ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA

GRADO EN INGENIERÍA INFORMÁTICA

Curso Académico 2022/2023

Trabajo Fin de Grado

DEFINICIÓN DE UN PROCESO DE INVESTIGACIÓN INFORMÁTICO-FORENSE EN EL ÁMBITO EMPRESARIAL

Autor: GEMA ALONSO BOTE
IVÁN MERINO MESA
DANIEL RODRÍGUEZ BORREGUERO

Directores: PALOMA CÁCERES GARCÍA DE MARINA

RESUMEN

La informática-forense se encuentra en pleno auge en la actualidad, como consecuencia de la transformación de la sociedad a una era totalmente digital. En este sentido, los delitos informáticos se encuentran a la orden del día, tales como fraude, robo de datos, filtración de información, espionaje, inclusive el ciberacoso, entre otros ejemplos.

Esta disciplina engloba los conocimientos propios de la informática en combinación con la rama del derecho, con el objetivo de realizar investigaciones de infracciones o delitos que hayan acontecido, interviniendo en la recopilando y análisis de las pruebas electrónicas implicadas, que deberán influir en el desarrollo y resolución del proceso legal.

En esta instancia, la informática-forense desempeña un papel fundamental dentro del entorno empresarial. Algunos de los objetivos de las entidades se centran en aspectos relacionados con la automatización de procesos, el almacenamiento y gestión masiva de datos, entre otros. De esta forma, implementando las últimas tecnologías de la información en su actividad diaria, surgen algunos desafíos y riesgos a los que se deben enfrentar las compañías. Por ejemplo, ataques cibernéticos, intrusiones en la red y cualquier otro tipo de incidente de seguridad o hecho relacionado con la propiedad intelectual de la entidad.

Por lo tanto, la rama de la informática forense se emplea como método para la resolución de las investigaciones de los incidentes mencionados, así como en la protección de los activos tangibles e intangibles de las empresas, actuando como medida preventiva de fraude interno dentro de las organizaciones. Además, promoviendo el cumplimiento normativo de las leyes que involucran la protección, seguridad y privacidad de los datos.

En consecuencia, se han desarrollado una serie de estándares y normativas que componen la definición de un procedimiento con el fin de elaborar un análisis forense, recopilando los datos de los dispositivos electrónicos en busca de la información relevante. Con el objetivo final, de elaborar un informe pericial detallado que sirva como prueba para ser utilizando ante un tribunal.

Palabras clave: informática-forense, incidente, seguridad, tecnologías de la información, estándares, privacidad, informe pericial.

ABSTRACT

Computer forensics is currently booming as a result of the transformation of society to a totally digital era. In this sense, computer crimes are the order of the day, such as fraud, data theft, information leakage, espionage, including cyberbullying, among other examples.

This discipline encompasses the knowledge of computer science in combination with the branch of law, with the aim of conducting investigations of infractions or crimes that have occurred, intervening in the collection and analysis of the electronic evidence involved, which should influence the development and resolution of the legal process.

In this instance, computer forensics plays a fundamental role within the business environment. Some of the objectives of the entities are focused on aspects related to the automation of processes, storage, and massive data management, among others. Thus, by implementing the latest information technologies in their daily activity, some challenges and risks arise that companies must face. For example, cyber-attacks, network intrusions and any other type of security incident or event related to the entity's intellectual property.

Therefore, the branch of computer forensics is used as a method for the resolution of the investigations of the mentioned incidents, as well as in the protection of tangible and intangible assets of companies, acting as a preventive measure of internal fraud within organizations. In addition, promoting regulatory compliance with laws involving the protection, security, and privacy of data.

Consequently, a series of standards and regulations have been developed that make up the definition of a procedure in order to elaborate a forensic analysis, collecting data from electronic devices in search of relevant information. The ultimate goal is to produce a detailed report that serves as evidence to be used in court.

Keywords: computer forensics, incident, security, information technology, standards, privacy, expert report.

AGRADECIMIENTOS

Nos gustaría agradecer a nuestras familias, en especial a nuestros padres y hermanos, por haber sido un apoyo fundamental y por la motivación recibida durante todo el camino que ha conllevado la realización de la doble titulación. Y, sobre todo el poder acompañarnos en la finalización de esta etapa tan importante.

También, nos gustaría dar las gracias a nuestros amigos y parejas, por haber estado haber sido un gran apoyo durante esta trayectoria. Gracias por siempre darnos fuerza y ánimos.

Por último, queremos dar las gracias a nuestra tutora Paloma por habernos dado las fuerzas y la confianza necesarias para poder realizar este trabajo, estar a nuestra disposición en todo momento y habernos aportado conocimientos suficientes para afrontar y lograr los objetivos establecidos.

ÍNDICE DE CONTENIDOS

RESUMEN 3
ABSTRACT 5
AGRADECIMIENTOS 7
ÍNDICE DE FIGURAS 11
ÍNDICE DE TABLAS 16
CAPÍTULO 1: MOTIVACIÓN, OBJETIVOS Y ESTRUCTURA 17
1.1. Motivación 17
1.2. Objetivos 17
1.3. Estructura 18
CAPÍTULO 2: ESTUDIOS PREVIOS 19
2.1. Introducción a la informática forense 19
2.1.1. El Caso *Enron Corporation* 19
2.1.2. Conceptos básicos 19
2.2. Estándares principales 21
2.2.1. Modelo EDRM (Electronic Discovery Reference Model) 21
2.2.2. Gobierno de la información. 21
2.2.3. Identificación 23
2.2.4. Preservación 26
2.2.5. Recopilación 26
2.2.6. Procesamiento 26
2.2.7. Revisión 33
2.2.8. Análisis 37
2.2.9. Producción 38
2.2.10. Presentación 39
2.2.2. Estándares ISO 40
2.2.2.1. ISO 27001 40
2.2.2.2. ISO 27037 42
2.3. Principales herramientas forenses 44
CAPÍTULO 3: DEFINICIÓN DEL PROCEDIMIENTO INFORMÁTICO 51
3.1. Propuesta de procedimiento informático-forense 51
3.1.1. Identificación de las evidencias 52
3.1.2. Recolección y preservación de la evidencia 53
3.1.3. Adquisición 54
3.1.4. Procesamiento 58
3.1.5. Revisión y análisis 60

3.1.6. Producción y preservación 62
CAPÍTULO 4: DESARROLLO DE LA HERRAMIENTA 65
4.1. Tecnologías empleadas 65
4.2. Actores y captación de requisitos 65
4.2.1. Registrarse 66
4.2.2. Iniciar sesión 68
4.2.3. Crear caso 69
4.2.4. Mostrar caso 70
4.2.5. Editar caso 70
4.2.6. Archivar caso 72
4.2.7. ¿De qué trata esta fase? 73
4.2.8. Avanzar a la siguiente fase 73
4.2.9. Cerrar caso 74
4.2.10. Eliminar caso 75
4.2.11. Diagrama de estados Caso 76
4.3. Navegación e Interfaz gráfica 77
4.3.1. Pantalla de bienvenida 77
4.3.2. Registro de usuarios 78
4.3.2.1. Posibles escenarios de error 80
4.3.3. Inicios de sesión 82
4.3.3.1. Posibles escenarios de error 83
4.3.4. Cerrar sesión 84
4.3.5. Guía para usuarios 84
4.3.5.1. Guía adquisición 86
4.3.5.2. Guía procesamiento 91
4.3.5.3. Guía filtrado 94
4.3.5.4. Guía análisis 95
4.3.5.5. Guía presentación de resultados 96
4.3.5.6. Posibles escenarios de error 97
4.3.6. Revisión de mis casos 98
4.4.1.1. Creación de casos 99
4.4.1.2. Casos abiertos 99
4.4.1.3. Casos cerrados 105
4.4.1.4. Casos archivados 106
4.4.1.5. Posibles escenarios de error 106
4.4. Diseño interfaz gráfica (*front-end*) 108
4.5. Diseño y gestión de la base de datos (back-end) 118

4.6. Gestión, comunicación front-end back-end y principales funciones.. 120
4.7. Instalación de las tecnologías y puesta en marcha de la aplicación.... 128
CAPÍTULO 5: VALIDACIÓN DEL PROCEDIMIENTO Y DE LA HERRAMIENTA 131
5.1. Caso práctico..... 131
5.2. Demostración del funcionamiento de la herramienta 132
5.3. Conclusión de los resultados tras el análisis..... 134
CAPÍTULO 6: CONCLUSIÓN Y TRABAJOS FUTUROS 137
6.1. Conclusiones..... 137
6.2. Trabajos futuros 139
6.3. Distribución del trabajo 139
BIBLIOGRAFÍA 141
ANEXO 1: GLOSARIO DE TÉRMINOS 143
ANEXO 2: ADQUISICIONES DE PORTÁTILES 145
2.1. Proceso de adquisición física..... 145
2.2. Proceso de adquisición en vivo..... 152
ANEXO 3: PREPROCESAMIENTO DE LOS PORTÁTILES 157
ANEXO 4: PROCESAMIENTO EN AXIOM DE LOS PORTÁTILES..... 163
ANEXO 5: PROCESAMIENTO EN NUIX DE LOS PORTÁTILES 167
ANEXO 6: ADQUISICIÓN Y PROCESAMIENTO DE LOS DISPOSITIVOS MÓVILES..... 175
ANEXO 7: ANÁLISIS DE LOS ORDENADORES PORTÁTILES Y DISPOSITIVOS MÓVILES..... 179
ANEXO 8: RESULTADOS DEL ANÁLISIS DE LOS DISPOSITIVOS ELECTRÓNICOS 195
PERMISO DE DISTRIBUCIÓN DE RESULTADOS DEL TFG..... 197

