

**Universidad de Buenos Aires**  
**Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e**  
**Ingeniería**

**Maestría en Seguridad Informática**

**Trabajo Final de Maestría**

**Peritaje Automatizado de Correos Electrónicos**

Autora: Lic. Andrea Francisca Metetiero

Director: Dr. Pedro Hecht

Año 2022

Cohorte 2020



## Declaración jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Andrea Francisca Metetiero

DNI 23515279

## Resumen

El presente trabajo de índole profesional práctico está enfocado en el desarrollo de una aplicación que automatice el peritaje de correos electrónicos de manera tal que sirva de herramienta de soporte a los peritos informáticos forenses en su tarea de análisis y validación de estos elementos probatorios.

Cada vez con mayor frecuencia se observan casos judiciales donde las partes intervinientes aportan correos electrónicos como prueba indiciaria para comprobar o no el hecho que se presume. A partir de la presentación de estas pruebas, las partes le solicitan al juez lo que se conoce como puntos de pericia que deben ser respondidos únicamente por un perito informático de oficio.

Los puntos periciales que ofrecen las partes, referidos a correos electrónicos, suelen repetirse con frecuencia. El fin de este trabajo es construir una aplicación que agilice la respuesta a estos puntos, teniendo en cuenta que la cantidad de correos presentados en un expediente puede ser significativa y que la revisión manual puede conducir a errores. Para lograrlo se estudiarán las características principales de los distintos tipos de archivos de correo electrónico, así como también la información relevante que se necesita capturar.

El ciclo de vida de la aplicación estará basado en la metodología de desarrollo iterativa incremental, que consiste en el desarrollo de software mediante incrementos hasta llegar al producto final deseado. Los requerimientos funcionales se obtendrán mediante el relevamiento de causas judiciales y encuestas a peritos informáticos. Una vez lograda la versión final del producto se expondrán las conclusiones basadas en los resultados obtenidos respecto a su utilidad y los beneficios que aporte.

Palabras claves: correo electrónico, email, pericia informática, informática forense, puntos de pericia.

## Contenido

Declaración jurada de origen de los contenidos .....	ii
Resumen.....	iii
<b>1. Introducción.....</b>	<b>1</b>
1.1. Contexto .....	1
1.2. Presentación Breve de la Situación Problemática .....	2
1.3. Objetivos.....	3
1.3.1. Objetivo general.....	3
1.3.2. Objetivos específicos .....	3
1.4. Alcance .....	3
1.5. No contempla .....	4
1.6. Hipótesis del Trabajo.....	4
1.7. Metodología.....	4
1.8. Plan de Actividades .....	5
<b>2. Situación Problemática.....</b>	<b>7</b>
2.1. Descripción .....	7
2.2. Explicación .....	9
2.3. Diagnóstico .....	14
<b>3. Marco Referencial .....</b>	<b>15</b>
3.1. Formato de Mensajes de Internet .....	15
3.2. Campos de Autenticación SPF, DKIM y DMARC.....	17
3.3. Tipos de Archivos .....	19
3.4. Análisis del Mercado .....	20
3.4.1. MXToolbox.....	20
3.4.2. MessageHeader.....	21
3.4.3. SystoolMbox.....	21
3.4.4. Aid4Mail.....	21
3.4.5. Paraben E-Mail Examiner.....	21
<b>4. Análisis del Sistema .....</b>	<b>24</b>
4.1. Descripción de Requerimientos.....	24
4.2. Descripción Detallada de Requerimientos .....	25
4.2.1. Requerimientos funcionales .....	25
4.2.2. Mapa de Historias de Usuario.....	32
4.2.3. Requerimientos no funcionales .....	34

5.	Modelado y Diseño del Sistema .....	35
5.1.	Diagrama de casos de uso .....	35
5.2.	Diagrama de actividades .....	35
5.3.	Diseño de Pantallas .....	50
6.	Consideraciones Finales .....	56
7.	Bibliografía .....	59

## Índice de figuras

Ilustración 1.	Desarrollo iterativo incremental.....	5
Ilustración 2.	Diagrama de Gantt.....	6
Ilustración 3.	Mensaje.....	15
Ilustración 4.	Muestra de mensaje original en Gmail.....	16
Ilustración 5.	Campos de autenticación DKIM y SFP .....	18
Ilustración 6.	Campos de firma DKIM.....	18
Ilustración 7.	Mapa de historias de usuario .....	33
Ilustración 8.	Casos de uso .....	35
Ilustración 9.	Selección de archivos EML.....	36
Ilustración 10.	Selección de archivos MBOX.....	37
Ilustración 11.	Selección de archivos EML por lotes .....	38
Ilustración 12.	Visualización de archivos TXT o EML por pantalla ....	39
Ilustración 13.	Visualización de cabeceras EML por pantalla.....	40
Ilustración 14.	Visualización de cabeceras MBOX por pantalla.....	41
Ilustración 15.	Generación de archivos CSV para EML.....	42
Ilustración 16.	Generación de archivos CSV para MBOX .....	43
Ilustración 17.	Validación de campos de autenticación .....	44
Ilustración 18.	Validación de dominios MX.....	45
Ilustración 19.	Búsqueda de información RDAP.....	46

Ilustración 20. Búsqueda de palabras clave .....	47
Ilustración 21. Listado de direcciones de correos.....	48
Ilustración 22. Listado de fechas .....	49
Ilustración 23. Pantalla de inicio .....	50
Ilustración 24. Visualización de archivo TXT .....	50
Ilustración 25. Visualización de archivos EML por lotes.....	51
Ilustración 26. Visualización de archivos MBOX .....	51
Ilustración 27. Archivo CSV.....	52
Ilustración 28. Archivo Excel .....	52
Ilustración 29. Visualización de campos de autenticación.....	52
Ilustración 30. Informe de cuentas de correos involucradas.....	53
Ilustración 31. Informe de fechas de envío.....	53
Ilustración 32. Búsqueda de palabras clave .....	54
Ilustración 33. Consulta nombres de dominio.....	54
Ilustración 34. Consulta dominio y registración .....	55

## **Índice de tablas**

Tabla 1. Campos del encabezado.....	17
Tabla 2. Análisis comparativo del mercado .....	23
Tabla 3. Historias de usuario.....	25
Tabla 4. Historia: 1.1 Selección de archivo TXT o EML .....	26
Tabla 5. Historia: 1.2 Selección de archivo MBOX.....	26
Tabla 6. Historia: 1.3 Selección de archivos EML por lotes.....	27
Tabla 7. Historia: 2.1 Visualización de archivo TXT o EML .....	27
Tabla 8. Historia: 2.2 Visualización de cabeceras EML .....	28
Tabla 9. Historia: 2.3 Visualización de cabeceras MBOX .....	28

Tabla 10. Historia: 3.1 Generación de archivo CSV con datos de cabeceras EML .....	28
Tabla 11. Historia: 3.2 Generación de archivo CSV con datos de cabeceras MBOX analizado.....	29
Tabla 12. Historia: 4.1 Validación de cabecera de autenticación de correos: SPF, DKIN, DMARC .....	29
Tabla 13. Historia: 5.1 Consulta de nombre de dominio del servidor de correo (MX) mediante dirección IP.....	30
Tabla 14. Historia: 5.2 Búsqueda de información de RDAP mediante dirección IP .....	30
Tabla 15. Historia: 5.3 Búsqueda de palabras clave .....	31
Tabla 16. Historia: 6.1 Listado de correos enviados, recibidos o en copia por cabeceras [From, To, Cc, Bcc] y por cuenta.....	31
Tabla 17. Historia: 6.2 Listado de fechas en las que se produjeron los intercambios.....	31



# 1. Introducción

## 1.1. Contexto

La informática forense es una ciencia relativamente novel que se encuentra en crecimiento constante y sostenido. Nuestros Códigos Procesales contienen artículos relacionados con los peritajes que definen quiénes pueden ejercer como peritos, pero no expresan los requisitos con los que se debe realizar una pericia, menos aún cuando se trata de informática ni tampoco hacen referencia al uso o no de software específicos.

El Código Procesal Civil y Comercial de la Nación en sus artículos 457 al 477 hace referencia a los peritos y a los puntos de pericia. El Art. 457 define la admisibilidad de la prueba pericial [1]: “Será admisible la prueba pericial cuando la apreciación de los hechos controvertidos requiere conocimientos especiales en alguna ciencia, arte, industria o actividad técnica especializada.”

El Art. 459 [2] describe las profesiones o especializaciones: “Al ofrecer la prueba pericial se indicará la especialización que ha de tener el perito y se propondrán los puntos de pericia...” Mientras tanto, el Art. 464 hace referencia a la idoneidad del perito:

Si la profesión estuviese reglamentada, el perito deberá tener título habilitante en la ciencia, arte, industria o actividad técnica especializada a que pertenezcan las cuestiones acerca de las cuales deba expedirse. En caso contrario, o cuando no hubiere en el lugar del proceso perito con título habilitante, podrá ser nombrada cualquier persona con conocimientos en la materia [3].”

Pero si bien existen metodologías y procedimientos estandarizados, tanto de manera local como internacional para la realización de pericias informáticas, queda al criterio de cada perito elegir los métodos o herramientas que prefiera utilizar para llevar a cabo sus tareas. Lo anteriormente expuesto, sumado a la naturaleza propia de la evidencia digital, puede presentar el riesgo de que se cometan errores durante la realización de una pericia y que las partes presenten impugnaciones.

A raíz de ello, el perito informático debe conocer las técnicas forenses apropiadas para cada caso y debe contar, de ser posible, con herramientas de software que den soporte a sus tareas. Sólo de este modo logrará el óptimo desempeño de su función.

Dentro del ámbito civil, entiéndase por ello juzgados civiles, laborales y comerciales, el correo electrónico representa uno de los tipos de prueba informática más comunes que se suelen presentar ya que constituye uno de los medios más utilizados para el intercambio de comunicaciones laborales, comerciales y de negocios. Este medio fue adoptado por particulares y empresas para transmitir todo tipo de datos y documentación, incluyendo contratos y conversaciones dentro de entornos de trabajo. Dentro del área que nos compete, que es el de las pericias informáticas, no nos debería sorprender que este alto número de comunicaciones aporte evidencias útiles para la resolución de litigios.

Es aquí donde el perito informático cumple un rol fundamental como auxiliar de la justicia, ya que un correcto análisis de estos correos electrónicos en sus archivos de origen puede responder a los puntos periciales planteados por las partes intervinientes tanto en procesos judiciales como en actuaciones preliminares.

Es así como por medio de este trabajo se estudiará la manera en que la información contenida en estos archivos digitales puede revelar datos sobre los hechos ocurridos. Teniendo en cuenta lo anterior, se decidió abordar el desarrollo de una aplicación que asista al perito en la búsqueda de respuestas a los interrogantes planteados como puntos de pericia.

## 1.2. Presentación Breve de la Situación Problemática

Con mayor frecuencia de lo imaginado, los peritos informáticos se enfrentan con la tarea de tener que analizar grandes cantidades de correos electrónicos mediante sus archivos digitales. Esta tarea, a menudo compleja y demandante, podría realizarse de manera más eficiente, mientras que se podría reducir los tiempos de entrega de los resultados y evitar el error humano si se automatizara de forma total o parcial.

Existen aplicaciones de software que cumplen con algunas de las funciones de análisis que se requiere, pero no se encontró ninguna que pueda contestar los puntos de pericia más recurrentes, que a la vez sea segura en lo que refiere al resguardo de la evidencia y principalmente, que sea económicamente accesible para los peritos informáticos.

Dentro de los puntos periciales más frecuentes, los peritos informáticos, pueden tener que responder a los siguientes interrogantes: validar la autenticidad de los correos electrónicos aportados a la causa, verificar las direcciones de correos e ips intervinientes en las distintas conversaciones, verificar fechas, remitentes y destinatarios, palabras clave y otros datos de interés para la causa.

### 1.3. Objetivos

#### 1.3.1. Objetivo general

Crear una aplicación que automatice el procesamiento de correos electrónicos que sea económicamente accesible y que sirva de soporte para los peritos informáticos forenses en la República Argentina.

#### 1.3.2. Objetivos específicos

- (a) Procesar archivos de correos de manera automatizada.
- (b) Generar reportes con los principales datos de los correos para facilitar la confección de informes.
- (c) Identificar direcciones de correo, ips, fechas, palabras claves y otros datos relevantes de manera automatizada.
- (d) Facilitar la validación de los campos de autenticación del emisor.
- (e) Responder a los puntos de pericia más frecuentes.

### 1.4. Alcance

La aplicación será capaz de procesar archivos de correo electrónico en formatos de software libre, luego de haber sido recolectados como evidencia durante la pericia y alojados en el equipo informático del perito para su análisis.

Se enfocará principalmente en el procesamiento de los encabezados de correos electrónicos que serán visualizadas por pantalla o copiados en un archivo para facilitar su lectura. Asimismo, se podrán realizar búsquedas por ips y palabras clave y además contempla la validación de los campos de autenticación del emisor.

#### 1.5. No contempla

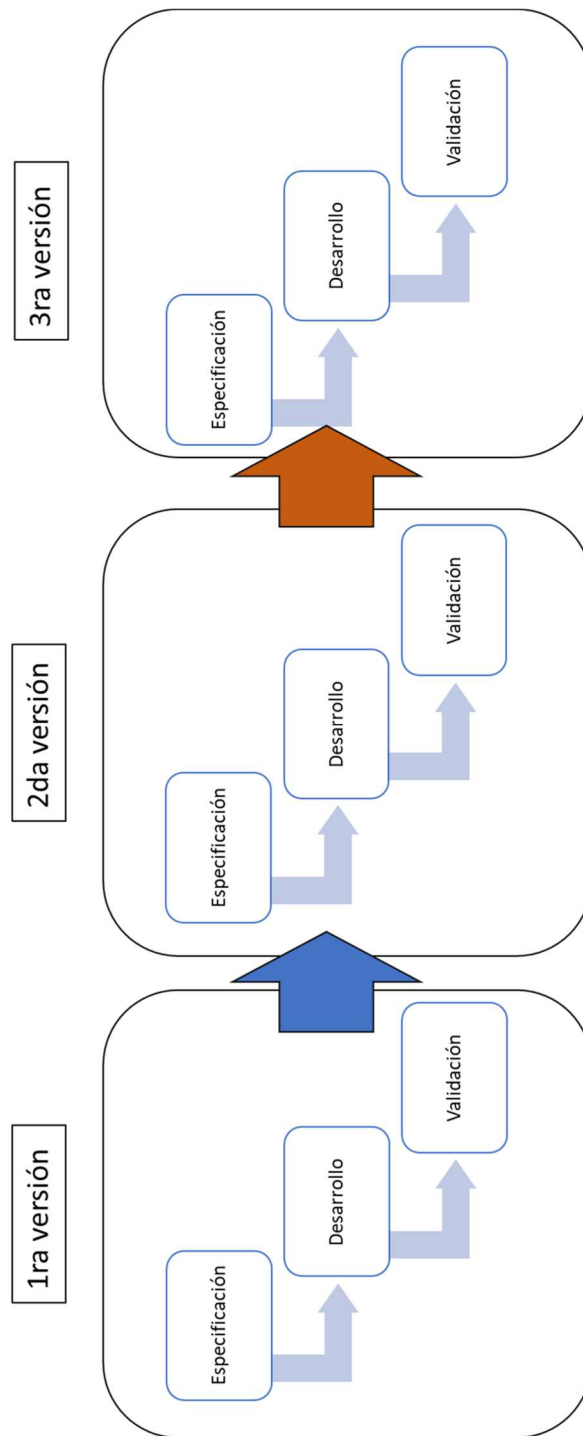
No contempla el procesamiento de correos de software propietario (Microsoft Outlook, Apple Mail) ni el procesamiento de correos electrónicos alojados en los dispositivos peritados.

#### 1.6. Hipótesis del Trabajo

Se desarrollará una aplicación que permitirá agilizar el proceso de análisis de correos electrónicos y facilitará la resolución a los puntos de pericia más comunes propuestos por las partes en expedientes judiciales que, además, servirá como herramienta de soporte en la confección de informes periciales.

#### 1.7. Metodología

Para cumplir con los pasos del ciclo de vida de desarrollo de software se eligió la metodología de desarrollo incremental. Esta metodología consiste en una implementación inicial para su primera evaluación y luego se crean distintas versiones que agregan nuevas funcionalidades hasta llegar a una versión final. El modelo incremental consta de tres etapas principales: especificación, desarrollo y validación. Las etapas se retroalimentan y se repiten de manera cíclica en iteraciones hasta lograr el resultado esperado.



*Ilustración 1. Desarrollo iterativo incremental*

### 1.8. Plan de Actividades

Se diagramó el plan de actividades de acuerdo con las tareas planificadas, su estimación y duración con la finalidad de completar este proyecto con fecha de entrega a finales de noviembre de 2022.

Id.	Nombre de tarea	Comienzo	Fin	Duración	mar. 2022			abr. 2022				may. 2022				jun. 2022				jul. 2022				ago. 2022				sep. 2022				oct. 2022				nov. 2022											
					13/3	20/3	27/3	3/4	10/4	17/4	24/4	1/5	8/5	15/5	22/5	29/5	5/6	12/6	19/6	26/6	3/7	10/7	17/7	24/7	31/7	7/8	14/8	21/8	28/8	4/9	11/9	18/9	25/9	2/10	9/10	16/10	23/10	30/10	6/11	13/11							
1	Justificación del problema	14/3/2022	25/3/2022	10d	█																																										
2	Encuestas y tareas de relevamiento	4/4/2022	22/4/2022	15d				█																																							
3	Definición del objeto de estudio	25/4/2022	13/5/2022	15d								█																																			
4	Definición de historias de usuario	16/5/2022	27/5/2022	10d												█																															
5	Selección de herramientas	1/6/2022	28/6/2022	20d												█																															
6	Definición de alcance y límites	15/6/2022	12/7/2022	20d												█																															
7	Desarrollo, pruebas y entregas incrementales	5/7/2022	7/11/2022	90d																█																											
8	Redacción de informe final	15/8/2022	11/11/2022	65d																				█																							
9	Evaluación y conclusiones	14/11/2022	25/11/2022	10d																												█															

Ilustración 2. Diagrama de Gantt

## 2. Situación Problemática

### 2.1. Descripción

Para comenzar a desarrollar temas relacionados con la problemática propia de la informática forense se debe entender primero que cuando se habla de ciencia forense, se hace referencia a la disciplina que sirve como soporte a la investigación judicial en causas civiles y penales. También se debe considerar a la criminalística como la disciplina que aporta métodos y técnicas de investigación. Finalmente se debe comprender a la informática forense dentro de las ciencias forenses y la importancia en el tratamiento de la evidencia digital que es el objeto de esta ciencia.

Guzmán [4] describe a la ciencia forense como "la profesión y disciplina científica dirigida al reconocimiento, individualización y evaluación de la evidencia física mediante la aplicación de las ciencias naturales en cuestiones legales".

El término ciencia forense engloba una variedad de disciplinas, cada una de las cuales posee sus propios métodos y técnicas, grado de madurez, investigaciones publicadas, etc. [5]. Algunas de estas ciencias se desarrollan en laboratorios como el análisis de ADN, otras se basan en la interpretación de expertos y la mayoría requieren del empleo de conocimientos científicos. Sin embargo, a pesar de las diferencias, todas ellas deben respetar ciertos principios para que la prueba analizada sea admisible en un juicio y pueda rebatir las impugnaciones o nulidades planteadas por la parte opuesta.

La criminalística surge como la disciplina centrada en la investigación aplicando el método científico. Darahuge & Arellano [6] la describe como "la disciplina auxiliar de la investigación judicial que aplica los conocimientos, métodos y técnicas de investigación de las ciencias naturales en el examen del material sensible, significativo relacionado con un supuesto hecho delictivo".

El objetivo principal de la criminalística es llegar a la verdad respecto a un hecho. Esta disciplina propone dos principios básicos que son aplicables a todas las ciencias forense. Al primero se lo conoce como principio de

intercambio de Locard [5] y dice que, cualquier interacción entre una persona u objeto con otro produce un intercambio de materiales físicos entre ambos, por lo cual siempre va a dejar rastros. Como ejemplo, se puede pensar en las huellas digitales de una persona que bebe agua de una copa puestas en esa copa.

El segundo es el principio del árbol envenenado, lo que significa que las pruebas deben obtenerse de manera legítima ya que de lo contrario no pueden ser admitidas en el proceso. Este principio intenta poner énfasis en el tratamiento correcto de la evidencia para evitar su contaminación.

