Universidad de los Andes
Facultad de Ingeniería

SISTEMA GUÍA PARA RECOLECCIÓN DE EVIDENCIA DIGITAL PARA NO EXPERTOS - LEGALEV

MATEO NIETO DIAZ
JOSE LUIS TELLEZ CUARTAS
OMAR JAVIER ROBAYO RODRIGUEZ

1. PROBLEMA

El desconocimiento de las personas y entidades en la adquisición de la evidencia digital y su validez en un proceso legal se expresa a través de procesos fallidos, evidencia no válida, así como tiempo y dinero desaprovechado tanto en el entorno personal como en el empresarial.

Dentro del universo analizado se tomó como referencia una empresa perteneciente al sector de prestación de servicios profesionales de asesoría jurídica. En esta compañía, se determinó a través de un tablero de control de su operación litigiosa, que existen 183 procesos judiciales gestionados por la firma en los que se aporta evidencia digital. De los 183, el 36% (65 casos) tienen un riesgo de fallo desfavorable con una potencial pérdida de más de 11 mil millones de pesos por desconocimiento en materia de reconocimiento de evidencia digital, su recolección y su validez.

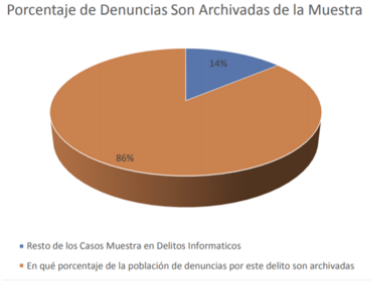
De ser aportadas y aceptadas estas pruebas, la tendencia de fallo permitiría a las empresas ahorrar más de 7 mil millones de pesos. Sin embargo, actualmente sólo es aportado y usado el contenido de estas pruebas como una referencia y no como una real evidencia digital. De los casos que se atienden en el área de litigios, los coordinadores señalan:

> *"… procuramos evitar usar ese tipo de pruebas porque generalmente los Jueces las rechazan debido a la metodología o al formato con que han sido aportadas... ".*

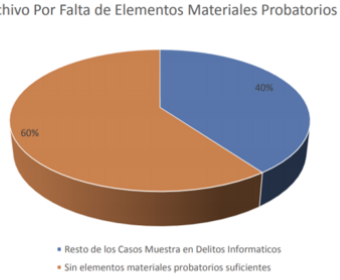
Esta situación se extrapola a otras empresas del sector, donde se manifiesta una problemática similar asociada a que la evidencia digital no es correctamente manejada haciendo que un proceso fundamentado en este tipo de evidencia llegue en situación de invalidez ante un juez por la misma razón.

Ahora bien, analizando esta misma problemática en el sector gobierno, se tomó como muestra las denuncias recibidas en la FISCALÍA GENERAL DE LA NACIÓN[1], SECCIONAL MEDELLIN donde se realiza un análisis concluyente en relación con el manejo de la evidencia digital. Se indica que para el mes de septiembre del año 2018 ingresaron solo por la sala de denuncias de la fiscalía de la seccional Medellín 4.242 denuncias, de las cuales 220 correspondieron y fueron asignadas al grupo de fiscales de la unidad de delitos informáticos de esa seccional, **todos sin indiciado conocido**.

Gráfica 1



Gráfica 2



Gráfica 3

De una muestra determinada de 50 denuncias, el 76% de ellas son personas naturales las que resultan afectadas por los delitos relacionados con los delitos informáticos. Son delitos que afectan directamente a la sociedad en su patrimonio u otro derecho fundamental, como la intimidad.

La gráfica 2 muestra **la poca identificación del sujeto activo en este tipo de procesos**, ya que como se ve en esta estadística, es solo el 30% de la población. Esto se explica por el aporte probatorio limitado y poca colaboración por parte de las víctimas y de aquellas personas encargadas del tratamiento de la información. En muchos casos cuando es solicitada la misma, **ya no existe por su volatilidad** y carencia de aplicación de métodos adecuados para recopilarla.

En la gráfica 3 muestra la cantidad de procesos archivados por falta de elementos con vocación probatoria, son procesos que "nacen muertos" y la principal razón es la **falta de conocimiento** en la adquisición de los elementos con vocación probatoria.

La gráfica 3 se une a la estadística de la imposibilidad de encontrar el sujeto activo, la cual cuenta con un porcentaje de 60%, el cual es bastante elevado y en la gran mayoría de los casos nuevamente producto de que no se cuenta con elementos con vocación probatoria y no se cuenta con el personal idóneo y capacitado en la recolección y tratamiento de la información. Sumado a esto, está la falta de celeridad en que se actúa, la falta de convenios o colaboración que no permiten acceder a dichas evidencias de manera oportuna o eficaz.

[1] *Tomado de DIFICULTADES EN EL MANEJO DE LA EVIDENCIA DIGITAL EN EL PROCESO PENAL COLOMBIANO, John Londoño*

Para concluir con el análisis de contexto de la problemática de los casos relacionados con evidencia digital, denota que las personas involucradas muchas veces no son personas con experticia en informática forense, por tanto se reconoce que hay una importante oportunidad para reducir la brecha de desconocimiento en el correcto levantamiento de evidencia digital y su validez legal en el país, así como mitigar la pérdida de tiempo y dinero en procesos que resultan desfavorables por mal manejo de información.