ÍNDICE DE FIGURAS

Figura 1: Esquema modelo EDRM 21
Figura 2: Esquema gobierno de la información 22
Figura 3: Esquema Preservación 26
Figura 4: Esquema Procesamiento 27
Figura 5: Esquema revisión a través de las tecnologías 34
Figura 6: Logicube Forensic Falcon 45
Figura 7: Cellebrite Reader 47
Figura 8: Diagrama de decisión del procedimiento informático forense 56
Figura 13: Diagrama de casos de uso y actores de la herramienta 66
Figura 14: Diagrama de actividad Registrarse 67
Figura 15: Diagrama de actividad Iniciar Sesión 68
Figura 16: Diagrama de actividad Crear Caso 69
Figura 17: Diagrama de actividad Mostrar caso 70
Figura 18: Diagrama de actividad Editar Caso 71
Figura 19: Diagrama de actividad Archivar Caso 72
Figura 20: Diagrama de actividad "¿De qué trata esta fase?" 73
Figura 21: Diagrama de actividad Avanzar a la siguiente fase 74
Figura 22: Diagrama de actividad Cerrar Caso 75
Figura 23: Diagrama de actividad Eliminar Caso 76
Figura 24: Diagrama de estados Caso 77
Figura 25: Pantalla de bienvenida de la aplicación (I) 78
Figura 26: Pantalla de bienvenida de la aplicación (II) 78
Figura 27: Barra de navegación de la interfaz (usuario no logueado) 78
Figura 28: Barra de navegación de la interfaz (usuario no logueado) 79
Figura 29: Formulario registrar un usuario (II) 79
Figura 30: Vista de inicio de sesión 80
Figura 31: Escenario de error registrar usuario (I) 80
Figura 32: Escenario de error registrar usuario (II) 81
Figura 33: Escenario de error registrar usuario (III) 81
Figura 34: Escenario de error registrar usuario (IV) 82
Figura 35: Barra de navegación de la interfaz (usuario no logueado) 82
Figura 36: Vista de inicio de sesión con datos introducidos 82
Figura 37:Pantalla de inicio tras iniciar sesión 83
Figura 38: Vista de inicio de sesión con el campo contraseña obligatorio 83
Figura 39: Vista inicio de sesión con mensaje de error por las credenciales introducidas 84
Figura 40: Barra de navegación usuario logueado 84
Figura 41: Barra de navegación usuario sin loguear 84
Figura 42: Acceso a guía desde pantalla de bienvenida 85
Figura 43: Acceso a guía barra de navegación usuario sin loguear 85
Figura 44: Acceso a guía barra de navegación usuario logueado 85
Figura 45: Bienvenida a sección guía 86
Figura 46: Descripción fase de adquisición 86
Figura 47: Guía del procedimiento de adquisición genérico 87
Figura 48: Guía del procedimiento de adquisición móvil 87
Figura 49: Procedimiento de adquisición mediante Cellebrite 88

Figura 50: Procedimiento de adquisición mediante Axiom 88
Figura 51: Guía del procedimiento de adquisición ordenador..... 89
Figura 52: Procedimiento de adquisición mediante Falcon..... 89
Figura 53:Procedimiento de adquisición mediante FTK 90
Figura 54: Procedimiento de adquisición mediante “adquisición especial”..... 90
Figura 55:Guía del procedimiento de adquisición almacenamiento externo..... 91
Figura 56: Descripción fase de procesamiento 91
Figura 57: Guía del procedimiento de procesado 92
Figura 58: Guía del procedimiento de procesamiento mediante FTK..... 92
Figura 59: Guía del procedimiento de procesamiento mediante Falcon 93
Figura 60: Guía del procedimiento de procesamiento mediante Cellebrite 93
Figura 61: Guía del procedimiento de procesamiento mediante Axiom 94
Figura 62: Descripción fase de filtrado..... 94
Figura 63: Buenas prácticas fase de filtrado 95
Figura 64: Descripción fase de análisis 95
Figura 65: Guía análisis eDiscovery..... 96
Figura 66: Guía análisis Computer Forensics..... 96
Figura 67: Descripción fase de presentación de resultados 97
Figura 68: Buenas prácticas fase de presentación de resultados 97
Figura 69: Posibles escenarios de error fase de adquisición..... 98
Figura 70:Posibles escenarios de error fase de adquisición..... 98
Figura 71: Barra de navegación tras iniciar sesión, “Mis casos”..... 99
Figura 72:Vista de “Mis Casos” con las opciones disponibles - Crear caso 99
Figura 73: Formulario a rellenar al Crear Caso 99
Figura 74: Vista de “Mis Casos”, con los casos abiertos y las distintas opciones 100
Figura 75: Vista “Mostrar Más” con toda la información relativa a un caso ... 100
Figura 76:Vista de Editar Caso, con los campos editables para un caso de ejemplo 101
Figura 77: Ventana confirmación avance de fase de un caso 102
Figura 78: Ventana confirmación Chrome avance de fase 102
Figura 79: Ventana confirmación eliminación caso 103
Figura 80: Ventana de Chrome confirmación eliminación de un caso..... 103
Figura 81: Ventana confirmación cierre de un caso 104
Figura 82: Vista detalle de un caso con Fase “Presentación”..... 104
Figura 83: Ventana emergente confirmación archivar caso 105
Figura 84: Ventana emergente Chrome confirmación archivado del caso..... 105
Figura 85: Pantalla de visualización de los casos cerrados del usuario..... 106
Figura 86: Visualización casos archivados..... 106
Figura 87: Error eliminación de caso, no siendo Owner de este 107
Figura 88: Error archivado de caso por no encontrarse en la última etapa..... 107
Figura 89: Error archivado de caso, no siendo el Owner de este 107
Figura 90: Error al no cumplimentar todos los campos en Crear Caso 108
Figura 91: Error en Crear Caso, identificador duplicado 108
Figura 92: Todas las plantillas HTML contenidas por la aplicación..... 109
Figura 93: Contenido template Layout.html (I)..... 110
Figura 94: Contenido template Layout.html (II) 110
Figura 95: Contenido template register.html (I) 111
Figura 96: contenido template register.html (II)..... 111
Figura 97: Contenido template misCasos.html (I)..... 112

Figura 98: Contenido template misCasos.html (II) 113
Figura 99: Contenido template misCasos.html (III) 113
Figura 100: Contenido template guide.html (I) 114
Figura 101:Contenido template guide.html (II) 114
Figura 102:Contenido template adquisicion-procedimiento-ordenador.html (I) 115
Figura 103: Contenido template adquisicion-procedimiento-ordenador.html (II) 116
Figura 104: Contenido template editar-caso.html (I) 117
Figura 105: Contenido template editar-caso.html (II) 117
Figura 106: Contenido template confirm_edit.html (I) 118
Figura 107: Contenido del fichero bd.py 118
Figura 108: Contenido del fichero models.py (I) 119
Figura 109: Contenido del fichero models.py (II) 119
Figura 110: Contenido del fichero models.py (III) 120
Figura 111: Contenido del fichero models.py (IV) 120
Figura 112: Contenido del fichero index.py (I) 121
Figura 113: Contenido del fichero index.py (II) 121
Figura 114: Contenido del fichero index.py (III) 122
Figura 115: Contenido del fichero index.py (IV) 122
Figura 116: Contenido del fichero index.py (V) 123
Figura 117: Contenido del fichero index.py (VI) 123
Figura 118: Contenido del fichero index.py (VII) 124
Figura 119: Contenido del fichero index.py (VIII) 125
Figura 120: Contenido del fichero index.py (IX) 125
Figura 121: Contenido del fichero index.py (X) 126
Figura 122: Contenido del fichero index.py (XI) 127
Figura 123:Contenido del fichero index.py (XII) 128
Figura 9: Comandos necesarios para activar el entorno virtual 128
Figura 10: Contenido del fichero requirements.txt 129
Figura 11: Configuración del entorno 129
Figura 12: Ejecución de la herramienta 129
Figura 124: Caso práctico prueba del procedimiento 132
Figura 125: Esquema acontecimientos caso práctico 132
Figura 126: Foto portátil ACER (I) 146
Figura 127: Foto portátil ACER (II) 146
Figura 128: Foto portátil ACER (III) 147
Figura 129: Foto portátil ACER (IV) 147
Figura 130: Paso I adquisición con Falcon 148
Figura 131: Paso II adquisición con Falcon 148
Figura 132: Paso III adquisición con Falcon (I) 149
Figura 133: Paso III adquisición con Falcon (II) 149
Figura 134: Paso IV adquisición con Falcon (I) 150
Figura 135: Paso IV adquisición con Falcon (II) 150
Figura 136: Paso IV adquisición con Falcon (III) 151
Figura 137: Paso IV adquisición con Falcon (IV) 151
Figura 138: Paso V adquisición con Falcon 151
Figura 139: Identificación de dispositivo (I) 152
Figura 140: Identificación de dispositivo (II) 153
Figura 141: Ejecutable herramienta FTK Imager (I) 153

Figura 142: Ejecutable FTK Imager (II) 153
Figura 143: Selección de la carpeta de Origen 154
Figura 144: Creación del contenedor forense AD1 154
Figura 145: Nombre y ruta destino de la evidencia 155
Figura 146: Ejecución del contenedor forense AD1 155
Figura 147: Verificación del contenedor forense AD1 156
Figura 148: Comando Robocopy (I) 156
Figura 149: Comando Robocopy (II) 156
Figura 150: Comando Robocopy (III) 156
Figura 151: Activación del disco duro con Veracrypt 157
Figura 152: Visualización de la evidencia 158
Figura 153: Paso I con herramienta Encase Forensic 158
Figura 154: Paso II con la herramienta Encase Forensic 159
Figura 155: Paso III con la herramienta Encase Forensic 159
Figura 156: Paso IV con la herramienta Encase Forensic 160
Figura 157: Paso V con la herramienta Encase Forensic 160
Figura 158: Paso VI con la herramienta Encase Forensic 161
Figura 159: Paso I con la herramienta Axiom 163
Figura 160: Paso II con la herramienta Axiom 163
Figura 161: Paso III con la herramienta Axiom 164
Figura 162: Paso IV con la herramienta Axiom 164
Figura 163: Paso V con la herramienta Axiom 165
Figura 164: Paso VI con la herramienta Axiom 165
Figura 165: Paso VII con la herramienta Axiom 166
Figura 166: Paso I con la herramienta Nuix 167
Figura 167: Paso II con la herramienta Nuix 167
Figura 168: Paso III con la herramienta Nuix 168
Figura 169: Paso IV con la herramienta Nuix 169
Figura 170: Paso V con la herramienta Nuix 170
Figura 171: Paso VI con la herramienta Nuix 170
Figura 172: Paso VII con la herramienta Nuix 171
Figura 173: Paso VIII con la herramienta Nuix (I) 172
Figura 174: Paso VIII con la herramienta Nuix (II) 172
Figura 175: Paso VIII con la herramienta Nuix (III) 172
Figura 176: Paso VIII con la herramienta Nuix (IV) 173
Figura 177: Paso IX con la herramienta Nuix (I) 173
Figura 178: Paso IX con la herramienta Nuix (II) 174
Figura 179: Paso IX con la herramienta Nuix (III) 174
Figura 180:Paso I adquisición de móviles con Cellebrite 175
Figura 181: Paso II adquisición de móviles con Cellebrite 176
Figura 182: Paso III adquisición de móviles con Cellebrite 176
Figura 183: Paso IV adquisición de móviles con Cellebrite 177
Figura 184: Paso V adquisición de móviles con Cellebrite 177
Figura 185: Búsquedas en explorador Edge 180
Figura 186: Historial de navegación en navegador Edge 181
Figura 187:Registros de actividad reciente del artefacto Jumplist 181
Figura 188: Registros de actividad reciente del artefacto Windows Office Alerts 182
Figura 189: Registros de borrado de información del artefacto $RecicleBin... 182