La informática forense forma parte de las ciencias forenses, si bien el término computación forense aparece por primera vez en 1992 en un artículo de Collier y Spaul [7], se la debe considerar y aplicar los mismos métodos aplicables a las disciplinas tradicionales. Cabe aclarar, que, tanto informática forense, como cómputo forense, análisis forense digital o examen forense digital se utilizan indistintamente. En este trabajo se utilizará el término informática forense. Darahuge & Arellano [6], define a la informática forense como “el conjunto multidisciplinario de teorías, técnicas y métodos de análisis, que brindan soporte conceptual y procedimental a la investigación de la prueba indiciaria informática”.

Cano [8] la describe como “la disciplina de las ciencias forenses que, considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso”.

Respecto al tratamiento de la evidencia digital, la norma ISO/IEC 27037 [9] expresa dos definiciones: (a) equipo electrónico utilizado para procesar o almacenar información en formato digital y (b) información o datos almacenados o transmitidos en formato binario que puede servir de evidencia.

Para Casey [10], la evidencia digital es “un tipo de evidencia física construida de campos magnéticos y pulsos electrónicos que por sus características deben ser recolectados y analizados con herramientas y técnicas especiales”.



Mas allá de las diferentes definiciones, es importante destacar el enorme desafío que la evidencia digital presenta debido a su propia naturaleza. Cano [11] describe cuatro características propias de la evidencia digital: (a) es volátil, lo que significa que se pierde al interrumpirse el suministro eléctrico; (b) es anónima, ya que si bien se le puede atribuir a un usuario no significa que se la pueda vincular a la persona física; (c) puede ser duplicada o modificada, se pueden crear copias idénticas y puede ser modificada quebrando su integridad; (d) puede eliminarse con facilidad.

## 2.2. Explicación

El perito informático de oficio debe ser un profesional poseedor de un título en informática, ya sea Analista, Ingeniero o Licenciado en Sistemas o Informática y debe estar inscripto en los fueros en los que desea desarrollarse como perito. Además de cumplir con los requisitos formales mencionados, debe aceptar el cargo para el que es designado por sorteo, realizar la pericia encomendada y contestar los puntos propuestos por las partes, manteniendo la imparcialidad y dentro de los tiempos procesales.

De no cumplir con alguno de los requisitos anteriormente mencionadas, se puede llegar a pedir su remoción y podría quedar inhabilitado para ejercer el cargo por dos años. El número de peritos informáticos inscriptos en los fueros judiciales es bajo y la presentación de evidencia digital como prueba en los expedientes judiciales es cada vez mayor. Esto hace que sean profesionales muy requeridos y resulten sorteados con gran frecuencia.

Las incumbencias de estos profesionales pueden abarcar cualquier tipo de evidencia de origen digital, ya sean imágenes fotográficas o videos, publicaciones en redes sociales, páginas web, bases de datos, códigos fuente de programas de computación, servidores, discos rígidos, memorias extraíbles, aplicaciones y bases de datos biométricos, archivos de planillas de cálculo, mensajería electrónica y lo que nos compete como objeto de estudio de este trabajo que son los correos electrónicos.

El interés en el estudio de los correos electrónicos como evidencia digital se basa en el resultado de un relevamiento realizado entre expedientes judiciales donde se solicitaban pericias informáticas. El resultado de este

relevamiento demostró que en la mayoría de estos expedientes las pruebas presentadas tenían que ver con mensajes de correos electrónicos intercambiados entre las partes. A continuación, a modo de ejemplo, se presentan puntos periciales extraídos de cinco expedientes judiciales en fueros civiles.

#### Expediente 1

En caso de que la demandada desconociere el intercambio existente entre las partes que surgen de los correos electrónicos que se adjuntan como prueba documental a la presente demanda solicito se ordene producir prueba pericial informática designándose perito en sistemas de oficio a fin de que, efectuando las constataciones que resulten necesarias, se expida sobre la autenticidad de dichos mails<sup>1</sup>.

Para el caso de que sean desconocidos los correos electrónicos acompañados y detallados como prueba documental (punto 4), solicito se designe perito ingeniero en sistemas a fin de que consultando los servidores y/o el sistema y/o computadoras de mi mandante, se expida sobre la autenticidad y originalidad de estos<sup>2</sup>.

#### Expediente 2

Para el caso en que las demandadas desconozcan los correos electrónicos que se le atribuyen y VS lo estime estrictamente necesario, mi parte solicita se designe perito informático de oficio, a fin de que, en base a sus conocimientos técnicos, revisando los servidores involucrados, sus archivos de bitácora y resguardos y los datos correspondientes al ISP (Proveedor de Servicios de Internet) y DNS (Servicio de Nombre de Dominio) y cualquier otra técnica que estime pertinente determine: (i) Si los correos electrónicos que se acompañan en forma impresa, han sido efectivamente enviados/recibidos con sus adjuntos, así como sus fechas y horas; (ii) Confirme el perito que los correos electrónicos enviados/recibidos de dichos

---

<sup>1</sup> COM 018289/2016, puntos de pericia solicitados por la actora.

<sup>2</sup> COM 018289/2016, puntos de pericia solicitados por la demandada.

servidores no han sido alterados y/o modificados con posterioridad a su envío/recepción<sup>3</sup>.

### Expediente 3

Para el supuesto que se desconociera la veracidad de los e-mails emitidos por la suscripta y/o los contestados por el demandado, se designe un perito ingeniero en informática para que, examinando la computadora personal de la actora en su domicilio, informe si envió y recibió los e-mails descriptos en la demanda. En su caso a quién fueron dirigidos y quién los contestó. En la máquina computadora de la actora (IP denunciado por el propio demandado), informe si se enviaron y recibieron los e-mails que se acompañan como prueba documental en este conteste.<sup>4</sup>

Fecha y hora de remisión, casilla de correos remitente y casilla destinataria del mail que obra acompañada como prueba documental<sup>5</sup>.

### Expediente 4

Teniendo a la vista los correos electrónicos y documentos que como prueba documental y en el apartado correspondiente se acompañan, determine: (a) Si los correos electrónicos acompañados como prueba documental han sido remitidos desde y hacia las direcciones que figuran en los mismos. (b) Si los correos electrónicos impresos y adjuntos a esta presentación coinciden con los obrantes en el equipo, en cuanto a su contenido, fecha y hora de envío y recepción y sujetos remitentes y receptores. (c) Si ha detectado algún indicio de manipulación de estos. (d) Dictamine acerca de la autenticidad e integridad de la totalidad de los correos electrónicos individualizados en el apartado documental, informando si los mismos pudieron haber sufrido alteraciones que varíen su contenido, teniendo en consideración los siguientes elementos de valoración o ponderación: análisis del equipo objeto de peritaje; datos de encabezados y, sobre todo, su correspondencia cronológica. (e) Si puede determinar la identidad de las

---

<sup>3</sup> CIV 42262/2015, puntos de pericia solicitados por la actora.

<sup>4</sup> CNT 006526/2018, puntos de pericia solicitados por la actora.

<sup>5</sup> CNT 006526/2018, puntos de pericia solicitados por la demandada.

partes autoras de los correos electrónicos identificados en el apartado documental.<sup>6</sup>

#### Expediente 5

Se designe perito informático especialista en sistemas a fin de que se expida sobre la autenticidad y/o emisión y/o recepción de los correos electrónicos ofrecidos como prueba, verificando además si la casilla desde la cual fueron enviados pertenece a la actora y/o a la demandada y si esta última es titular de la cuenta y/o casilla de la cual fue remitida, indicando los datos de la persona y/o empleada usuaria de esta.<sup>7</sup>

De los expedientes consultados resulta que los puntos de pericia solicitados suelen ser comunes y se pueden dividir en tres tipos. Los que tienen que ver con la evidencia digital propiamente dicha como autenticidad e integridad, los relacionados con las empresas proveedoras de servicio o registraciones como ISP, direcciones de IP o DNS y finalmente los metadatos que se obtienen de los encabezados como ser casillas de correo del emisor y receptor, fecha y hora de envío o recepción, etc.

Con esta información relevada se procedió a realizar una encuesta entre peritos informáticos miembros del COPITEC y peritos cursantes de la Maestría en Seguridad Informática de la UBA para capturar con mayor detalle aquellas funcionalidades que les resultarían útiles encontrar en una herramienta que automatice el análisis de correos electrónicos. La encuesta se basó en diez preguntas más dos puntos a dónde los peritos podían dejar sus datos en caso de querer participar de ser necesario en la etapa de pruebas.

Los resultados de la encuesta arrojaron que el 93,5% de los peritos realizan peritajes sobre correos electrónicos. Esto coincide con lo relevado de los expedientes judiciales. Respecto a los puntos de pericia que se solicitan con mayor frecuencia las respuestas también coinciden con lo visto en los expedientes, ya que validación de autenticidad obtuvo un 93,5% de

---

<sup>6</sup> CNT 3316/2017, puntos de pericia solicitados por la actora.

<sup>7</sup> CNT 039437/2021, puntos de pericia solicitados por la actora.

respuestas, remitentes el 48,4% y fechas el 45,2%. A estas tres primeras le siguen validación de integridad y direcciones de IP.

Respecto a los métodos utilizados, el 96,7% de los peritos respondió que realizaban las tareas de validación de forma manual y el conocimiento acerca de herramientas que brinden soporte resultó ser escueto. Entre las funcionalidades más críticas o que resultaron de mayor interés, los encuestados eligieron la validación automatizada de encabezados con el 90%, le siguieron la presentación de resultados con el 53,3% y la carga y lectura de archivos de correo de manera automatizada obtuvo el 46,9% de los votos.

Asimismo, los participantes respondieron que una herramienta que cumpla con las funcionalidades que se quieren implementar ahorraría tiempo en la generación de los informes periciales y podría ayudar a reducir el error humano. Entre los datos principales que se requiere validar, el 28% respondió direcciones de correo del remitente y el receptor, mientras que un 21% respondió fecha y hora de envío y otro 21% respondió que los más importante eran las validaciones de autenticidad e integridad.

En cuanto al tipo de archivos con el que trabajan, el 80% respondió que trabajan con archivos en formato EML, que son los generados por aplicaciones de webmail como Gmail o Yahoo! Mail, el 50% dijo trabajar con archivos de texto plano, TXT, un 26,7% respondió que trabaja con archivos MBOX, que son archivos extraídos de Gmail que contienen grupos de varios correos en un solo archivo y solamente el 3,3% dijo trabajar con archivos MSG, propiedad de Microsoft y por último el 3,3% respondió que utilizaba Apple Mail.

El 90% de los peritos encuestados dijo utilizar el sistema operativo Windows, el 40% dijo utilizar Linux y solo el 3,3% manifestó que utilizaban Apple iOS. En cuanto a sus preferencias respecto a una interfaz para la aplicación a desarrollar, el 55,2% respondió que prefiere una aplicación de escritorio sin conexión a internet, mientras que el 34,5% preferiría una aplicación web. Ninguno de los entrevistados dijo preferir una aplicación por línea de comandos.

### 2.3. Diagnóstico

La encuesta realizada entre peritos informáticos confirma lo relevado a través de los expedientes judiciales. Esto reafirma que los puntos periciales solicitados por las partes suelen repetirse en la mayoría de los expedientes judiciales. Que el perito se expida sobre la autenticidad y la integridad de los correos es un punto común a todas las causas. Le siguen en importancia los datos contenidos en los encabezados de los correos electrónicos como las direcciones de remitente y destinatario y las fechas y horas de envío y de recepción, es decir los metadatos.

De la encuesta también surge la necesidad de automatizar el proceso de validación, hecho hasta el momento de manera manual, para hacer un trabajo más eficiente, lo cual coincide con el objetivo de este trabajo.

### 3. Marco Referencial

#### 3.1. Formato de Mensajes de Internet

La estructura de un mensaje de correo electrónico fue definida en agosto de 1982 mediante el RFC 822: "Formato de Mensajes de Internet" [12] y actualizada por el RFC 2822 [13] en abril de 2001 y más tarde por el RFC 5322 [14] en octubre de 2008. La especificación se centra en mensajes en formato de texto y describe al mensaje de correo electrónico como un sobre con información útil para poder realizar la transmisión, entrega y el contenido del mensaje, siendo esto último lo que se quiere enviar al receptor.

La estructura de un mensaje se divide en encabezado y cuerpo. El encabezado contiene una serie de campos con sus respectivos valores conformando un diccionario de datos del tipo clave-valor. Los campos más comunes en un encabezado son: 'From', 'To', 'Subject', 'Date', 'Message-id' [15]. Estos metadatos contenidos en el encabezado de un mensaje resultan indispensables para poder responder puntos de pericia.

El cuerpo del mensaje, generalmente en formato de texto, aunque este no sea el único posible, representa lo que se quiere transmitir, el mensaje que el emisor envía al receptor. Los tipos de formatos están definidos en el RFC 1437 (Extension of MIME Content-Types TO A new Medium) [16], donde MIME significa Extensiones de Correo Internet Multipropósito y contiene una serie de especificaciones relacionadas con el intercambio de archivos de texto, audio, video, imágenes, etc.

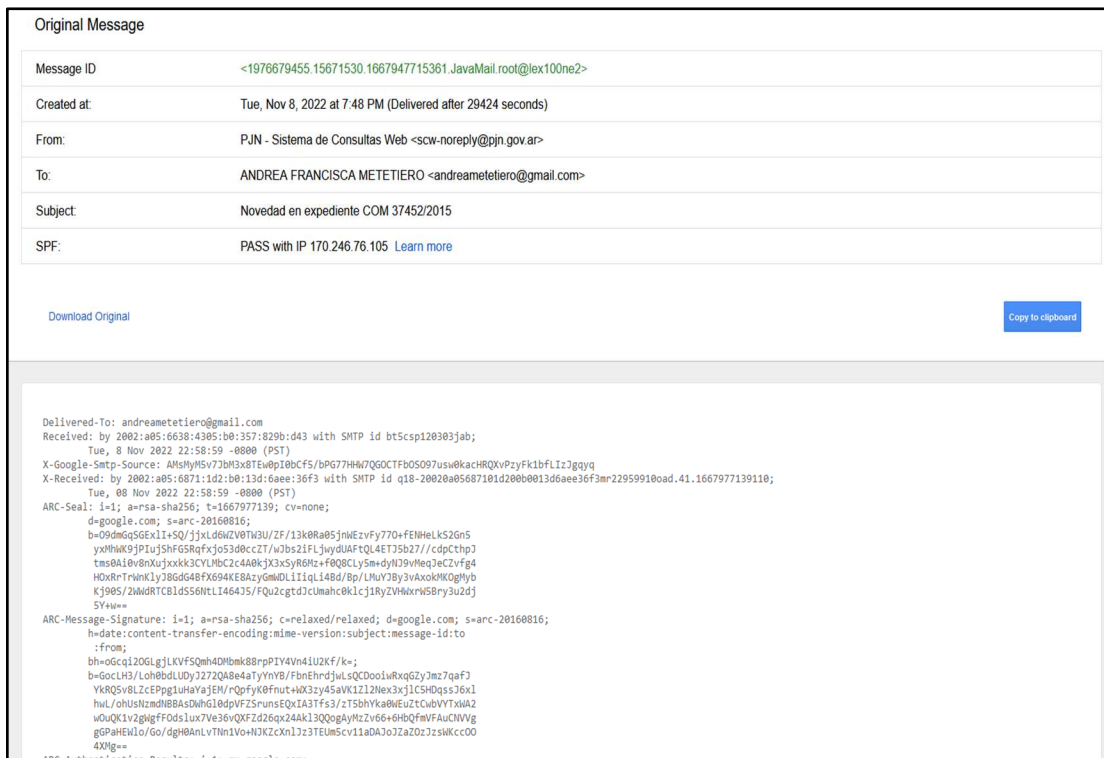
```
From: ABC-Enterprise <abc@abcenterprise.com>¶
To: Maria <maria@abcenterprice.com>¶
Subject: Mensaje de prueba¶
Message-ID: <abcde1234@abcenterprise.server.com>¶
Este es un mensaje de prueba. ¶
¡Saludos!¶
```

*Ilustración 3. Mensaje*

### 3.2. Campos del Encabezado

Los campos que conforman el encabezado de un correo electrónico aportan datos de suma importancia para una pericia informática. Como se describió anteriormente, se componen de campo y valor, separados por dos puntos y pueden aparecer en cualquier orden. Según el estándar RFC 2822 [13] únicamente los campos fecha de origen (“Date”) y dirección del origen (“From” o “Sender”) son obligatorios, el resto de las cabeceras son opcionales.

Para poder visualizar los campos de un correo electrónico de tipo webmail como Google o Yahoo! se debe ingresar a la cuenta de correo y seleccionar la opción “Ver Original”. Seguidamente la aplicación webmail nos mostrará una pantalla similar a la siguiente con información de los campos del correo seleccionado. Asimismo, la opción “Descargar original” permite descargar el archivo con la extensión EML.



The screenshot displays the 'Original Message' header of an email. The fields are as follows:

- Message ID:** <1976679455.15671530.1667947715361.JavaMail.root@lex100ne2>
- Created at:** Tue, Nov 8, 2022 at 7:48 PM (Delivered after 29424 seconds)
- From:** PJN - Sistema de Consultas Web <scw-noreply@pjn.gov.ar>
- To:** ANDREA FRANCISCA METETIERO <andreameteliero@gmail.com>
- Subject:** Novedad en expediente COM 37452/2015
- SPF:** PASS with IP 170.246.76.105 [Learn more](#)

Below the header, there are buttons for 'Download Original' and 'Copy to clipboard'. The bottom section shows the raw email source code, including headers like 'Delivered-To', 'Received', 'X-GoogLe-Smtp-Source', 'ARC-Message-Signature', and 'ARC-Authentication-Results'.

Ilustración 4. Muestra de mensaje original en Gmail

La siguiente tabla muestra los principales campos de un encabezado y una breve descripción.



Dato	Cabecera	Descripción
Fecha de origen	Date	Fecha y hora en que el mensaje ingresa al sistema para su transmisión. No necesariamente la fecha y hora de envío que puede ser posterior.
Direcciones de origen	From	Casilla de correo perteneciente al autor del mensaje.
	Sender	La dirección del agente responsable por la transmisión del mensaje, si este lo hiciese en nombre del autor. En caso de ser el mismo no debe estar presente.
	Reply-To	Casilla de correos en la cual el autor desea recibir respuesta. De no estar presente las respuestas son enviadas a "From:"
Direcciones de destino	To"	Direcciones de correo de los destinatarios primarios.
	Cc	Otras cuentas receptoras del mensaje en modo de "copia de carbón".
	Bcc	Direcciones de correo de destinatarios que el autor no desea revelar.
Identificación	Message-Id	Identificación global única del mensaje, que está garantizada por el host que lo genera.
	In-Reply-To	Contiene el "Message-Id" del mensaje al que se está respondiendo.
	References	Si está presente, contiene los datos de "Referencia" del mensaje padre.
Información	Subject	Asunto del mensaje.
	Comments	Comentarios adicionales en el cuerpo del mensaje.
	Keywords	Palabras clave o frases de utilidad para el receptor.

Tabla 1. Campos del encabezado

### 3.2. Campos de Autenticación SPF, DKIM y DMARC

Otro estándar de interés es el RFC 6376: “Claves de Dominio para la Identificación de Correos-DKIM” [17]. Este campo junto con los denominados SPF y DMARC representan protocolos de autenticación de correos que certifican a los servidores que el remitente es seguro. Por sus características, estos metadatos resultan indispensables a la hora de responder puntos relacionados con la autenticidad y la integridad de un correo.

SPF (*Sender Policy Framework*): identifica a los servidores autorizados para el transporte de correos a través de sus registros de dominio DNS. De este modo se evita la falsificación de direcciones o la suplantación de identidad. El servidor receptor de correos compara el dominio de la dirección del remitente con los servidores autorizados para enviar mensajes desde ese dominio. Es importante destacar que, para que el servidor receptor pueda realizar esta comprobación, el servidor del remitente debe tener configurado un registro SPF [18]

```
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@novedades.santander.com.ar header.s=santanderargentina header.b=J6FpuzKm;
spf=pass (google.com: domain of bounce@novedades.santander.com.ar designates 130.248.183.97 as permitted sender)
```

*Ilustración 5. Campos de autenticación DKIM y SFP*

DKIM (*DomainKeys Identified Mail*): es un mecanismo de autenticación del remitente, quien puede ser el autor del mensaje, el servidor de ese dominio o un servidor intermedio. Utiliza criptografía de clave pública que permiten al origen firmar los correos electrónicamente permitiendo así validar la autenticidad del remitente. A su vez, añade al encabezado del correo una firma digital del contenido del mensaje, lo que permite validar su autenticidad e integridad [18].

