procesal Informático: E-mails, chats, WhatsApp, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías. Validez probatoria en el proceso civil, comercial , penal y laboral. Ed. El Dial.com, Bs. As, p. 224.

[27] apartado construido a partir de las siguientes fuentes bibliográficas. BID, 2013, Manual de orientación para participar en redes sociales, disponible en: https://publications.iadb.org/es/publicacion/14832/manual-de-orientacion-para-participar-en-redes-sociales (consultado 28 de abril de 2023); Corvalán, J, Coord., 2021, Tratado de inteligencia artificial y Derecho, Ed. La Ley, Bs. As, Tomo I, p. 515-554

[28] CNAL Santa Fe, Sala II, 16/9/16, "Perticarari, Marcelo Betiana y ot, c/ la Red Informátiva SRL y ots s/ CPL

[29] CSJN, Competencia N° 778, L. XLIX, in re "Díaz, Sergio Darío s/violación correspondencia medios elect. arto 153 2° p", sentencia 24 de junio de 2014.

También menciona que es viable apelar a la declaración testimonial de las personas vinculadas a las cuentas de usuario en análisis, a fin de determinar si existía alguna interrelación o no con el hecho o el sujeto que se investiga o que se quiere probar.[31]

Entendemos que, en el caso concreto, cada juez o jueza deberá analizar la información que pretenda aportarse al proceso y cómo ha sido recolectada, y ponderarla a la luz del perfil del titular de la cuenta, de la configuración de privacidad de la red social y de las políticas institucionales de la red social.

Por último, no debemos olvidar que las redes sociales son un medio más que propicio para profundizar los conflictos ya generados y la posibilidad permanente de dañar o perjudicar la reputación de personas, sus sentimientos, el acoso o el chantaje sexual, y nuevas formas de violencia de género (art. 5 inc. 2 e, inc. 5, Ley 26485).

C. Procedimiento.

Al momento de preservar la prueba que se encuentra en una red social, se debe diferenciar el procedimiento según dónde se encuentre la información de interés: si está publicada en la cuenta del usuario, o, si es información que se encuentra en un perfil público o en la cuenta de un contacto del usuario. A continuación, se brindará una serie recomendaciones y buenas prácticas para la obtención de este tipo de pruebas dependiendo el caso, siempre tomando como referencia los Pasos Metodológicos - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses* -. Para cada una de las actividades y pasos propuestos, se detalla a la fase que pertenece de dichos pasos.

Preservación de la prueba que se encuentra en un perfil público o en un contacto de la cuenta del usuario

Si bien se suele recomendar no presentar como prueba las capturas de pantalla *(ver apartado general de Captura de Pantalla)*, cuando la información que se desea preservar se encuentra en un perfil público o en una cuenta de un contacto, no se puede guardar la información de otra manera que permita asegurar que la información quede completa.

---

[30] QUADRI, H, 2019, La prueba electrónica y los procesos de familia (WhatsApp, archivos multimedia y Facebook), en GRANERO, H, Derecho Procesal Informático: E-mails, chats, WhatsApp, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías. Validez probatoria en el proceso civil, comercial , penal y laboral. Ed. El Dial.com, Bs. As, p. 209

[31] Quadri, G. H, Testimonial y prueba electrónica en Bielli-Ordoñez-Quadri, 2021, Tratado de la Prueba Electrónica, La Ley, Bs. As, p. 663

1. *Registrar el nombre de usuario y la cuenta de mail* a la que se asocia la cuenta del usuario. (Fase “Análisis de Escenario”)

2. *Registrar el nombre de usuario y la cuenta de mail* a la que se va a acceder (ya sea un contacto o una cuenta pública) desde la cuenta del usuario. (Fase “Análisis de Escenario”)

3. *Capturar cada una de las pantallas* siguiendo alguno de los siguientes métodos (Fase de “Descarga de Información”:

    a. Captura de pantalla de Windows. Tecla Inicio+PrintScreen.
    (se almacena automáticamente en formato imagen png una instantánea de la pantalla en la carpeta C:\Users\usuario\Pictures\Screenshots o C:\Users\usuario\Imagenes\Capturas de Pantalla).

    b. Función Imprimir y Guardar como PDF del navegador.

4. *Generar archivo comprimido y obtener valor hash:* guardar todas las imágenes o archivos pdf dentro de una carpeta, comprimir la carpeta y generar el código hash correspondiente. (Fase de “Compresión”) - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Hash -*

5. *Generar un sellado de tiempo (Fase de “Hash”):*

    a. Si se posee firma digital, inmediatamente después de haber obtenido las imágenes podría aplicarle la firma digital a los mismos con un servidor de sellado de tiempo (timestamp) configurado. Para ello se necesita tener las imágenes en formato pdf. Si se usó la opción uno, se deberá generar un archivo pdf con las imágenes.

6. Dejar constancia

    Dejar una constancia escrita o realizar un informe. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - El Informe -*. Agregar al informe sugerido los datos recolectados en los puntos 1 y 2 del procedimiento.

7. Preservar y aportar

   Adjuntar el archivo de texto conteniendo el mensaje completo original que se quiere aportar en el medio que se considere pertinente. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Dispositivos de Almacenamiento -*

   Aportar los archivos de interés por el medio más adecuado, y respetando las normas de procedimiento.

Preservación de la prueba que se encuentra en el perfil de usuario del usuario

Como ya fue mencionado a lo largo de esta guía, realizar capturas de pantalla no es el procedimiento más aconsejable *(ver apartado general de Captura de Pantalla)*.

En reemplazo o como complemento de la captura de pantalla, se recomienda la descarga del archivo de datos del usuario. Hay que tener en cuenta que, para ello, el usuario deberá acceder a su cuenta con sus datos de login.

El archivo de datos registra toda la actividad de una cuenta en la red social, desde la creación de la misma hasta el momento en que se realiza la solicitud de datos. Cualquier información o dato posterior al momento del pedido no será incorporado en el archivo correspondiente.

Este procedimiento debe llevarse a cabo con la autorización del usuario (el propietario de la cuenta en la red social).

Si bien tanto la solicitud del archivo de datos como su descarga es posible realizarla desde la aplicación móvil de la red social, recomendamos hacer la descarga desde el equipo del estudio jurídico, perito o funcionario interviniente.

1. *Registrar el nombre de usuario y la cuenta de mail* a la que se asocia la cuenta del usuario.

   Esta tarea corresponde a la Fase “Análisis de Escenario” de los pasos metodológicos.

2. *Solicitud de datos a la red social:*

   a. Cada red social tiene una forma distinta de cómo se puede acceder a los datos, que deberá ser consultada para cada caso en particular. Si es posible

especificar el formato que tendrá el archivo de datos, tener en cuenta que los formatos JSON o XML son más fáciles de analizar con herramientas de procesamiento de datos, mientras que el formato HTML será más fácil de leer para una persona.

b. La disponibilidad del archivo de datos puede ser inmediata, o demorar en función de la cantidad de datos que se pidan y del período de tiempo solicitado y el formato del archivo de descarga.

Esta tarea corresponde a la Fase "Análisis de Escenario" de los pasos metodológicos.

3. *Descarga del archivo de datos:*

a. Una vez que el archivo está disponible para ser descargado, la red social envía un link de descarga con un período de validez a la dirección de correo electrónico asociada con la cuenta.

b. Algunas redes sociales imponen un período de restricción para repetir el pedido de descarga del archivo de datos, por ejemplo, de un mes. Es decir, una vez que se pide la descarga **del archivo de datos completo**, éste se procesará y no se podrá hacer un nuevo pedido de toda la información por el plazo de restricción establecido.

c. De acuerdo al tamaño del archivo de datos, es posible que el mismo se encuentre dividido en varios archivos comprimidos.

Esta tarea corresponde a la Fase "Descarga de Información" de los pasos metodológicos.

4. *Generar archivo comprimido y obtener valor hash:*

Una vez que se cuenta con el **archivo de datos completo**, si no estuviera comprimido se sugiere comprimir el mismo y calcular la función hash a fin de garantizar la integridad.

Esta tarea corresponde a la Fase "Comprensión y Hash" de los pasos metodológicos. -*ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Hash* -.

5. *Extracción de **archivo de interés**:* El **archivo de datos completo** tiene toda la información de la cuenta que fue recopilada por la red social durante el período solicitado, por lo tanto, es importante desglosarlo para extraer únicamente la información relevante, y, en la medida de lo posible, se recomienda detallar la utilidad y relevancia del aporte presentado. Asimismo, para cada archivo extraído, o fragmento de información que se separe del conjunto, es necesario dejar constancia de:

    a. Origen del dato o archivo: nombre de la Red Social, cuenta del usuario, archivo origen de datos completo la extracción, fecha de la descarga, entre otros. *Por ej: Extraído de la cuenta xx de la red social xx de la descarga xx.zip solicitada para el período entre xx y xx y descargada en la fecha xx.*

    b. Valores de hash de los archivos extraídos y función utilizada. Por ej: Se realizó el cálculo de hash con la función SHA-256 obteniendo el valor. xx - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Hash -.*

6. *Dejar constancia*

    Dejar una constancia escrita o realizar un informe. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - El Informe -.* Agregar al informe sugerido los datos recolectados en los puntos 1 y 2 del procedimiento.

7. *Preservar y aportar*

    Adjuntar el archivo de texto conteniendo el mensaje completo original que se quiere aportar en el medio que se considere pertinente. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Dispositivos de Almacenamiento -.*

    Aportar los archivos de interés por el medio más adecuado, y respetando las normas de procedimiento.

D. Casos de uso. Ejemplos.

Se busca aportar como prueba comunicaciones electrónicas llevadas a cabo a través de una red social (Twitter, Instagram, Facebook, TikTok). Para proceder con la mayor rigurosidad posible, se plantea descargar el archivo de datos completo (en general disponible, pues casi todas las redes sociales operan en el espacio europeo y deben cumplir con el Reglamento General de Protección de datos de la Unión Europea- RGPD), y de esta manera se contará con toda la información, mensajes, archivos multimedia, interacciones, y otras formas de comunicación que hayan sucedido entre las dos partes a través de la red social en cuestión.

Caso de Uso: Facebook

1. Registrar el nombre de usuario y la cuenta de mail a la que se asocia la cuenta del usuario. La cuenta de mail y/o nombre de usuario podrá ser aportada por el usuario. En caso de no poseer alguno de los dos datos se deberá buscar dentro de la información del usuario de Facebook

2. Solicitar a Facebook, el archivo de datos o información de perfil.

    a. Elegir el formato de la solicitud de descarga (HTML, JSON).

    b. Definir la calidad con la que se descargará el contenido multimedia (alta, media, baja)

    c. Establecer un rango de fechas para el archivo de datos.

    d. Iniciar el pedido. El mismo se encontrará pendiente hasta que Facebook lo genere. Una vez finalizado este proceso Facebook le avisará por un mail a la cuenta asociada al usuario.

3. En cuanto esté disponible, proceder a descargar el archivo en la computadora. Dependiendo de la cantidad de información solicitada puede ser que sea más de un archivo.

4. Generar el Hash correspondiente al o los archivos que se descargan.

5. Proceder a la descompresión de los archivos y a su análisis.

6. Una vez encontrada la información que se necesita, separarla, colocarla en una carpeta aparte. Generar el hash de cada archivo individual. Comprimir la carpeta y volver a

calcular el valor de hash. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Hash -.*

Dejar una constancia escrita o realizar un informe. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - El Informe -.* Agregar al informe sugerido los datos recolectados en los puntos 1 y 2 del procedimiento.

6. Preservar y aportar

Adjuntar el archivo de texto conteniendo el mensaje completo original que se quiere aportar en el medio que se considere pertinente. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Dispositivos de Almacenamiento -.*

5.4 Recomendaciones para el aseguramiento de información de Sitios Web.

A. Conceptos generales.

Los conceptos de *página web* y *sitio web* se emplean, en numerosas ocasiones, indistintamente, y no son pocas las personas que denominan página web a aquello que, en realidad, es un sitio web. Si bien esta asimilación es errónea son conceptos estrechamente vinculados.