Figura 190: Registros de conexiones externas del artefacto Storage Device Events 182
Figura 191: Búsquedas de Google 183
Figura 192: Historial de navegación en navegador Edge 183
Figura 193: Registros de actividad reciente del artefacto Jumplist 184
Figura 194: Registros de borrado de información del artefacto $RecicleBin... 184
Figura 195: Registros de conexiones externas del artefacto Storage Device Events 185
Figura 196: Evidencia sujeto de análisis con la herramienta FTK Imager..... 185
Figura 197: Aplicaciones instaladas 186
Figura 198: Información contenida en el usuario del custodio..... 186
Figura 199: Análisis de las Descargas realizadas 186
Figura 200: Lanzamiento palabras clave en Nuix (I) 187
Figura 201: Lanzamiento palabras clave en Nuix (II) 187
Figura 202: Consulta de análisis de comunicaciones 188
Figura 203: Listado de emails (I)..... 189
Figura 204: Listado de emails (II) 189
Figura 205: Listado de emails (III)..... 190
Figura 206: Listado de emails (IV)..... 190
Figura 207: Conversación WhatsApp (I)..... 191
Figura 208: Conversación de WhatsApp (II)..... 191
Figura 209: Conversación de WhatsApp (III) 191
Figura 210: Conversación de WhatsApp (IV) 192
Figura 211: Paso I adquisición de Microsoft Teams 192
Figura 212: Paso II adquisición de Microsoft Teams..... 193
Figura 213: Paso III adquisición de Microsoft Teams..... 193
Figura 214: Paso IV adquisición de Microsoft Teams 193
Figura 215: Conversación de Microsoft Teams (I)..... 194
Figura 216: Conversación de Microsoft Teams (II) 194

ÍNDICE DE TABLAS

Tabla 1 Principales fuentes ESI 24
Tabla 2: Tipos de filtrado 29
Tabla 3 Tipos de formatos de archivos 32
Tabla 4 Tipologías de producción 38
Tabla 5 Fases establecidas por la norma ISO 270001 41
Tabla 6 Tipos de adquisiciones Cellebrite 45
Tabla 7: Tabla comparativa Modelo EDRM y procedimiento definido 51
Tabla 8: Flujo de eventos del caso de uso “Registrarse” 67
Tabla 9: Flujo de eventos del caso de uso “Iniciar Sesión” 68
Tabla 10: Flujo de eventos del caso de uso “Crear Caso” 69
Tabla 11: Flujo de eventos del caso de uso “Mostrar Caso” 70
Tabla 12: Flujo de eventos del caso de uso “Editar Caso” 70
Tabla 13: Flujo de eventos del caso de uso “Archivar Caso” 72
Tabla 14: Flujo de eventos del caso de uso ¿De qué trata esta fase? 73
Tabla 15: Flujo de eventos del caso de uso “Avanzar a la siguiente fase” 73
Tabla 16:Flujo de eventos del caso de uso “Cerrar caso” 74
Tabla 17: Flujo de eventos del caso de uso “Eliminar Caso” 75
Tabla 18: Identificación de los dispositivos 145
Tabla 19: Identificación del dispositivo 152
Tabla 20: Principales categorías y artefactos analizados 179

CAPÍTULO 1: MOTIVACIÓN, OBJETIVOS Y ESTRUCTURA

1.1. Motivación

La motivación que ha impulsado la realización de este trabajo ha sido definir y analizar el proceso, así como los elementos intervinientes en la introducción de evidencias digitales en casos de fraude, ciberdelitos, y, en definitiva, en los procedimientos judiciales. Las tecnologías se han incorporado como una parte más de nuestra vida cotidiana. Por lo que, en concreto, se pretende definir los diferentes modelos o estándares que se han desarrollado en la disciplina *eDiscovery* (descubrimiento electrónico), analizar cada una de sus etapas y llevar a cabo un procedimiento informático forense, tomando de referencia el estándar internacional de mejores prácticas.

En esta misma línea, se procura demostrar las principales acciones y procedimientos que se deben seguir en la investigación de un caso de fraude electrónico o ciberdelito, de tal forma, que se conozcan las diferentes etapas y pasos a seguir, ya que es de suma importancia al tratarse de la huella digital. Por tanto, su correcto entendimiento y aplicación es clave para la investigación y su ratificación en el juzgado.

Además, se pretende exponer una serie de técnicas para agilizar la investigación y ayudar a automatizar estos procedimientos, y para ello, se ha desarrollado una herramienta, para que el investigador tenga más accesible su histórico de casos y pueda documentar y aglutinar toda la información relevante en el caso en el que esté trabajando en el momento.

1.2. Objetivos

El objetivo principal del trabajo es la determinación de un procedimiento de investigación informático-forense que aborda los distintos sucesos acontecidos en el caso del fraude corporativo.

A su vez, el objetivo se fragmenta en otros de carácter específico que se corresponden con los estudios previos. En este sentido, la configuración de la investigación se basa en el conocimiento de los siguientes fundamentos teóricos:

- Instaurar procedimiento informático-forense basado en el Modelo EDRM (*Electronic Discovery Reference Model*).
- Apoyar todo el procedimiento en las mejores prácticas informático-forense, a través de entre los estándares ISO relacionados con esta materia.
- Exposición de algunos conceptos informático-forense (código *hash*, contenedor forense…), y su relevancia de cara a la elaboración de informes Experto-Independientes o informes periciales.
- Cumplimiento del Reglamento General de Protección de Datos (GDPR).
- Analizar el contexto legal y marco actual.
- Determinar la finalidad de la informática forense y aplicaciones reales, ilustrado con ejemplos actuales.
- Realización de un caso práctico que documente algunas de las características que pueden ser observadas mediante el empleo de estas técnicas.

- Estudio del comportamiento de los documentos mediante distintos artefactos contenidos por los dispositivos electrónicos (*Master File Table (MFT), logs* de eventos…) basado en un caso práctico.

Posteriormente, el culmen del trabajo es la validación del procedimiento mediante la realización de la simulación de una investigación, bajo el análisis de la actividad desarrollada en las empresas por la cúpula directiva (entre diversos agentes intervinientes). Por lo tanto, resulta una de las motivaciones para desarrollar un proyecto grupal, con el fin de incorporar más actores implicados.

Además, se pretende lograr un intercambio de ideas y de perspectivas en la realización del trabajo, que a nivel individual podrían quedarse en una visión preliminar, mientras que en el fomento del trabajo en grupo se pueden obtener conclusiones más sólidas y completas, que refuercen el objetivo fundamente del trabajo, así como nuestras habilidades en equipo, pues se trata de un caso que podría ocurrir en nuestra actividad laboral.

En definitiva, ser capaces de establecer y desarrollar cuál es el procedimiento adecuado de actuación y análisis ante la situación mencionada, delimitando el campo de intervención y cuáles son las herramientas apropiadas para reconocer, basándonos en las pruebas recopiladas a través de los dispositivos, de quiénes son las personas implicadas y el reconocimiento de los inocentes.

1.3. Estructura

Este trabajo se encuentra estructurado en seis capítulos que engloban las distintas partes necesarias para desarrollar el análisis de contenido y el desarrollo de la herramienta y, en definitiva, obtener unas conclusiones determinadas y bien fundamentadas:

- Capítulo I: Introducción, motivación y estructura. En este capítulo se desarrollan los objetivos perseguidos en la realización del trabajo, la estructura seguida, y cuál ha sido la motivación que sustenta las bases de este.

- Capítulo II: Informática forense y estado del arte. En este capítulo se define el concepto de informática forense, y se realiza un análisis de los estándares principales de la misma siguiendo las mejores prácticas internacionales.

- Capítulo III: Definición del procedimiento informático. En este capítulo se realiza un estudio sobre cada una de las etapas que forman parte del procedimiento definido, que se ha servido de guía desarrollar el caso práctico.

- Capítulo IV: Desarrollo de la herramienta. En este capítulo, se pretende documentar las anotaciones más relevantes en el desarrollo de la herramienta.

- Capítulo V: Validación del procedimiento y de la herramienta. En este capítulo, se pretende exponer el caso práctico desarrollado y se hace referencia a los anexos que contienen la demostración de todo el proceso. Además, se relaciona el caso práctico con la herramienta, documentada en el capítulo anterior.

- Capítulo VI: Conclusiones y trabajos futuros. Por último, se pretende definir las principales conclusiones del trabajo y exponer una serie de propuestas y mejoras para seguir desarrollando la herramienta de cara al futuro.

CAPÍTULO 2: ESTUDIOS PREVIOS

2.1. Introducción a la informática forense

2.1.1. El Caso *Enron Corporation*

El origen de la informática forense se establece con el caso de la empresa energética estadounidense *Enron Corporation*, uno de los fraudes financieros más grandes que se ha producido en la historia, declarándose en quiebra en diciembre de 2001.

Según establecía la compañía, mantenía activos que se estimaban en 63.000 millones de dólares y, facturaba 100.000 millones de dólares anuales. Sin embargo, estos datos no eran verídicos, ya que los pasivos se convirtieron en los activos, los créditos como ingresos, y, en consecuencia, los beneficios fueron inflados. Esta serie de acciones provocaron que la acción en bolsa que cotizaba a noventa dólares se hundiera pasando a costar un dólar.

De esta forma, comenzaron a salir a la luz los distintos fraudes financieros, deduciendo que la empresa tenía deudas de 30.000 millones de dólares, provocando su bancarrota. Este hecho también afectó a la firma de auditoría *Arthur Andersen*, considerada una de las cinco sociedades auditoras más grandes del mundo, ya que algunos de sus empleados destruyeron documentos.

Tras la realización de las investigaciones correspondientes se descubrió que el responsable principal de la contabilidad de la entidad realizaba ingresos ficticios, de tal forma, que ocultaba las pérdidas y encubría sus deudas. El escándalo salió a la luz, tras la publicación de un artículo, en el que se cuestionaba la posición creciente de la compañía tras pasar en el ranking de empresas estadounidenses de la 141 a la séptima más importante; ya que el responsable de la contabilidad renunció a su cargo y, vendió las acciones que tenía de la empresa.

Por consiguiente, tanto el fundador de la firma, como el director de esta y el responsable de la contabilidad fueron acusados por delitos de engaño, conspiración y fraude. De esta forma, surgió la normativa de establecer que el auditor de una empresa debería de ser independiente de su cliente, de tal manera, que se incrementaron las medidas restrictivas y las sanciones, para mantener una correcta regulación.

Cabe mencionar que hoy en día continúan produciéndose este tipo de incidentes, con motivo del hecho de la introducción de nuevas tecnologías y la refinación de estas. Por consiguiente, más adelante el proyecto en las fases o pautas a seguir a la hora de actuar ante un descubrimiento de fraude empresarial.