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=novedades.santander.com.ar; s=santanderargentina; t=1669916042;
bh=MsUmApJMR27EYjBw4CRuYrFQEHZGK+ML7+SADctN/Gc=; h=From:Date:Subject:To:MIME-Version:Message-ID:Content-Type;
b=J6FpuzKmoXxPnpjYZYok1K/DLqLMhy09zAIBg7NOYjylyijViHecJSyubNLRXvS1
0RX+hPA3/Tiv1BHph7s0KoD5A+YSmR89Pda14YzikJiSqep16njhkoNoNcn19mTtIj
D9/qxHg/EEz2SrzP80Bdh7GuWsiqfjJWhTCHCQ1tr5Ifw8inApNu4eEAVUkrPDAD
MfvUKAPzdQ8ttp/sSMm1wpNhEWLZYzFQw7ZyRqtTNlVgs8cPMPUa7b43GAYuojvBVc
uulWP4bqm1A9RhKJTIeDvN1M1fcbN5i21nUdZe6B30HrPeM9YhDxi7gxU/N2K7e10HJ
kELH1TQ/ZnTyg==
```

*Ilustración 6. Campos de firma DKIM*

DMARC (*Domain-based Message Authentication, Reporting & Conformance*): verifica que los campos SPF y DKIM estén correctamente autenticados y previene la suplantación de identidad, bloqueando actividades fraudulentas [18]. Para el objeto que nos compete, que son las pericias informáticas, este campo indica que el remitente del mensaje es quien dice ser y que el mensaje no fue modificado.

### 3.3. Tipos de Archivos

Los archivos de correo electrónico pueden presentarse en distintos formatos de acuerdo con la aplicación que se esté utilizando. Existen formatos de software libre como EML y MBOX, que no son más que archivos de texto y por lo tanto pueden abrirse y leerse con cualquier editor de texto o aplicación de correo. Pero también existen archivos de propiedad de Microsoft como MSG, PST, OST y EDB, representados por objetos binarios, que solo pueden leerse con la aplicación de correos Outlook. Apple por su parte tiene su propio formato de archivos. A continuación, se describen algunos de estos.

EML: este tipo de archivo contiene un mensaje en formato de texto plano que por sus características puede abrirse con diversas aplicaciones cliente de correo como Mozilla Thunderbird y Outlook Express, editores de texto o aplicaciones de web mail como Yahoo! o Gmail.

MBOX: presenta las mismas características que el anterior, pero contiene un grupo de correos almacenados en un mismo archivo de manera secuencial.

EMLX: es un formato desarrollado e implementado por la firma Apple que al igual que los anteriores puede abrirse y leerse con un editor de texto.

MSG: es el formato de Outlook para almacenar un objeto *Message*, que puede ser un correo, una entrada en agenda, un contacto, etc. que contiene el texto del correo junto a sus metadatos, archivos adjuntos y otros objetos. Está basado en CFB <sup>8</sup> y su implementación consiste en un sistema de

---

<sup>8</sup> CFB 3: Compound File Binary File Format 3.

archivos a través de una colección de objetos de almacenamiento y objetos de secuencias de caracteres [19].

PST (*Personal Storage Table*): son archivos con las mismas características que MSG pero que almacenan grupos de correos exportados desde Outlook.

EDB (*Exchange Database*): son archivos de Microsoft Exchange Server, la aplicación servidor de correos de Microsoft, que almacenan grandes cantidades de archivos PST.

OST (*Offline Storage Table*): este formato se utiliza para el almacenamiento de archivos PST que, en caso de no contar con una conexión a internet, al volver a conectarse se sincronizan con sus respectivos archivos PST.

Por múltiples razones, tanto diferencias técnicas como de índole práctico, este proyecto se centrará únicamente en el procesamiento de mensajes en formatos de software libre, es decir, EML y MBOX, dejando a los archivos propietarios de Microsoft y Apple para un posible desarrollo futuro.

### 3.4. Análisis del Mercado

Se realizó una comparación entre productos disponibles en el mercado, teniendo en cuenta las necesidades de los peritos informáticos en la República Argentina. A partir de esa comparación se pasa a describir las características principales de cada uno de ellos y se confecciona una tabla mostrando aquellas funcionalidades que son de interés por ser de utilidad para la resolución de puntos periciales.

#### 3.4.1. MXToolbox

Interpreta cabeceras de correos de archivos EML en forma individual de acuerdo con el RFC822. El usuario debe copiar y pegar uno por uno los correos que quiera analizar. La aplicación devuelve el resultado en la misma página web y posee una opción de borrar los archivos analizados en forma

definitiva. La versión web es gratuita dado que la empresa comercializa otros productos [20].

### 3.4.2. MessageHeader

Se encuentra dentro de la caja de herramientas de Google Admin [21], presenta características similares a la anterior como la validación de cabeceras de correos en formato EML en forma individual y también es gratuita.

### 3.4.3. SystoolMbox

Es una aplicación gratuita de escritorio que puede interpretar archivos en formato MBOX. Su versión paga, soporta una gran variedad de archivos como EML, OST y PST. Además, posee capacidad de generar hashes, realizar búsquedas, gestionar casos y generar reportes. Ambas versiones tienen la capacidad de procesar archivos adjuntos [22].

### 3.4.4. Aid4Mail

Esta aplicación de escritorio posee capacidad de análisis forense sobre distintos tipos de archivos mediante la conversión de formatos. Sus prestaciones y costo varían de acuerdo con la versión [23].

### 3.4.5. Paraben E-Mail Examiner

Es una herramienta de escritorio muy completa con capacidad de soportar la mayoría de los archivos existentes, realizar búsquedas, generar reportes y gestionar casos. Posee la capacidad de importar archivos de distintos medios, tanto locales como en línea. Su licencia tiene un costo fijo más se debe pagar un costo adicional por cada licencia que se desee adquirir [24].

Características	MXToolbox	MessageHeader	SystoolMbox	Aid4Mail	Paraben Email Examiner
<b>Verificaciones</b>					
<b>Autenticidad</b>	No	No	No	No	No
<b>Integridad</b>	No	No	No	No	No

Características	MXToolbox	MessageHeader	SystoolMbox	Aid4Mail	Paraben Email Examiner
<b>DKIM</b>	Si	Si	Si	Si	Si
<b>SPF</b>	Si	Si	Si	Si	Si
<b>DMARC</b>	Si	Si	Si	Si	Si
<b>Cabeceras</b>					
<b>Dirección de correo del remitente</b>	Si	Si	Si	Si	Si
<b>Dirección de correo del destinatario</b>	Si	Si	Si	Si	Si
<b>Fechas de envío o recepción</b>	Si	Si	Si	Si	Si
<b>Búsquedas</b>					
<b>Palabras clave</b>	No	No	sólo versión paga	Si	Si
<b>Direcciones de correo</b>	No	No	No	Si	Si
<b>Historial de fechas</b>	No	No	No	Si	Si
<b>Tipos de archivos</b>					
<b>EML</b>	Si	Si	No	Si	Si
<b>MBOX</b>	No	No	Si	Si	Si
<b>PST</b>	No	No	No	Si	Si
<b>OST</b>	No	No	No	Si	Si
<b>EDB</b>	No	No	No	No	Si
<b>MSG</b>	No	No	No	Si	Si
<b>Tipo de interfaz</b>					
<b>Web</b>	Si	Si	No	No	No
<b>Escritorio</b>	No	No	Si	Si	Si
<b>Sistema operativo</b>					
<b>Windows</b>	no aplica	no aplica	Si	Si	Si
<b>Linux</b>	no aplica	no aplica	No	No	No
<b>Mac</b>	no aplica	no aplica	Si	No	No
<b>Otras funcionalidades</b>					