El *sitio web* o *website*, es un conjunto de páginas web vinculadas o documentos de temática relacionada, es decir, un gran espacio virtual que contiene documentos (páginas), organizados en Internet y se identifica con un nombre de dominio. Por otro lado, la *página web* es una parte o sección de dicho sitio. El *sitio web* puede alojar una o más *páginas web*.

El conglomerado de todos los sitios web existentes da lugar a una red muy amplia de información que se conoce como World Wide Web (WWW).

Por otro lado, los *website* tienen un determinado formato (escritos en código HTML) que alberga información, ya sea textual, gráfica, visual o sonora. Esa información está en

Internet y es accesible gracias al protocolo HTTP, y para acceder a ellos, es necesario un navegador, como Internet Explorer, Google Chrome, Safari o Mozilla Firefox.

Como señalamos, la información en el *website* tiene cierta organización que podemos caracterizar como jerárquica. Así, la información principal estará en la página de portada o *homepage*, que coincide con la URL raíz del website. A partir de esta página de inicio nos encontraremos con los llamados hipervínculos que nos dirigirán hacia el resto de páginas que integran el sitio.

Cuando hablamos de sitios web podemos encontrar sitios de noticias (diarios digitales), sitios de descarga de software (ej. Softonic), sitios de compraventa o subasta de productos y servicios (ej. Mercado Libre, Amazon, eBay), buscadores (ej. Google, Safari), blogs, sitios de empresas (ej. bancos), sitios educativos (ej. Moodle), redes sociales (ej. Facebook, Instagram). En particular, las redes sociales son analizadas en un apartado específico de la guía.

En cuanto a las páginas web, pueden dividirse en dos tipos: estáticas y dinámicas. Las páginas más estáticas se componen básicamente de texto e imagen, y se caracterizan por un contenido que no varía -o varía muy poco- en un periodo de tiempo.

Las páginas dinámicas, como su nombre lo indica, son dinámicas y permiten la interacción con el usuario en tiempo real. Tal es el caso de las tiendas virtuales, los buscadores, las redes sociales.

En cuanto a la naturaleza jurídica, podemos decir que, en general, la página web se asimila a la de documento electrónico.

Será entonces la página web, contenida en el sitio web o *website*, en donde estará la fuente de prueba que se quiere adquirir, resguardar o preservar, esto es imágenes/fotografías, textos, videos, blogs, transmisiones en vivo, cortometrajes, documentales, grabaciones de audio, links o enlaces, entre otros elementos .

B. Aspectos jurídico-legales.

El conjunto de páginas web conforman el sitio web, y ese sitio web necesitará un *dominio* y un servicio de *hosting*.

El nombre de dominio (dominio) es un nombre fácil de recordar asociado a una dirección IP física de Internet. Es la dirección que tendrá un sitio web y que las personas escribirán en la barra de búsqueda de su navegador para visitarlo. Cada sitio web tiene un dominio y se trata de un nombre único en el Sistema de Nombres de Dominio (DNS) de Internet.

Por otra parte, el hosting es el almacenamiento que aloja la información de diversos sitios web y que, por tanto, resguarda el contenido de un dominio.

En forma sencilla podemos decir que el nombre de dominio es como la dirección de su hogar. Por otro lado, el alojamiento web es la casa en la que vive su página web. En ella se almacenan todos los archivos correspondientes a su sitio web. Esto es ofrecido por las empresas de hosting.

Para iniciar una página web, se necesitará un nombre de dominio y también un alojamiento web.

En el caso de los dominios, existen distintos niveles: nivel superior (TLD), segundo nivel (SLD), tercer nivel y subdominios.

En los dominios de primer nivel (TLD), tenemos a su vez:

a) Nombres de Dominio Internacionalizados (IDNs) o de Nivel Superior de Código de País: son los dominios genéricos, en este grupo se pueden encontrar las extensiones más conocidas y comunes: .com, .net, .org, etc. Las extensiones de los gTLDs en sus inicios iban dirigidas a la creación de un tipo de web temática en concreto, por ejemplo, los .org para organizaciones, .net para empresas tecnológicas, o los .edu para organizaciones educacionales. Esta orientación hoy día no sigue vigente, ya que se ha generalizado el uso de extensiones como .com para todo tipo de proyectos.
b) Dominios Geográficos/Territoriales: Estos tipos de dominios suelen corresponderse con las iniciales del nombre de los países. Así, cada país tiene su regulación específica sobre dominios y su propia denominación: en Argentina los dominios terminan en *.ar*, en España en *.es*, en México en *.mx*.

En el caso de Argentina, bajo la órbita de la Dirección Nacional del Registro de Dominios de Internet dependiente de la Secretaría Legal y Técnica de la Presidencia de la

Nación existe NIC Argentina[32]. Según el tipo de dominio (.ar, .com.ar, .net.ar, .gob.ar, .org.ar., .edu.ar., entre otros) deben cumplir ciertos requisitos y trámites, y pagar aranceles diferenciados [33]. No son trámites anónimos, pues se deben gestionar con número de CUIL/CUIT y clave fiscal (para personas residentes en nuestro país) o bien generar un usuario y contraseña (personas no residentes). Algunos dominios solo pueden ser registrados por Personas Jurídicas (.org.ar, .gob.ar). Los dominios tienen validez de 1 (un) año computado a partir de la fecha de su registro, pudiendo ser renovado en forma periódica.

C. Procedimientos

Constatar el Contenido de Páginas Web

Según la RAE, constatar es comprobar un hecho, establecer su veracidad, dar constancia de él. Al referirnos a una página web, cuando aplicamos el término constatar, hacemos referencia a comprobar o dar constancia de la existencia o del contenido de un sitio web en un momento específico.

Los sitios web son dinámicos, cambiantes. Con una simple actualización del sitio, en un momento determinado (por ejemplo, un diario) su contenido puede verse modificado. Por ese motivo se deben tomar todos los recaudos para la obtención de la prueba, siguiendo los pasos necesarios para poder constatar que el contenido de la web (incluyendo texto, imágenes, videos, links, etc.) sea real en un determinado momento.

Si bien a lo largo de esta guía recomendamos no presentar como prueba las capturas de pantalla - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital. - Captura de pantalla-* cuando la información que se desea preservar es la constatación de la existencia de una página web o sitio, y no se encuentra un procedimiento que funcione en todos los navegadores y que permita que toda la información quede completa, podrá utilizarse este mecanismo.

A continuación, se brindará una serie recomendaciones y buenas prácticas para la obtención de este tipo de pruebas dependiendo el caso, siempre tomando como referencia los Pasos metodológicos mencionados en el capítulo “3.2 - Actuación Metodológica”. Para cada una de las actividades y pasos propuestos, se detalla la fase que pertenece a dichos

[32] https://www.argentina.gob.ar/servicio/registrar-un-dominio-de-internet

[33] https://nic.ar/es/dominios/dominios_y_aranceles

pasos. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses -.*

Procedimiento para la constatación de una página Web

Se recomienda realizar el procedimiento de constatación mediante el uso de un navegador con una ventana de incógnito.

1. *Registrar URL del sitio a constatar*. Tener en cuenta que deben ser la o las URLs específicas a constatar, no siendo suficiente el nombre del dominio donde se alojan. Esta tarea corresponde a la Fase "Análisis de Escenario" de los pasos metodológicos. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Análisis de escenario -.*

2. *Fecha y hora*: verificar que el equipo con el que se realizará la constatación se encuentre con la fecha, hora y zona horaria bien configurada. Una vez comprobado esto, registrar fecha y hora de la constatación.

3. *Consultar y registrar la titularidad de un dominio*: Cuando una persona, empresa, organización, etc., quiere utilizar un dominio para su sitio web debe verificar que el mismo no se encuentre en uso. Si esto no ocurre, el dominio está disponible. El trámite mediante el cual se reserva el dominio asocia al mismo los datos del registrante, así como datos técnicos como son la fecha de registro y expiración, información de los DNS, servidor donde se encuentra alojado, entre otros. Todos estos datos son almacenados en una base de datos pública, que puede ser consultada.

   Existen dominios que se conocen como Dominios de Nivel Superior Genéricos que son aquellos que no se encuentran asociados a ningún país en particular. Son aquellos cuya terminación, por ejemplo, es .com .org, etc.

   Por otro lado, encontramos aquellos Dominios de Nivel Superior Geográfico que son los regionales, asociados a un determinado país, como por ejemplo los .ar .mx .br, etc. Cada país del mundo cuenta con una autoridad encargada de registrar los dominios. Dicha autoridad es NIC (Network Informacion Center – Centro de Información de la Red).

Para averiguar la titularidad de un dominio se utilizará el servicio WHOIS. Este protocolo permite realizar consultas a las bases de datos que almacenan la información referente al registro de los dominios.

En ocasiones hay dominios que no tienen disponible toda la información en el WHOIS porque tienen activada una opción de privacidad. Esto no nos permitirá conocer la información sobre el registro del dominio.

Se utilizará el WHOIS según el dominio del sitio:

a. Si es un dominio regional se deberá utilizar el WHOIS perteneciente al NIC de cada país. Por ejemplo, para los dominios .ar utilizar https://nic.ar/whois

b. Si es un sitio con otro dominio genérico se podrá utilizar algún sitio web que otorgue esta información, como por ejemplo: https://www.whois.com/ o https://whois.domaintools.com/

4. *Capturar el sitio web*

Esta tarea corresponde a la Fase "Descarga de Información" de los pasos metodológicos. Se sugiere la grabación de todo el procedimiento. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Descarga de información* -.

Si bien se podrían utilizar varias técnicas para el guardado de un determinado sitio web completo o de una URL (utilizando herramientas de terceros, o desde el mismo navegador), muchas de ellas no se pueden utilizar en todas las ocasiones ya que no siempre funcionan debido a restricciones de acceso a las páginas, configuraciones de cortafuegos, limitaciones de los navegadores, etc. Por otro lado, se debe tener en cuenta que en ciertos casos se deben guardar no sólo URLs de acceso público, sino también, URLs en las que para poder ingresar se requiera de usuario y contraseña (es el usuario quien debería proporcionar dicha información para poder ingresar) y las posibles herramientas anteriormente mencionadas, encuentran limitaciones ante esta situación.

Por lo mencionado es que, para la constatación del contenido de una determinada URL, se recomienda la técnica de capturar cada una de las pantallas correspondientes a la o las URLs que se desean guardar. Para ello se deberán seguir los siguientes pasos:

a. Abrir el navegador a utilizar e ingresar la URL a constatar. Escribir la dirección en la barra de dirección y no introducirla a través de un buscador para evitar algún posible error o confusión al seleccionar los resultados del buscador.

b. Capturar cada una de las pantallas siguiendo alguno de los siguientes métodos:

   i. Captura de pantalla de Windows. Tecla Inicio+PrintScreen. (se almacena automáticamente en formato imagen png una instantánea de la pantalla en la carpeta C:\Users\usuario\Pictures\Screenshots o C:\Users\usuario\Imagenes\Capturas de Pantalla).

   ii. Función Imprimir y Guardar como PDF del navegador.

5. Comprimir todos los archivos generados

Esta tarea corresponde a la Fase "Compresión y Hash" de los pasos metodológicos. Se sugiere la grabación de todo el procedimiento. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Compresión - Hash -.*

c. Si se posee firma digital, inmediatamente después de haber obtenido las imágenes aplicarle la firma digital a los mismos con un servidor de sellado de tiempo (timestamp) configurado. Para ello se necesita tener las imágenes en formato pdf. Si se usó la opción uno, se deberá generar un archivo pdf con las imágenes. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación*

metodológica - Pasos metodológicos sin herramientas forenses - Hash -

6. Dejar una constancia escrita o realizar un informe. - ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - El Informe -. Agregar al informe sugerido los datos recolectados en los puntos 1 y 2 del procedimiento.