2.1.2. Conceptos básicos

Asimismo, antes de comenzar con el desarrollo práctico del proyecto es necesario exponer una serie de estudios o conocimientos previos para que se pueda llegar a entender correctamente toda la terminología que se va a usar en el trabajo.

El proceso principal que se va a seguir en este trabajo es un procedimiento informático-forense en el ámbito empresarial, por lo que se debe tener muy claro en qué consiste exactamente. "*La informática forense consiste en un proceso de investigación*

de los sistemas de información para detectar toda evidencia que pueda ser presentada como prueba fehaciente en un procedimiento judicial"[1].

Antes de empezar a definir conceptos más técnicos, cabe destacar que el procedimiento informático-forense, debe ser un proceso auditable, reproducible y defendible. Un proceso auditable en lo que concierne a que todos los procedimientos y documentaciones deben estar contrastados por buenas prácticas profesionales. Debe ser reproducible, en el sentido de que todos los métodos seguidos deben poder ser verificables y argumentables por otros profesionales del área. Por último, debe ser defendible, de tal forma que todas las herramientas que se utilizan para el procedimiento, que se mencionará posteriormente, deben de ser validadas y contrastadas para que se valide todo el procedimiento.

Estas características son muy importantes, ya que las pruebas informática-forenses son aportadas en juicios por peritos forenses, es decir, son pruebas digitales que tienen un propósito muy importante como es el demostrar hallazgos y aportar luz en un juicio.

Una vez definida correctamente la informática forense, se va a definir las dos técnicas más utilizadas y que serán el núcleo del ejemplo práctico del proyecto, aunque se profundizará más en ellas a lo largo del trabajo. Las técnicas referidas anteriormente son las siguientes:

eDiscovery: Se define como "*La exhibición de documentos electrónicos, o eDiscovery, es el proceso de identificación y entrega de información electrónica que se puede usar como prueba en casos legales*"[2]. ("Soluciones de exhibición de documentos electrónicos de Microsoft [16] ...") Algunos ejemplos de documentos electrónicos son correos electrónicos, documentos archivos CAD/CAM, bases de datos, archivos de imagen, *chats* de mensajería instantánea de *Slack* y otras plataformas, sitios *web* y cualquier otra información electrónica relevante. El proceso de *eDiscovery* también incluye metadatos y datos sin procesar que pueden incluir pruebas que los investigadores forenses pueden revelar.

Computer Forensics: Es una disciplina científica que considera los procedimientos en relación de las evidencias digitales para descubrir e interpretar información encontrada en dispositivos informáticos con el objetivo de establecer una serie de hipótesis o hechos relacionados con una investigación.

En este tipo de técnica se va a poder visualizar eventos y registros de Windows que van a dar respuestas a las preguntas de la investigación y, en consecuencia, van a ser hechos fácticos de qué ha pasado, cómo ha pasado y cuando ha pasado cada evento.

Además, en el *ANEXO 1: GLOSARIO DE TÉRMINOS* se encuentra un glosario de términos, donde se han agrupado los vocablos específicos de la informática forense, con el objetivo de tener claro su significado previamente y para cuando se utilicen, se esté familiarizado con ellos y se entienda de forma correcta todo el procedimiento.

Por otro lado, más términos *eDiscovery* serán analizados con mayor detalle en la sección de estándares, en concreto en el estándar EDRM definido previamente en el índice de contenidos.

[1] Definición Informática Forense: https://bit.ly/3rzYJpJ

[2] Definición eDiscovery: https://bit.ly/3rwpaNd

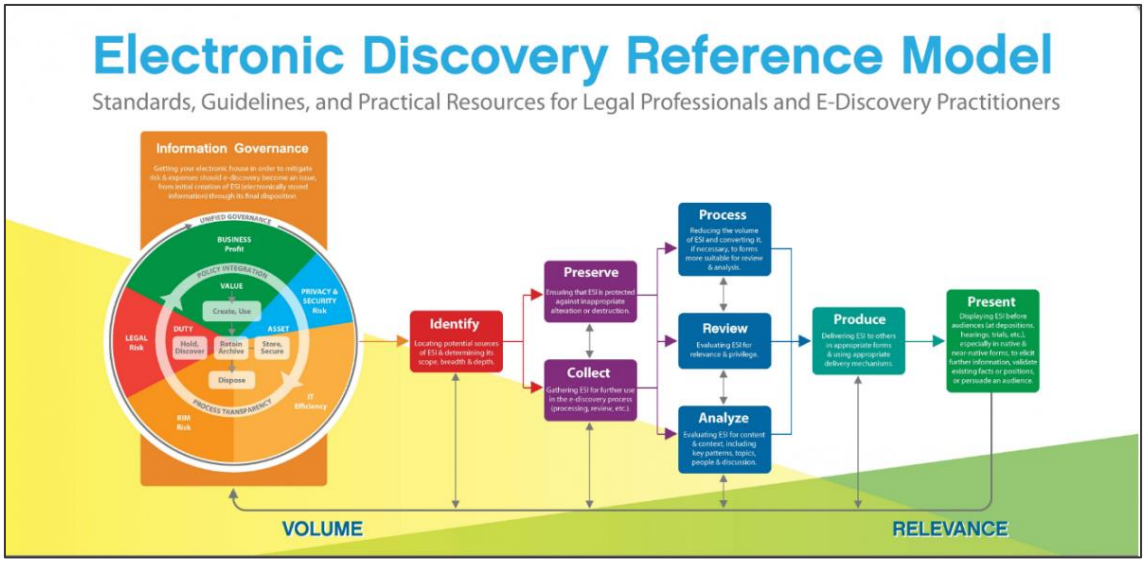
2.2. Estándares principales

2.2.1. Modelo EDRM (Electronic Discovery Reference Model)

El modelo EDRM [5] es un estándar que representa de forma conceptual el proceso de *eDiscovery* o descubrimiento electrónico. Se trata de un procedimiento en el que no es necesario seguir el orden de los pasos, ni el cumplimiento de estos tal y como se muestran en el diagrama. Por lo tanto, no tendría sentido definirlo como un modelo literal, lineal o en cascada.

La finalidad del diagrama es ser una guía durante la discusión y el análisis de grandes cantidades de datos. En consecuencia, se puede realizar la misma fase en varias ocasiones, de tal forma que se obtengan resultados más precisos. Asimismo, está permitido el retroceso a etapas anteriores con el objetivo de reforzar el enfoque de resultados de los datos o la necesidad de iniciar una nueva perspectiva en la investigación.

Figura 1: Esquema modelo EDRM



Fuente: EDRM, 2012 [5]

En esta misma línea, se establece un proceso conformado por un conjunto de etapas y modelos, que se describirán a lo largo de las siguientes subsecciones, y que son las siguientes: gobierno de la información, identificación, preservación, colección, procesado, revisión, análisis, producción y presentación.

2.2.2. Gobierno de la información.

El Modelo de Referencia de Gobernanza de la Información (MRGI) surgió como consecuencia del interés en desarrollar un modelo de gestión de la información. Era tal la dimensión de la información recopilada que era necesaria la creación de un modelo propio. En este sentido, para lograr la consecución del diagrama actual, se ha conformado un grupo diverso de participantes que aportan su enfoque y experiencia de forma colaborativa.

Los *stakeholders*: Componen las partes externas que presentan mayor interés. Sin embargo, uno de los principales desafíos se ha centrado en la insuficiente colaboración entre estos miembros claves en el proceso. Se establece una clasificación de los participantes en tres categorías principalmente:

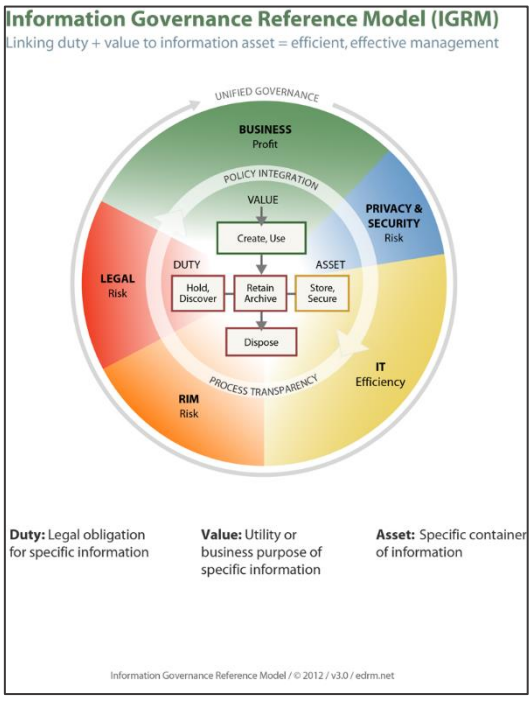
- Los usuarios de la empresa que requieren la información para el funcionamiento de la organización.
- El departamento de TI formado por quienes deben implementar los mecanismos de la gestión de la información.
- Los departamentos legales, de riesgos y de regulación que conocen de primera mano el deber en la preservación de la información empresarial, indistintamente de su valor comercial.

Anillo exterior: En relación con la parte exterior del diagrama, es necesario conocer un conjunto de procesos y procedimientos que involucran a los elementos estructurales de la empresa para poder llevarlo a la práctica. En consecuencia, los requerimientos fundamentales son los siguientes: pleno conocimiento de las herramientas apropiadas en la gestión de la información, así como de la sensibilidad legal (restricciones y normas) obligada a cumplir por parte de la empresa. En este sentido, se engloba dentro de la definición de empresa un concepto más amplio, entendido como el entramado formado por todos los usuarios involucrados en la información. cuyos objetivos finales pueden incluir o no la obtención de beneficios.

Por su parte, las organizaciones TI deberán garantizar la gestión de la información, seguridad y privacidad de las empresas bajo la normativa empresarial y legal.

El núcleo: Se encuentra constituido por el flujo de trabajo que ilustra la importancia de la gestión de la información desde que es creada hasta que finalmente es eliminada. Además, se emplea de apoyo junto con otros diagramas con el fin de concretar de forma sencilla los pasos a seguir por las organizaciones para la gestión de la información.

Figura 2: Esquema gobierno de la información



Fuente: EDRM, 2012 [5]

2.2.3. Identificación

Durante la fase de identificación, se reconocen las principales fuentes de información que resultarán relevantes en el proceso. Dentro de estas fuentes se incluyen empresas, personas, sistemas de IT y archivos en formato físico. Además, es esencial localizar los datos con el fin de que se produzca de manera efectiva la retención legal. Por lo tanto, se caracteriza por ser una etapa minuciosa y exhaustiva para no obviar ninguna fuente de información que pudiera ser relevante para el estudio del caso.

Por otro lado, en ocasiones el origen de la disputa legal, así como las personas involucradas en la misma puede verse modificado durante el proceso. En consecuencia, el equipo a cargo de la identificación deberá prevenir los cambios e incorporar información potencial recién identificada.