Características	MXToolbox	MessageHeader	SystoolMbox	Aid4Mail	Paraben Email Examiner
<b>Carga automatizada de archivos</b>	No	No	Si	Si	Si
<b>Presentación de resultados en pantalla</b>	Si	Si	Si	Si	Si
<b>Generación de reportes</b>	No	No	sólo versión paga	Si	Si
<b>Generación de hashes</b>	No	No	sólo versión paga	Si	Si
<b>Procesamiento de adjuntos</b>	No	No	Si	Si	Si
<b>Precio</b>	Gratuita	Gratuita	USD 0 - 539	USD 299-5000/año	USD 1295

*Tabla 2. Análisis comparativo del mercado*

Como se puede observar, las herramientas que brindan mayores prestaciones tienen un costo relativamente alto para un perito informático en la República Argentina, más aún, si se tiene en cuenta que los precios de las herramientas son en dólares y los peritos cobran honorarios en pesos y en los fueros civiles, el cobro de honorarios ocurre varios años después de haber entregado su informe pericial.

## 4. Análisis del Sistema

### 4.1. Descripción de Requerimientos

Dentro de las metodologías ágiles, los requerimientos se describen como escenarios denominados historias de usuario [25]. Cada historia refleja una tarea realizada en un momento dado desde el punto de vista del usuario y suele escribirse en lenguaje no técnico.

Las historias de usuario tienen un formato estándar: COMO <tipo de usuario> QUIERO <acción> PARA QUE <motivo del negocio para esta historia>. Ejemplo: “como perito informático quiero poder seleccionar los archivos de correo EML contenidos en una carpeta dentro de mi disco C para poder visualizar sus cabeceras”.

Deben tener criterios de aceptación que describan la funcionalidad mínima necesaria para poder aprobar esa historia y se escriben en el siguiente formato: DADO QUE <precondiciones> CUANDO <acciones> ENTONCES <resultado esperado>. El desarrollo de una historia concluye cuando su estado es DONE, lo que significa que su análisis y desarrollo han concluido y las pruebas resultaron exitosas.

Historia	Prioridad	Complejidad	Estado	
<b>1. Selección de archivos</b>				
1.1	Selección de archivo TXT o EML.	Alta	Baja	Hecho
1.2	Selección de archivo MBOX.	Media	Media	Hecho
1.3	Selección de archivos EML por lotes.	Alta	Media	Hecho
<b>2. Visualización de archivos</b>				
2.1	Visualización de archivo TXT o EML por pantalla.	Alta	Baja	Hecho
2.2	Visualización de cabeceras de correos EML por pantalla.	Alta	Media	Hecho
2.3	Visualización de cabeceras de correos MBOX por pantalla.	Media	Media	Hecho



Historia		Prioridad	Complejidad	Estado
<b>3. Generación de CSV</b>				
3.1	Generación de archivo CSV con datos de cabeceras EML.	Alta	Media	Hecho
3.2	Generación de archivo CSV con datos de cabeceras MBOX.	Alta	Media	Hecho
<b>4. Autenticación</b>				
4.1	Validación de cabeceras de autenticación: SPF, DKIN, DMARC.	Media	Media	Hecho
<b>5. Consultas</b>				
5.1	Consulta de nombre de dominio del servidor de correo (MX) mediante dirección IP.	Media	Media	Hecho
5.2	Consulta de información de RDAP mediante dirección IP.	Media	Baja	Hecho
5.3	Consulta de palabras clave.	Media	Baja	Hecho
<b>6. Estadísticas</b>				
6.1	Listado de correos enviados, recibidos o en copia por cabeceras [From, To, Cc, Bcc] y por cuenta.	Media	Media	Hecho
6.2	Listado de fechas de envío.	Media	Baja	Hecho

*Tabla 3. Historias de usuario*

## 4.2. Descripción Detallada de Requerimientos

### 4.2.1. Requerimientos funcionales

Historia: 1.1 Selección de archivo TXT o EML.
Enunciado: Como perito informático quiero poder buscar un archivo de correo TXT o EML para poder procesarlo.
Criterios de aceptación:

Historia: 1.1 Selección de archivo TXT o EML.
<ul style="list-style-type: none"> <li>• Dado que estoy en la ventana principal de la aplicación, cuando hago clic en el botón “Buscar”, se abre una nueva ventana con el explorador de archivos del sistema.</li> <li>• Dado que estoy en el explorador de archivos, cuando selecciono un archivo, EML o TXT el nombre y la ruta se visualizan en el campo de entrada de texto “Seleccionar un archivo”.</li> </ul> <p>Precondiciones:</p> <ul style="list-style-type: none"> <li>• Archivo TXT o EML existente.</li> </ul>

*Tabla 4. Historia: 1.1 Selección de archivo TXT o EML*

Historia: 1.2 Selección de archivo MBOX.
Enunciado: Como perito informático quiero poder buscar un archivo de correo MBOX para poder procesarlo.
<p>Criterios de aceptación:</p> <ul style="list-style-type: none"> <li>• Dado que estoy en la ventana principal de la aplicación, cuando hago clic en el botón “Buscar”, se abre una nueva ventana con el explorador de archivos del sistema.</li> <li>• Dado que estoy en el explorador de archivos, cuando selecciono un archivo con formato MBOX el nombre y la ruta se visualizan en el campo de entrada de texto “Seleccionar un archivo”.</li> </ul> <p>Precondiciones:</p> <ul style="list-style-type: none"> <li>• Archivo MBOX existente.</li> </ul>

*Tabla 5. Historia: 1.2 Selección de archivo MBOX*

Historia: 1.3 Selección de archivos EML por lotes.
Enunciado: Como perito informático quiero poder buscar una carpeta para poder procesar los archivos EML.
Criterios de aceptación:

Historia: 1.3 Selección de archivos EML por lotes.
<ul style="list-style-type: none"> <li>• Dado que estoy en la ventana principal de la aplicación, cuando hago clic en el botón “Buscar”, se abre una nueva ventana con el explorador de archivos del sistema.</li> <li>• Dado que estoy en el explorador de archivos, cuando selecciono una carpeta el nombre y la ruta se visualizan en el campo de entrada de texto “Seleccionar una carpeta”.</li> </ul> <p>Precondiciones:</p> <ul style="list-style-type: none"> <li>• Archivos EML existentes.</li> </ul>

*Tabla 6. Historia: 1.3 Selección de archivos EML por lotes*

Historia: 2.1 Visualización de archivo TXT o EML por pantalla.
Enunciado: Como perito informático quiero poder abrir un archivo de correo TXT o EML para visualizar sus cabeceras y cuerpo.
<p>Criterios de aceptación:</p> <ul style="list-style-type: none"> <li>• Dado que estoy en la ventana principal de la aplicación, cuando hago clic en el botón “Abrir”, se visualiza el archivo completo por pantalla.</li> </ul> <p>Precondiciones:</p> <ul style="list-style-type: none"> <li>• Archivo TXT o EML abierto.</li> </ul>

*Tabla 7. Historia: 2.1 Visualización de archivo TXT o EML por pantalla*

Historia: 2.2 Visualización de cabeceras EML por pantalla.
Enunciado: Como perito informático quiero poder seleccionar los archivos de correo EML contenidos en una carpeta para visualizar sus encabezados.
<p>Criterios de aceptación:</p> <ul style="list-style-type: none"> <li>• Dado que se encuentra seleccionada una carpeta conteniendo archivos EML, cuando hago clic en el botón “EML”, se muestra por pantalla el nombre del archivo y todos los encabezados de los correos contenidos en la carpeta seleccionada.</li> <li>• Dado que se procesaron todos los correos dentro de una carpeta se muestra por pantalla el número de archivos analizados.</li> </ul>