7. Preservar y aportar

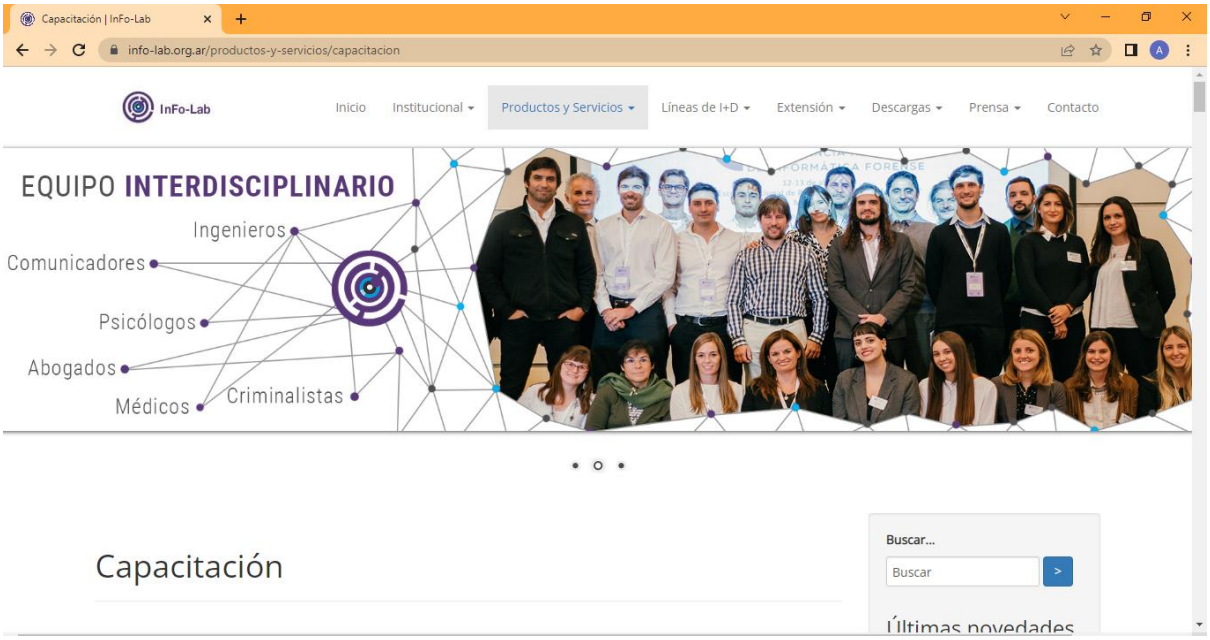
Adjuntar el archivo de texto conteniendo el mensaje completo original que se quiere aportar en el medio que se considere pertinente. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Dispositivos de Almacenamiento -.*

D. Casos de uso. Ejemplos.

Caso de uso: Preservación de un Sitio Web

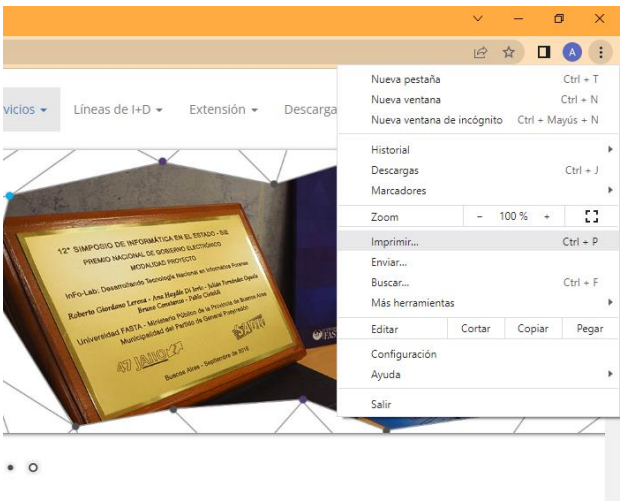
Se requiere guardar dos URLs correspondientes al sitio www.info-lab.org.ar. Las URLs son las que corresponden a Capacitación, que se encuentra dentro de Productos y Servicios https://info-lab.org.ar/productos-y-servicios/capacitacion y la de Novedades que se encuentra dentro de Prensa y cuya URL es https://info-lab.org.ar/prensa/novedades.

1. Registrar el nombre del sitio.
2. Verificar que el equipo tenga bien configurada la fecha, hora y huso horario.
3. Verificar y registrar el propietario.
4. Grabar todo el procedimiento.
5. Abrir el navegador e ingresar en la barra de direcciones la URL https://info-lab.org.ar/productos-y-servicios/capacitacion

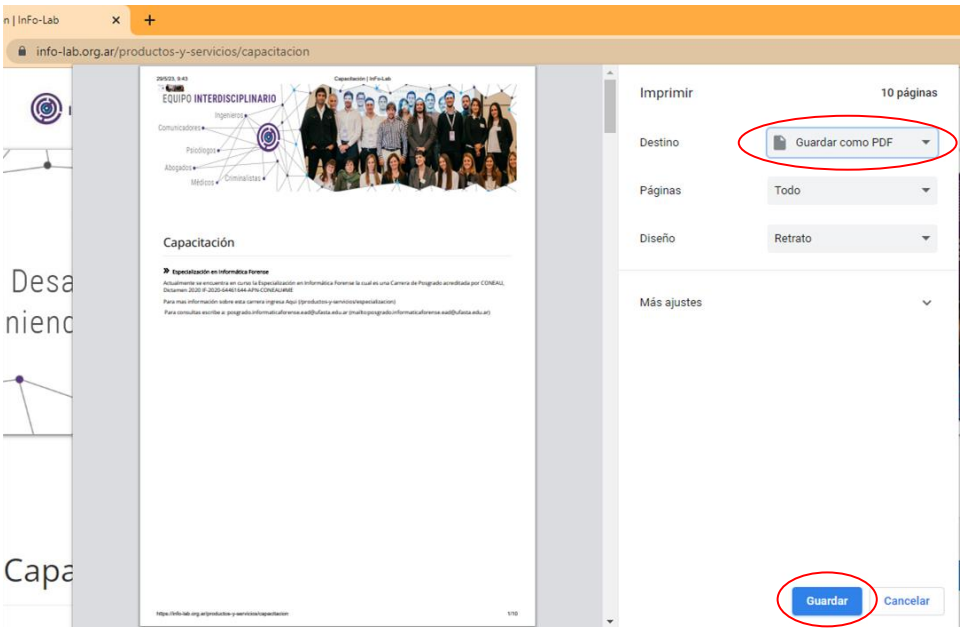


6. Guardar la página. En este ejemplo se muestran los pasos para guardarla como archivo PDF.

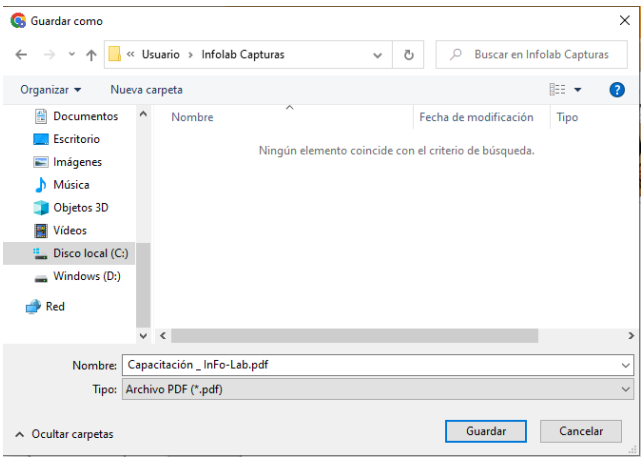
    a. Seleccionar la opción Imprimir dentro del navegador



b. Como destino seleccionar Guardar como PDF y luego hacer clic en Guardar.



c. Seleccionar la carpeta de destino donde quedará almacenado el archivo PDF y hacer clic en Guardar.



d. Repetir el proceso con la siguiente URL: https://info-lab.org.ar/prensa/novedades

7. Una vez que obtuvo todos los archivos, ya sea en forma de imagen o como archivo PDF proceder a comprimir la carpeta y generar el Hash correspondiente. *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Compresión - Hash -.*

8. Dejar una constancia escrita o realizar un informe. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - El Informe* -. Agregar al informe sugerido los datos recolectados en los puntos 1, 2 y 3 del procedimiento.

9. Preservar y aportar

   Adjuntar el archivo de texto conteniendo el mensaje completo original que se quiere aportar en el medio que se considere pertinente. - *ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Dispositivos de Almacenamiento* -.

Caso de Uso: Preservación de un Contenido obrante en YouTube

En este ejemplo se verá el caso particular en el que lo que se deba almacenar es un contenido del sitio www.youtube.com. Este caso de ejemplo deberá aplicarse cuando el contenido que deba guardarse sea el de un video que se encuentra en YouTube, porque directamente esa es la URL que se requiera, o puede ocurrir el caso en el que dentro de la página que se debía constatar se encontraba la referencia a un video de YouTube, por ejemplo, una URL de un diario donde en el desarrollo de la noticia se encuentra un link a un video que se encuentra en YouTube.

Este tipo de preservación requiere de cierta experticia y conocimientos más técnicos, por lo tanto, aconsejamos que lo asista una persona idónea o con conocimientos en dichos procedimientos.

Caso de uso: Constatación de información de sitios web inexistentes o actualizados

Preservar sitios Web mediante "Internet Archive - WayBack Machine"

Existen situaciones en las que se debe preservar un sitio web de acceso público[34] donde podría resultar ser un procedimiento engorroso y que, sí o sí, se necesite de un idóneo en la materia para poder llevarlo a cabo. A continuación, se presentará una alternativa muy eficaz a la hora de preservar un sitio web, de la que no se necesite más que una conexión a

[34] Se refiere a todos los sitios web que no requieran ningún tipo de acceso mediante credenciales, es decir, que sean vistos simplemente ingresando su dirección web.

Internet, y claro está, la dirección web del sitio a preservar, según las condiciones mencionadas anteriormente.

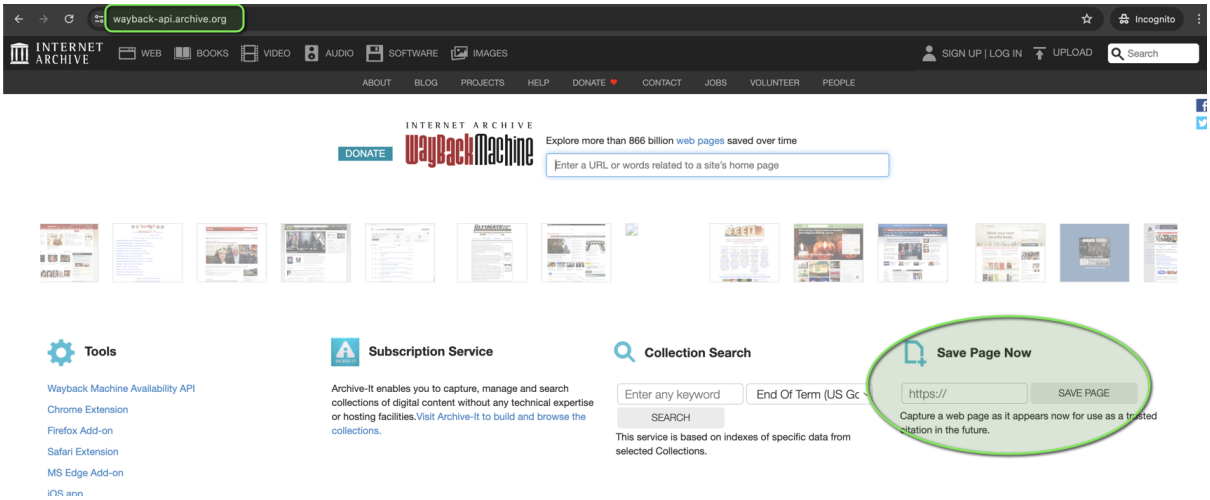
Internet Archive, como se ha mencionado en algunos otros pasajes de la guía, no sólo sirve para acceder a una instantánea de un sitio que ya no está disponible, sino que también, podría ser útil para almacenar una instantánea de un sitio en una fecha determinada, es decir, almacenar una captura del sitio web según cómo es que se lo ve al momento de realizar este procedimiento.