Para garantizar el éxito durante la identificación, se presentarán cuatro fases fundamentales: desarrollar la estrategia y el plan de identificación, establecer el equipo de identificación, identificar fuentes *ESI* relevantes y certificar estas fuentes. Asimismo, estas fases se encuentran respaldadas por procesos que garanticen una correcta auditoria o un control de calidad.

2.2.3.1. Desarrollar la estrategia y en plan de identificación

Tal y como se ha mencionado anteriormente durante el proceso de identificación, por un lado, es esencial reconocer a los individuos clave, la ubicación de datos, los custodios, así como la trazabilidad de los datos a las personas y departamentos correspondientes. Por otro lado, los actores intervinientes en la gestión del proyecto tales como asesores legales, personal de administración, personal de IT, asesores externos o consultores y proveedores de servicios.

Según establecen las organizaciones jurídicas y penales, las empresas se encuentran en la obligación de establecer una serie de medidas razonables que garanticen la identificación y preservación de las fuentes. En este sentido, se originan las Oficinas del Asesor Jurídico y de Tecnología de la Información responsables de la gestión de las *ESI*.

En consecuencia, las entidades deben promover la asignación de los datos, para facilitar su almacenamiento y difusión necesaria en investigaciones y litigios. Esto quiere decir que deberían poseer los medios requeridos para conocer la utilidad de sus sistemas de información, así como la interrelación que se produce entre ellos, ubicación y personal que se encuentra en la manipulación de estos.

Mapeo de datos. Se corresponde con la imagen general de las distintas fuentes de datos de la empresa. Por lo que, se deberán incluir todas las infraestructuras de *hardware* y *software*, en lo referente a correo electrónico, copias de seguridad, tipos de servidores, dispositivos de los usuarios, entre otros. Además, se incluyen archivos de datos inactivos como discos duros, CD-ROM, unidades flash…

Preparar el plan de identificación. Hace referencia al establecimiento de las tareas y herramientas que se emplearán para reconocer las potenciales fuentes. Para que resulte más eficaz se elabora una lista con los distintos individuos, estableciendo las características sobre el mismo: nombre, tipo de fuente, clave o no, identificación, preguntas, seguimiento… Asimismo, este plan se encontrará delimitado en función de las herramientas, información previa, mapa de datos de los que disponga la organización.

2.2.3.2. Establecer el equipo de identificación.

El equipo de identificación resulta fundamental durante el proceso pues se trata del responsable para reconocer a las personas claves, custodios de datos y la información relevante en el asunto. Por lo que, se recomienda que esté formado por una o más personas.

- **Asesoramiento legal corporativo:** Departamento encargado de poseer un plan de identificación electrónico, para conocer los principales sistemas y unidades de negocio con información notable. Además, otra de las funciones es ser el medio para comunicar información de carácter legal.
- **Abogado externo:** Entendimiento del plan y asegurar la defensa de este.
- **Personal de IT:** Aquellas personas que pueden proporcionar información detallada sobre los sistemas de borrado automático, ubicaciones de los archivos y datos, así como el conocimiento de las políticas informáticas sobre copias de seguridad y almacenamiento.
- **Personal de gestión de registros:** Informar sobre el almacenamiento y políticas de los datos, y sobre la eliminación de los registros.
- **Custodios de datos:** Persona que tiene asignadas las fuentes de información objeto de la investigación informático forense.
- **Personal de recursos humanos:** Obtención de listas de empleados e información sobre estos, con el fin de reconocer custodios.
- **Líderes comerciales:** Identificación de los sistemas empleados en la unidad de negocio, así como reconocimiento del personal con información relevante. Por otro lado, pueden ser el medio de comunicación con el departamento legal.
- **Proveedores de servicios/consultores de descubrimiento:** Conocimiento previo sobre la localización de información potencial.

2.2.3.3. Identificar las fuentes *ESI* potencialmente relevantes.

A continuación, se presenta, en formato de tabla, las fuentes *ESI* que pueden ser potencialmente relevantes:

Tabla 1 Principales fuentes ESI

ETAPA	DEFINICIÓN
Identificación de testigos clave y custodios	- Conocer la infraestructura corporativa de las empresas, así como la distribución de la organización. - Determinar el personal relevante en la investigación (i.e. Personal de IT).
Determinación de los marcos de tiempo clave	- Localizar y seleccionar los datos, una vez se ha establecido cuál es el tiempo relevante del asunto.
Listados de palabras clave	- Conocer la jerga o acrónimos particulares de la empresa que han podido ser utilizados en el correo, informes, comunicaciones…
Identificación de tipos de datos y documentos potencialmente relevantes	- Identificar dónde se almacenan físicamente los datos en la red, y el tipo de datos en función de su ubicación (correo, documentos Office). - Entrevistar a los custodios para conocer si son actores relevantes para la investigación. - Identificar si se están produciendo actualizaciones, migraciones o consolidación de datos en la empresa.
Almacenamiento de archivos	- Existencia y permisos de un sistema de gestión de documentos. - Almacenamiento en local o disco duro. - Políticas de reciclaje de servidores o discos duros. - Almacenamiento de archivos en medios extraíbles (CD – ROM, DVD, USB, unidades zip…).
Sistemas de correo electrónico	- Existencia de servidores de correo electrónico. - Existencia de un software de administración de correo electrónico.

	- Políticas de retención. - Almacenamiento en discos duros de usuarios.
Determinación de la relevancia de los medios de copia de seguridad, el hardware retirado y los sistemas de recuperación ante desastres	- Sistemas de copia de seguridad en cinta, con el fin de restaurar uno o varios sistemas tras un evento catastrófico. - El departamento de IT debe proporcionar información acerca de cómo, cuándo y dónde se realizan las copias de seguridad.
Sistemas heredados	- Conocimiento de los sistemas anteriores que han manejado información, durante el tiempo clave. - Identificar el *hardware* y versiones anteriores de *software*.
Computación en la nube o sistemas de terceros	- Existencia de sistemas de computación en la nube, SaaS, instalaciones de almacenamiento fuera de la empresa, almacenamiento de datos o cintas de terceros.
Fuentes de datos adicionales	- Tiendas de correo de voz digital y/o tiendas VOIP. - Los dispositivos portátiles incluyen asistentes personales digitales (*Palm Pilot, BlackBerry*, etc.) - Información sobre la intranet/extranet de la empresa y la posibilidad de exportar desde estas fuentes. - Uso de los empleados de los ordenadores personales para almacenamiento de información y asuntos de negocio. - Mensajería instantánea.

Fuente: Elaboración propia

2.2.3.4. Certificar fuentes ESI potencialmente relevantes

Una vez que se han identificado todas las fuentes *ESI* potencialmente relevantes, tal y como se ha mencionado anteriormente, es necesario que el jefe que lidera el equipo de investigación informático-forense o el abogado implicado las verifique.

Para ello, se indicarán las objeciones en lo referente a las fuentes que no han podido ser seleccionadas o buscadas de forma razonada. Así como se dará comienzo da un proceso de preservación de datos por parte de una autoridad. Por tanto, quedará documentado las herramientas y metodología empleada para identificar finalmente cuáles son las principales fuentes.

2.2.3.5. Informes de estado y riesgos

Se tratan de documentos que recogen la situación y el progreso de los proyectos. De tal forma, que la tanto la gerencia como las personas que se encargan del caso pueden localizar los errores o problemas que han surgido y que impiden que el proyecto se realice en tiempo y forma.

2.2.3.6. Documentación para la pista de auditoría defendible

Resulta fundamental realizar una documentación del proceso de identificación con el fin de incorporar posibles nuevas fuentes de información, así como para demostrar que se trata de un procedimiento razonable y completo. Por consiguiente, sería conveniente recoger de manera cronológica los registros, mapas y diagramas de sistemas informáticos. Además, de las políticas de IT, la estrategia que se ha seguido, las entrevistas que se han ido realizando, entre otros.

2.2.3.7. Control de calidad/validación

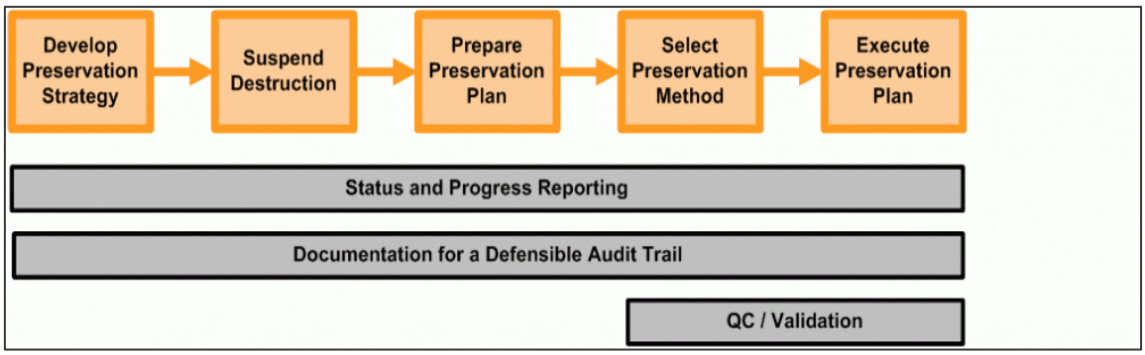
Durante esta última etapa en el proceso de identificación es necesario revisar algunos aspectos para garantizar la completitud de este. En este sentido, asegurarse de que los datos con susceptibilidad de eliminación se encuentren retenidos de forma adecuada. Así como que se hayan incluido todas las fuentes de correo electrónica como

relevantes y haber realizado la documentación del proceso bajo las políticas correspondientes de retención, copias de seguridad y reciclaje de los datos.

2.2.4. Preservación

El proceso de preservación de la información comienza una vez que se han identificado los datos relevantes en la investigación, con el fin de garantizar su correcta protección y aislamiento, mitigando los riesgos de una destrucción inapropiada para que finalmente que resulten defendibles de forma legal, razonables, auditables.

Figura 3: Esquema Preservación



Fuente: EDRM, 2012 [5]

Tal y como se puede observar en la imagen la etapa puede resultar en primera instancia como un flujo de trabajo de izquierda a derecha. Sin embargo, se pueden desarrollar cada una de las fases de forma iterativa con el fin de refinar el objetivo en cada uno de los mismos.