Historia: 2.2 Visualización de cabeceras EML por pantalla.
Precondiciones: <ul style="list-style-type: none"> <li>• Carpeta conteniendo archivos EML seleccionada.</li> </ul>

*Tabla 8. Historia: 2.2 Visualización de cabeceras EML por pantalla*

Historia: 2.3 Visualización de cabeceras MBOX por pantalla.
Enunciado: Como perito informático quiero poder seleccionar un archivo de correo MBOX contenidos en una carpeta para visualizar sus encabezados.
Criterios de aceptación: <ul style="list-style-type: none"> <li>• Dado que se encuentra seleccionada una carpeta conteniendo archivos, cuando hago clic en el botón “MBOX”, se muestra por pantalla el nombre del archivo y todos los encabezados de los correos contenidos en la carpeta seleccionada.</li> <li>• Dado que se procesaron todos los correos dentro de una carpeta se muestra el número de archivos analizados.</li> </ul> Precondiciones: <ul style="list-style-type: none"> <li>• Carpeta conteniendo archivos MBOX seleccionada.</li> </ul>

*Tabla 9. Historia: 2.3 Visualización de cabeceras MBOX por pantalla*

Historia: 3.1 Generación de archivo CSV con datos de cabeceras EML.
Enunciado: Como perito informático quiero poder generar un archivo CSV con cabeceras EML de los archivos analizados.
Criterios de aceptación: <ul style="list-style-type: none"> <li>• Dado que estoy en la ventana principal de la aplicación, cuando hago clic en el botón “Exportar-EML”, se genera un archivo con los encabezados predefinidos de los correos: ['From', 'To', 'CC', 'Bc', 'Subject', 'Date', 'Message-Id', 'Authentication-Results'] como cabeceras del archivo y los datos de esos campos como filas.</li> </ul> Precondiciones: <ul style="list-style-type: none"> <li>• Carpeta conteniendo archivos EML seleccionada.</li> </ul>

*Tabla 10. Historia: 3.1 Generación de archivo CSV con datos de cabeceras EML*

Historia: 3.2 Generación de archivo CSV con datos de cabeceras MBOX analizado.
Enunciado: Como perito informático quiero poder generar un archivo CSV con cabeceras MBOX de los archivos analizados.
<p>Criterios de aceptación:</p> <ul style="list-style-type: none"> <li>• Dado que estoy en la ventana principal de la aplicación, cuando hago clic en el botón “Exportar-MBOX”, se genera un archivo tipo CSV con las cabeceras predefinidos de los correos: ['From', 'To', 'CC', 'Bc', 'Subject', 'Date', 'Message-Id', 'Authentication-Results'] como encabezado del archivo y los datos de esos campos como filas.</li> </ul> <p>Precondiciones:</p> <ul style="list-style-type: none"> <li>• Carpeta conteniendo archivos MBOX seleccionada.</li> </ul>

*Tabla 11. Historia: 3.2 Generación de archivo CSV con datos de cabeceras MBOX analizado*

Historia: 4.1 Validación de cabecera de autenticación de correos: SPF, DKIN, DMARC.
Enunciado: Como perito informático quiero poder generar validaciones de las cabeceras SFP, DKIM, y DMARC.
<p>Criterios de aceptación:</p> <ul style="list-style-type: none"> <li>• Dado que estoy en la ventana principal de la aplicación, cuando hago clic en los botones EML o MBOX, el programa devuelve los correos analizados junto con los resultados de las cabeceras de autenticación.</li> </ul> <p>Precondiciones:</p> <ul style="list-style-type: none"> <li>• Archivo EML o MBOX abierto.</li> </ul>

*Tabla 12. Historia: 4.1 Validación de cabecera de autenticación de correos: SPF, DKIN, DMARC*

Historia: 5.1 Consulta de nombre de dominio del servidor de correo (MX) mediante dirección IP.
Enunciado: Como perito informático quiero poder ingresar la dirección IP del servidor de correo y obtener el nombre de dominio.

<p>Historia: 5.1 Consulta de nombre de dominio del servidor de correo (MX) mediante dirección IP.</p>
<p>Criterios de aceptación:</p> <ul style="list-style-type: none"> <li>• Dado que estoy en la ventana principal de la aplicación, cuando ingreso la dirección IP obtenida de las cabeceras 'Received', 'Received-SPF' o 'spf' el campo de entrada de texto "Consultar MX", se muestra el nombre del servidor por pantalla.</li> </ul> <p>Precondiciones:</p> <ul style="list-style-type: none"> <li>• Dirección IP válida.</li> </ul>

*Tabla 13. Historia: 5.1 Consulta de nombre de dominio del servidor de correo (MX) mediante dirección IP*

<p>Historia: 5.2 Búsqueda de información de RDAP mediante dirección IP.</p>
<p>Enunciado: Como perito informático quiero poder ingresar la dirección IP del servidor de correo y obtener los datos de ese dominio y registración.</p>
<p>Criterios de aceptación:</p> <ul style="list-style-type: none"> <li>• Dado que estoy en la ventana principal de la aplicación, cuando ingreso la dirección IP obtenida de las cabeceras 'Received', 'Received-SPF' o 'spf' el campo de entrada de texto "Consultar RDAP", se muestran los datos de dominio y registración.</li> </ul> <p>Precondiciones:</p> <ul style="list-style-type: none"> <li>• Dirección IP válida.</li> </ul>

*Tabla 14. Historia: 5.2 Búsqueda de información de RDAP mediante dirección IP*

<p>Historia: 5.3 Búsqueda de palabras clave.</p>
<p>Enunciado: Como perito informático quiero poder ingresar una palabra clave y si existe en un archivo EML mostrar por pantalla la línea completa, el nombre del archivo y la cantidad de apariciones.</p>
<p>Criterios de aceptación:</p> <ul style="list-style-type: none"> <li>• Dado que estoy en la ventana principal de la aplicación, cuando hago clic en el botón "Buscar palabras clave", se muestra la línea completa, el nombre del archivo donde se encuentra y la cantidad total de apariciones de la palabra ingresada.</li> </ul>

Historia: 5.3 Búsqueda de palabras clave.
Precondiciones: <ul style="list-style-type: none"> <li>• Archivo EML abierto.</li> </ul>

*Tabla 15. Historia: 5.3 Búsqueda de palabras clave*

Historia: 6.1 Listado de correos enviados, recibidos o en copia por cabeceras [From, To, Cc, Bcc] y por cuenta.
Enunciado: Como perito informático quiero poder seleccionar archivos EML y obtener un listado con direcciones de correos en las cabeceras 'From', 'To', 'Cc' y 'Bcc, con su número de aparición.
Criterios de aceptación: <ul style="list-style-type: none"> <li>• Dado que estoy en la ventana principal de la aplicación, cuando selecciono una carpeta para su análisis y hago clic en el botón "EML", luego de haberse procesado todos los correos se muestran los listados de correos en los s 'From', 'To', 'Cc' y 'Bcc'.</li> <li>• Dado que se muestra el listado de todas las direcciones de correos involucrados en esa carpeta se muestra la cantidad de apariciones de cada dirección por cabecera.</li> </ul> Precondiciones: <ul style="list-style-type: none"> <li>• Archivo EML abierto.</li> </ul>