Para lograr esto, se debe utilizar la función de "Save Page Now" que presenta cuando se ingresa a https://wayback-api.archive.org/. Es importante mencionar que sólo se capturará "lo que se ve" al acceder a una dirección web o URL. La aplicación no preservará el sitio web completo, es decir, todo lo que aparece cada vez que se hace un clic sobre algún enlace. Si se desea preservar un sitio completo, o gran parte de este, se deberá acceder a cada enlace, o los que se requieran del sitio web, e ingresar cada una de las URLs (direcciones web) de las partes que se pretenden preservar.

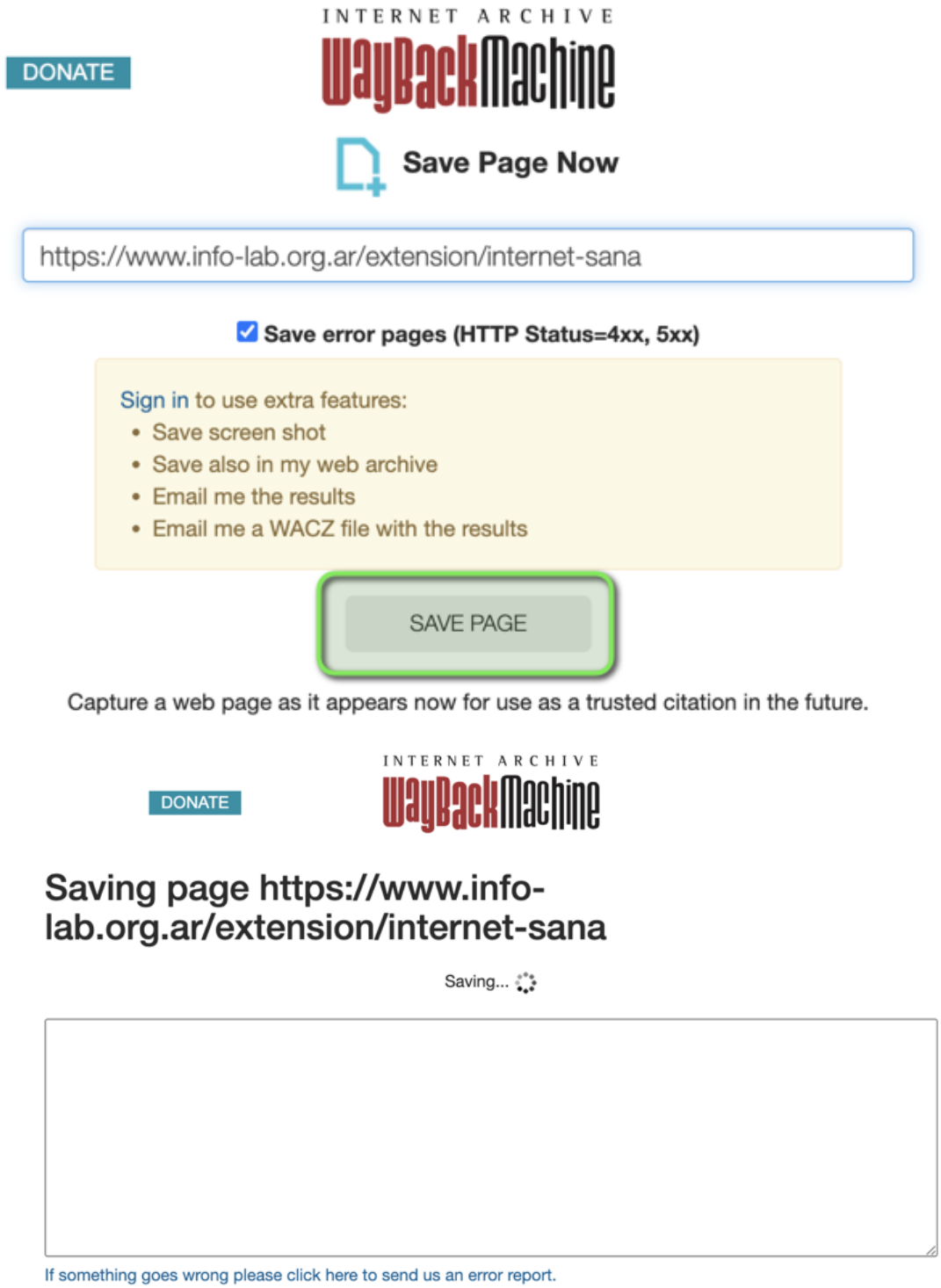
A continuación, se grafican y explican cada uno de los pasos necesarios para preservar un sitio web. De esta manera, se comprenderá de una manera más acabada su funcionamiento:

1. En primer lugar, se deberá tener la dirección web de una de las páginas del sitio web que se desea preservar. Para este ejemplo, se usará la URL https://www.info-lab.org.ar/extension/internet-sana, cuya página se muestra en la siguiente imagen:

2. Una vez copiado el enlace, se debe ingresar a https://wayback-api.archive.org/ y observar la sección de "Save Page Now", según se muestra en la siguiente imagen:



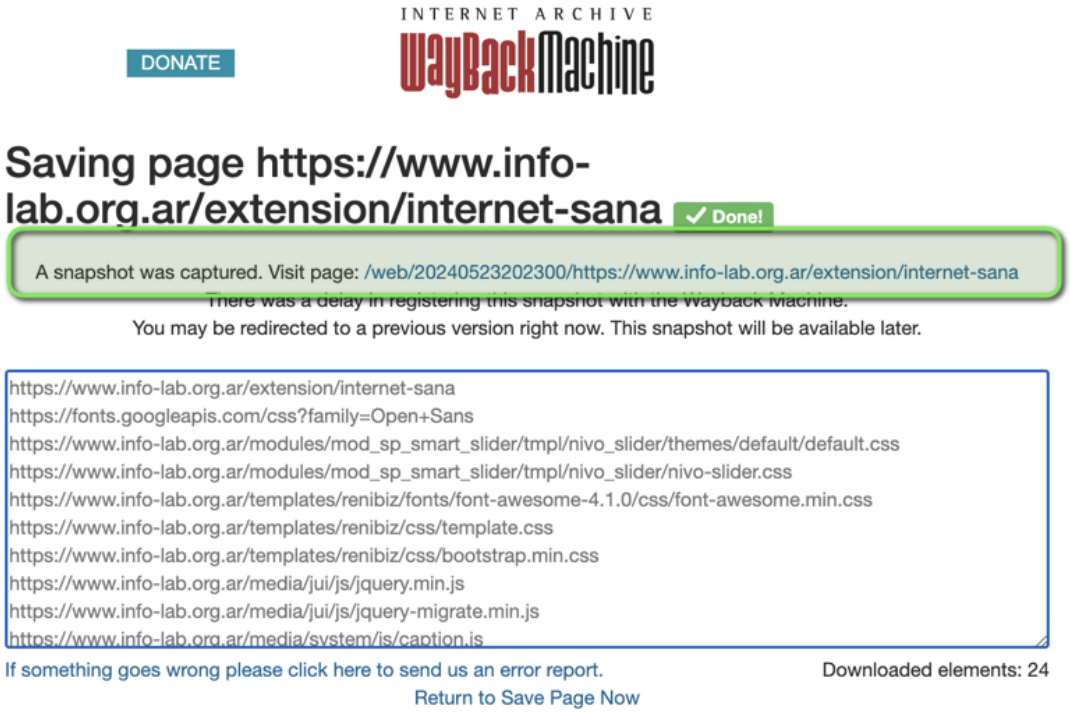
3. Luego, se debe pegar, o escribir, el enlace obtenido en el Paso 1, y hace clic en el botón "Save Page", como muestran las siguientes imágenes:



Es importante destacar que si nos registramos en "Internet Archive", podremos capturar mayor información sobre el sitio a preservar, como por ejemplo, guardar capturas de pantalla del mismo.

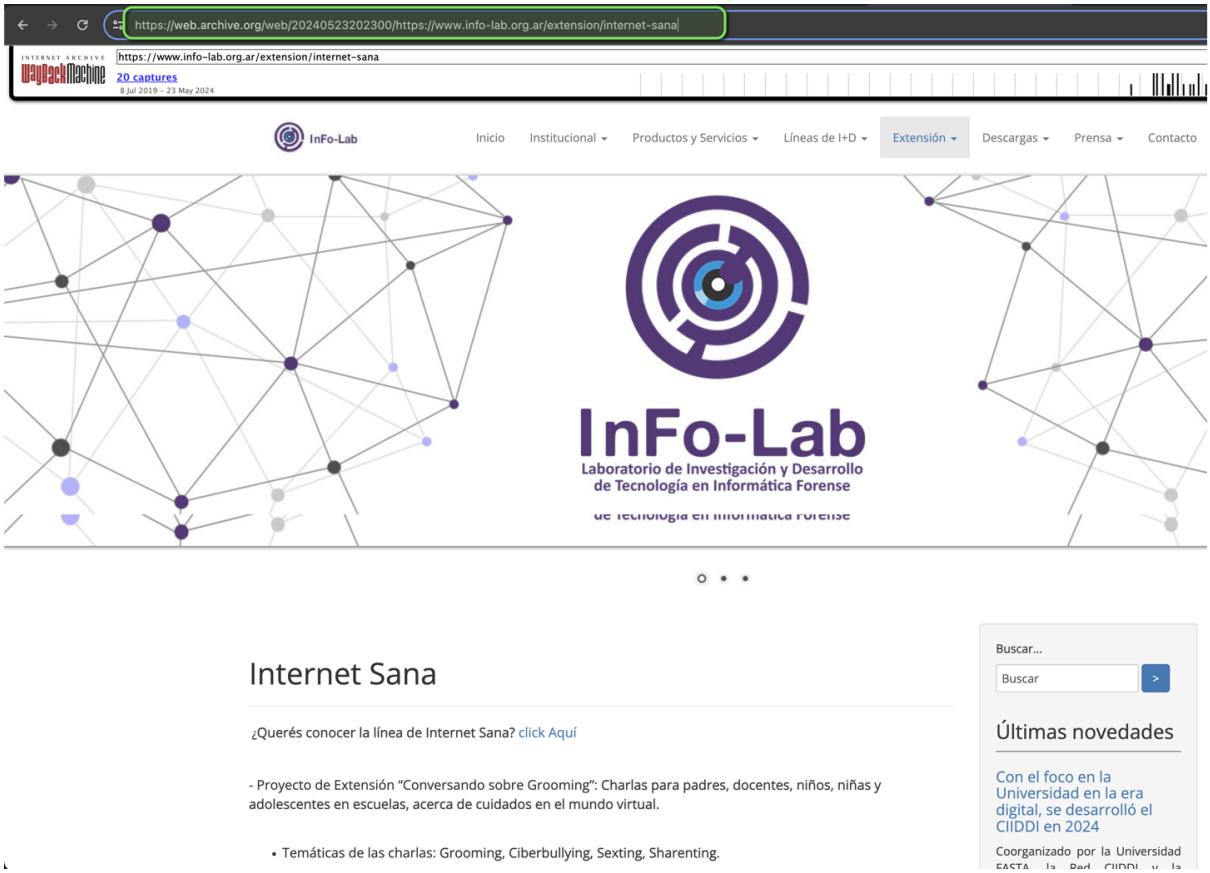
4. Una vez finalizado el proceso de preservación, "Internet Archive", nos informará la URL, o dirección web, en la cual quedará preservado el sitio web. Esta dirección web

no se modifica y perdura en el tiempo, lo que genera que siempre estará disponible para su consulta, como muestra la siguiente imagen:

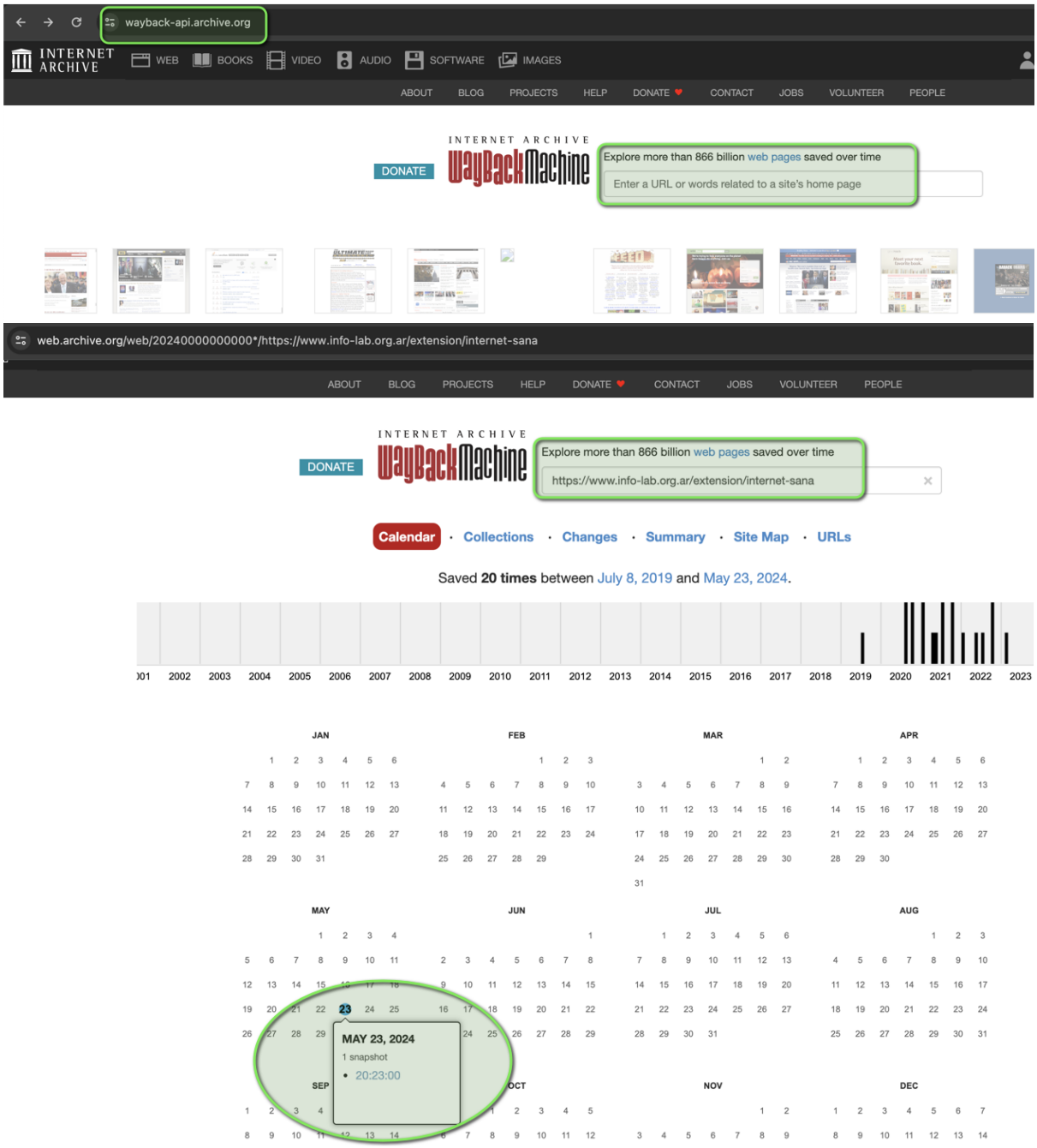


Para este ejemplo, la URL que se debe dejar asentada en el procedimiento es https://web.archive.org/web/20240523202300/https://www.info-lab.org.ar/extension/internet-sana. Esta dirección web presenta la marca de tiempo de la instantánea -20240523202300- donde los primeros 8 (ocho) números corresponde a la fecha y los restantes 6 (seis) corresponde a la hora en huso horario UTC+0. Para este caso, la fecha y hora de la captura sería el 23 de mayo de 2024 a las 20:23:00hs UTC+0. Si se desea pasar a horario local argentino (UTC-3), se deben restar 3 (horas) a la informada. La fecha y hora ahora quedaría como el 23 de mayo de 2024 a las 17:23:00hs. UTC-3.

5. Para acceder al sitio, es posible acceder simplemente pegando la dirección web informada en el paso anterior, como muestra la siguiente imagen:



También, y a modo informacional, es posible consultar cuántas capturas existen para ese sitio o dirección web en particular o bien consultar el histograma de capturas para ese sitio web o dirección web en particular. Para esto, simplemente se debe ingresar a la página principal de "Internet Archive - WayBack Machine"-https://wayback-api.archive.org/- y pegar o escribir la dirección web por la que se quiere consultar en la sección destinada a tales efectos. Una vez escrita la dirección web, se debe presionar la tecla "Enter" y se mostrará un histograma por año según capturas y, para cada año dentro de un almanaque, se mostrará los días en los que existen capturas de esa dirección web. A continuación, las siguientes imágenes, muestran estas características según el ejemplo realizado en los pasos anteriores:



Para ingresar a la captura, o instantánea deseada, sólo basta con hacer clic sobre el día y hora que se desea consultar.

Como se pudo ver este resulta ser un proceso sencillo del cual no se requieren conocimientos expertos ni una herramienta en particular para realizar un proceso de preservación de sitios web de acceso público. Por ejemplo, si se requiere preservar el contenido de un perfil de una red social o bien, una sección de un sitio web, pero luego de haber iniciado sesión en el mismo, este procedimiento no podrá ser utilizado.

Una vez finalizado el procedimiento de preservación, sólo es suficiente registrar la URL o dirección web informada por la aplicación web, la cual presenta también, las marcas de

tiempo. Esta URL no se modifica ni se elimina en el tiempo, por lo que, podrá perdurar durante todo el proceso judicial.

5.5 Recomendaciones generales para el aseguramiento de cualquier tipo de archivos cualquiera sea su formato

La presente guía ha mencionado los aspectos fundamentales para el correcto tratamiento de la información digital cuando ésta se encuentra en redes sociales, mensajería instantánea, correos electrónicos, entre otros. Pero es importante mencionar que el proceso para este correcto tratamiento es perfectamente aplicable a cualquier tipo de información digital, aun cuando el formato de archivo de la misma no se corresponde a los mencionados precedentemente.

Es por esta razón que siempre se debe intentar seguir los pasos metodológicos mencionados en el apartado *"Actuación Metodológica" - ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses -*. Es decir, en la fase de "Análisis de Escenario", se deben identificar las formas posibles de adquisición de la información digital. Luego, en la fase de "Descarga", se procederá a realizar la adquisición de esta información digital, por ejemplo, un archivo PDF. Acto seguido, en la fase de "Compresión", se procederá a generar un único archivo que contenga todos los archivos generados en la fase anterior para, posteriormente, calcular su valor de hash y redactar el informe o acta del procedimiento realizado. *- ver sección 4. Recomendaciones generales para el aseguramiento de la Prueba Digital - Actuación metodológica - Pasos metodológicos sin herramientas forenses - Análisis de escenario - Descarga de información - Compresión - Hash -.*

De esta manera, la Actuación Metodológica es siempre aplicable a cualquier tipo de formato de archivo que contenga la información digital que se requiera preservar, perdurando, este procedimiento en el tiempo, y sólo cambiando las técnicas de extracción según el tipo de información digital que se quiera preservar, custodiar y aportar a un proceso judicial.

6. Conclusiones y a futuro.

Las fuentes digitales de prueba ocupan un lugar creciente en los casos judiciales y generan un sinnúmero de desafíos para los operadores jurídicos: desconcierto, falsas certezas, subutilización y sobreutilización, procedimientos y valoraciones sumamente dispares, por mencionar sólo algunos de ellos.

Todo ello se proyecta sobre los grados de efectividad y equidad del acceso a justicia. Por ello insistimos en que esta guía propone un conjunto de requisitos que debería cumplir una prueba para ser considerada valiosa y útil en los procesos judiciales no penales, y que a un tiempo permita la búsqueda (y hallazgo) de la mejor evidencia posible dentro un contexto real y concreto de acceso a justicia.

Los fenómenos mencionados justifican ampliamente los esfuerzos para mejorar la utilización de estas fuentes probatorias. La presente guía se enmarca en dicho esfuerzo. Pero *no es una solución completa ni definitiva*.

Nuestra época presenta ciertos rasgos y tendencias que muy probablemente serán *perdurables* durante años. Por ejemplo, subsistirán:

- la digitalización de la información y de las comunicaciones
- las brechas digitales y su impacto en materia de acceso a justicia
- la mayor parte de los criterios generales sobre búsqueda, ofrecimiento, presentación y valoración probatoria
- la brújula del debido proceso y la tutela judicial efectiva, como contribución al logro de sociedades más justas, pacíficas e inclusivas

Este conjunto de desafíos nuevos y antiguos convivirá con nosotros durante bastante tiempo. Ello exige *profundizar* -y mucho- la investigación empírica y la reflexión, ampliar los espacios de intercambios transdisciplinarios y transversales, identificar las mejores prácticas e incorporar la variable de la prueba tecnológica en las evaluaciones de desempeño y en las iniciativas de mejora del acceso a justicia. Con esta guía no alcanza para lograr estos niveles de profundidad, y es bueno saberlo. Esta guía es sólo el inicio y un pequeño impulso que aporte a ese desafío.

A las cuestiones perdurables se les suman los *cambios* que se avizoran. Nuevos dispositivos y aplicaciones, modificaciones en los términos de servicios de las empresas tecnológicas,

novedosos hábitos sociales de uso de la tecnología, reformas normativas en todos los niveles y lugares, creciente impacto de la robótica y la inteligencia artificial (como fuente de conflictos y de prueba)...

Cada novedad genera nuevas preguntas en materia probatoria. Además, esta incesante corriente de cambios va modificando las fronteras entre ciencia, técnica y sentido común. Por ejemplo, el porvenir de la inteligencia artificial, internet de las cosas o la computación cuántica son escenarios que acrecentarán la ignorancia y/o el error de los profesionales del derecho. Por otro lado, la masificación del uso de tecnologías y la vulgarización de términos como IMEI, IP, hash, mutear o emoticon, muestran cómo se está ampliando la base de conocimiento común, con el riesgo de que algunos de esos conocimientos no sean certeros. En tales condiciones, la prueba indiciaria basada en fuentes digitales deberá ser permanentemente revisada y mejorada, no sólo en cuanto a su búsqueda y obtención, sino también en lo relativo a su comprensión, a la solidez de las premisas que ofrecen y a la confiabilidad de las máximas de la experiencia que se pretendan utilizar.

La topografía de las distintas brechas digitales también va cambiando, lo cual plantea desafíos para garantizar el acceso a justicia en condiciones de igualdad.

Por las razones mencionadas, quien piense que leer y aplicar esta guía es suficiente para estar al día, pronto se irá quedando en el pasado.

Será imprescindible mantener los conocimientos y la información actualizados, y esto refuerza la necesidad de participar de comunidades de aprendizaje y reflexión. El vínculo entre las instituciones judiciales, los colegios de abogados y la universidad debe fortalecerse, al igual que la fecundación cruzada entre disciplinas científicas. También se requiere aprovechar las posibilidades que ofrece la tecnología para lograr una ágil y eficaz gestión interinstitucional de la información y del conocimiento. Todo ello contribuirá a acortar, o cuanto menos no incrementar, la distancia temporal entre la aparición de nuevas fuentes de prueba tecnológica y la adopción de procedimientos probatorios fiables y justos.