2. PROPUESTA DE SOLUCIÓN

Ante la necesidad de brindar un conocimiento comprensible por usuarios finales, proponemos crear un sistema interactivo con contenido procedimental de referencia para recolección de evidencia digital dirigida a usuarios no expertos y alineada con el marco legal colombiano. Sus componentes explicarán conceptos base usando un lenguaje genérico para todo tipo de usuario y, así mismo, brindará contexto jurídico vigente en relación con el manejo de la evidencia digital en Colombia. Debido a la extensión del ámbito técnico y la cantidad de posibles temas a incluir, se limitará inicialmente a los tipos de archivos más comunes.

2.1. DISEÑO

2.1.1. DISEÑO DE INFRAESTRUCTURA PARA LOS SERVICIOS

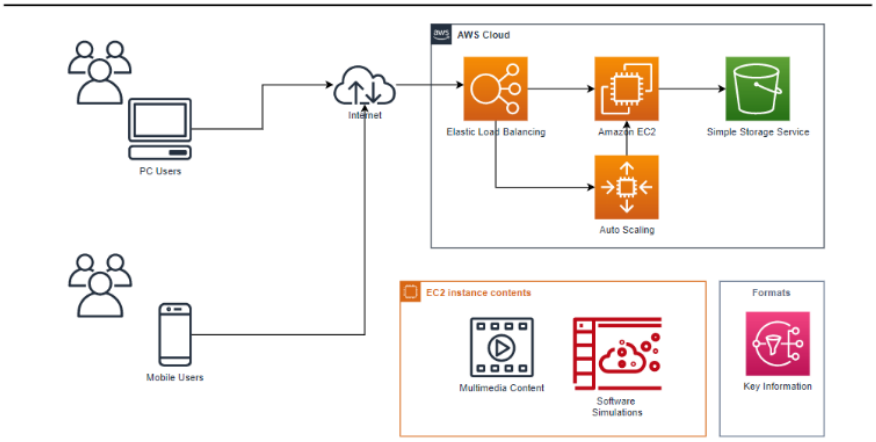


Imagen 1. Flujo y recursos en Nube

Una vez realizada la evaluación de opciones, se determinó usar servicios en la núbe para la implementación de la plataforma propuesta ya que es la mejor opción por flexibilidad, escalabilidad y costo.

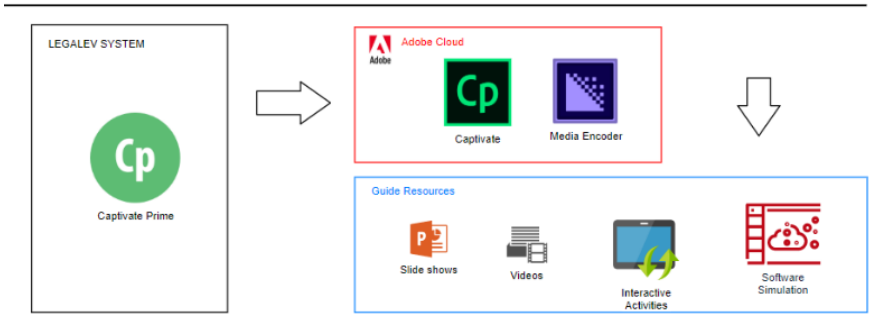


Imagen 2. Elementos clave de la aplicación

El corazón de la plataforma LEGALEV es la aplicación Captivate[2] sobre la cual se despliegan los principales recursos de orientación interactiva para los procedimientos de extracción de evidencia.

[2] https://www.adobe.com/products/captivate.html

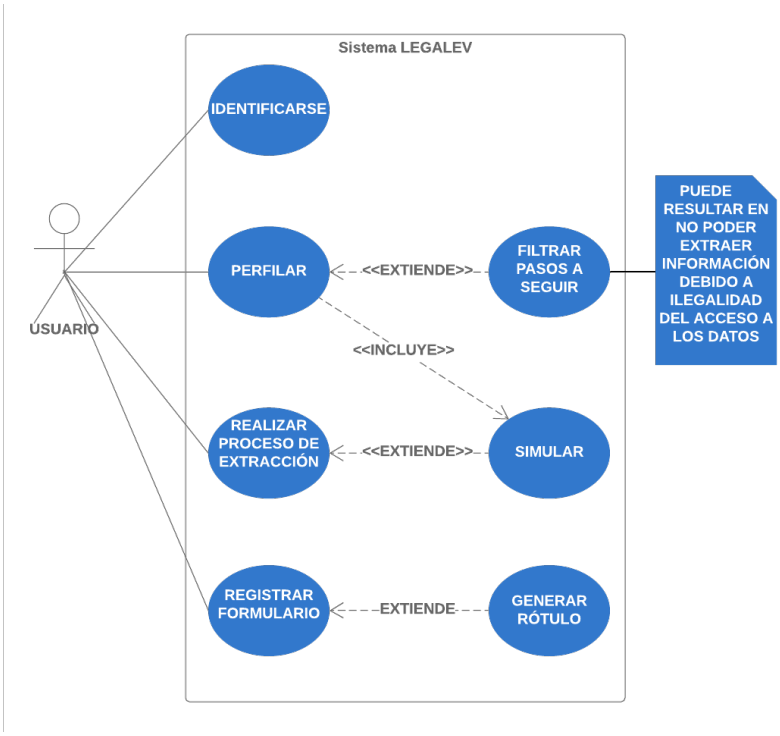


Imagen 3. Diagrama de casos de uso

Los casos de uso estarán basados inicialmente en el flujo plasmado en la Imagen 3. Más adelante, se explicarán en detalle los respectivos contenidos trabajados dentro de la plataforma interactiva.