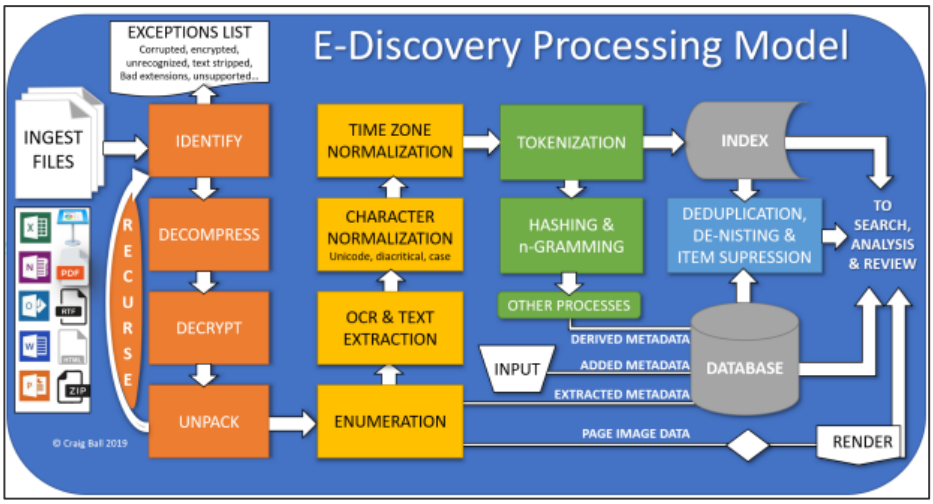
2.2.5. Recopilación

Durante la fase de recopilación se realiza una adquisición de toda la información que se encuentra almacenada de forma electrónica, que ha sido calificada como potencialmente relevante e identificada previamente. En este sentido, es necesario que la colección de los metadatos sea de manera legalmente defendible y auditable. Además, la recolección de las fuentes *ESI* permitirá establecer el alcance del proceso de *eDiscovery*.

2.2.6. Procesamiento

Las fases clave que conforman la etapa de procesamiento son las siguientes: ingestión de ESI y extracción de archivos, filtrado inicial, extracción de texto, metadatos e imágenes, salida e informes

Figura 4: Esquema Procesamiento



Fuente: eDiscovery Best Practices[9]

2.2.6.1. Ingestión de ESI y extracción de archivos

Cualquier sistema de procesamiento debe de tener la capacidad y compatibilidad para incorporar datos como correos electrónicos, documentos *Office*, mensajes instantáneos, redes sociales, archivos de audio o video, así como otros formatos de contenedores. Este tipo de archivos se corresponden a los comprimidos generados por *WinZip* o *WinRAR* con extensión "*zip*" o "*rar*".

Asimismo, los programas de *software* forense generan sus propios archivos contenedores, de tal forma que se crean imágenes exactas de una unidad con el fin de preservar la información. Por tanto, se obtiene archivos de tipo *FTK* o *E01*.

En cualquier caso, los motores de procesamiento deberán poder extraer los tipos de archivos contenedores indistintamente de su tipo, con el fin de ser más eficientes en la cadena de procesamiento. La secuencia de pasos para descomprimir los archivos contenedores es la siguiente:

- **Recibir y extraer datos de formatos de contenedores comunes:** Obtener e identificar los datos de los archivos contenedores, como *ZIP* y *RAR*. Además, de extraer los datos de forma recursiva de tal forma que se hayan alcanzado los de los contenedores dentro de contenedores. En esta misma línea, con los datos de formato de recolección forense: *FTK*, *L01*, *DD*, *E01* y *AFF*. De esta manera posteriormente se puede hacer un registro de los archivos que contienen los contenedores para la cadena de custodia.
- **Identificar y extraer contenido de contenedores correo electrónico:** Las recopilaciones correos electrónicos normalmente se transportan en archivos contenedores *PST* (tabla de almacenamiento personal), para archivos de *Microsoft Exchange*, u *OST* para copias temporales locales y *NSF* para *Lotus Notes*. Esta clasificación influye para seleccionar el esquema de codificación apropiado para extraer de forma correcta el contenido de los mensajes.
- Por otro lado, para los correos electrónicos individuales, por ejemplo, de *Microsoft Outlook* se identifica con *.msg*, son contenedores pequeños que contienen archivos adjuntos y objetos en el cuerpo del mensaje.

  - Con el fin de que el *software* extraiga todo el contenido del mensaje, debería de realizar recursiones hasta que se ha obtenido los mensajes y archivos adjuntos. Así como, averiguar la información sobre las relaciones familiares y extraer los objetos incrustados mostrándolos como archivos adjuntos.
  - **Identificar otros tipos de archivos básicos:** Resulta fundamental que el sistema de procesamiento sea capaz de reconocer los distintos tipos de archivo (imagen, audio, video), de tal forma que se traten adecuadamente para que no se produzcan fallos en el procesamiento. Por ejemplo, en el caso de *Windows*, el sistema operativo genera la identificación de los tipos de archivos según su extensión. Sin embargo, el hecho de que se pueda cambiar el nombre de los archivos con cualquier extensión puede provocar que cualquier individuo de forma engañosa puede ocultar la identidad de un archivo. Por consiguiente, otros sistemas operativos como *Mac* y *Linux*, y algunas funcionalidades de *Windows*, se emplea la información en el propio archivo para identificarlo. Para ello, se coloca una firma de archivo binario en los primeros *bytes* para detallar su tipo.
    - Además, en el caso en el que el software no identifique el tipo de archivo, debe incorporarlo a una lista de errores.
- **Analizar en busca de virus:** Los archivos deben analizarse lo antes posible con el fin de identificar virus, para ponerlos en cuarentena o eliminarnos de tal forma que no afecten al procesamiento, ni tampoco infecten a otros datos. En relación con esta instancia, es necesario que el software de procesamiento se encargue de escanear los archivos, partiendo de una base de datos que contenga firmas de virus regulada por proveedores de protección antivirus. Así como asegurarse de salvaguardar el resto de la información e informar sobre los archivos que han ocasionado problemas o se encuentran infectados.
- **Archivos *hash* para identificación y comparación:** El proceso de *hashing* se emplea para crear un identificador único, una vez que se han analizado su contenido. Por tanto, en cuanto se realice una modificación sobre el archivo su código *hash* cambie los valores. En consecuencia, se emplea para analizar si el contenido del archivo fue alterado en la etapa posterior al procesamiento, así como eliminar de forma confiable aquellos archivos que se encuentren duplicados. Existen diferentes algoritmos *Hash*, uno de los primeros fue el algoritmo *MD5* (resumen de mensajes cinco), y algoritmo hash seguro (*SHA*) fue desarrollado por la Agencia de Seguridad Nacional. Otro de los hechos para tener en cuenta es que es necesario emplear el mismo algoritmo para todos los archivos.
- **Crear una lista de excepciones:** En la tapa inicial del procesamiento pueden surgir fallos por muchas razones, como es el caso de cifrado, eliminación, identificación falsa… Además, es necesario que estos archivos se pongan en cuarentena o permanezcan identificados para que se encuentren custodiados de formas adecuada. En esta misma línea, algunos sistemas de procesamiento realizan informes de excepción para todas las fases del proceso. De tal manera, que finalmente se obtiene información sobre el error, la excepción y el estado de estas.

2.2.6.2. Filtrado inicial

Una vez que se ha procesado toda la información, se deberá de realizar un filtrado sobre la misma, en base a la naturaleza o alcance de la investigación. Por consiguiente, será necesario identificar el intervalo de tiempo y otra serie de factores que conviene analizar. Se establecen una serie de filtrados que se detallarán a continuación:

Tabla 2: Tipos de filtrado

TIPOS	DESCRIPCIÓN
Identificar archivos de sistema y de programa según la lista NIST	- Identificar los archivos comparando su valor hash con la lista mantenida por el Instituto Nacional de Estándares y Tecnología (NIST). - Si el valor coincide, el archivo se identifica de forma segura. - Sirven para reducir el número de datos, no contienen contenido detectable y no se emplean en el proceso de *eDiscovery*.
Identificar y eliminar archivos duplicados	- Eliminar aquellos archivos que se encuentren duplicados, gracias al reconocimiento que proporcionan los códigos *hash*. - Proceso de deduplicación que consiste en dejar una copiar del archivo y retener el resto.
Filtrado por intervalo de fechas o tipos de archivos	- El proceso tendrá establecido un intervalo de fechas. - Excluir los archivos que se encuentren fuera de este rango.

Fuente: Elaboración Propia

2.2.6.3. Extracción de texto, metadatos e imágenes

Tras finalizar el proceso de extracción y filtrado de los archivos es necesario obtener el contenido. Por consiguiente, el software de procesamiento tendrá que extraer toda la información que comprende los metadatos de los archivos, como por ejemplo los campos de para, asunto, fecha, hora de los correos electrónicos. Además, resulta fundamental que la opción de añadir más campos, la actividad y el contenido oculto se encuentre disponible.

- Acceder al contenido del archivo

El software de procesamiento debe de poder acceder al contenido de diferentes tipos de archivo, desde mensajes de correo electrónico, como PDF… de tal forma que integre los distintos tipos de archivos disponibles. Dentro de estos programas se podría ejemplificar con los siguientes: *Outside In de Oracle*, H*yland Document Filters*, *dtSearch*, *Aspose* y *Tika*.

- Detectar archivos cifrados y corruptos

El sistema de procesamiento utilizado debe detectar las excepciones o errores que surjan durante el proceso. Asimismo, debe reconocer los archivos que se encuentran protegidos con contraseñas, y poder probar de formar automática aquellas contraseñas conocidas. Además, de identificar los archivos corruptos con el fin de generar un informe de error para que sean tratados con otro método.

- Detectar codificación

En el momento en el que se accede al contenido del archivo es necesario determinar cuál ha sido la codificación del contenido.

Las primeras herramientas codificaban con el conjunto de caracteres ASCII. Posteriormente, se dieron cuenta que los 128 caracteres ASCII eran insuficientes, por lo tanto, a Organización Internacional para la Estandarización (ISO) y el Instituto Nacional Estadounidense de Estándares (ANSI) comenzaron a crear una extensión de ese conjunto de caracteres para crear distintas codificaciones. Finalmente, en 1900 gracias a un

consorcio mundial se científicos se desarrolló el estándar de codificación universal Unicode (actualmente UTF-8 o UTF-16).

En definitiva, resulta esencial que el sistema de procesamiento reconozca la codificación del sistema con el objetivo de poder utilizar el texto extraído y realizar las búsquedas de forma exacta.

- Detectar idioma

El proceso de descubrimiento electrónico involucra una gran cantidad de archivos que pueden encontrarse en distintos idiomas. Por consiguiente, la correcta identificación de este asegura que se filtre de forma adecuada para extraer el texto y la *tokenización*. En esta misma línea, durante la etapa de revisión los documentos se clasifican por idiomas para garantizar que aquellas personas asignadas la revisión de información extranjera se realice con exactitud.