Más concretamente, a fin de mantener conocimientos e información actualizados y accesibles, la presente guía podría evolucionar hacia una wiki con contenidos dinámicos de calidad. Este espacio también podría brindar otros servicios, como, por ejemplo:

- difusión de noticias tecnológicas, normativas o jurisprudenciales

- encuestas e investigaciones empíricas sobre las principales problemáticas y tendencias en materia de fuentes de prueba tecnológica, para detectar las carencias críticas de conocimiento de operadores judiciales y abogados
- directorios de entidades especializadas en prueba digital, de empresas y de organismos públicos vinculados con las nuevas tecnologías y la información digital
- tutorías científicas en casos paradigmáticos
- clínicas de casos y análisis de mejores prácticas
- foros permanentes de consulta

Esto exige algunos cambios de paradigmas y de prácticas. En primer lugar, pensar en la información y el conocimiento no como productos acabados, sino como algo que evoluciona. Es también necesario renunciar a la ilusión de que la jerarquía funcional es sinónimo de mayor conocimiento en todas las áreas de la prueba tecnológica. Asimismo, es preciso reconocer que necesitamos de otras personas y de otras disciplinas. Por último, pero no menos importante, estamos llamados a salir del rol de simples consumidores de información y volcarnos a la coproducción de nuevas preguntas y conocimientos.

Anexo I - Glosario

Autenticidad: La autenticidad en el contexto de la seguridad informática se refiere a la propiedad de un sistema, dato o entidad de ser genuino y confiable, es decir, de ser lo que dice ser y provenir de una fuente legítima. La autenticidad se utiliza para garantizar que la información no ha sido alterada, manipulada o falsificada de ninguna manera y que sólo es accesible o modificable por personas o sistemas autorizados.

La autenticidad es un componente esencial en la seguridad informática, ya que garantiza la integridad y la confianza de los datos y sistemas, evitando la suplantación de identidad, el acceso no autorizado y las manipulaciones maliciosas. Además, la autenticidad también es importante para establecer la trazabilidad y la responsabilidad en el uso de los recursos informáticos.

Base de datos: Se define una base de datos como una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa, organismo o negocio en particular. Desde el punto de vista informático, la base de datos es un sistema formado por un conjunto de datos almacenados en discos que permiten el acceso directo a ellos y un conjunto de programas que manipulan ese conjunto de datos. Cada base de datos se compone de una o más tablas que guardan un conjunto de datos. Cada tabla tiene una o más columnas y filas. Las columnas guardan una parte de la información sobre cada elemento que queramos guardar en la tabla, cada fila de la tabla conforma un registro.
Una base de datos es una herramienta para recopilar y organizar información. Pueden almacenar información sobre personas, productos, pedidos u otras cosas. Muchas bases de datos comienzan como una lista en una hoja de cálculo o en un programa de procesamiento de texto. A medida que la lista aumenta su tamaño, empiezan a aparecer redundancias e inconsistencias en los datos. Cada vez es más difícil comprender los datos en forma de lista y los métodos de búsqueda o extracción de subconjuntos de datos para revisión son limitados. Una vez que estos problemas comienzan a aparecer, una buena idea es transferir los datos a una base de datos creada con un sistema de administración de bases de datos (DBMS).

Compresión de datos: La compresión de datos reduce el tamaño de los mismos al minimizar los datos redundantes. En un archivo de texto, los datos redundantes pueden producirse con frecuencia en caracteres como el carácter de espacio o las vocales comunes. La compresión de datos crea una versión comprimida de los datos de entrada generando un único archivo

permitiendo una mejor manipulación de los mismos. Por ejemplo, en el caso por el cual será necesario adjuntar varios documentos o archivos en un proceso judicial, esta técnica no sólo es utilizada para reducir su tamaño sino también para aplicar una única función de hash al archivo comprimido generado.
Luego, para visualizar el contenido completo del archivo comprimido, se procede a realizar la descompresión del mismo y así visualizar la totalidad de los archivos que éste contiene.

Correo electrónico: El correo electrónico, conocido también por su nombre en inglés: e-mail, es un servicio de comunicación electrónica que, usando internet, permite el intercambio de mensajes y archivos digitales entre personas.

El correo electrónico se basa en el concepto de enviar mensajes electrónicos de un remitente a uno o varios destinatarios. Cada usuario tiene una dirección de correo electrónico única, que consta de un nombre de usuario seguido de un símbolo "@" y un dominio (por ejemplo, usuario@example.com). Esta dirección se utiliza para identificar y recibir mensajes de otras personas. Además, es posible adjuntar archivos de cualquier tipo al mensaje de correo electrónico, siempre respetando las condiciones de tamaño de archivo que impone el prestador de servicio, por lo general soporta archivos de un máximo de 20MBytes por mensaje.

Para enviar un correo electrónico, el remitente redacta un mensaje en un cliente de correo electrónico (programa que se utiliza para el envío y recepción del correo), como Gmail, Outlook o Yahoo Mail, etc., donde puede escribir el asunto, el cuerpo del mensaje y adjuntar archivos si es necesario. El mensaje se envía a través de servidores de correo electrónico que se encargan de su entrega al destinatario.

El destinatario puede acceder a su correo electrónico mediante un cliente de correo electrónico o mediante un servicio web de correo electrónico.

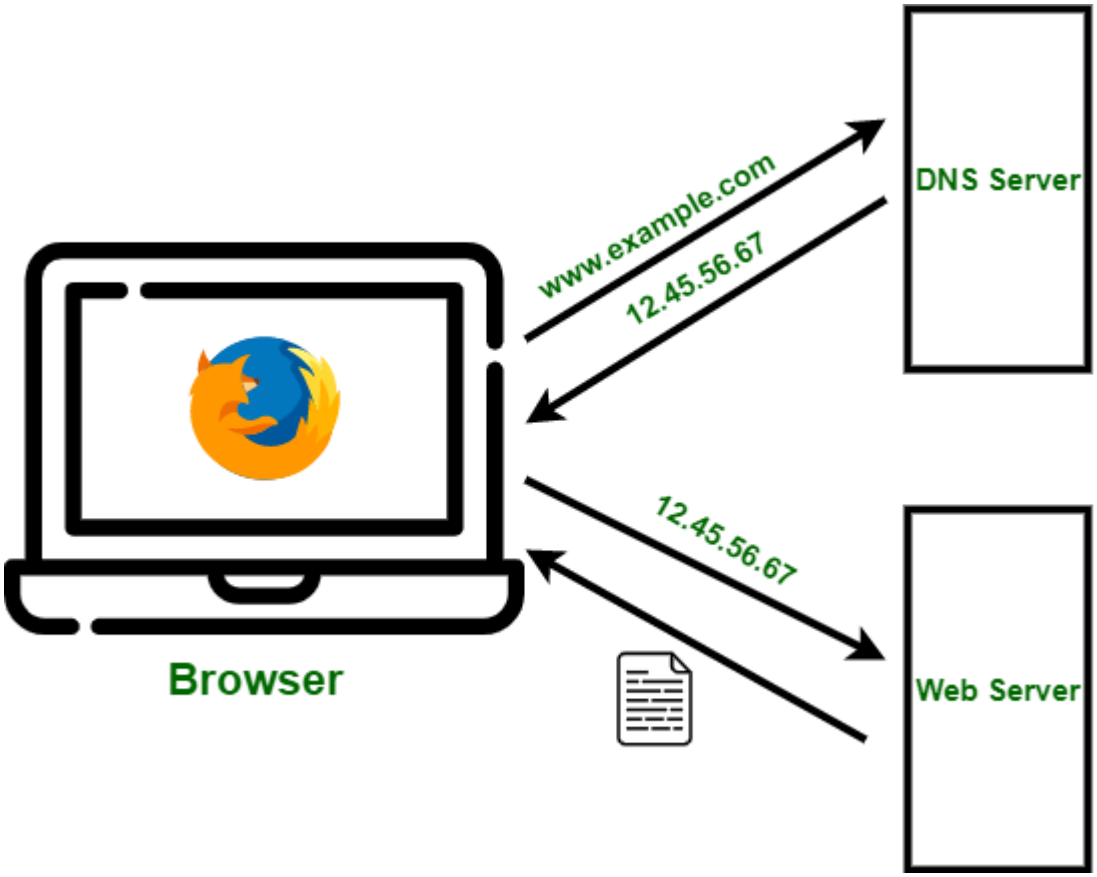
La mayoría de los clientes de correo electrónico permiten la descarga de los mensajes de correo electrónico de forma completa, conocida como "Mensaje original" o "Mensaje completo" entre otros. Este mensaje permite observar todas las características técnicas del mensaje y no sólo los remitentes, destinatarios, asunto y cuerpo del mensaje. Dicha descarga por lo general consiste en un archivo de texto, cuya extensión, suele ser ".eml" en la cual pueden observar y analizar las características mencionadas.

Servidores de correo electrónico: Los servidores de correo electrónico son los encargados de almacenar toda la información referente al envío y recepción de los mails: correos entrantes y salientes, carpetas del usuario, etc.

Dirección IP Pública: Es un número que en un momento particular identifica unívocamente cuando el equipo se encuentra conectado a Internet. Es decir, que las direcciones de IP pública son únicas en Internet, no hay duplicaciones, no puede haber dos dispositivos con la misma dirección IP pública conectado a Internet. En general, los dispositivos que se conectan a internet lo hacen a través de un router, un dispositivo que vincula a la red local (el wifi de una oficina, por ejemplo) con internet. Es función del router coordinar los pedidos de cada equipo de la red local para que lleguen a Internet, y que, al recibir una respuesta, estos sean dirigidos en la red local al equipo correspondiente. Dado que la cantidad de direcciones IP son limitadas, es común que una dirección IP sea asignada a múltiples clientes de un proveedor de internet en distintos momentos. Para dar acceso a Internet, un ISP debe contar con direcciones IP para asignar, y por lo tanto son los que pueden establecer la relación.

Dirección IP privada: Una dirección IP privada es un número que el router de red asigna a un dispositivo conectado a él por Wifi o por cable. Cada uno de los dispositivos de una misma red recibe una dirección IP privada exclusiva así es como se comunican los dispositivos dentro de una misma red interna o lo que es lo mismo, red de área local (LAN - Local Area Network). Las direcciones de IP privada están reservadas, esto quiere decir que existen rango de direcciones que sólo podrán ser utilizadas para una red privada y no podrán utilizarse para direcciones de IP pública.

DNS (Domain Name Server o Servidor de Nombres de dominio): es aquel dispositivo que se encarga de almacenar las direcciones IP para los nombres de dominio y de esta manera, responder traducir un nombre de dominio en su dirección IP correspondiente. El funcionamiento básico para una comunicación web de este procedimiento, es el siguiente:



Fuente: https://www.geeksforgeeks.org/working-of-domain-name-system-dns-server/

En primer lugar, el dispositivo que sea acceder al sitio web de "www.example.com", consulta, al DNS que tiene asignado, cuál es la dirección IP del dominio. Luego, el DNS responde con dicha dirección IP. Por último, el dispositivo que realizó la consulta establece la comunicación con la dirección IP que el DNS le respondió.

EML - Electronic Mail: Extensión de un archivo que contiene un mensaje de correo electrónico sin formato. Éste podría contener los archivos adjuntos si en el mensaje de correo fueron adjuntados.

Enmascaramiento: comúnmente, en informática, se conoce como la forma de anonimizar nuestra identidad en Internet. Generalmente se realiza ocultando nuestra dirección IP pública real mediante varios protocolos. Estos pueden ser a través de VPN o de protocolos más complejos de enmascaramiento de direcciones IP como la red Tor.

Firma digital: Se entiende por firma digital 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.[35]

Hash o función de resumen: Una función criptográfica hash- usualmente conocida como "hash"- es un algoritmo matemático 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. Permite identificar inequívocamente a un archivo, garantizando su integridad. Es decir que, ante modificaciones en el contenido de un archivo, los valores resultantes de la aplicación de la misma función de hash serán diferentes. Además, una de sus propiedades es que no es posible reconstruir el dato de entrada (el original que se desea hashear) a partir del valor resultado del hash.