2.1.2. PROCESO DE DISEÑO

En el proceso de diseño se realizó la recopilación del material jurídico que sirvió como referencia en este proyecto tanto en la fase de planeación, como en la ejecución del prototipo. Este material permitió desarrollar los procedimientos técnicos necesarios respetando ante todo el derecho a la intimidad y la privacidad del sujeto sobre el que se desea imputar una conducta reprochable.

Se realizó también la recolección del material técnico y de los procedimientos para ejecutar tareas de recolección específicas a través del uso de determinadas herramientas de software, pero siempre permitiendo garantizar la preservación y la integridad de los datos a la luz de las técnicas actuales de informática forense siendo ésta última el mayor recurso a explotar en este proyecto. Se persiguió la simplificación de instrucciones y guías técnicas complejas para expresar en lenguaje claro y sencillo un procedimiento adecuado de extracción.

Se trabajó también en el "*perfil de la evidencia*" que es una sección previa o de línea base en la que se realizó de forma interactiva una serie de preguntas a fin de encaminar la legitimidad (es decir, que respete los preceptos básicos de intimidad amparados por el Art. 15 de la Constitución Política de Colombia). Se realizó el diagrama de flujo para los caminos que podrá tomar un usuario. En la imagen 4 se descompone en las categorías (Identificación, Perfilación y Respuesta) y se describen de la siguiente manera:

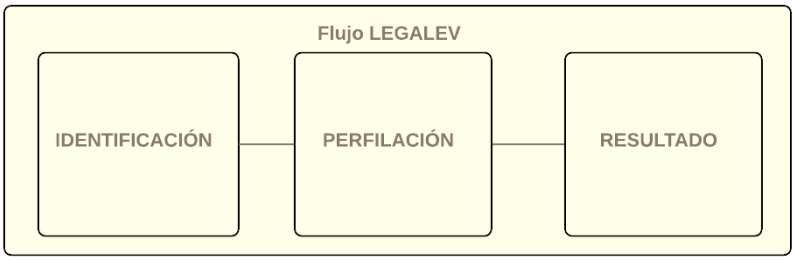


Imagen 4. Flujo base de la herramienta

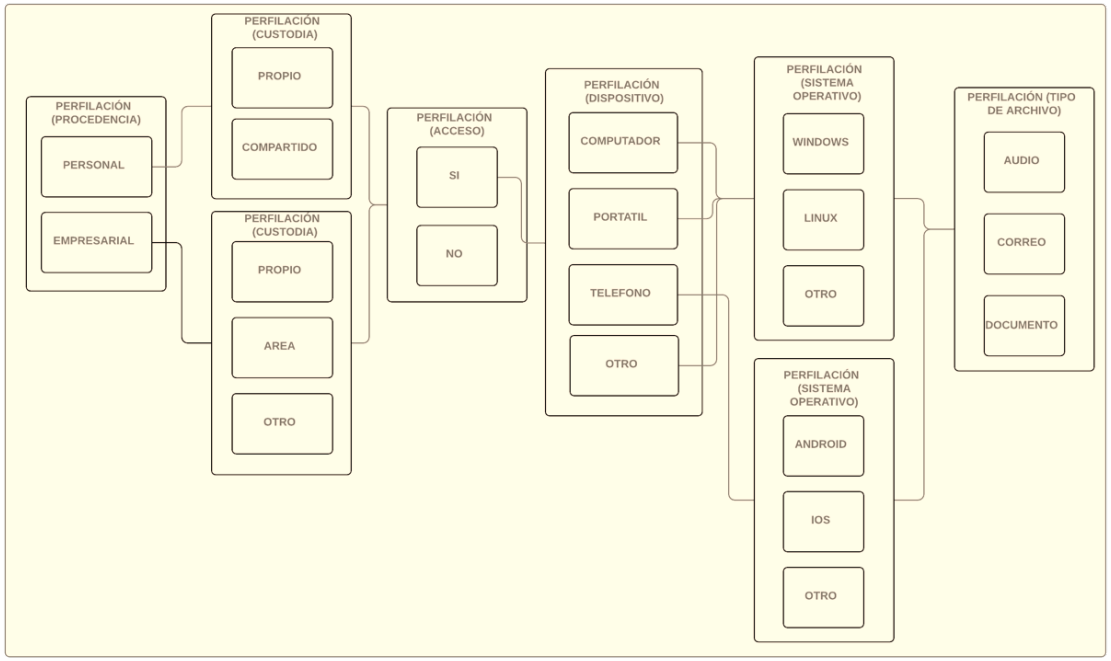


Imagen 5. Flujo de perfilación de usuario

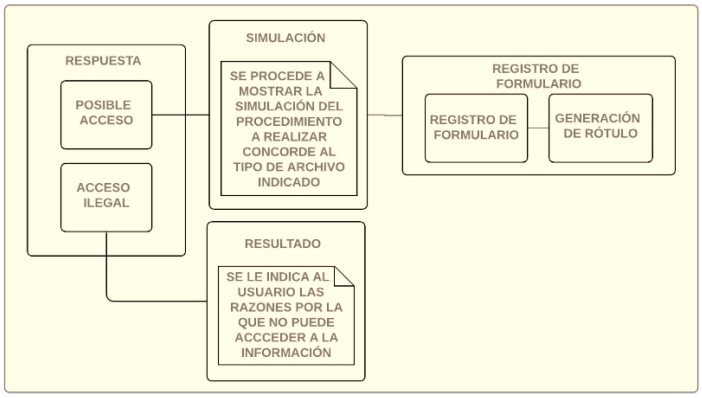


Imagen 6. Flujo de resultados del usuario

Se diseñaron mockups basados en los diagramas anteriores e inspirados en la simplicidad. A continuación, se ilustran algunos mockups de la fase de diseño y planeación:

Imagen 7. Mockup de la sección de perfilamiento del dispositivo

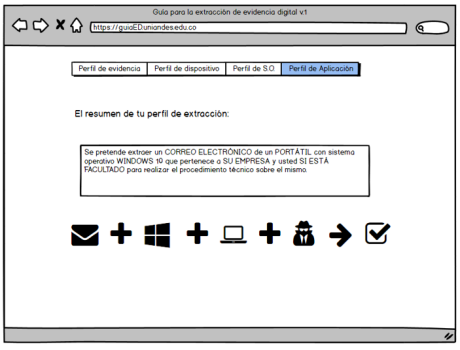


Imagen 8. Mockup del resumen del perfilamiento hecho

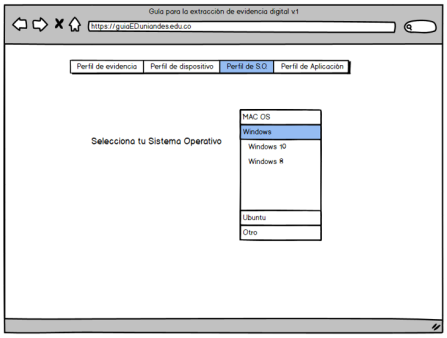


Imagen 9. Mockup de la sección de perfilamiento del sistema operativo

Imagen 10. Mockup de la sección de perfilamiento del tipo de archivo

2.1.3. USABILIDAD

Esta herramienta será entonces un buen punto de inicio tanto para aquellos actores que quieran realizar una extracción y cuyo campo de acción puede o no estar dentro de las ramas del conocimiento técnico. También puede ser usado por jueces y demás personas de afinidad jurídica que quieran ampliar su conocimiento y así poder tener mejores criterios para la aceptación o rechazo de este tipo de pruebas.

Una característica importante del producto desarrollado es la posibilidad de habilitar el modo "Lectura en Voz Alta" directamente en la aplicación, facilitando su usabilidad y acercando este tipo de soluciones tecnológicas a usuarios con limitaciones visuales, ampliándose el rango de público objetivo.

3. RESULTADOS Y EVALUACIÓN

A continuación, se evidencian los resultados que satisfacen los requerimientos planteados. Se retomará en la parte final los requerimientos iniciales establecidos para evidenciar su cumplimiento junto con los casos de uso. Adicionalmente el demo de la fase de prototipo fue publicado en el sitio http://legalev.sinergiatic.co/.

3.1. CASO DE USO LINEA BASE LEGAL Y TÉCNICA

***Aspectos legales trabajados**: El Código Penal Colombiano prevé en el artículo 269a el delito de acceso abusivo a sistema informático que, además de proteger directamente la seguridad e integridad de los sistemas informáticos e indirectamente los datos y la información informatizada, como bien jurídico colectivo, también resguarda el derecho constitucional fundamental a la intimidad personal informática (C. N., ART. 15)*[3]. A continuación, de manera interactiva, se establece la línea base legal y la perfilación técnica del dispositivo.

Imagen 11. Explicación sencilla y clara de la aplicación

Imagen 12. Inicio del perfilamiento

[3] *Referencia http://legal.legis.com.co/*

Imagen 13. Uso del dispositivo

Imagen 14. Perfilación de línea base EMPRESARIAL

Cuando el usuario de manera interactiva selecciona las respuestas a las preguntas mostradas en las imágenes 11-14, se obtiene una noción de origen y custodia del elemento que se va a analizar, filtrando inicialmente posibles casos de extracción a dispositivos que podría ser ilegal.

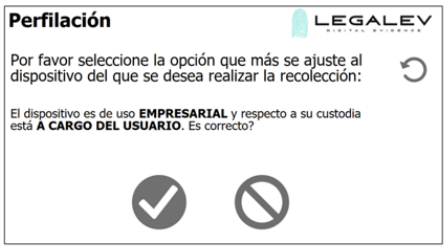


Imagen 15. Perfilación de línea base EMPRESA

Imagen 16. Tipo de dispositivo para la recolección

Imagen 17. Perfil sin autorización de equipo

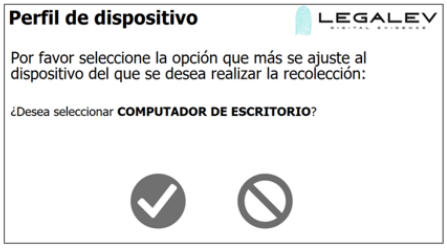


Imagen 18. Confirmación de dispositivo

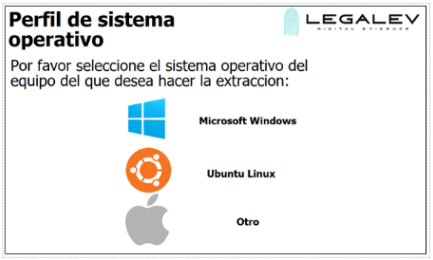


Imagen 19. Selección del sistema operativo

Imagen 20. Selección del objeto a ser tomado como evidencia.