- Extraer y normalizar texto

El texto deberá de extraerse de tal forma que se almacene comprensible y coherente para las etapas posteriores del proceso. En este sentido, es necesario tener en cuenta una serie de consideraciones al respecto, como es el caso de la normalización de mayúsculas y minúsculas; así como la normalización diacrítica, en función de los acentos en los distintos idiomas; la normalización Unicode; la normalización de zona horaria, en relación con las fechas y hora de los correos electrónicos que integran diferentes zonas horarias, estableciendo los valores estándares correspondientes a *Greenwich* (GMT).

Además, la *tokenización* de texto se emplea para la búsqueda de las palabras clave con el fin de obtener los resultados de forma más eficiente. El procedimiento que sigue el sistema consiste en la separación de las palabras para posteriormente indexarlas. En este sentido, resulta esencial que el sistema de procesamiento se encuentre adaptado a la para los distintos idiomas.

Por otro lado, con respecto a los documentos *Office*, una de sus características es que durante la edición de estos se pueden incluir notas o comentarios, que en su vista de impresión se encuentran ocultos. Por consiguiente, el *software* debe tener la opción de configuración para extraer esta información adicional e incorporarla para su revisión posterior.

- Extraer metadatos

En esta misma línea, el *software* de procesamiento deberá extraer los metadatos básicos, así como los requeridos por el administrador de este. Permitiendo obtener numerosos campos de metadatos como el nombre del archivo, última fecha en la que se guardó, información almacenada en el archivo… Así como para los correos electrónicos establecer un seguimiento de la información de la base de datos.

- Extraer imágenes

Numerosos tipos de archivos permiten incluir imágenes en su contenido. Fundamentalmente, se adjuntan en correos electrónicos, archivos de *Word* o *PowerPoint*, además de los mensajes de texto. Por consiguiente, el sistema de procesamiento deberá permitir que el administrador escoja extraer la imagen en relación con su valor fuera del fichero original. Es decir, en el caso de extraer el logotipo adjuntado en un correo electrónico provocaría que no tuviera valor fuera del mensaje original, así como que se incrementaría el gran volumen la cantidad de archivos a analizar de carácter irrelevante.

- Manejo de dispositivos móviles SMS e IM

Prácticamente, en la actualidad los teléfonos móviles se han convertido en ordenadores que almacenan archivos, imágenes, correos electrónicos, registros de llamadas, contactos, eventos de calendario etc. Por consiguiente, han adquirido una gran importancia el servicio de mensajes cortos (SMS) y la mensajería instantánea (IM), de tal magnitud, que registran una gran parte de la actividad social de los seres humanos.

En este sentido, presentan información que puede ser relevante en el procesamiento, bajo dos perspectivas de interés. Por un lado, la mensajería de texto propia de los teléfonos móviles como es el caso de los SMS y la mensajería multimedia, en el caso de *Apple* se encontraría relacionado con el entorno *iMessage*. Y, por otro lado, las aplicaciones de mensajería de terceros como por ejemplo *WhatsApp* y *Facebook Messenger,* donde su contenido se encuentra almacenado en bases de datos que pueden ser extraídas mediante sistemas especializados.

Normalmente, el formato de la exportación se caracteriza por ser un documento *Excel,* que contiene varias hojas, que se corresponden a un tipo de datos del dispositivo, es decir, una para el registro de llamadas, otra para los mensajes…

- Manejo de datos recopilados de redes sociales y plataformas de colaboración

En esta misma línea, relacionando con los datos de los teléfonos móviles se encuentran las redes sociales que poseen una fuente de comunicación a través de publicaciones, mensajería, intercambio de archivos, como por ejemplo las aplicaciones de colaboración en el entorno laboral, tras la aparición del teletrabajo de forma general a raíz del Covid-19. Plataformas como *Microsoft Teams* o *Google Chat* brindan la funcionalidad necesaria para el intercambio de documentos, conversaciones y videollamadas.

Por otro lado, las redes sociales que involucran tanto aspectos de la vida personal como laboral como es el caso de *Facebook*, *LinkedIn* que albergan contenido que puede ser utilizado en investigaciones criminales, comerciales hasta asuntos de carácter personal. Además, cabe mencionar que en el caso de *Instagram* que permiten publicaciones que se borran de forma automática a las 24 horas, existen softwares que permiten recopilar esos datos.

Asimismo, existe la posibilidad de extraer contenido de los sitios web, a través de extracción de información de texto o representaciones, que presentan fecha y hora, se pueden obtener como PDF o como archivo HTML.

- Exportación de datos móviles, de colaboración y de sitios web

Anteriormente, se ha comentado cómo sería la exportación de datos que resultan de un formato tradicional. No obstante, con el paso de los años los *softwares* de procesamiento se han ido refinando con el fin de obtener aquella información derivada de los dispositivos móviles, sitios *web*… Por consiguiente, se permite observar los metadatos relevantes, con el fin de filtrar la información relevante para el proceso de descubrimiento electrónico.

2.2.6.4. Salida de procesamiento

El formato de salida obtenido en el procesamiento puede seleccionarse en función de los requerimientos necesarios para continuar con el proceso de *eDiscovery*.

En primer lugar, establecer un filtrado por palabras clave y metadatos, con el fin de obtener una reducción del volumen de archivos que se han obtenido finalmente en el

procesamiento. Para ello, se realizarán búsquedas por palabras clave o metadatos en la base de datos del procesamiento, teniendo en cuenta que es necesario ajustarse a la precisión.

En segundo lugar, el software de procesamiento debe permitir incluir la información adjuntada en los documentos y mensajes. Por consiguiente, en los resultados del procesamiento se debería de incluir un archivo de carga que indique la información de ese documento y facilite cargar esos datos y archivos en el sistema. Además, de la información propia de los SMS e IM, que en ocasiones contienen *emojis* o imágenes que el sistema debería de reproducir de forma consistente.

En tercer lugar, en ocasiones es necesario que ciertos archivos se conviertan en imágenes para permitir su visualización. Por tanto, hay establecidos una serie de formatos de carácter estándar:

Tabla 3 Tipos de formatos de archivos

Tipos	Descripción
Tiffs de una sola página	Incluir una imagen por cada archivo, sin incluir texto.
Tiffs de varias páginas	Incluir varias imágenes por cada archivo, sin incluir texto. Son las menos utilizadas.
PDF	Archivo en color en varias páginas, que puede incluir texto. Es de los más utilizados.
JPEG o PNG	Formato empleado para las imágenes a color que depende de TIFF.

Fuente: Elaboración propia.

En cuarto lugar, la creación de archivos de texto de forma separada para los documentos de salida o cada una de las imágenes. De tal forma, que se puedan recuperar posteriormente para analizar su contenido para el asunto o litigio que concierne.

En quinto lugar, a veces las imágenes no poseen un texto extraíble, por lo que, no se pueden recuperar por palabras clave. En este sentido, los *softwares* de procesamiento deben de ser capaces de tener reconocimiento óptico de caracteres (OCR) con el fin de poder extraer el texto de la imagen para utilizarlo en la búsqueda posteriormente.

En sexto lugar, requiere gran importancia el nombre de los archivos, de tal forma, que se modifican en la salida del procesamiento, con el objetivo de asignarle el número de un control en concreto. Asimismo, el *software* de procesamiento puede incluir un prefijo o sufijo para incorporar más información sobre el archivo en cuestión.

En séptimo lugar, tal y como se ha comentado con anterioridad muchos archivos presentan archivos adjuntos que el sistema de procesamiento tiene que extraer de forma recursiva, ya que a su vez pueden contener otros archivos. Por lo tanto, es necesario numerar esa serie de archivos de tal manera que permanezcan registrado los archivos que pertenece y qué relación se establece en la familia de archivos.

En octavo lugar, estableciendo analogía con las relaciones familiares entre los archivos, es necesario tener en cuenta que los correos electrónicos incluyen conversaciones complejas que involucran a distintos destinatarios, una serie de respuestas que se pueden repetir. Por consiguiente, estos hilos de correo electrónico deberán tratarse para conocer cuál es el correo original y asociarlo a esa comunicación.

Por último, cabe mencionar que existen algunos softwares de procesamiento que permiten reconocer archivos que presentan un contenido similar a pesar de que su código *hash* no coincida. Suelen ser prácticamente iguales salvo pequeñas modificaciones en los metadatos, o incluso resultan ser borradores del documento original. Como consecuencia, agrupar estos archivos facilita su revisión posterior, etiquetándolos en el mismo grupo.

2.2.6.5. Informes

La última etapa que comprende el procesamiento consiste en la generación de informe, que documenta todas las acciones desarrolladas durante el proceso, así como los archivos disponibles que se utilizarán para la búsqueda de información.

Por lo tanto, se pueden distinguir varios tipos de informe; por un lado, los informes de inventario de archivos, que se corresponden la cantidad, el tipo, el tamaño, la ubicación y otras características que presentan los archivos que han sido procesados. Por otro lado, se elaboran los informes a nivel de custodio, que se corresponden con aquellos archivos que se han proporcionado para cada uno de los custodios, incluyendo los archivos que han podido ser procesados y aquellos que han generado una excepción o error durante el proceso.

Asimismo, se realizan informes de filtrado que muestran la cantidad de archivos que han sido eliminados o no han pasado los filtros requeridos en la búsqueda de la información. En este sentido, se incluye la eliminación de virus, filtrado por intervalo de fechas, tipos de archivos…

Además, es fundamental mencionar el término de la cadena de custodia, puesto que se emplea para normalizar que la evidencia no debe de alterarse durante el tiempo que se encuentra bajo la pertenencia de la policía. Por lo tanto, se generará un informe de custodia durante la etapa del procesamiento que recoge la forma en la que se ha realizado el proceso para cada uno de los archivos, es decir, desde su recepción hasta la salida. Generando la seguridad de que el contenido y los metadatos del propio archivo no se han visto modificados y garantizando que han sido mantenidos en las zonas apropiadas para evitar la manipulación de estos.

Por último, como se ha mencionado anteriormente se generará un informe de excepción que recogerá todos los archivos que no se han podido procesar, debido a que no se ha podido extraer su texto o los metadatos no representan imagen, así como para los archivos dañados, con algún tipo de virus, encriptados u otro tipo que no proporcionan información.

2.2.7. Revisión

Durante la etapa de revisión comprende el proceso de analizar la información obtenida anteriormente, con el fin de establecer el alcance, así como realizar un entendimiento sobre cuáles van a ser los métodos y procedimientos de la supervisión, teniendo en cuenta las diferentes herramientas que se ajustan al mismo.

Asimismo, la tecnología actual ha permitido que se desarrollen diferentes plataformas de revisión, con el objetivo de agilizar este proceso ante la gran cantidad de datos existentes, a través del reconocimiento de patrones y otros aspectos más avanzados.