*Tabla 16. Historia: 6.1 Listado de correos enviados, recibidos o en copia por cabeceras [From, To, Cc, Bcc] y por cuenta*

Historia: 6.2 Listado de fechas en las que se produjeron los intercambios.
Enunciado: Como perito informático quiero poder seleccionar archivos de correo EML y obtener un listado con las fechas en las que se produjeron los envíos.
Criterios de aceptación: <ul style="list-style-type: none"> <li>• Dado que estoy en la ventana principal de la aplicación, cuando selecciono una carpeta para su análisis y hago clic en el botón "EML", luego de haberse procesado todos los correos se muestra un listado con las fechas obtenidas del campo 'Date' de todos los correos.</li> </ul> Precondiciones: <ul style="list-style-type: none"> <li>• Archivo EML abierto.</li> </ul>

*Tabla 17. Historia: 6.2 Listado de fechas en las que se produjeron los intercambios*

#### 4.2.2. Mapa de Historias de Usuario

El mapa de historias de usuarios es una representación visual que ordena las actividades del usuario en un eje horizontal en el orden que este seguiría dentro de la aplicación. En el eje vertical, las historias se ordenan por prioridad y complejidad.

Esta representación le sirve al equipo de desarrollo para seleccionar y priorizar las funcionalidades que se incorporarán en cada iteración. En este caso se diseñó un mapa con las historias del usuario perito Informático teniendo en cuenta cómo este recorrerá las opciones que la aplicación le brinda.



### Historias de Usuario Perito Informático







												
<b>Objetivos</b>	Selección de archivos			Visualización de archivos		Generación de reporte	Validación caberas	Consultas			Estadísticas	
<b>Actividades</b>	Selección de archivos TXT o EML	Selección de archivos MBOX	Selección de archivos EML por lotes	Visualización de archivos por pantalla	Visualización de cabeceras por pantalla	Generación reporte CSV	Validación de campos de autenticación	Consulta de nombre de dominio del servidor de correo (MX)	Consulta de información de RDAP	Consulta de palabras clave	Listado de correos enviados, recibidos o en copia	Listado de fechas de envío
<b>Historias</b>	Como usuario quiero poder buscar un archivo TXT o EML para poder procesarlo	Como usuario quiero poder buscar un archivo MBOX para poder procesarlo	Como usuario quiero poder buscar una carpeta para poder procesar los archivos EML	Como usuario quiero poder abrir un archivo de correo TXT o EML para visualizar sus cabeceras y cuerpo	Visualización de cabeceras EML por pantalla	Como usuario quiero poder generar un archivo CSV con cabeceras EML de los archivos analizados.	Como usuario quiero poder generar validaciones de los campos SPF, DKIM, y DMARC.	Como usuario quiero poder ingresar la dirección IP del servidor de correo y obtener el nombre de dominio	Como usuario quiero poder ingresar la dirección IP del servidor de correo y obtener los datos de dominio y registración	Como usuario quiero poder ingresar una palabra clave y si existe en archivo EML mostrar palabra, nombre de archivo y apariciones	Como usuario quiero poder seleccionar archivos EML y obtener un listado con direcciones de correos	Como usuario quiero poder seleccionar archivos EML y obtener un listado con las fechas en las que se produjeron los envíos
					Visualización de cabeceras MBOX por pantalla.	Como usuario quiero poder generar un archivo CSV con cabeceras MBOX de los archivos analizados.						

Ilustración 7. Mapa de historias de usuario

### 4.2.3. Requerimientos no funcionales

**Sistema Operativo:** inicialmente se desarrolló para funcionar bajo entornos Windows, pero puede adaptarse a otros sistemas operativos con mínimos ajustes ya que el lenguaje de programación Python no posee restricciones respecto al sistema operativo.

**Licencias:** se trabajará con el lenguaje de programación Python y diversas bibliotecas desarrolladas en este lenguaje de programación. El desarrollo de la interfaz gráfica de usuario se realizará utilizando la biblioteca PySimpleGUI<sup>9</sup>. Tanto el lenguaje de programación como las bibliotecas utilizadas poseen licencia de software libre.

**Observaciones:** para el correcto funcionamiento de la aplicación se la debe ejecutar desde la misma carpeta donde se encuentran los archivos que se quiere procesar.

**Tipos de archivos:** permite procesar archivos en formato TXT, EML y MBOX.

**Performance:** debe poder procesar 200 archivos en un tiempo razonable y sin bloquearse. Si bien no se determinó aún que se entiende por tiempo razonable, cabe aclarar que se trata de unos minutos, pero esto último no fue probado aún.

**Otras recomendaciones:** puede ser que el antivirus bloquee la ejecución o envíe un mensaje de alerta ya que este software no posee una firma reconocida. En ese caso es necesario habilitar la aplicación en su PC o bloquear el antivirus de modo que no bloquee la ejecución.

---

<sup>9</sup> PySimpleGUI: <https://www.pysimplegui.org/en/latest/>

## 5. Modelado y Diseño del Sistema

### 5.1. Diagrama de casos de uso

El diagrama de casos de uso representa las funcionalidades de un sistema desde el punto de vista de las interacciones de los actores. Estos actores pueden ser tanto un usuario como aplicaciones internas o externas. Los diagramas de casos de uso se utilizan para capturar requerimientos funcionales de un sistema [26].

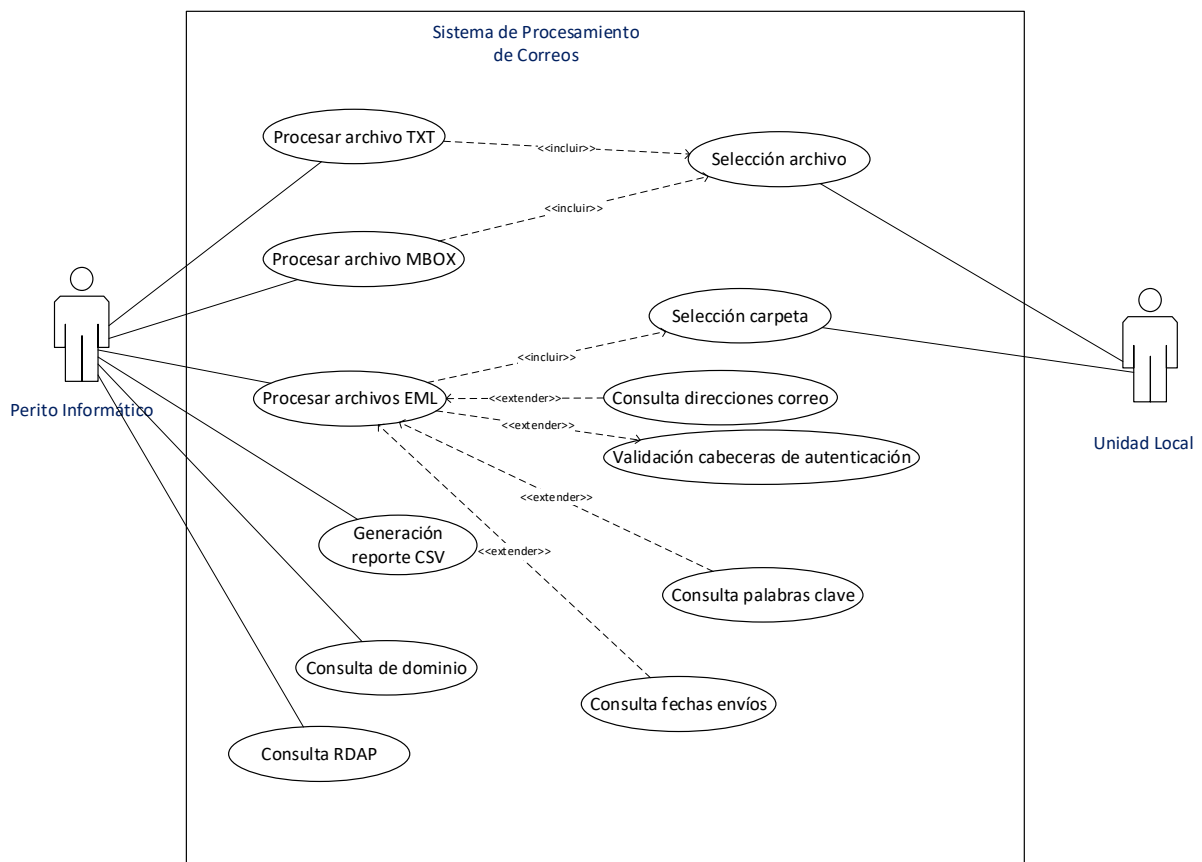


Ilustración 8. Casos de uso

### 5.2. Diagrama de actividades

El diagrama de actividades representa el flujo de actividades u operaciones del sistema. Captura el comportamiento dinámico del sistema representado por el flujo secuencial de una operación hacia otra. Se utiliza para modelar los requerimientos del negocio y proporcionan una descripción de sus funcionalidades a alto nivel [27].

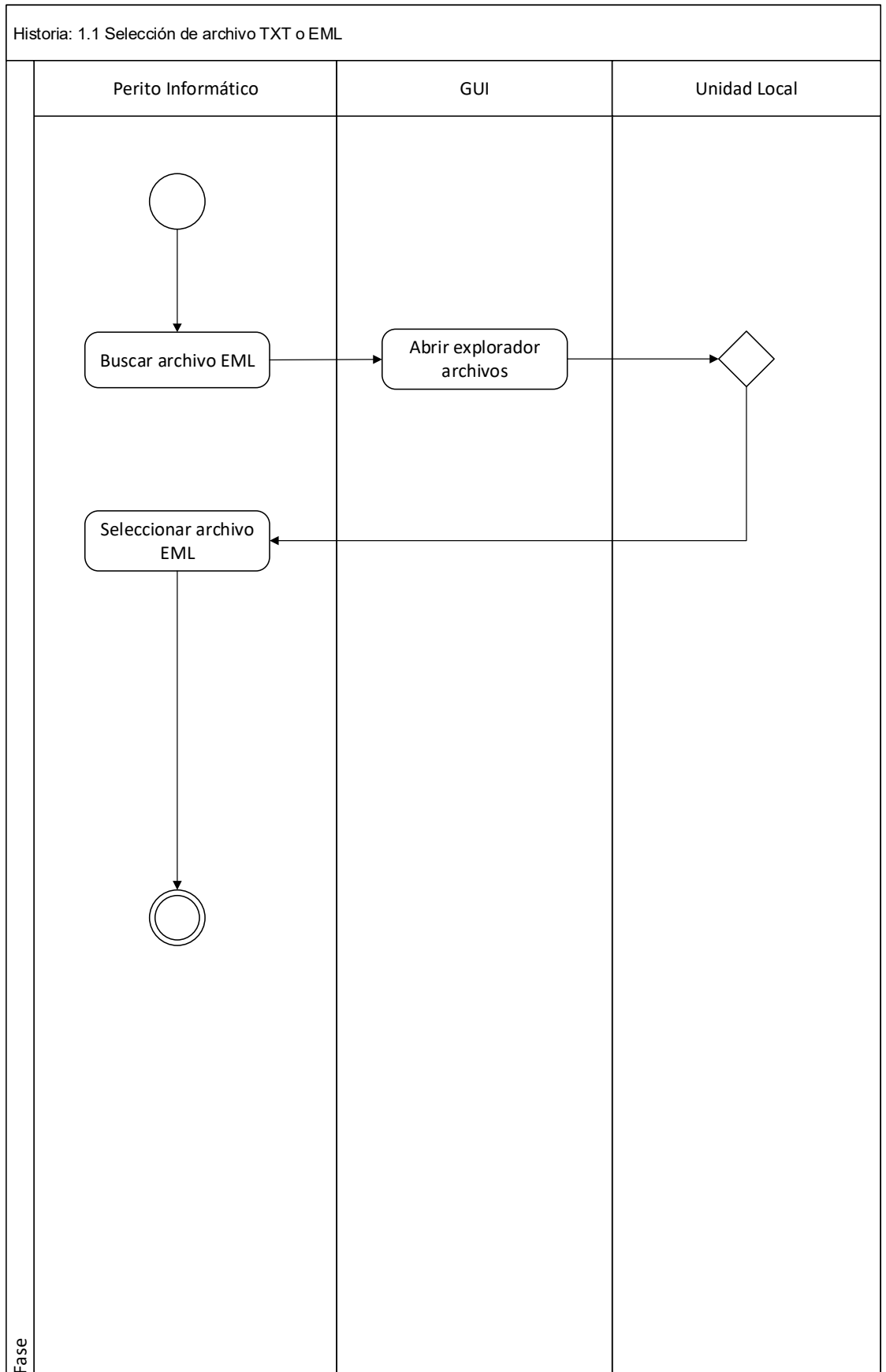


Ilustración 9. Selección de archivos EML

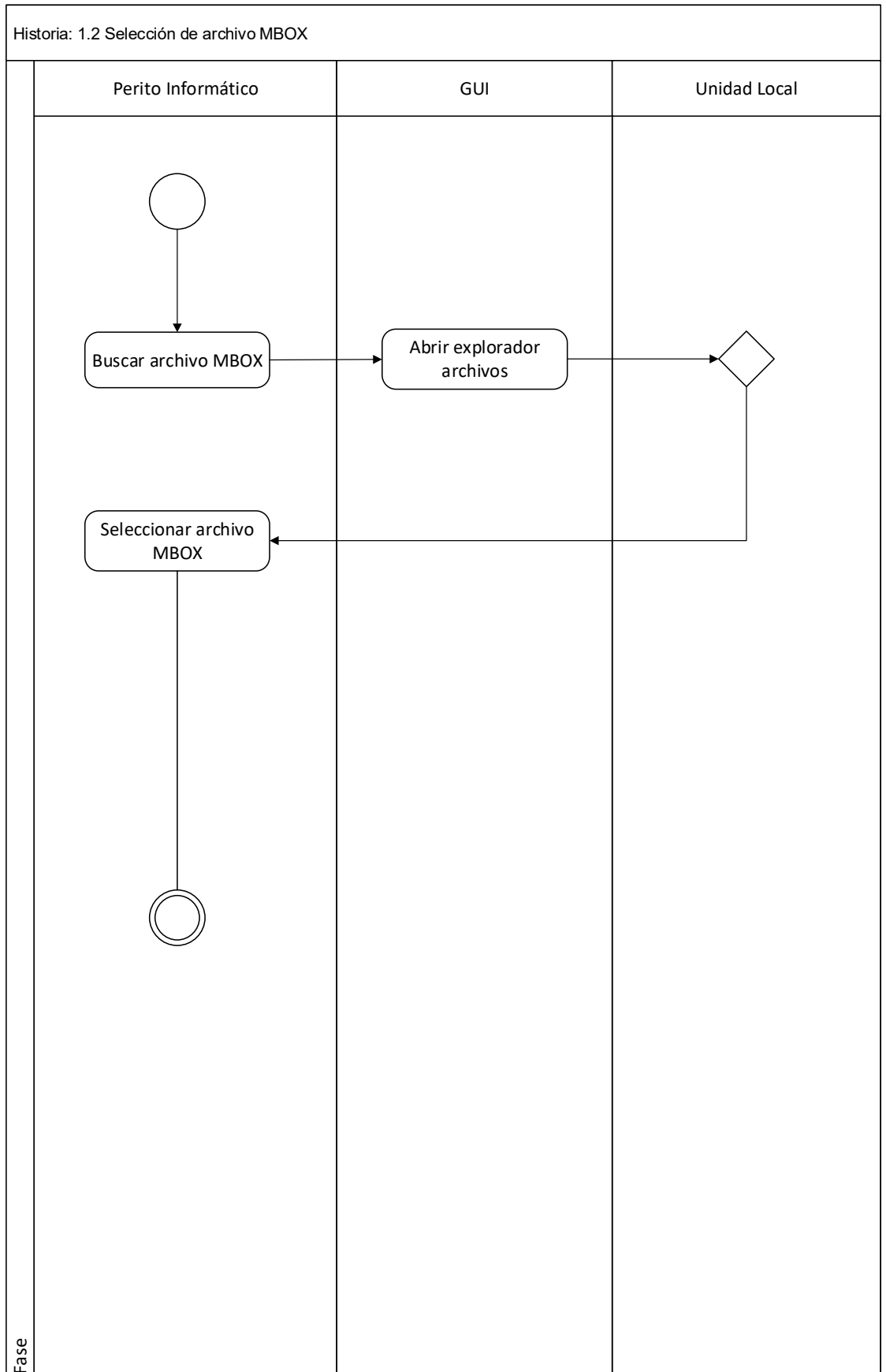


Ilustración 10. Selección de archivos MBOX

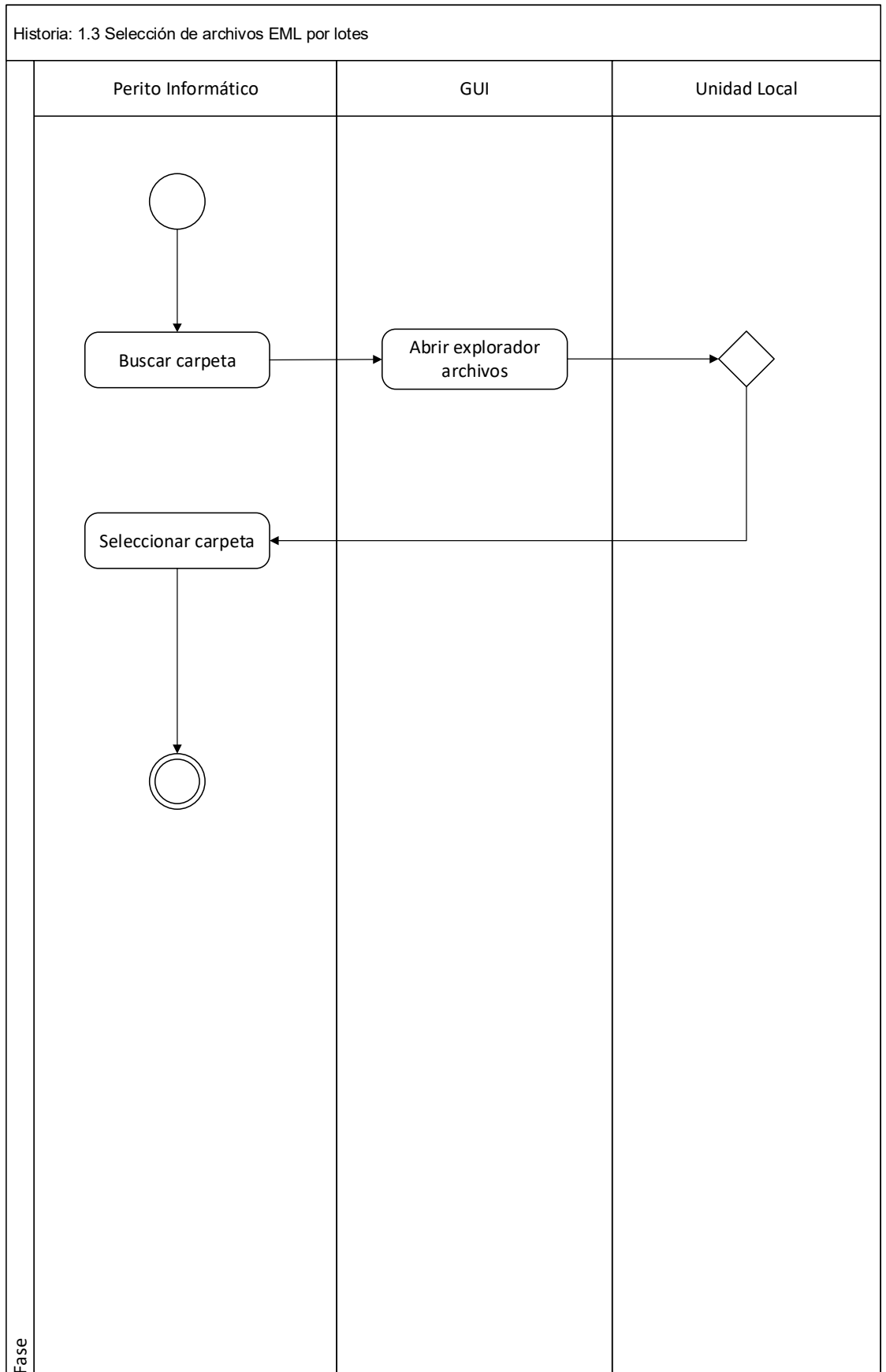


Ilustración 11. Selección de archivos EML por lotes

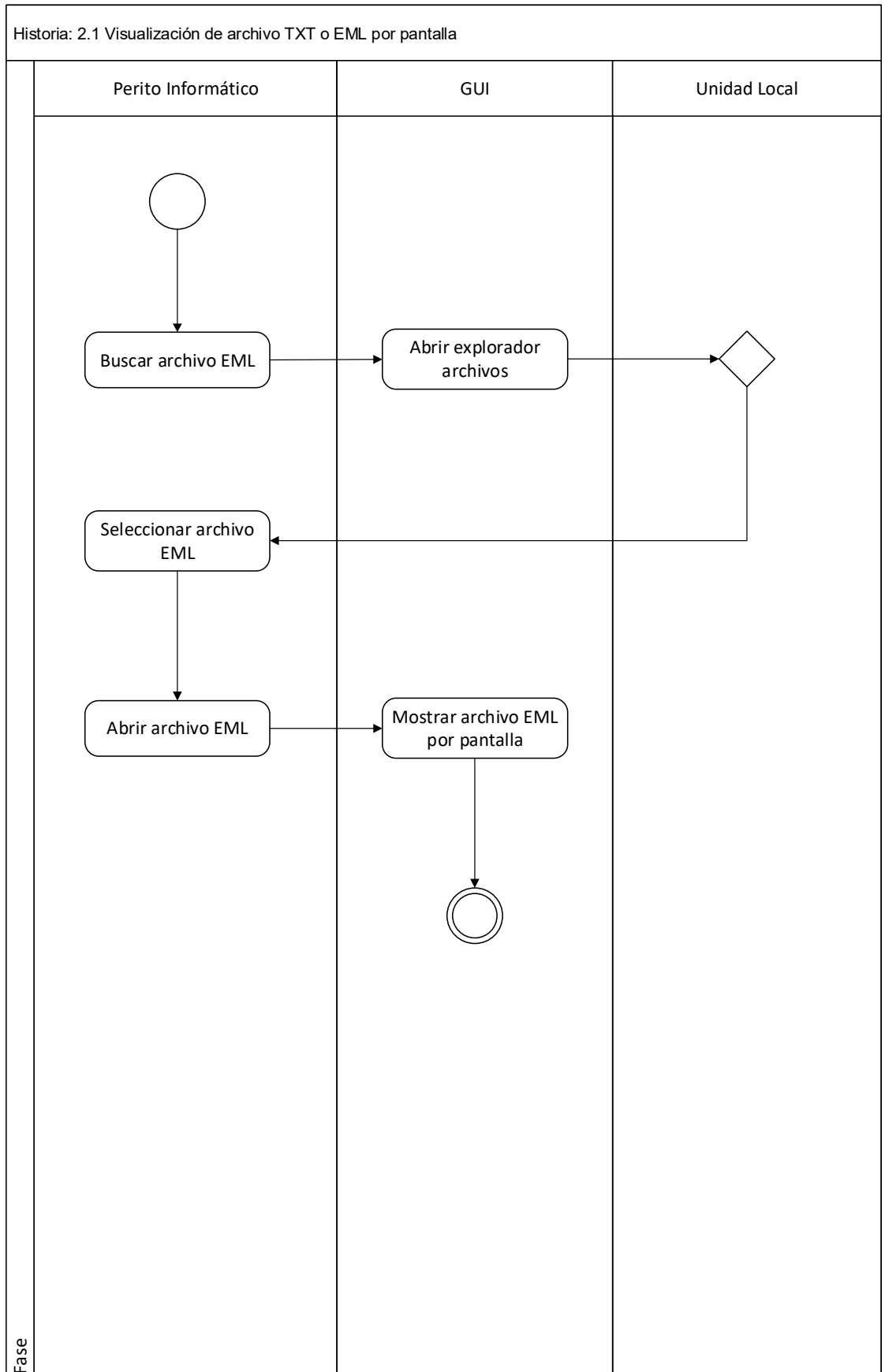


Ilustración 12. Visualización de archivos TXT o EML por pantalla

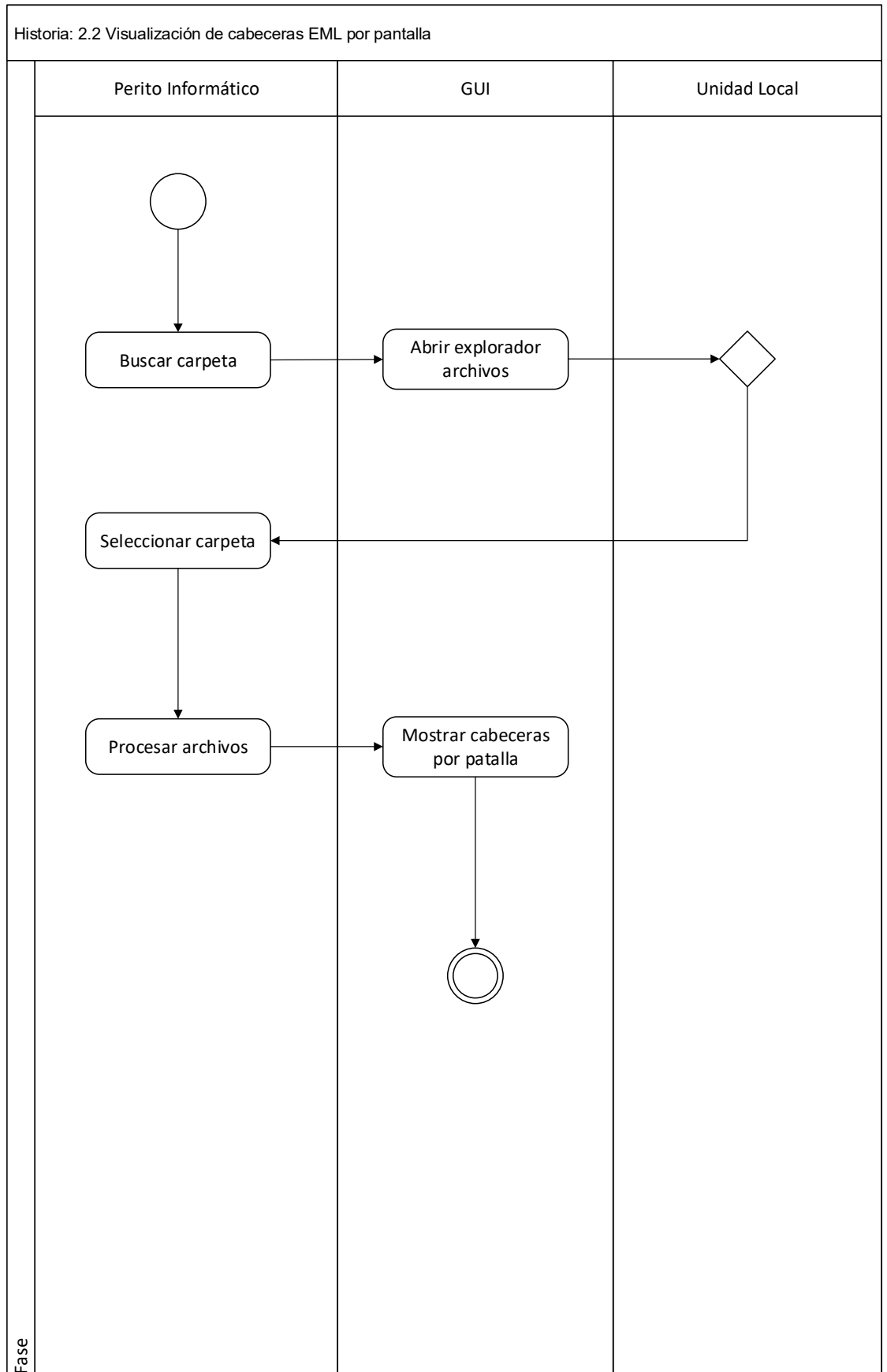


Ilustración 13. Visualización de cabeceras EML por pantalla



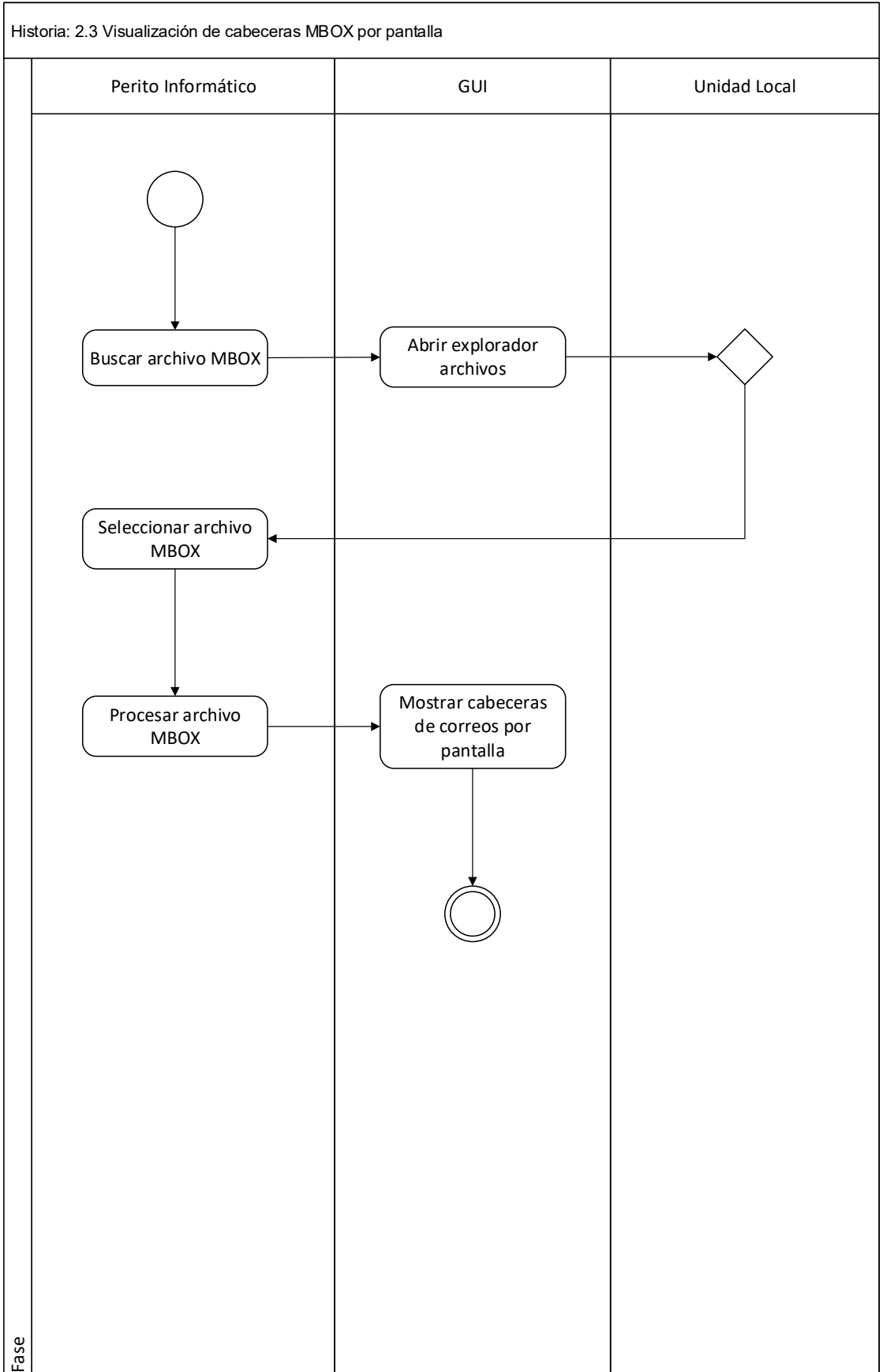


Ilustración 14. Visualización de cabeceras MBOX por pantalla

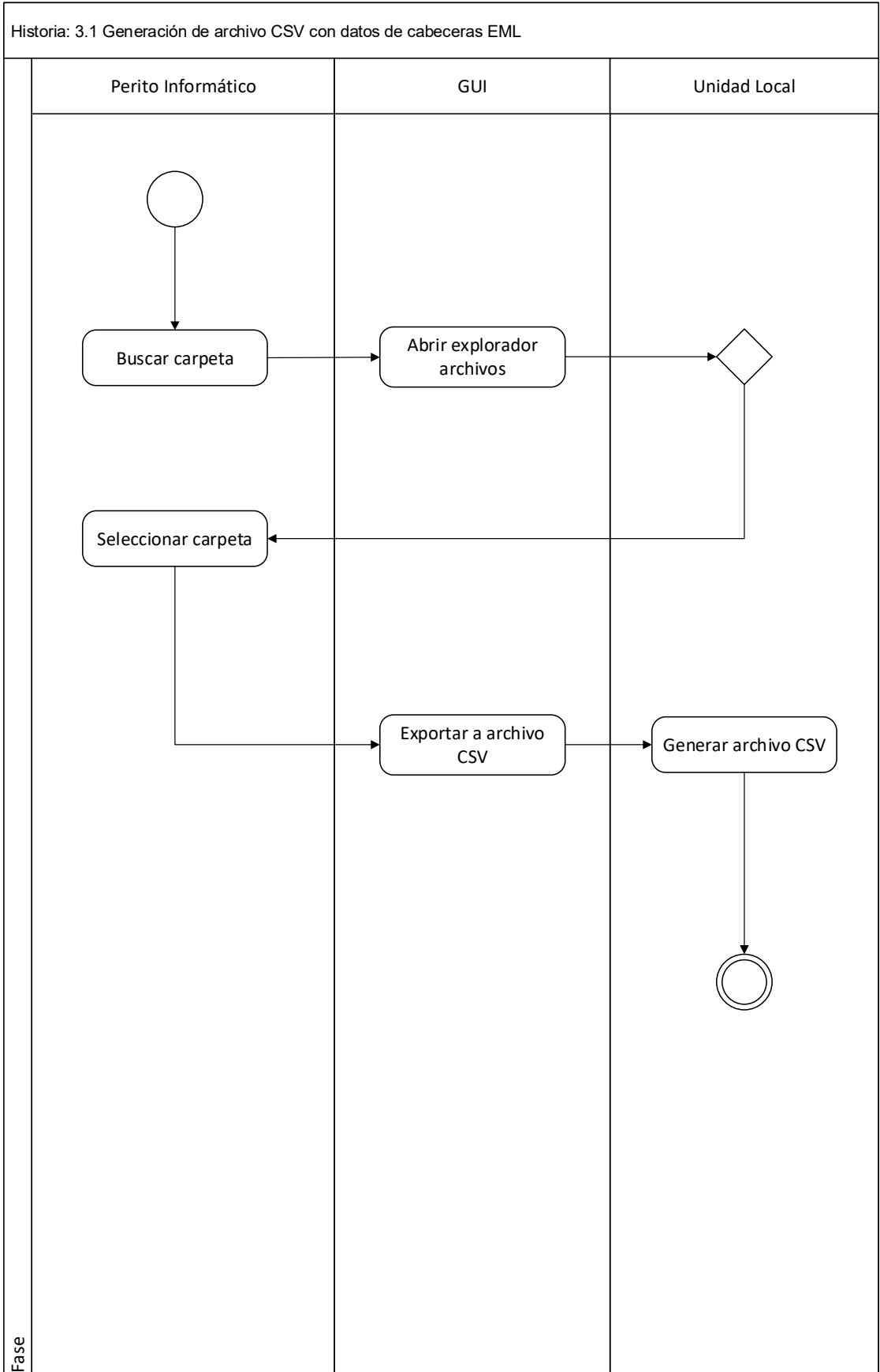


Ilustración 15. Generación de archivos CSV para EML

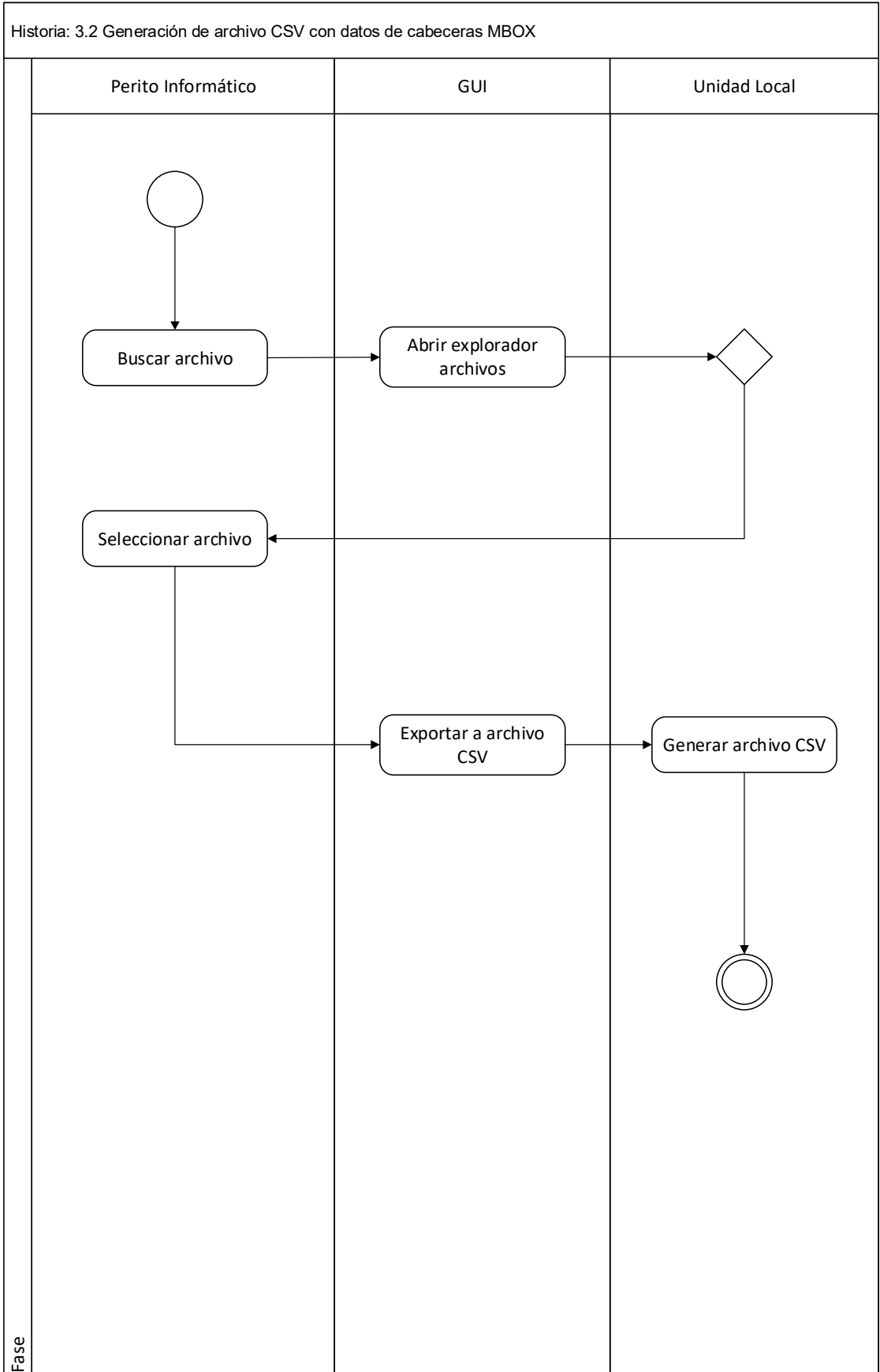


Ilustración 16. Generación de archivos CSV para MBOX

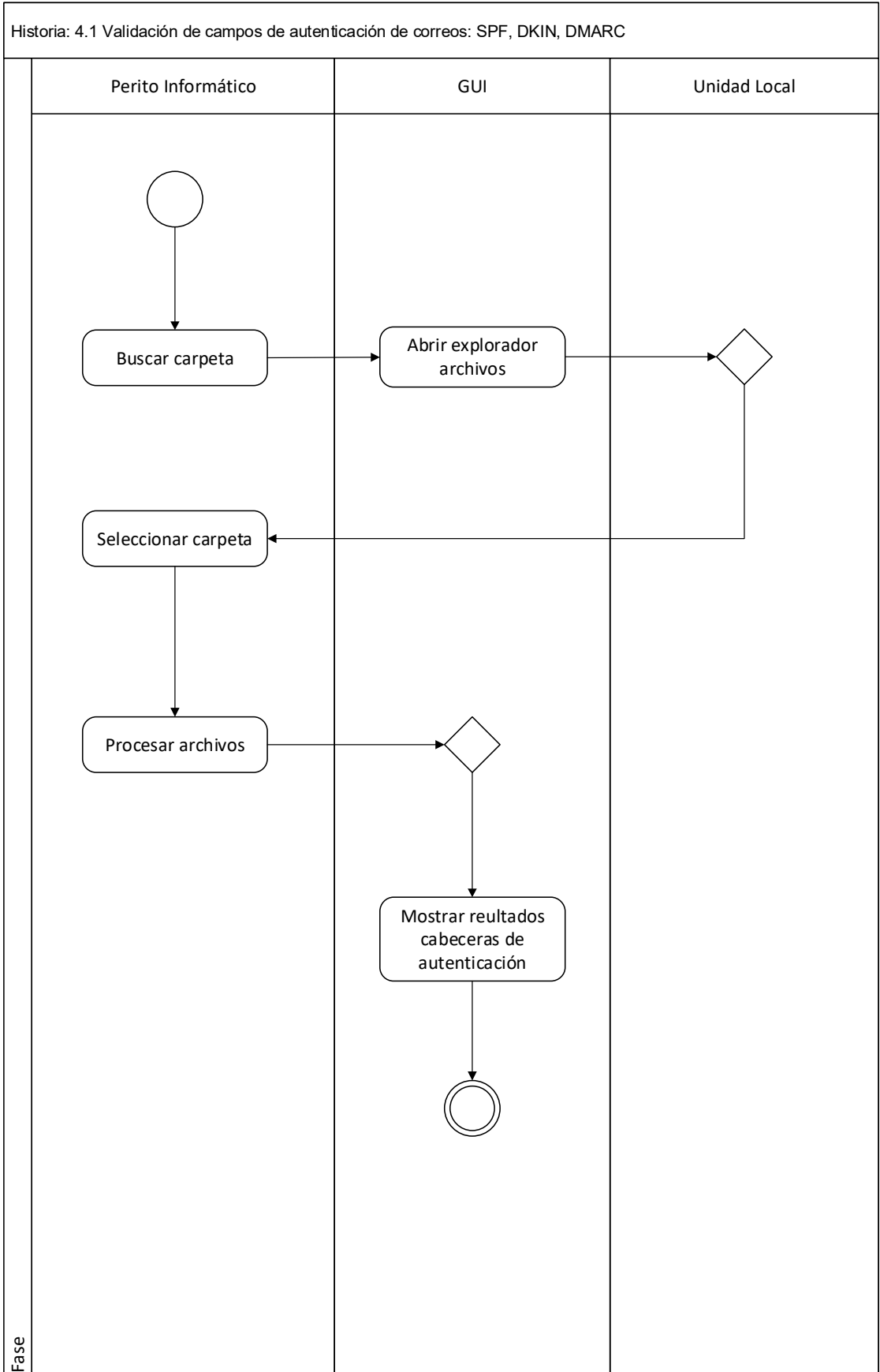


Ilustración 17. Validación de campos de autenticación

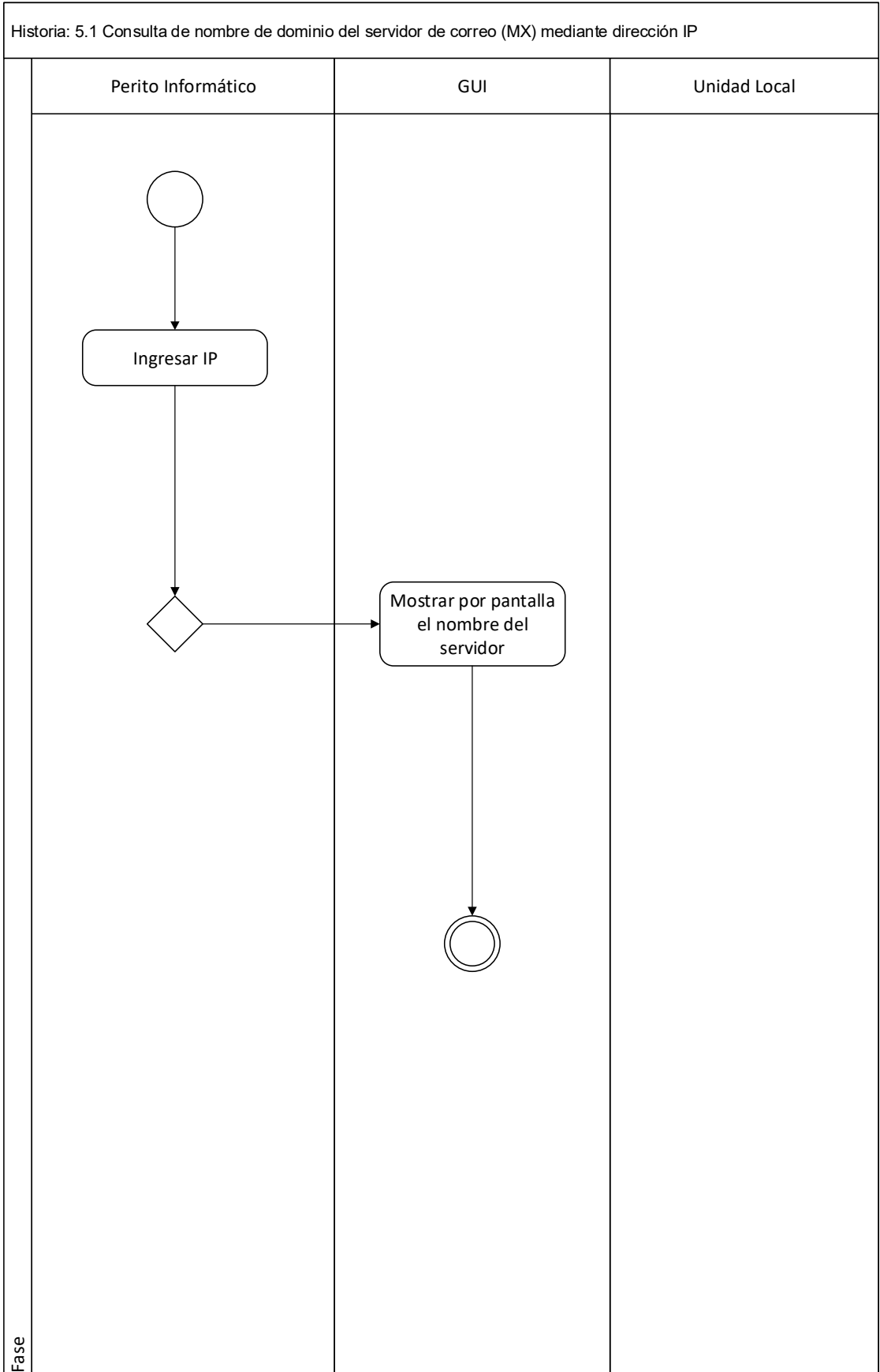


Ilustración 18. Validación de dominios MX