Imagen 21. Opciones para simular y contexto legal asociado

Las imágenes 15-21 confirman la culminación de la información de origen y custodia, siguiendo por las preguntas de descripción de formato y sistema en el que se encuentra el archivo a evaluar.

A continuación, se mostrarán algunos snapshots de los casos de uso para fines informativos y evidenciar cómo un proceso de extracción se realiza de una manera amigable, sencilla y clara con nuestra instructora virtual.

3.2. CASO DE USO CORREO ELECTRÓNICO

Aspectos técnicos trabajados: *Confiabilidad: Este aspecto es resaltado en el Art. 11 de la ley 527 de 1999 y se logra técnicamente almacenando el mensaje de correo en un formato conocido (msg o pst) tal que el mismo es generado por la suite de ofimática y aunque se cambie de equipo de cómputo o sistema operativo, seguirá conservando los atributos de metadatos y legibilidad del original. Además permite que sea accesible para su posterior consulta por lo que abrirlo con una versión más reciente de ofimática no va a representar un problema en el análisis. El nombre del archivo, la extensión y el tamaño de este, son valores requeridos para el diligenciamiento del formulario y posterior impresión del rótulo.*

Integridad: Se realiza la demostración de cómo calcular la función criptográfica HASH aprovechando las características propias de resumen para que ante una futura consulta, se pueda determinar si el contenido del archivo ha sido alterado. Si bien no se hace énfasis en las características técnicas de los diferentes algoritmos disponibles para calcular HASH, se muestra en el simulador que usando el mismo algoritmo para el mismo archivo, el resultado de la función es exactamente el mismo. El valor de HASH es requerido para el diligenciamiento del formulario y posterior impresión del rótulo.

Identificación del iniciador: Este aspecto se trabaja usando los metadatos de las cabeceras MIME del correo electrónico. Esta identificación así como el criterio de integridad podrían ser fácilmente demostrados si el correo electrónico fuese firmado digitalmente. Sin embargo, la mayor cantidad de casos presentan ausencia de este atributo por lo que con un apoyo legal se ha abordado la identificación a través de las cabeceras, donde es posible establecer un vínculo entre la identidad digital y el remitente del mensaje. En el simulador se utiliza el valor del Sender-x junto con el Message-ID para poder notar esta información. Esto constituye información relevante según lo señalado en el artículo antes mencionado.

Aspectos legales trabajados*: Aseguramiento, custodia, integridad y disponibilidad. El Artículo 11 de la Ley 527 de 1999 indica que un mensaje de datos debe poseer 3 elementos clave para ser una evidencia digital: (1) la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, (2) la confiabilidad en la forma en que se haya conservado la integridad de la información, (3) la forma en la que se identifique a su iniciador.* El prototipo de caso de uso fue publicado en el sitio http://legalev.sinergiatic.co/.

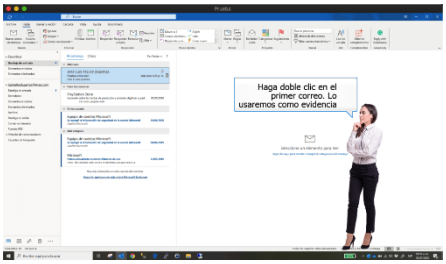
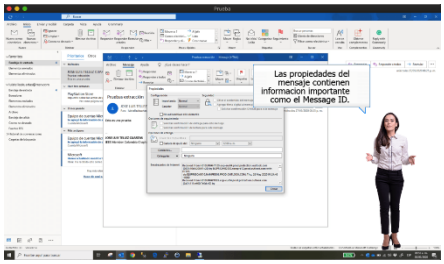


Imagen 22. Selección de correoImagen.



23. Información del correo

En las imágenes previas nuestra instructora nos muestra cómo obtener la identificación del mensaje.

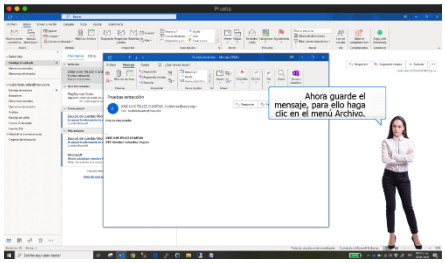


Imagen 24. Indicación de guardado

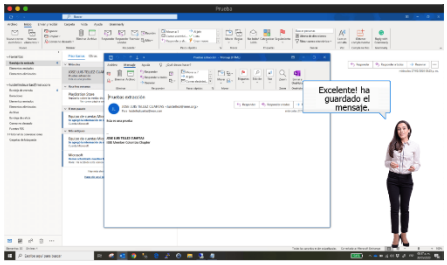


Imagen 25. Proceso de guardado

En esta etapa se nos indicará como debemos guardar nuestro objeto.