ICANN (Corporación de Internet para la Asignación de Nombres y Números): es una agencia internacional encargada de la asignación de direcciones IP, nombres de dominio, entre otros en Internet. Con respecto a las direcciones IP, el mundo se encuentra dividido en 5 Registros Regionales de Internet (RIR). El ICANN, es el responsable de asignarle el rango de direcciones IP públicas, que podrá administrar cada RIR.

Integridad: se refiere a la cualidad de los datos o la información de mantenerse completa, exacta y sin alteraciones no autorizadas. Es un principio fundamental en la seguridad de la información, ya que asegura que los datos se mantengan consistentes y confiables a lo largo del tiempo. Esto implica proteger la información contra cambios no autorizados o corrupción, garantizando que los datos se almacenen, transmitan y procesen de manera íntegra y precisa.

Internet Archive[36]: es una organización sin fines de lucro, que contiene una biblioteca digital de sitios de Internet y otros artefactos culturales en forma digital. Al igual que una biblioteca en papel, brindan acceso gratuito a investigadores, historiadores, académicos, personas con problemas de lectura y el público en general. Su misión es proporcionar Acceso Universal a Todo el Conocimiento.
Comenzó en 1996 archivando la propia Internet, un medio que estaba empezando a crecer en uso. Al igual que los periódicos, el contenido publicado en la web era efímero, pero a diferencia de los periódicos, nadie lo guardaba. Hoy tienen más de 25 años de historial web

[35] Art. 2. Ley nacional argentina de Firma Digital: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm
[36] https://archive.org/about/

accesibles a través de “Wayback Machine” y trabajan con más de 950 bibliotecas y otros socios a través de su programa “Archive-It” para identificar páginas web importantes.

Hoy su archivo contiene:

625 mil millones de páginas web.

38 millones de libros y textos.

14 millones de grabaciones de audio (incluyendo 240.000 conciertos en vivo).

7 millones de videos (incluidos 2 millones de programas de noticias de televisión).

4 millones de imágenes.

790.000 programas de software.

Internet: Internet es una red global que interconecta distintas redes distribuidas en todo el mundo. Estas redes pueden ser tanto redes privadas, académicas, o redes de proveedores de internet que interconectan su red local para brindar acceso “al resto del mundo”. El valor de Internet está, precisamente, en la interconexión y las capacidades de comunicación que brinda.

ISP (Internet Service Provider): refiere a las empresas o instituciones que proveen servicio de internet en una determinada región.

LACNIC[37]:El Registro de Direcciones de Internet de América Latina y Caribe es una organización no gubernamental internacional, establecida en Uruguay en el año 2002. Su función es asignar y administrar los recursos de numeración de Internet (IPv4, IPv6), números autónomos y resolución inversa para la región.

Log-in: el término "loguin o logueo" se refiere al proceso de inicio de sesión o autenticación en un sistema. Con la expresión "loguearse", se hace referencia a proporcionar las credenciales de acceso, como un nombre de usuario y una contraseña, que permite comprobar la identidad y obtener acceso a una cuenta o sistema protegido.

El logueo es una medida de seguridad utilizada para controlar y limitar el acceso a la información y a funcionalidades específicas.

[37] https://www.lacnic.net/966/1/lacnic/acerca-de-lacnic

Medio de almacenamiento: también nombrado como unidad de almacenamiento, es un dispositivo o soporte físico que se utiliza para guardar y preservar información digital(sistemas operativos, programas, archivos de usuario, documentos, imágenes, videos, música y otros tipos de información digital) o datos de manera temporal o permanente. Estos medios permiten el almacenamiento y la recuperación de datos de forma posterior, brindando la posibilidad de acceder a ellos cuando sea necesario.

Las unidades de almacenamiento pueden ser dispositivos físicos, como discos duros, unidades de estado sólido (SSD), discos ópticos, memorias USB, tarjetas de memoria, entre otros. También existen unidades de almacenamiento virtuales, como las unidades de almacenamiento en la nube.

Características que definen a las unidades de almacenamiento son la velocidad de lectura y escritura con la que trabaja el dispositivo, si es una unidad interna (instalado dentro de la computadora) o externa (se conecta a través de un puerto, por ejemplo, USB), capacidad de almacenamiento, portabilidad y seguridad del dispositivo.

- Propiedad de sólo lectura: se aplica esta propiedad a aquellos medios de almacenamiento o medios que permiten únicamente la lectura de la información almacenada, sin la posibilidad de que los datos allí almacenados se modifiquen o que se puedan escribir nuevos datos en ellos. Esta característica de los dispositivos permite preservar la integridad y seguridad de los datos almacenados, evitando cambios accidentales o intencionales en la información.

Ejemplo de este tipo de unidades de almacenamiento son el CD-ROM y el DVD-ROM.

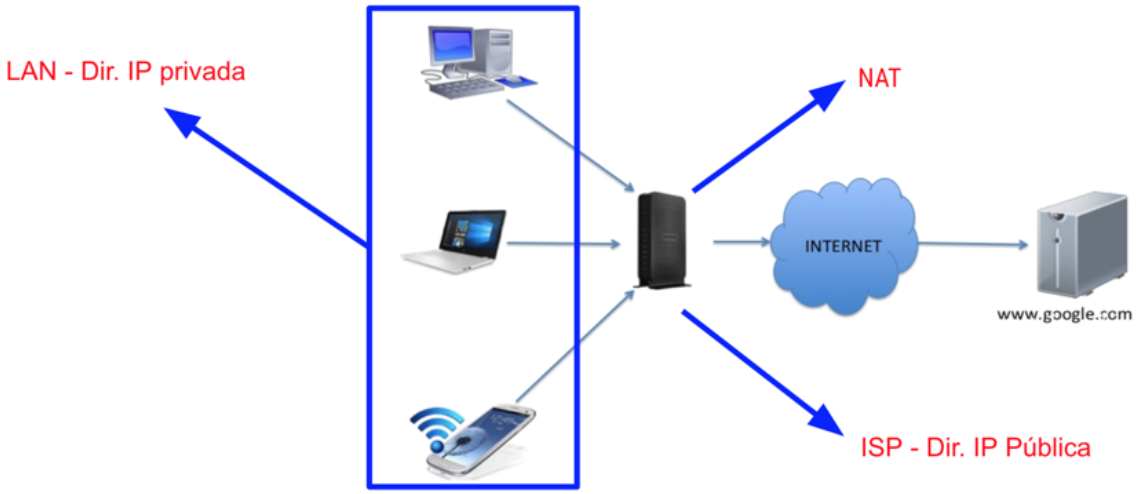
Metadatos: son información descriptiva que brindan detalles sobre otros datos. Ofrecen información adicional sobre el contenido, contexto, calidad, formato, origen, fecha de creación, autoría y otros atributos relevantes.

Los metadatos de un archivo incluyen detalles sobre el nombre del archivo, ubicación, tamaño, formato, fecha de creación, fecha de modificación y permisos de acceso.

Timestamp: es una marca o registro que representa un momento específico en el tiempo. Por lo general, se expresa en una combinación de fecha y hora, y se utiliza para registrar y comparar eventos.

Un timestamp en una imagen se refiere a la marca de tiempo asociada a la imagen, indicando cuándo fue capturada o creada.

NAT (Network Address Translation): Es un protocolo que debió utilizarse por la escasez de direcciones de IP pública (v4) existentes. Además, brinda cierta seguridad a los dispositivos conectados en una red local, ya que no se expone directamente a estos en Internet. La idea de NAT es que varios dispositivos puedan acceder a Internet, utilizando una única dirección IP pública. Es así que, en una red hogareña o empresarial clásica, el router, provisto por el proveedor de servicios de Internet, será quien tenga asignada la dirección de IP pública, mientras que los dispositivos conectados a él, se les asignará una dirección de IP privada. A través de NAT, cuando un dispositivo de la red local (LAN), intente conectarse a un servicio en Internet, el pedido tendrá que pasar por el router, y éste último, a través de NAT tendrá la capacidad de direccionarlo y, una vez recibida la respuesta, sabrá qué dispositivo fue el que inició la solicitud, para enviársela. De esta manera, se aísla la red local o LAN de Internet, para que se pueda navegar de una forma más segura y sin que se conozcan las direcciones IP privadas.



Registro Regional de Internet (RIR): es una organización que supervisa la asignación y el registro de direcciones IP de Internet dentro de una región particular del mundo. Es la que, según su disponibilidad, determine cuáles serán los rangos de direcciones IP públicas que podrán utilizar los diferentes ISP pertenecientes a esa región. Cada ISP, según esta asignación, brindará la dirección IP pública a sus clientes finales. Los 5 RIR existentes son:

American Registry for Internet Numbers (ARIN) para Estados Unidos y Canadá.

RIPE Network Coordination Centre (RIPE NCC) para Europa, el Oriente Medio y Asia Central.

Asia-Pacific Network Information Centre (APNIC) para Asia y la Región Pacífica.

Latin American and Caribbean Internet Address Registry (LACNIC) para América Latina y el Caribe.

African Network Information Centre (AfriNIC) para África.

Nombre de Dominio: Un nombre de dominio (a menudo denominado simplemente dominio) es un nombre fácil de recordar asociado a una dirección IP. Se trata del nombre único que se muestra después del signo @ en las direcciones de correo y después de www. en las direcciones web. Otros ejemplos de nombres de dominio podrían ser google.com y wikipedia.org. Al utilizar un nombre de dominio en lugar de una dirección IP numérica para identificar una ubicación en Internet, es mucho más fácil recordar y escribir direcciones web. Cualquiera puede comprar un nombre de dominio. Solo se tiene que ir a un registrador o un host de dominios, encontrar un nombre que nadie más utilice y abonar una pequeña cuota anual para ser su propietario.
Existen dominios regionales e internacionales. Los primeros son aquellos que poseen extensión de país, por ejemplo info-lab.org.ar. Y tanto para su registración, consulta y mantenimiento se debe dirigir al Network Information Center (NIC) del país correspondiente. Para el caso de Argentina es https://nic.ar. En cambio, los segundos, son aquellos que no poseen extensión de país, por ejemplo, aquellos terminados en ".com". Para su registración y mantenimiento se los debe gestionar a través de un ISP (Internet Service Provider) que ofrezca este servicio.
La consulta de, tanto la existencia como datos técnicos, de un nombre de dominio es de acceso público y debe realizarse a través de los servicios de "WhoIS". Para el caso de los dominios regionales, se realiza a través de los sitios web de los NICs de ese país. Para el caso de los dominios internacionales se realiza a través de un WhoIs Internacional, por ejemplo http://who.is.
Cabe destacar que la consulta y registración de dominios de tipo educacional (".edu" o ".edu.ar") no es pública y requiere de ciertas autenticaciones de quien solicita estos datos. Lo mismo ocurre para el caso de la registración de dominios de gobierno (".gov" o ".gov.ar").
Perfil de usuario (en sistema operativo): Es un entorno personalizado específicamente para

un usuario. Contiene configuración y datos del usuario. Cuando se inicia sesión en un equipo o aplicación por primera vez, se crea automáticamente un perfil para ese usuario.