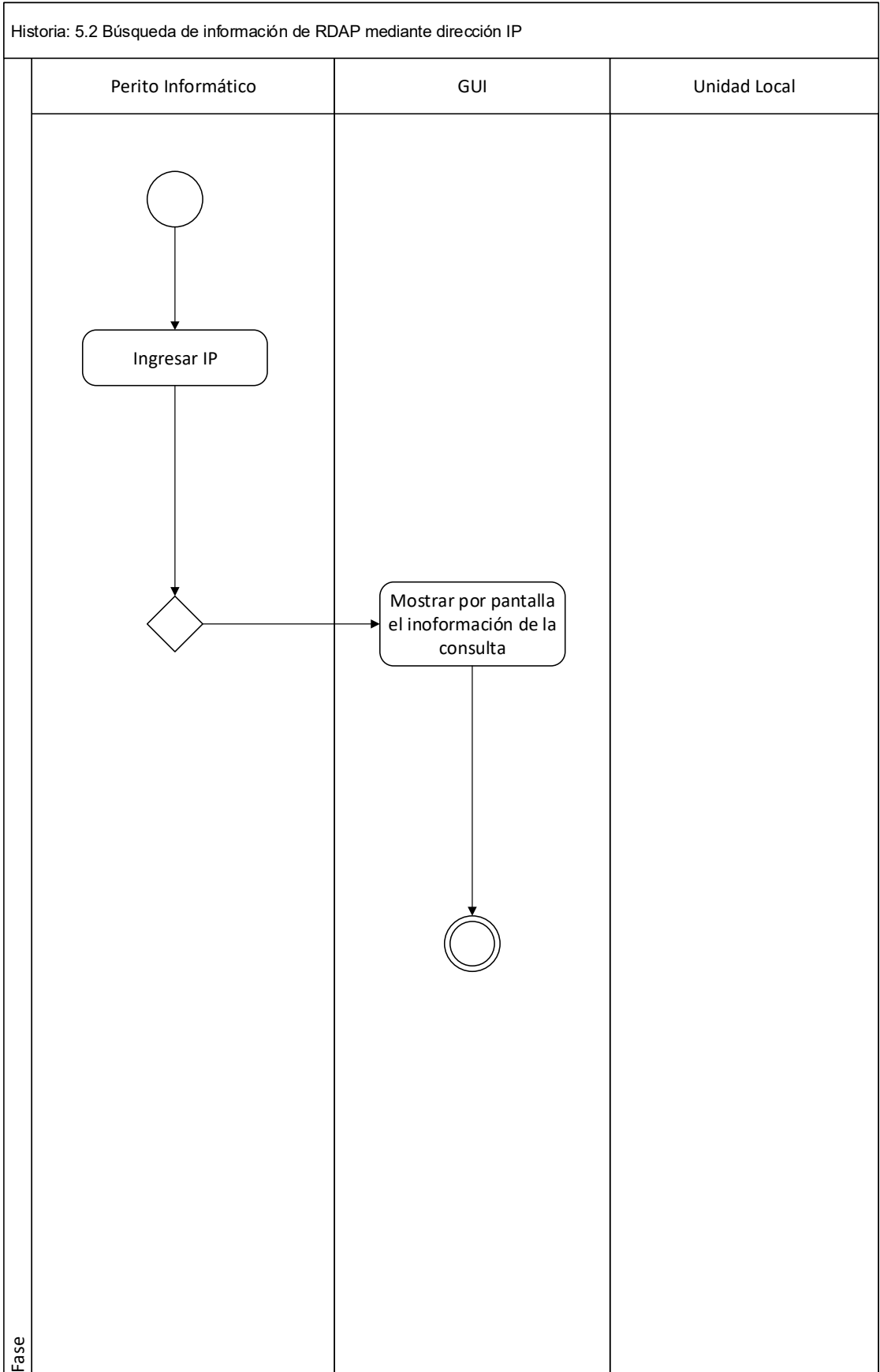


Ilustración 19. Búsqueda de información RDAP

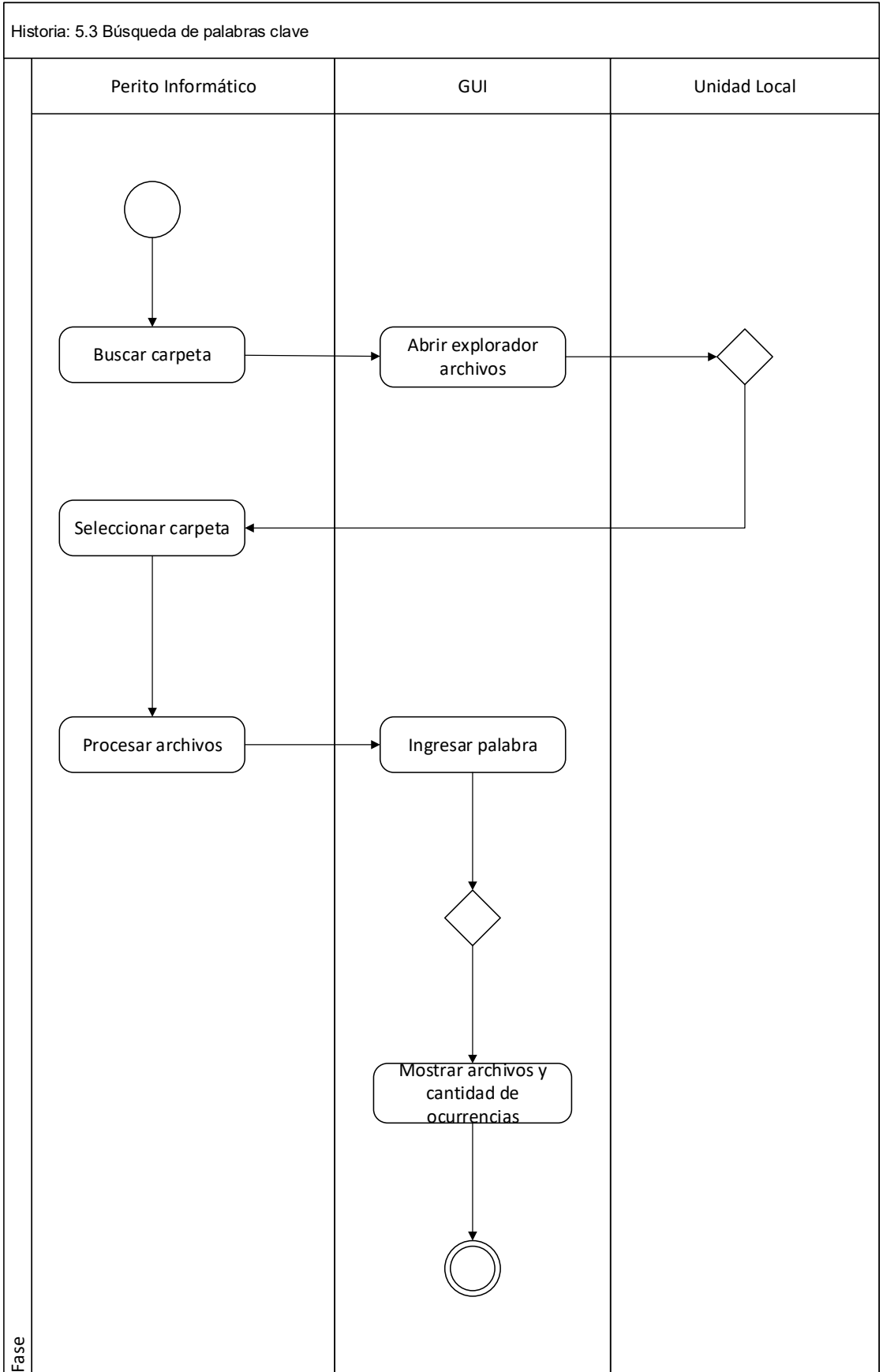


Ilustración 20. Búsqueda de palabras clave

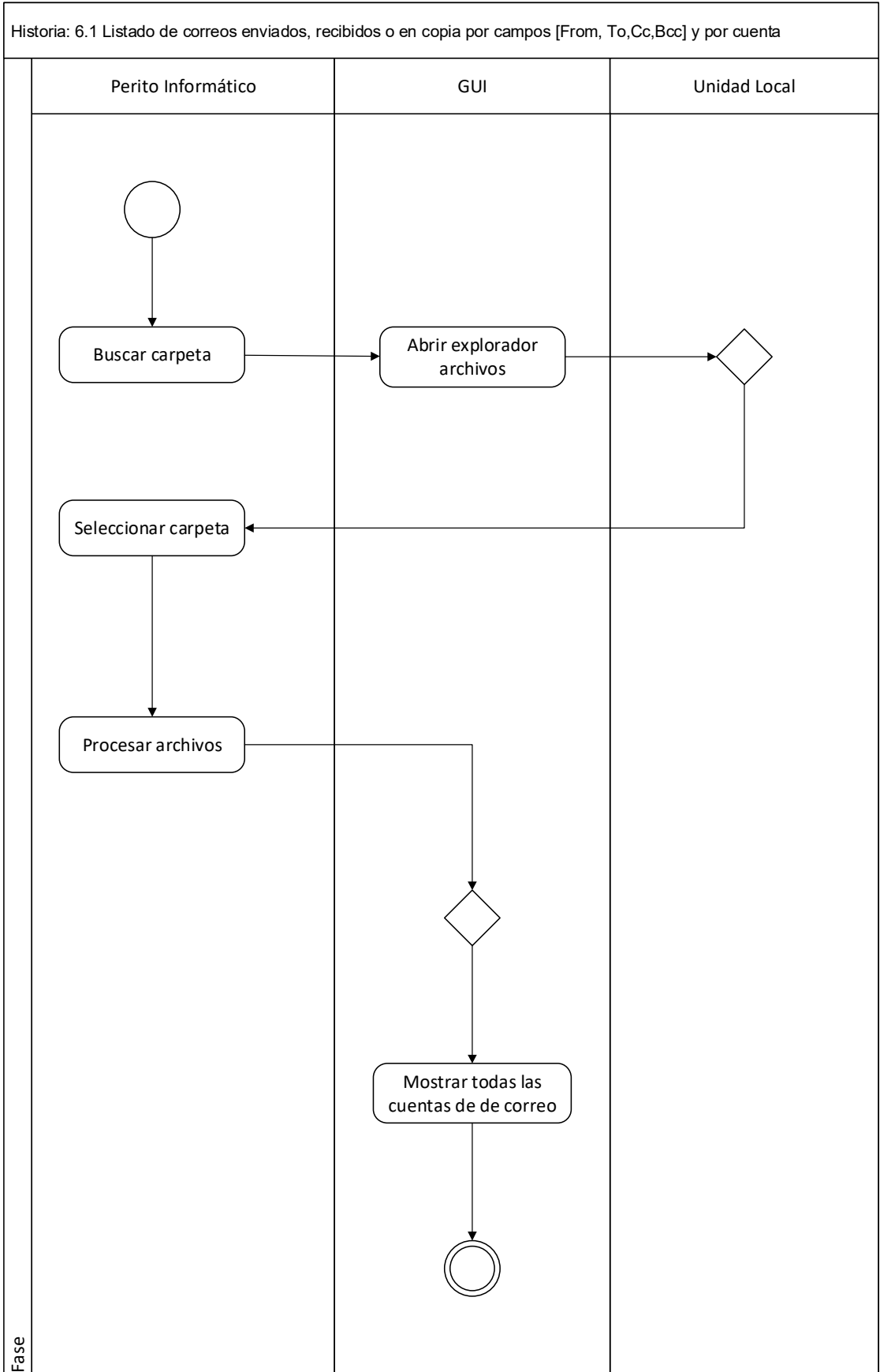


Ilustración 21. Listado de direcciones de correos



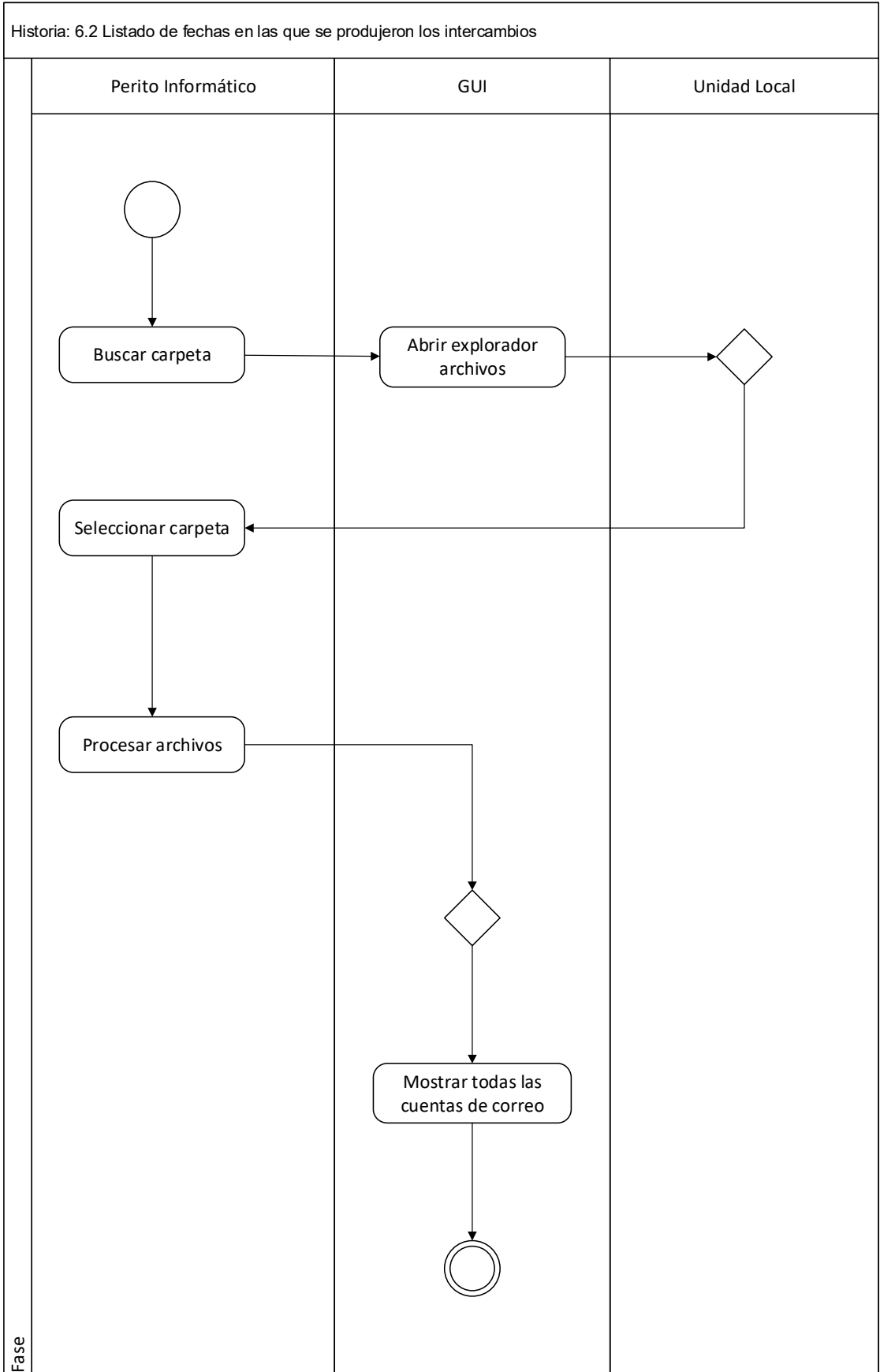


Ilustración 22. Listado de fechas

### 5.3. Diseño de Pantallas

#### Pantalla de inicio

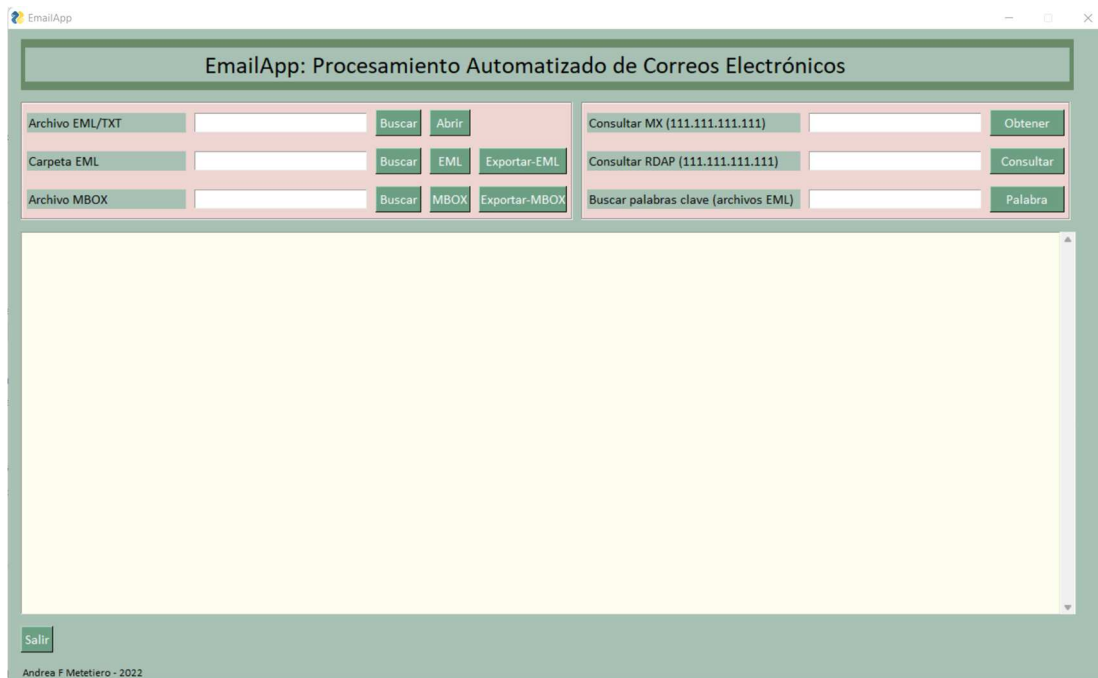


Ilustración 23. Pantalla de inicio

#### Visualización de un archivo TXT o EML por pantalla

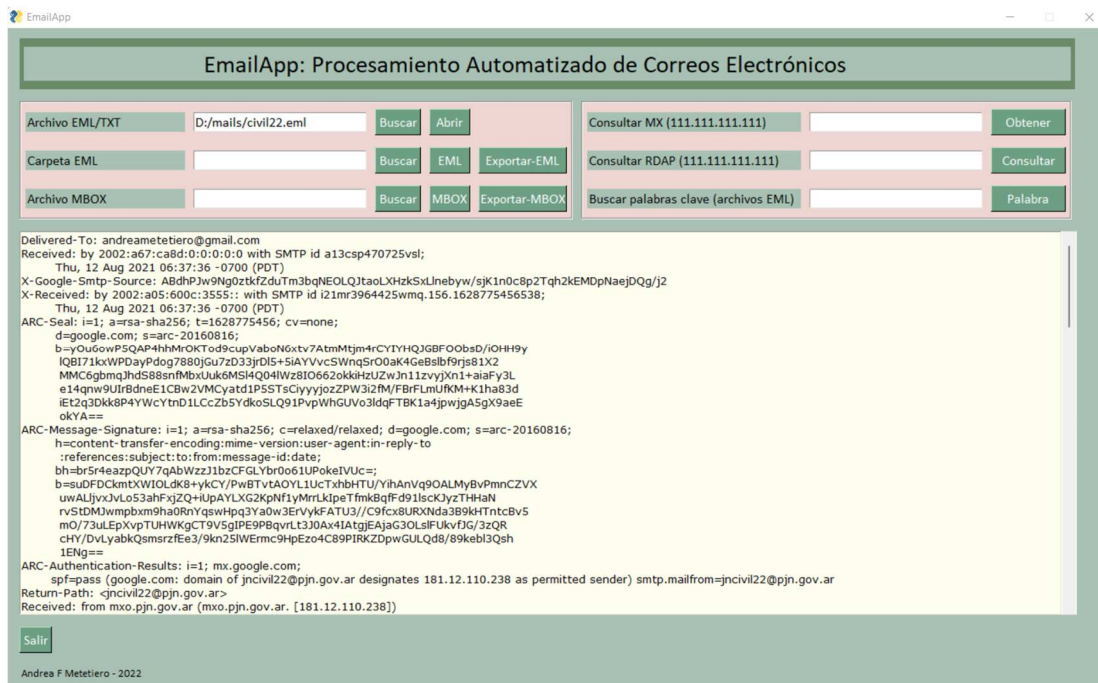


Ilustración 24. Visualización de archivo TXT

## Visualización de archivos EML por lotes

The screenshot shows the EmailApp interface with the title "EmailApp: Procesamiento Automatizado de Correos Electrónicos". It features a search and action panel with the following fields and buttons:

- Archivo EML/TXT: D:/mails/civil22.eml, with buttons "Buscar" and "Abrir".
- Carpeta EML: D:/mails, with buttons "Buscar", "EML", and "Exportar-EML".
- Archivo MBOX: (empty), with buttons "Buscar", "MBOX", and "Exportar-MBOX".
- Consultar MX (111.111.111.111): (empty), with button "Obtener".
- Consultar RDAP (111.111.111.111): (empty), with button "Consultar".
- Buscar palabras clave (archivos EML): (empty), with button "Palabra".

The main content area displays the following email metadata and body text:

Archivo 4 . Nombre: EmailTest

Delivered-To: andreametetiero@gmail.com  
Received: by 2002:a05:6102:242:0:0:0 with SMTP id a2csp1585443vsq;  
Mon, 29 Mar 2021 17:57:23 -0700 (PDT)  
X-Google-Smtp-Source: ABdHPJz8lLxfoX24iQQ1hg9HrCEMcGjfmPvXTeNHuWPP6oQh0wxdBkUuU/gwcuVrvG+NmY6dF  
X-Received: by 2002:a37:6785: with SMTP id b127mr28511110qk.184.1617065843806;  
Mon, 29 Mar 2021 17:57:23 -0700 (PDT)  
ARC-Seal: i=1; a=rsa-sha256; t=1617065843; cv=none;  
d=google.com; s=arc-20160816;  
b=Cr7LcNO67XldQ0J/FIF+DAQvpoXImwoikpWpUGm9rz2SN1xCr/JUSXG0cWbL7sK  
I4yMwGuE6o1cWV25j27FQQLdOmQ3onkSAwejymfS+zAdj1xd3Vadz965OwkmeTcd  
fdUuZpvURFIIGGgT6XtdPHFZJx8wBd770y9EDcukCAxNJE+732aAfjgSOWWSTgqz  
i80k/hikHu7q3Nges76pe7JkVW1t3mhJ6eP6327aIKlrJP/k/4HC/+fCf+ffmg6aUJ  
IbcprRC6oZ3Jtkap7GUCe3d1SxUR/URPx0nfzNz90+ya0prxY19pHjSm/eZ130SNy  
s9DQ==  
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;  
h=date:content-transfer-encoding:mime-version:subject:message-id:to  
:from;  
bh=EcxvEuDch3xdC1F1VO1a5t3WOemkQNORf3CNKYIwxA=;  
b=DSLzypQYol4U5392cAjXhRRtuQk8ktN0khVad9hZfHOPqzNH1wq/UFu7cDM96+qV  
GpNamm/Afyn3Q8xjQpwi1InzzeVjGomCz1mUj9zU7mj9z7vJY7a0570ZOY8GiseP  
GwWMDV1z4x7v6Gy/UberqY++0ewCE7ZoadctmwAkh5jA9dK37idzsrN1VauGq5/6PE  
X2e4uFl0D5CTp1d4K/RvW/qAffQjBAeL2YMpnNNGS3MfyG7ULbJQdbiSglwVrTU  
TTHN1V50mrjXTWkCGzF6pVY1xCXgSLFUnOvYGe2A0dhqTATCS7fuv8lQV72dB3/  
RFJQ==

Salir

Andrea F Metetiero - 2022

Ilustración 25. Visualización de archivos EML por lotes

## Visualización de archivos MBOX

The screenshot shows the EmailApp interface with the title "EmailApp: Procesamiento Automatizado de Correos Electrónicos". It features a search and action panel with the following fields and buttons:

- Archivo EML/TXT: D:/mails/civil22.eml, with buttons "Buscar" and "Abrir".
- Carpeta EML: D:/mails, with buttons "Buscar", "EML", and "Exportar-EML".
- Archivo MBOX: D:/mails/CVs.mbox, with buttons "Buscar", "MBOX", and "Exportar-MBOX".
- Consultar MX (111.111.111.111): (empty), with button "Obtener".
- Consultar RDAP (111.111.111.111): (empty), with button "Consultar".
- Buscar palabras clave (archivos EML): (empty), with button "Palabra".

The main content area displays the following email metadata and body text:

X-GM-THRID: 1520929165623680464  
X-Gmail-Labels: Archived,Important,Opened,Category Personal,CVs  
Delivered-To: andreametetiero@gmail.com  
Received: by 10.202.108.208 with SMTP id h199csp938721oic;  
Fri, 18 Dec 2015 12:38:02 -0800 (PST)  
X-Received: by 10.55.27.146 with SMTP id m18mr7749927qkh.84.1450471082465;  
Fri, 18 Dec 2015 12:38:02 -0800 (PST)  
Return-Path: <fede\_martignoni@hotmail.com>  
Received: from BLU004-OMC4S29.hotmail.com (blu004-omc4s29.hotmail.com. [65.55.111.168])  
by mx.google.com with ESMTPS id 97si6247102qj.96.2015.12.18.12.38.02  
for <andreametetiero@gmail.com>  
(version=TLS1\_2 cipher=ECDHE-RSA-AES128-SHA bits=128/128);  
Fri, 18 Dec 2015 12:38:02 -0800 (PST)  
Received-SPF: pass (google.com: domain of fede\_martignoni@hotmail.com designates 65.55.111.168 as permitted sender) client-ip=65.55.111.168;  
Authentication-Results: mx.google.com:  
spf=pass (google.com: domain of fede\_martignoni@hotmail.com designates 65.55.111.168 as permitted sender) smtp.mailfrom=fede\_martignoni@hotmail.com;  
dmarc=pass (p=NONE dis=NONE) header.from=hotmail.com  
Received: from BLU174-W33 ([65.55.111.137]) by BLU004-OMC4S29.hotmail.com over TLS secured channel with Microsoft SMTPSVC(7.5.7601.23008);  
Fri, 18 Dec 2015 12:38:02 -0800  
X-TMNI: [kpxBxv/V205QeavFIVInwkH+Jma/TxY0xjID9xa29SA=]  
X-Originating-Email: [fede\_martignoni@hotmail.com]  
Message-ID: <BLU174-W3317282C39E0365D98F04990E10@phx.gbl>  
Return-Path: fede\_martignoni@hotmail.com  
Content-Type: multipart/mixed;  
boundary="\_52a8f7b3-ac17-4427-abb5-2053b12597f0\_"  
From: federico martignoni <fede\_martignoni@hotmail.com>

Salir

Andrea F Metetiero - 2022

Ilustración 26. Visualización de archivos MBOX

## Creación de archivos CSV

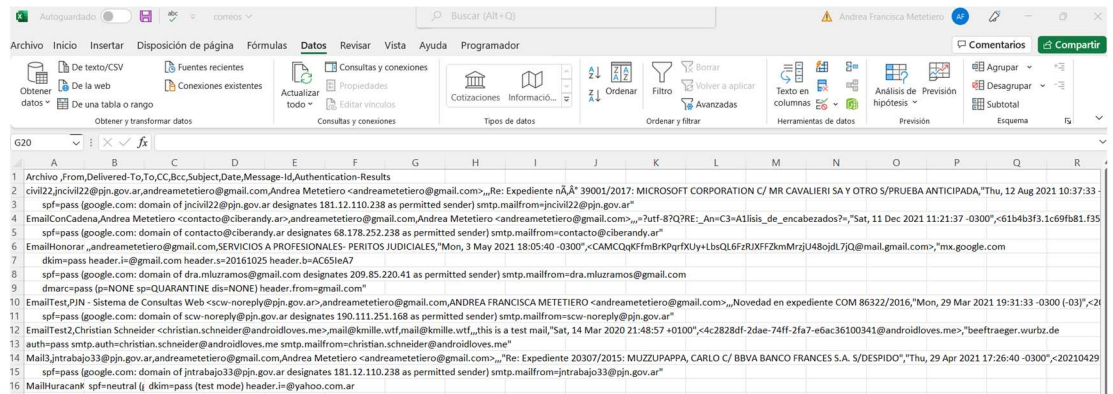


Ilustración 27. Archivo CSV

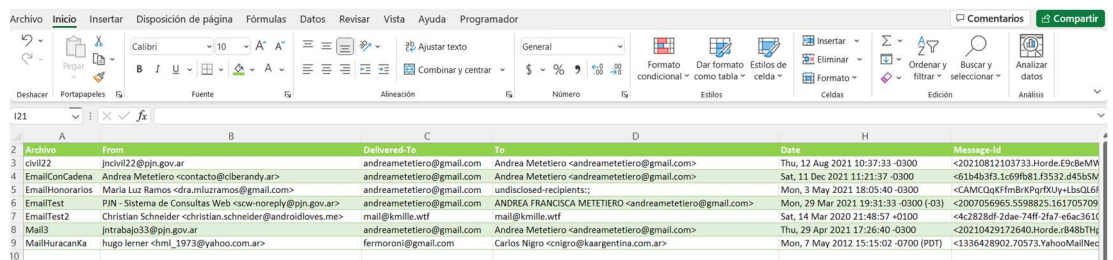


Ilustración 28. Archivo Excel

## Visualización de campos de autenticación

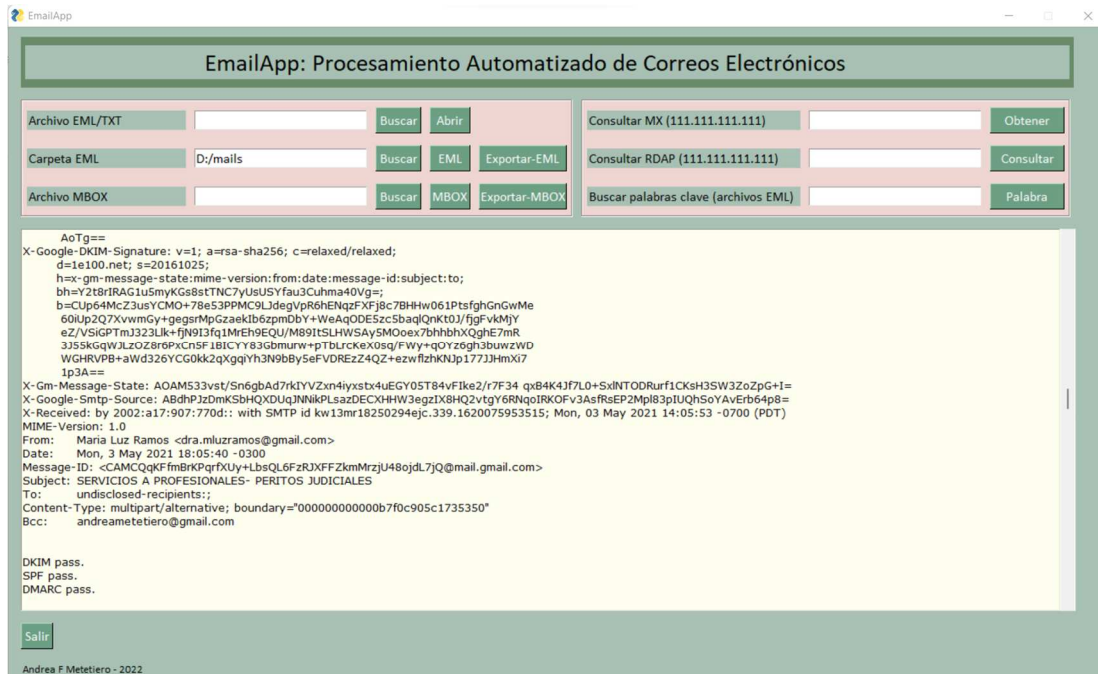


Ilustración 29. Visualización de campos de autenticación

## Extracción de cuentas de correos involucradas

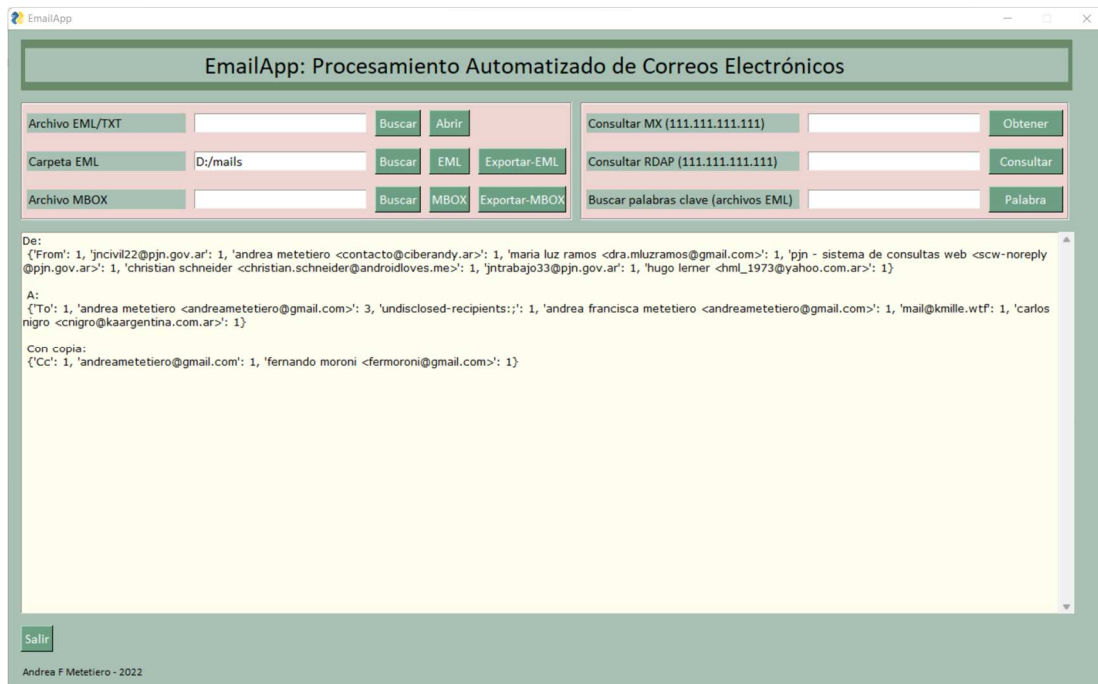


Ilustración 30. Informe de cuentas de correos involucradas

## Extracción de fechas

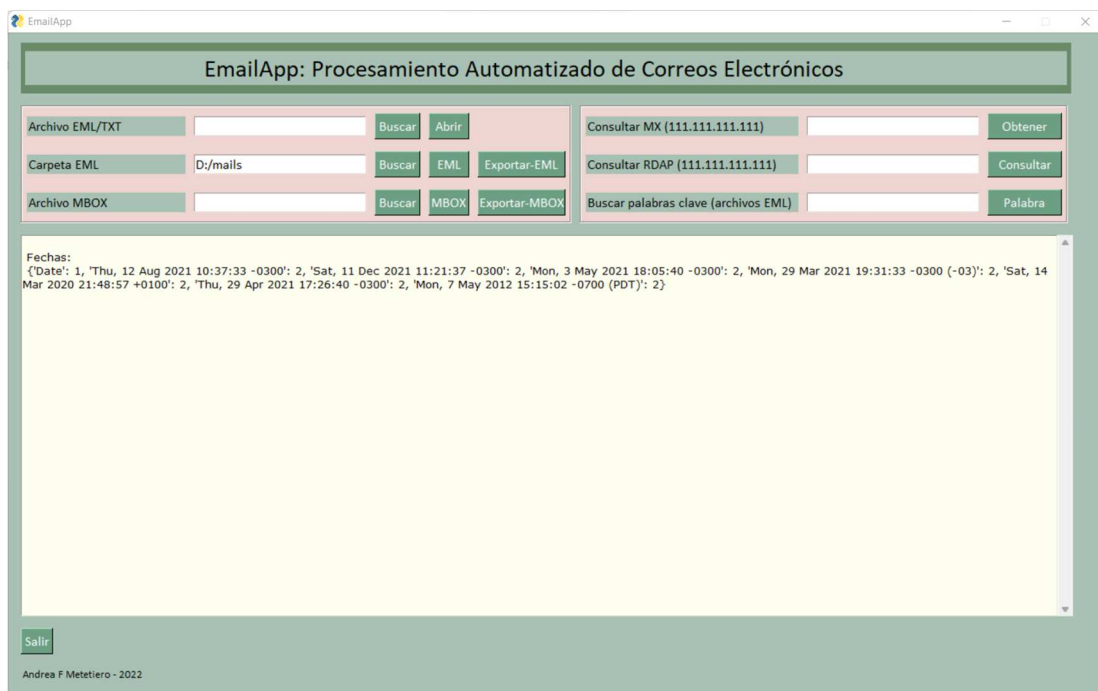


Ilustración 31. Informe de fechas de envío

## Consulta de palabras clave

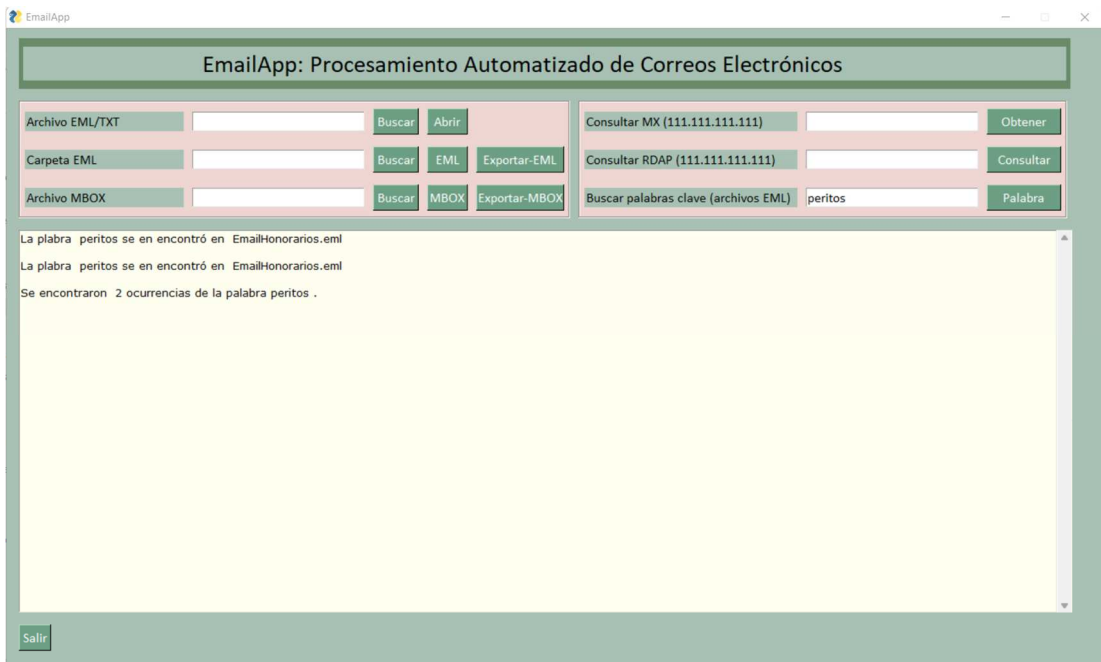


Ilustración 32. Búsqueda de palabras clave

## Consulta de nombre de dominio del servidor de correos

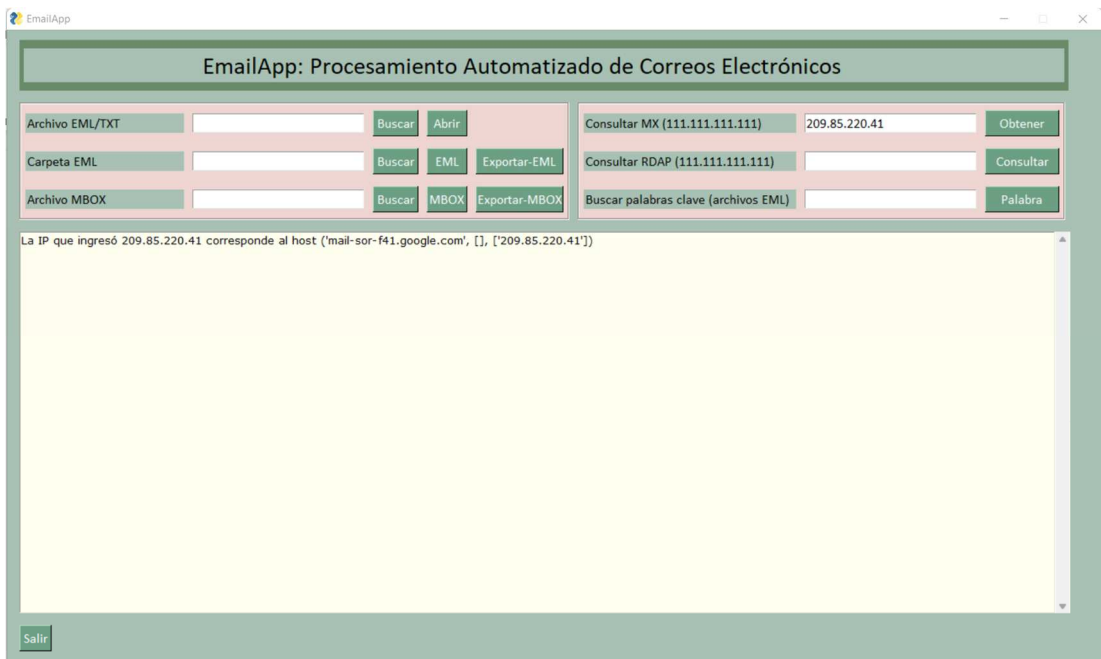


Ilustración 33. Consulta nombres de dominio

## Consulta de datos de dominio y registración

The screenshot shows the EmailApp interface with the title "EmailApp: Procesamiento Automatizado de Correos Electrónicos". The interface includes several search and action buttons:

- Archivo EML/TXT: Buscar, Abrir
- Carpeta EML: Buscar, EML, Exportar-EML
- Archivo MBOX: Buscar, MBOX, Exportar-MBOX
- Consultar MX (111.111.111.111): Obtener
- Consultar RDAP (111.111.111.111): 209.85.220.41, Consultar
- Buscar palabras clave (archivos EML): Palabra

The main content area displays a JSON object representing domain and registration data:

```
{'asn': '15169',
'asn_cidr': '209.85.128.0/17',
'asn_country_code': 'US',
'asn_date': '2006-01-13',
'asn_description': 'GOOGLE, US',
'asn_registry': 'arin',
'entities': ['GOGL'],
'network': {'cidr': '209.85.128.0/17',
'country': 'None',
'end_address': '209.85.255.255',
'events': [{'action': 'last changed',
'actor': 'None',
'timestamp': '2012-02-24T09:44:34-05:00'},
{'action': 'registration',
'actor': 'None',
'timestamp': '2006-01-13T13:42:45-05:00'}]},
'handle': 'NET-209-85-128-0-1',
'ip_version': 'v4',
'links': ['https://rdap.arin.net/registry/ip/209.85.128.0',
'https://whois.arin.net/rest/net/NET-209-85-128-0-1'],
'name': 'GOOGLE',
'notices': [{'description': 'By using the ARIN RDAP/Whois '
'service, you are agreeing to the '
'RDAP/Whois Terms of Use'},
{'description': 'If you see inaccuracies in the '
'service, you are agreeing to the '
'RDAP/Whois Terms of Use'}]},
'links': ['https://www.arin.net/resources/registry/whois/tou/'],
'title': 'Terms of Service'},
'description': 'If you see inaccuracies in the '
'service, you are agreeing to the '
'RDAP/Whois Terms of Use'}
```

At the bottom left, there is a "Salir" button and the text "Andrea F Metetiero - 2022".

Ilustración 34. Consulta dominio y registración

## 6. Consideraciones Finales

El presente trabajo expuso los posibles interrogantes que se les presentan a los peritos informáticos a la hora de realizar sus actuaciones periciales, considerando que nuestro Código Procesal Civil y Comercial de la Nación solamente describe los requisitos que deben cumplir los profesionales para ejercer como peritos, pero nada dice sobre cómo se debe llevar a cabo una pericia y menos aun cuando se trata de una pericia informática. Este hecho es comprensible ya que se espera que los profesionales estén capacitados tanto por sus conocimientos como por su experiencia para realizar las tareas que le sean encomendadas.

La Informática Forense se encarga del análisis de la prueba indiciaria informática, la que se presenta siempre en algún formato digital y suele requerir de la utilización de algún software especializado. El objetivo principal de este trabajo era crear una aplicación que automatizase el peritaje de correos electrónicos que sea económicamente accesible y que sirviese de soporte para los peritos informáticos forenses en la República Argentina. Este objetivo surgió luego de analizar una cantidad de expedientes judiciales en el fuero civil que solicitaban pericias informáticas y la mayoría de ellas implicaban el análisis de correos electrónicos que fueran aportados por alguna de las partes intervinientes en el litigio.

Se presentaron como ejemplo puntos periciales correspondientes a cinco expedientes. De allí se relevó que los puntos periciales solicitados se repetían con frecuencia y podían resumirse en no más de una docena. Para dar mayor sustento a la elicitación de requerimientos se realizó una encuesta entre peritos informáticos del COPITEC y de la Maestría en Seguridad Informática de la UBA. Los resultados de la encuesta coincidieron con lo relevado de los expedientes.

Para poder desarrollar una aplicación que pueda dar respuesta a los puntos periciales más frecuentes, se estudió el formato de los mensajes de internet, compuestos por encabezado y cuerpo. Los encabezados que contienen campos que representan los metadatos de un correo electrónico fueron estudiados en detalle. Asimismo, se estudiaron los campos de validación



SPF, DKIM y DMARC, por ser indispensables para responder sobre la autenticidad de un correo electrónico. Además, se analizaron los tipos de archivo que se pueden presentar de acuerdo con la aplicación de correo que se utilice, ya que cada tipo requiere un tipo de procesamiento distinto. Como último paso de la elicitación de requerimientos se hizo un análisis comparativo de herramientas existentes en el mercado.

Para el ciclo de vida de desarrollo de software se eligió la metodología de desarrollo incremental. Por ser una metodología ágil, la especificación de requerimientos funcionales fue detallada mediante historias de usuario. Luego se representaron las interacciones del usuario con el sistema mediante un diagrama de casos de uso. El flujo de operaciones dentro del sistema se representó mediante diagramas de actividades.

Una vez completa la etapa de especificación de requerimientos y detallada mediante historias de usuarios y diagramas se procedió a comenzar con el desarrollo del programa utilizando el lenguaje Python, que fue elegido entre otras cosas porque cuenta con numerosas bibliotecas que facilitan el procesamiento de mensajes de internet. Además, se necesitaba resolver el diseño de una GUI y para esto Python cuenta con PySimpleGUI, un framework que si bien presenta algunas limitaciones, como su nombre lo indica es de fácil implementación.

Respecto con los objetivos que se habían planteado, la aplicación es capaz de procesar archivos de correo en formatos TXT, EML y MBOX de manera automatizada, siempre y cuando estos archivos se hayan descargado del servidor. Este procesamiento consiste en el recorrido de los campos de los encabezados que son tratados como un diccionario campo-clave y se imprimen por pantalla. Los resultados de procesamiento responden a preguntas como cuáles fueron los remitentes o destinatarios, fechas en que fueron enviados los correos, cuenta de correo del emisor o del receptor, asunto, direcciones IP, etc.

Además de responder a los puntos periciales mencionados, también permite buscar palabras clave, obtener un listado de las direcciones de correo y fechas de envío entre todos los correos procesados en un mismo lote y obtener información acerca de las direcciones de IP como los datos de

registro del dominio. En cuanto a la validación de los campos de autenticación, la aplicación puede responder con 'PASS' o 'FAIL', obteniendo estos resultados de los propios campos de autenticación SPF, DKIM y DMARC.

También se había planteado la generación automatizada de reportes. Esto se cumple ya que la aplicación puede exportar una serie de encabezados predefinidos en el código fuente a un archivo CSV, que se puede abrir con cualquier herramienta compatible o con editores de archivos de texto. Otras funcionalidades que quedaron fuera de esta versión pero que podrían agregarse son la lectura de archivos adjuntos y la posibilidad de generar hashes de cada archivo o carpeta.

Respecto a los requerimientos no funcionales, se cumplió con el planteo de desarrollar una herramienta de escritorio con interfaz gráfica de usuario que funcione en entornos Windows. El principal interrogante en este punto es sobre el rendimiento de la aplicación, se espera que sea capaz de procesar hasta doscientos archivos en un solo lote en pocos minutos, pero esto último no fue puesto a prueba.

Hasta el momento la aplicación fue utilizada en la investigación de algunos pocos casos reales y resultó de gran utilidad, ya que fue capaz de procesar los archivos de correo de manera rápida y generó el reporte que fue agregado al informe pericial con los detalles de los correos analizados.

Como conclusión se puede decir que la aplicación cumplió con los objetivos planteados al principio de este trabajo y que sirvió como soporte al perito informático en las causas en las que fue utilizada. Si se pensara en ella como un producto comercial, habría que utilizar un framework más potente ya que PySimpleGUI presenta algunas limitaciones. Además, podría incorporarse una base de datos para que los peritos puedan guardar los resultados de los correos analizados, que por el momento solo persisten en memoria o en un archivo en caso de que sea generado. Por último se podría analizar la incorporación de la capacidad de incorporar los tipos de archivo que quedaron fuera de esta versión.

## 7. Bibliografía

### 8.

- [1] «Infoleg, Código Procesal Civil y Comercial de la Nación - Art 457,»  
[En línea]. Available:  
<http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16547/texact.htm#8>. [Último acceso: 18 11 2022].
- [2] «Infoleg, Código Procesal Civil y Comercial de la Nación - Art 459,»  
[En línea]. Available:  
<http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16547/texact.htm#8>. [Último acceso: 18 11 2022].
- [3] «Infoleg - Código Procesal Civil y Comercial de la Nación - Art 464,»  
[En línea]. Available:  
<http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16547/texact.htm#8>. [Último acceso: 18 11 2022].
- [4] Guzmán, C., Manual de criminalística, Ciudad de Buenos Aires: Ediciones La Rocca, 2000, pp. 37-37.
- [5] Locard, E., Manuel de Technique Policière, Paris: Payot, 1923.
- [6] Darahuge, M.E., Arellano González, L.E., Manual de Informática Forense, Ciudad de Buenos Aires: Errepar S.A., 2011, p. 8.
- [7] Collier, P. A., & Spaul, B. J., «A forensic methodology for countering computer crime.,» 1992. [En línea]. Available: <https://link.springer.com/article/10.1007%2FBF00150234>. [Último acceso: 24 02 2021].
- [8] Cano, J. J., Computación Forense: Descubrimiento de los Rastros Informáticos. 2da Edición., México: Alfaomega Grupo Editor, S.A., 2015.
- [9] ISO Standards, *ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*, Geneva: ISO, 2012.
- [10] Casey, E., Digital Evidence and Computer Crime. Third Edition, Baltimore, Maryland, USA: Elsevier, Inc., 2011.
- [11] Cano, J., «Introducción a la Informática Forense,» 2009. [En línea]. Available: [https://52.0.140.184/typo43/fileadmin/Revista\\_96/dos.pdf](https://52.0.140.184/typo43/fileadmin/Revista_96/dos.pdf). [Último acceso: 24 02 2021].

- [12] University of Delaware. Dept. of Electrical Engineering, «RFC,» 13 08 1982. [En línea]. Available: <https://www.rfc-editor.org/rfc/rfc822>. [Último acceso: 19 11 2022].
- [13] The Internet Society, «RFC,» 04 2001. [En línea]. Available: <https://www.rfc-editor.org/rfc/rfc2822>. [Último acceso: 19 11 2022].
- [14] Network Working Group , «RFC,» 10 2008. [En línea]. Available: <https://www.rfc-editor.org/rfc/rfc5322>. [Último acceso: 19 11 2022].
- [15] W. Stallings, Cryptography and Network Security. 7ma Edición, Madrid: Pearson Educación, 2004.
- [16] «RFC Editor,» 01 04 1993. [En línea]. Available: <https://www.rfc-editor.org/info/rfc1437>. [Último acceso: 04 12 2022].
- [17] Internet Engineering Task Force (IETF), «RFC,» 09 2011. [En línea]. Available: <https://www.rfc-editor.org/rfc/rfc6376>. [Último acceso: 19 11 2022].
- [18] M. Biré, «blogEmBlue,» 19 08 2020. [En línea]. Available: <https://blog.embluemail.com/proximo-webinar-configuracion-de-los-registros-spf-y-dkim/>. [Último acceso: 19 11 2022].
- [19] «Sustainability of Digital Formats,» 28 03 2014. [En línea]. Available: <https://www.loc.gov/preservation/digital/formats/fdd/fdd000379.shtml>. [Último acceso: 14 04 2022].
- [20] «MX Toolbox. Email Header Analyzer,» [En línea]. Available: <https://mxtoolbox.com/EmailHeaders.aspx>. [Último acceso: 19 11 2022].
- [21] Google Inc., «Caja de herramientas de Google Admin,» [En línea]. Available: <https://toolbox.googleapps.com/apps/messageheader/>. [Último acceso: 19 11 2022].
- [22] SysTools Software, «SysTools,» [En línea]. Available: <https://www.systoolsgroup.com/email-forensics.html>. [Último acceso: 19 11 2022].
- [23] Fookes Holding Ltd. , «Aid4Mail,» [En línea]. Available: <https://www.aid4mail.com/>. [Último acceso: 19 11 2022].
- [24] Paraben Corporation, «Complete Email Processing,» [En línea]. Available: <https://paraben.com/email-forensics/>. [Último acceso: 19 11 2022].
- [25] I. Sommerville, Ingeniería de Software, Mexico: Pearson Educación, 2011, p. 32.

- [26] «Tutorials Point,» [En línea]. Available: [https://www.tutorialspoint.com/uml/uml\\_use\\_case\\_diagram.htm](https://www.tutorialspoint.com/uml/uml_use_case_diagram.htm). [Último acceso: 19 11 2022].
- [27] «Tutorials Point,» [En línea]. Available: [https://www.tutorialspoint.com/uml/uml\\_activity\\_diagram.htm](https://www.tutorialspoint.com/uml/uml_activity_diagram.htm). [Último acceso: 19 11 2022].
- [28] «Phrasee,» [En línea]. Available: <https://phrasee.co/blog/a-brief-history-of-email/>. [Último acceso: 14 04 2022].
- [29] A. Mathai, «Goldfynch,» 3 septiembre 2019. [En línea]. Available: <https://goldfynch.com/blog/2019/09/03/6-email-ediscovery-file-types-must-know-pst-msg-edb-ost-eml-and-mbox.html>. [Último acceso: 14 abril 2022].
- [30] The National Academies, Sthrenghtening Forensic Sciences in the United States, Washington D.C.: The National Academic Press, 2009.
- [31] Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires, «Protocolo de Cadena de Custodia,» La Plata, 2015.
- [32] Ministerio Público Fiscal, «Manual de procedimiento de cadena de custodia,» 07 2015. [En línea]. [Último acceso: 06 04 2021].