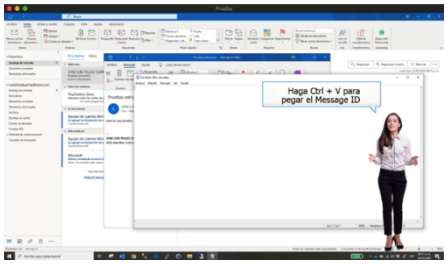


Imagen 26. Replicación de ID del mensaje

Para la obtención del identificador hash asociado a la evidencia, la plataforma orientará como obtenerlo vía web o a través de la instalación de una aplicación.

3.3. CASO DE USO IMAGEN

Aspectos técnicos trabajados: *Confiabilidad: Este aspecto se logra técnicamente almacenando el archivo en sí. La autenticidad de este archivo no es tema de discusión técnica ya que podría tratarse de una reproducción. Sin embargo, se hace uso de la información que reposa en los metadatos EXIF para extraer información relevante como la fecha en la que fue adquirida la imagen, el dispositivo con el que fue adquirida, cierta configuración como obturación, foco, saturación, flash y en algunos casos cuando existe dispositivo de posicionamiento, la ubicación (latitud, longitud).*

Integridad: Se realiza la demostración de cómo calcular la función criptográfica HASH aprovechando las características propias de resumen para que ante una futura consulta, se pueda determinar si el contenido del archivo ha sido alterado. Esta función se aplica para un paquete zip formado por la imagen en si y un pantallazo donde se exhiben los metadatos EXIF. Se orienta a usar una aplicación Windows para el cálculo del HASH y así evitar usar una aplicación online que requiera enviar el archivo en cuestión.

Aspectos legales trabajados: *Aseguramiento, custodia, integridad y disponibilidad. Código Penal Artículo 269F. Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*

A continuación, se muestra la simulación para el caso en el que se haya seleccionado el tipo de archivo Imagen. El prototipo de caso de uso fue publicado en el sitio http://legalev.sinergiatic.co/.

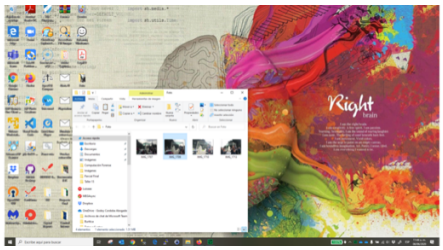


Imagen 27. Selección de imagen

Imagen 28. Toma de snapshot de metadata

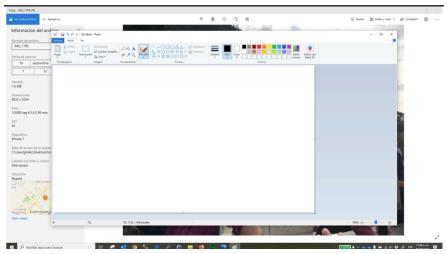


Imagen 29. Escritura de snapshot

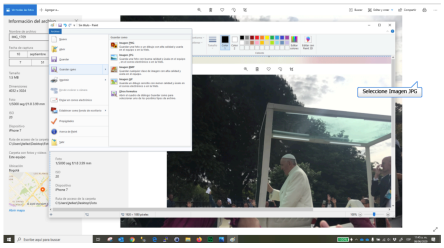


Imagen 30. Guardado de snapshot

En las imágenes 29 y 30 se le indica al usuario el proceso de toma de snapshot de la metadata de la imagen a evaluar, ya que esta metadata confirmará el estado de la imagen hasta el punto previo a la extracción de evidencia.

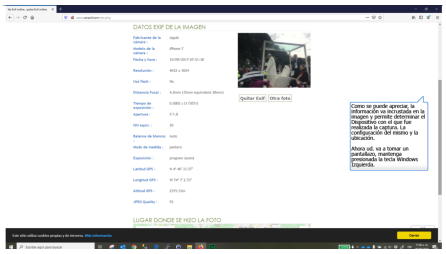


Imagen 31. Busqueda de la herramienta

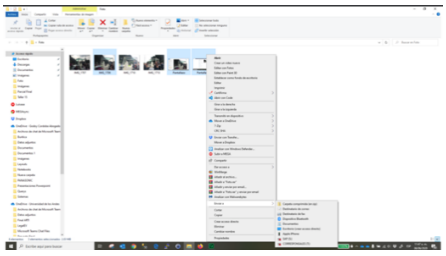


Imagen 32. Descripción del archivo cargado

En las imágenes 31 y 32 se carga el archivo evaluado en la herramienta EXIF para visualización de metadata adicional y finalmente se toma un snapshot adicional para comprimir con la evidencia anterior y la imagen original. Se procederá finalmente al cálculo del hash del archivo comprimido generado.