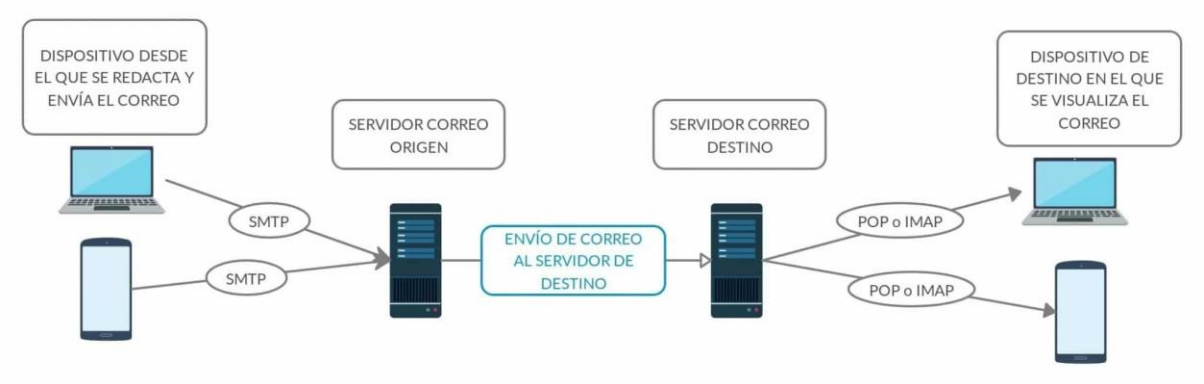
Permisos y roles de usuarios: Los permisos refieren a lo que el usuario está autorizado a realizar en el sistema. Todo aquello que intente realizar, y no posea autorización para ello, le será denegado por el sistema operativo o sistema. El rol describe al grupo al que pertenece ese usuario. Los grupos poseen permisos preestablecidos, lo que permite que no se deban configurar permisos cada vez que estos son creados. Existen roles de Administrador, Invitado, etc., dependiendo el sistema y la organización en la que se esté trabajando.

Protocolos de correo electrónico: Los protocolos definen las reglas y los estándares que los servidores de correo utilizan para intercambiar mensajes y gestionar las operaciones relacionadas con el correo electrónico.

Los protocolos que se utilizan más comúnmente son:

- **SMTP (Simple Mail Transfer Protocol):** es el protocolo utilizado para enviar correos electrónicos desde un cliente de correo a un servidor de correo saliente. SMTP define cómo se deben transmitir los mensajes de correo electrónico y cómo los servidores de correo deben interactuar entre sí para entregar los mensajes.
- **POP (Post Office Protocol):** Protocolo de recepción utilizado por los clientes de correo electrónico para recuperar mensajes de un servidor de correo. La versión más común es POP3 (Post Office Protocol 3).
- **IMAP (Internet Message Access Protocol)**: es otro protocolo de recepción utilizado por los clientes de correo electrónico para acceder a los mensajes almacenados en un servidor de correo. IMAP permite a los usuarios administrar los mensajes en el servidor sin necesidad de descargarlos localmente.

El proceso para el envío y recepción de un mensaje de correo electrónico, es el siguiente:

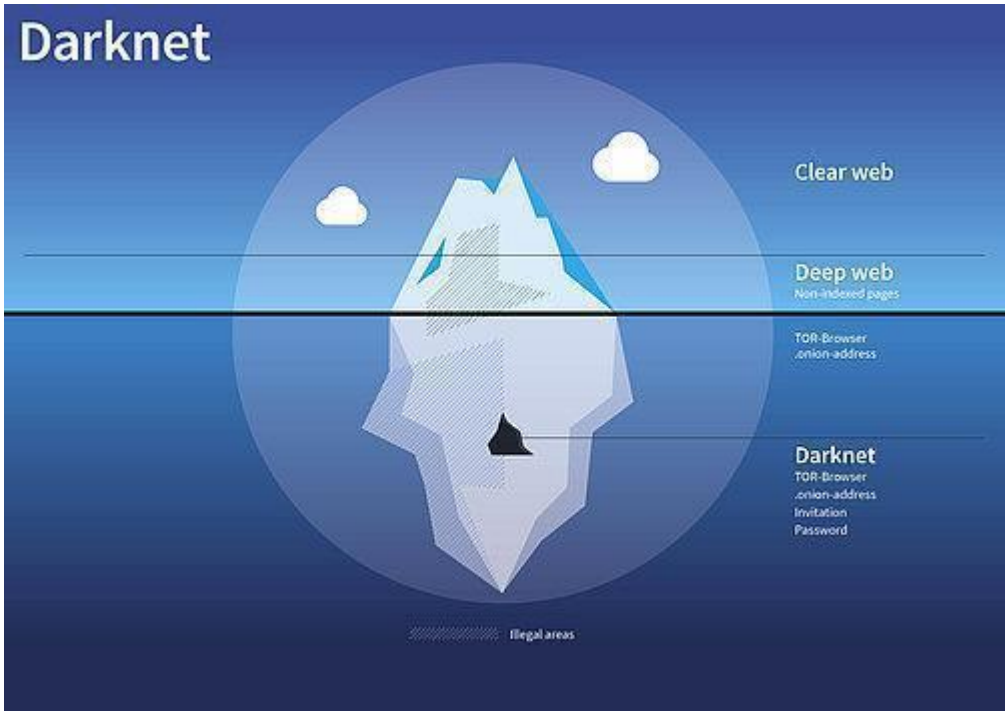


Fuente: elaboración propia

Cuando se procede a visualizar el "Mensaje original o Completo", además de cuestiones de seguridad del propio mensaje, se tendrá disponible información relevante a los servidores y usuarios (reales) intervinientes desde el envío hasta la recepción de dicho mensaje. No será posible obtener información acerca del dispositivo desde el cual el mensaje fue enviado.

Red superficial, Web Profunda y Web Oscura (Deep y Dark Web): Se dice que la red superficial es todo aquello que está indexado por los buscadores, es decir, todo lo que un buscador devuelve como resultado. Ahora bien, todo lo que los buscadores no devuelven como resultado podría estar clasificado en dos tipos de redes diferentes: La Web profunda y la Web Oscura. La primera de ellas describe a todos esos sitios que no están indexados por los buscadores, pero que no requieren ningún protocolo para poder navegar sobre ellos. Es así que podríamos mencionar, a modo de ejemplo, que en ella están incluidos los correos electrónicos de un usuario, el contenido de los perfiles de las redes sociales de usuarios, y, además, aquellos sitios que bloquean que los buscadores puedan acceder a ellos para arrojar resultados sobre los mismos. En cambio, en la web oscura, sí se debe utilizar un protocolo de enmascaramiento o anonimato para acceder a ella. El más conocido es la red Tor. Esta red es utilizada para mantener la privacidad de sus usuarios, y el contenido compartido por ellos no es rastreable. A modo de ejemplo, se podría mencionar a la red de periodistas de investigación que utilizan este tipo de servicios, para compartir información. ¿Es la web oscura un medio para el delito? La respuesta es NO. La finalidad de navegar bajo el protocolo Tor o similar radica en mantener la privacidad de sus usuarios sin que puedan ser rastreados. Por supuesto que también podría ser utilizado para el delito por las características que brinda, pero su finalidad no es esa. Dentro de las redes de delincuencia que se encuentran bajo este tipo de navegación, se puede mencionar al tráfico de drogas, trata de personas, venta de armamento, entre otros.

Se dice que sólo un 15% del contenido total de Internet está bajo la red superficial, mientras que el otro 85% se encuentra distribuido bajo las web profunda y oscura.



Fuente: https://www.gdata.es/

Sitio Web: un sitio web es una colección de páginas web relacionadas que están alojadas en un servidor web y accesibles a través de una dirección de Internet (URL). Un sitio web es una forma común de presentar información y contenido en línea de manera organizada y accesible para los usuarios de Internet. **JSON (JavaScript Object Notation), XML (eXtensible Markup Language) y HTML (HyperText Markup Language)** son formatos utilizados para representar y estructurar información en la web. Cada uno de estos formatos tiene características y propósitos distintos.

Servidor Web: Un servidor web es un equipo informático dedicado (de uso exclusivo para), que se encarga de almacenar, administrar y distribuir páginas web y otros recursos digitales (imágenes, videos u otros archivos multimedia) a los clientes que las solicitan a través de Internet. Un servidor web es el encargado de "servir" o entregar las páginas web cuando son solicitadas por los navegadores web de los usuarios.

Tor (The Onion Router)[38]: hace rebotar las comunicaciones a través de una red distribuida de repetidores administrados por voluntarios de todo el mundo: evita que alguien que esté viendo una conexión a Internet se entere de los sitios que se visitan, y evita que los sitios que

[38] https://support.torproject.org/es/faq/

se visitan se enteren de tu ubicación física. Este conjunto de repetidores voluntarios se llama la red Tor. La forma en que la mayoría de la gente usa Tor es con el Navegador Tor que es una versión de Firefox que corrige muchos problemas de privacidad.
Tor encamina el tráfico a través de, al menos, 3 servidores diferentes antes de mandarlo a su destino. Como hay una capa de cifrado para cada uno de los tres repetidores, alguien examinando la conexión a internet no puede modificar ni leer lo que se está enviando a la red Tor. El tráfico va cifrado entre el cliente Tor (en el ordenador) y allá donde termina en algún lugar del mundo.

URL (Uniform Resource Locator - Localizador de Recursos Uniforme). Una URL no es más que una direccion que es dada a un recurso único en la Web. En teoría, cada URL válida apunta a un único recurso. Dichos recursos pueden ser páginas HTML, documentos CSS, imágenes, etc. En la práctica, hay algunas excepciones, siendo la más común una URL apuntando a un recurso que ya no existe o que ha sido movido. Como el recurso representado por la URL y la URL en si son manejadas por el servidor Web, depende del dueño del servidor web manejar ese recurso y su URL asociada adecuadamente.[39]

Usuario: un usuario es un actor que utiliza una computadora o un servicio de red. Por lo general, un usuario tiene una cuenta de usuario y se identifica en el sistema o aplicación por un nombre de usuario. Otros términos para nombre de usuario incluyen nombre de inicio de sesión, nombre de cuenta, seudónimo, apodo y alias

VPN (Virtual Private Network - Red privada virtual): Es una forma de hacer que dos o más dispositivos, físicamente en lugares diferentes, puedan pertenecer a una misma red local (LAN), utilizando Internet para ello, por eso es que es virtual. Es muy utilizada para ingresar a servicios específicos del lugar donde se trabaja, sin la necesidad de estar físicamente en él y utilizando dispositivos dentro de ese lugar físico. Al conectarse a una VPN, el equipo que se está utilizando, es como si estuviera físicamente y utilizando la misma red local del lugar que ofrece el servicio de VPN. Es decir, que la dirección de IP pública que utiliza el equipo conectado a una VPN, no es la que tiene en su lugar físico, sino que se le asigna, por lo general, la dirección IP pública del lugar a dónde se está conectado. Por esta razón es que, también, es utilizado como enmascaramiento de una dirección IP pública, ya que se oculta la dirección IP real del dispositivo.

[39] https://developer.mozilla.org/es/docs/Learn/Common_questions/Web_mechanics/What_is_a_URL

Las fuentes digitales de prueba ocupan un lugar cada vez más relevante en los casos judiciales, generando una serie de desafíos para los operadores jurídicos, como el desconcierto, la creación de falsas certezas, la subutilización y sobreutilización, procedimientos y valoraciones sumamente dispares, por mencionar solo algunos. Todo esto impacta en los niveles de efectividad y equidad en el acceso a la justicia.

Los fenómenos mencionados justifican plenamente los esfuerzos destinados a mejorar la utilización de estas fuentes probatorias.

En esta obra, se presentan guías y recomendaciones para garantizar la integridad de la información contenida en correos electrónicos, servicios de mensajería, redes sociales, sitios web y archivos en general. Todo esto se enmarca en un conjunto de etapas del proceso de prueba digital.

Este desarrollo fue posible gracias a una demanda institucional sostenida en el tiempo y al comprometido trabajo de un amplio equipo interdisciplinario de investigadores.

Esta guía se integra en estos esfuerzos y, aunque no constituye una solución completa ni definitiva, tiene como objetivo motivar y servir como catalizador para promover la adopción de buenas prácticas.

INSTITUTO DE CIENCIAS FORENSES
UNIVERSIDAD FASTA
InFo-Lab
UNIVERSIDAD FASTA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
FACULTAD DE INGENIERÍA
IFITEJ
INSTITUTO FEDERAL DE INNOVACIÓN TECNOLOGÍA Y JUSTICIA
JUSLAB
UCH
UNIVERSIDAD CHAMPAGNAT

ISBN 978-631-90546-6-8