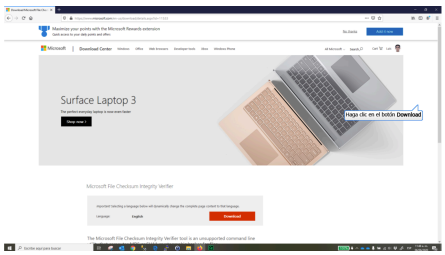


Imagen 33. Descarga de la herramienta

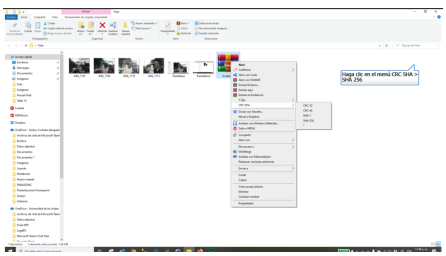


Imagen 34. Uso de la herramienta

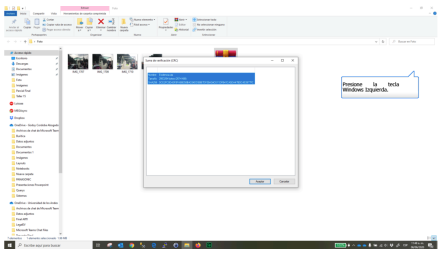


Imagen 35. Visualización de la respuesta

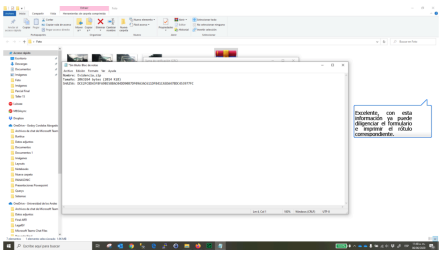


Imagen 36. Guardado local de la respuesta

En las imágenes 33-36 se le indica al usuario el proceso de descarga de la herramienta de cálculo de checksum, se instala y se usa para el cálculo del hash asociado al archivo comprimido que contiene la imagen de interés y las evidencias de su metadata. De esta forma, se está conservando la representación de la evidencia con el hash retornado para que, en el momento que se presente ante un juez, se pueda demostrar que la información no se ha alterado.

3.4. CASO DE USO CONVERSACIÓN DE WHATSAPP

Aspectos técnicos trabajados: *Confiabilidad: Este aspecto se implementa utilizando la misma aplicación donde reposan los mensajes para realizar la exportación de la conversación, se sugiere incluir el conjunto de archivos adjuntos con el fin de aumentar la confiabilidad de la evidencia y proporcionar un panorama completo de la conversación y su contexto. Whatsapp genera un archivo ZIP que puede ser enviado a través de correo electrónico y que contiene el log de mensajes y los archivos adjuntos relacionados.*

Integridad: Al enviar el archivo generado a través de correo electrónico no se está alterando su contenido por lo que una vez descargado en un ambiente más amigable para el usuario (sistema operativo de escritorio) se puede realizar el cálculo de la función HASH de este. Este log tiene consistencia con el backup que podría ser almacenado (si se tiene activa la opción).

Identificación del iniciador: En el caso de las conversaciones, las evidencias se convierten en indiciables, el log de mensajes contiene además de los estampados de fecha y hora de cada mensaje, tiene el nombre según el directorio de contactos de cada uno de los interlocutores. Para poder realizar plena asignación con el número de teléfono se tendría que realizar un análisis de la base de datos que Whatsapp almacena en cada dispositivo. El indicio de identificación del interlocutor tiene que ser evaluado por el operador de justicia.

Aspectos legales trabajados*: Aseguramiento, custodia, integridad y disponibilidad. El Artículo 11 La Ley 527 de 1999 indica que un mensaje de datos debe poseer 3 elementos clave para ser una evidencia digital: (1) la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, (2) la confiabilidad en la forma en que se haya conservado la integridad de la información, (3) la forma en la que se identifique a su iniciador.* A continuación, se muestran las imágenes para el caso en el que el usuario requiera obtener evidencia de una conversación de WhatsApp del teléfono celular. El prototipo de caso de uso fué publicado en el sitio http://legalev.sinergiatic.co/.

Imagen 37. Inicio de simulación

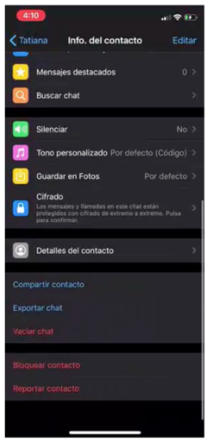


Imagen 38

Imagen 39

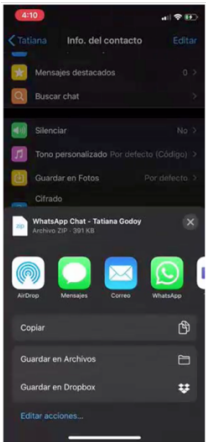


Imagen 40

Las imágenes 37-40 se indica al usuario los pasos para ingresar al historial de chat con alguna persona, exportar la conversación y realizar el proceso correspondiente para obtener este objeto como evidencia. De esta forma, se tiene el registro de todo lo ocurrido en la conversación aún si se llegasen a borrar mensajes o sufrieran otra alteración. Se puede demostrar la existencia de todos sus contenidos hasta ese punto en el tiempo que se sacó la evidencia. El propio aplicativo ofrece la opción de exportar las conversaciones de manera muy conveniente para estos procedimientos.

En la imagen 41 se evidencia el snapshot asociado al artículo legal asociado a la integridad de la información.

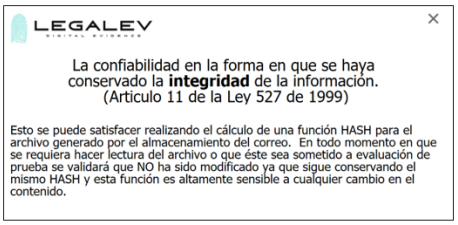


Imagen 41. Detalle del contexto legal

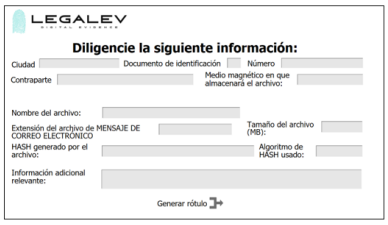


Imagen 42. Opción de diligenciamiento de información

Imagen 43. Previsualización de registro

Imagen 44. Confirmación de finalización de registro

En las imágenes 42 y 43 se muestra la funcionalidad que permitirá diligenciar los parámetros asociados a la evidencia para obtener el reporte de recolección y adjuntarlo a la evidencia digital. La imagen 44 concluye el uso de resultados obtenidos.

3.2. CUMPLIMIENTO DE REQUERIMIENTOS

REQUERIMIENTOS FUNCIONALES Y CASOS DE USO	CUMPLE	NO CUMPLE
1. La plataforma debe solicitar al usuario su nombre completo o la razón social de la empresa para personalizar el proceso de obtención de evidencia.	✓	
2. La plataforma debe establecer una línea base legal para todas las adquisiciones de evidencia.	✓	
3. La plataforma debe habilitar, el poder obtener evidencia digital a través de un proceso simple y claro.	✓	
4. Los procesos de adquisición de evidencia deben mostrarse y poder accederse en una plataforma centralizada	✓	
5. La plataforma debe guiar al usuario de manera interactiva para adquirir la evidencia de su interés.	✓	
6. El caso de uso será inicialmente realizado para la extracción de tres objetos puntuales de diferente tipo, pero debe ser escalable para los casos que se requieran integrar posteriormente.	✓	
7. La plataforma debe poder generar de manera automática la rotulación asociada a la evidencia digital.	✓	
8. El sistema debe permitir en una etapa posterior, monetizar cada proceso de extracción para apalancar un modelo de negocio.	✓	

3.5. ASPECTOS TECNICOS

LegalEV aprovecha las TIC para ampliar su alcance geográfico permitiendo llegar y transmitir conocimiento asociado a seguridad de la información a locaciones donde la capacitación presencial no es viable. De la misma forma, LegalEV utiliza herramientas como simulaciones de software para guiar paso a paso y sin riesgo de error a través de procedimientos técnicos que revisten complejidad, como lo es la recolección de evidencia digital.

Una vez el usuario ha interactuado con el escenario simulado, puede replicar las mismas condiciones en su dispositivo local permitiendo asegurar el logro de cada módulo de recolección. Las herramientas y condiciones que ambientan los escenarios de simulación están basadas en sistemas operativos, aplicaciones y objetos actuales, que pueden ser actualizados para evitar la obsolescencia tecnológica de su contenido.

LegalEV entonces, es la extrapolación didáctica de un conjunto de normas técnicas informáticas y legales que se ofrece a los usuarios de diferente formación académica o laboral para poder ser orientados en procedimientos forenses.

4. VISIÓN EMPRESARIAL

En el ámbito tecnológico, se ha vuelto una tendencia la creación de startups las cuales son empresas innovadoras que comercializan productos y/o servicios a través del uso intensivo de TIC, con un modelo escalable el cual habilita un crecimiento activo y continuado en el tiempo. Gracias a su alto componente tecnológico permite escalar de forma dinámica y rápida, con un requerimiento de capital inferior a las empresas tradicionales.

Para llevar la solución a un contexto empresarial, se propuso la creación de una empresa startup con un caso de negocio TIC enfocado en seguridad con la idea semilla planteada y la elaboración de una proyección en el tiempo, puntualmente a 4 años, para tener el road map de inicio, planeación y ejecución requerido en la línea de tiempo propuesta.

Las características de los productos resultantes del presente proyecto contienen la solución a la problemática planteada y ofrecen un diferencial importante que puede llevar a la compañía a navegar en un océano azul como lo plantea W. Chan Kim y Renée Mauborgne en su libro “La estrategia del océano azul”.

5. CONCLUSIONES

Como solución a los requerimientos planteados, el prototipo desarrollado puntualmente trabajó cuatro casos de uso, sin embargo, la plataforma es escalable y permite la agregación de casos de uso adicionales o complementarios. Lo anterior es una interesante alternativa para grupos de interés que deseen participar en el proyecto, continuando su desarrollo y crecimiento a través de nuevas funcionalidades.

El diseño del proyecto se centró en hacer accesible, sencillo y claro al usuario, temas complejos asociados a extracción de evidencia digital de una manera interactiva. No obstante, hay una importante oportunidad de evaluar y potenciar su usabilidad con un público objetivo más amplio y de acuerdo con su feedback, actualizar la plataforma para mejorar sus características.

Cada caso de uso del proyecto es monetizable, sin embargo, esta característica no fue explotada en la fase de prototipo trabajada. Se puede considerar en una etapa posterior, el desarrollar las interfaces y complementos necesarios para que las funcionalidades puedan ser consumidas pasando previamente por una plataforma digital de pagos.