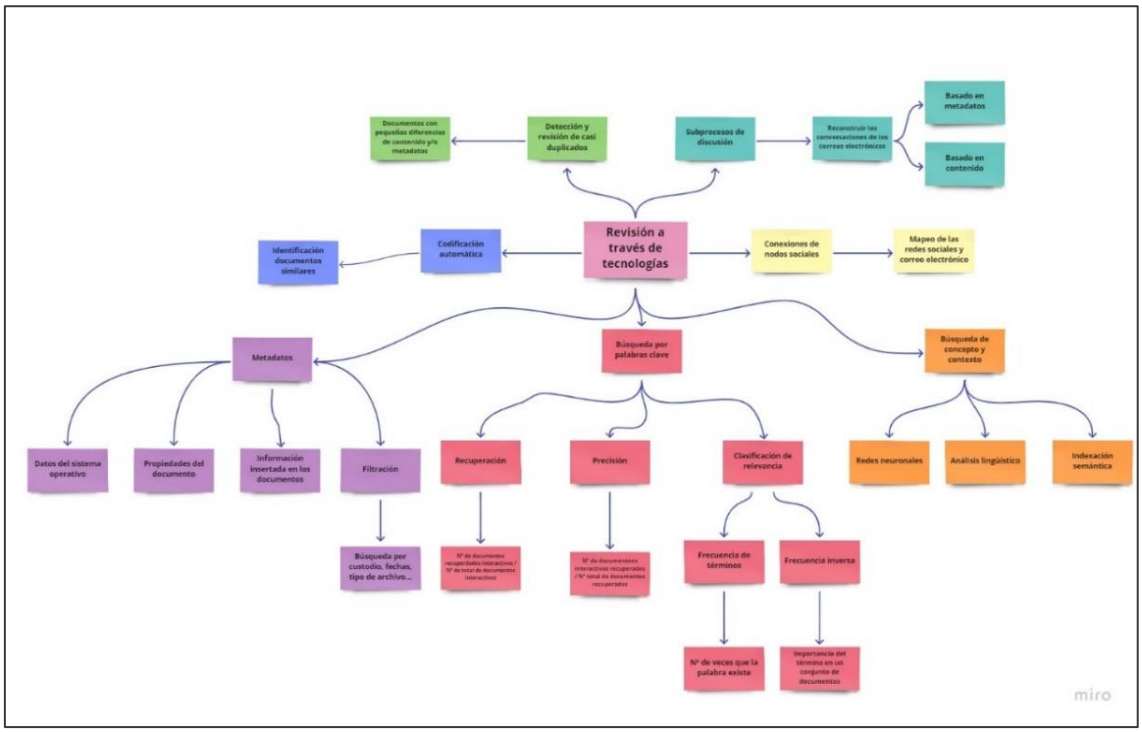
En esta misma línea, cabe mencionar que es necesario tener en cuenta una serie de factores a la hora de optimizar el proceso de revisión:

- Desarrollar una estrategia de revisión: Para ello, es necesario delimitar el perímetro de la revisión, mediante una recolección selectiva de los datos del custodio, filtrando los datos que han sido recopilados en base a ciertos criterios como fechas, palabras clave, así como mantener las fuentes *ESI* de forma original. De tal forma, que los focos principales de la revisión sea concretar qué se va a revisar, los métodos que se van a emplear y cuáles son los resultados que se esperan.

Posteriormente, es necesario establecer una serie de protocolos y flujo de trabajo en lo correspondiente a desarrollar unas directrices a la hora de organizar la información, como por ejemplo categorizar los documentos, realizar notas, distribuir la revisión de los documentos entre los distintos miembros del equipo estableciendo el cronograma a seguir, entre otras pautas para garantizar que el trabajo avanza de forma exitosa.

Además, cabe mencionar que en la actualidad gracias al empleo de las tecnologías el proceso resulta más rápido y eficiente que la revisión manual, así como propia el aumento de la calidad de la revisión al limitarse en base a palabras clave, metadatos... A continuación, se muestra un esquema que recoge los principales métodos para la revisión:

Figura 5: Esquema revisión a través de las tecnologías



Fuente: Elaboración propia

- Configuración de la sala de revisión: En función de las necesidades que se requieran para el caso, en ocasiones es conveniente establecer un lugar centralizado para la revisión. Por otro lado, existe la posibilidad a través de protocolos de comunicación que el equipo de revisión pueda teletrabajar o trabajar desde sus oficinas. En cualquier posibilidad, debe ser un lugar iluminado, ausente de ruidos o distracciones y además que no sea transitado.

En este sentido, resulta fundamental poseer la tecnología apropiada para realizar la revisión y que no propicie a la distracción. Así como asegurarse que tanto el hardware como el *software* requerido se encuentran correctamente instalados y han sido probados

previamente, por el líder de tecnología. Además, el equipo de revisión debe de disponer de una pizarra para definir nuevos procedimientos, o reglas, así como toda la documentación en cuadernos de anillas para mantener la información consolidada.

En otro orden de cosas, se establecen una serie de métricas de productividad para detectar desde el primer momento si se están produciendo problemas en el flujo de trabajo. Por lo tanto, se medirá el rendimiento del equipo teniendo en cuenta el número de documentos o páginas que completa cada revisor por hora, número de documentos que se marcan como confidenciales… entre otras. De esta forma, se tendrá conciencia sobre el estado del proyecto y los progresos que alcanza el equipo. Así como de aquellos revisores que realizan una revisión más exhaustiva o no a la documentación. No obstante, cabe mencionar que en función de los documentos a analizar se espera un rendimiento u otro.

Asimismo, durante el proceso de descubrimiento electrónico es fundamental tener en cuenta los costes que repercuten a los clientes, en relación con sus accionistas, así como capitales de riesgo. Por consiguiente, es necesario que el abogado realice un control exhaustivo sobre cada una de las fases que se lleven a cabo, manteniendo un control de los costes.

Por otro lado, dependiendo del caso se establecerá una herramienta de revisión u otra, por lo tanto, es conveniente analizar cuáles son los objetivos de cada uno de los proyectos con el fin de asignar la herramienta más adecuada, además de maximizar la potencia de la herramienta, en el sentido de que se trate de una revisión dinámica y continua para aumentar el ritmo del proceso y ayudar a las personas involucradas en esta.

En esta misma línea, es necesario designar al equipo que va a llevar a cabo esta fase, ya que deberá de variar en función de un proyecto u otro. Por una parte, se encuentra el abogado principal, que es aquel que tiene pleno conocimiento sobre los hechos acontecidos, así como las herramientas que se van a utilizar a la hora de realizar la revisión. Trabajará mano a mano con el proveedor, así como el departamento IT de la empresa. Además, de garantizar que la información analizada se trata de forma adecuada durante todo el proceso.

Otro de los factores para tener en cuenta, es si se trata de una revisión de una aplicación que se encuentra alojada de forma interna, o alojada en un proveedor de servicios. En esta misma línea, en función del asunto del proyecto se deberá recurrir a un equipo de expertos en esa materia, con el fin de comprender la documentación que se está analizando.

- Realizar análisis de datos/flujo de datos: Tal y como se ha comentado con anterioridad a la hora de seleccionar el *software* de revisión resulta esencial tener en cuenta sus características, de tal forma que cumpla los requerimientos exigidos para el proceso.

Por un lado, debería de permitir etiquetar o codificar los documentos de manera predeterminada o ya sea permitiendo la creación de un propio esquema de codificación. En suma, esta codificación debería permitir crear un código específico para aquellos documentos que requieran un trato especial debido a motivos de privilegios y confidencialidad. Por otro lado, la plataforma debería permitir realizar búsquedas de tanto de tipo booleano, como de texto y metadatos. Obteniendo los resultados de forma inmediata y ordenarlos en base a diferentes criterios.

En este sentido, algunos proyectos presentan documentación tanto de carácter electrónico como manual. Por ello, es conveniente seleccionar una plataforma proveedora de servicio que admita el manejo de los distintos formatos posibles.

Asimismo, el *software* debería permitir compartir o incluso imprimir. los documentos ante la ausencia de conexión. Por otra parte, con respecto a las funciones de carácter administrativo, la aplicación debe posibilitar crear nuevos usuarios, así como revisar los ya creados. De tal forma, que como se ha mencionado anteriormente, se muestre la productividad de estos, y tener constancia de los documentos que ya han sido revisados.

En esta misma línea, la herramienta debe permitir generar informes con el fin de conocer en todo momento el estado del proyecto y el avance que ha conseguido el equipo, la cadena de custodio, registros de privilegios y confidencialidad. Por un lado, convendría que hubiera informes de carácter diario y otros de carácter general.

Otros elementos para tener en cuenta para visualizar el flujo de trabajo serían incluir el resultado de *hits*, la posibilidad de realizar búsquedas a través de conceptos, visualización de correo electrónico…

- Revisión de conducta: Durante esta etapa se producen eliminación de aquellos documentos que no son relevantes, de tal forma, que se supriman para las revisiones que se van a realizar posteriormente o incluso eliminándolos de la propia base de datos.

Asimismo, debería posibilitar la selección de aquellas fuentes sobre las que no es necesario realizar un análisis, de tal forma que únicamente sean codificados los documentos que se requieran en base, al autor, las fechas o los destinatarios incluidos en el proceso de descubrimiento electrónico.

Una vez que se ha producido a realizar esta primera eliminación, conviene asignar los documentos a revisar para cada uno de los componentes del equipo. Por tanto, se pueden llevar distintas asignaciones simplemente bajo volumen, de tal manera, que se asignan un número de documentos para cada uno de los revisores. Sin embargo, en algunos casos conviene repartir la información a analizar a aquellas personas que sean especialistas en esa materia. También, existiría otro caso en el que se distribuyen bajo criterios de confidencialidad o privacidad.

Además, durante el proceso se requiere tener presente el idioma sobre el que van a estar los documentos en el caso de que aparezcan distintos idiomas, con el fin de detectar si es necesario contratar un equipo especialista que hable ese idioma, además, de que la propia aplicación permita el reconocimiento de texto en diferentes idiomas.

- Evaluación: Posteriormente, es necesario realizar a modo de resumen una evaluación sobre el estado general del proyecto. Teniendo en cuenta si se ha logrado conseguir los objetivos, así como la minuciosidad de la revisión. Clarificando aquellos documentos que se calificaron como privilegiados, si se ha encontrado alguno duplicado, cuál ha sido el coste general…
- Informes de estado y progreso: En el proceso que involucra los informes de estado, conviene tener en cuenta cuatro objetivos principales. Por un lado, la auditoría de entrada de control de calidad, con el fin de verificar que se hayan obtenido todos los documentos esperados, así como que se hayan tratado aquellos que han generado algún error. Además, de una estimación del alcance para cada uno de los archivos,

teniendo en cuenta los custodios, si existe duplicados, tipos de archivos, si es relevante…

Asimismo, poner en conocimiento cuál ha sido la eficiencia del revisor teniendo en cuenta las métricas mencionadas anteriormente. Y, por último, plasmar la fecha de finalización de la revisión, a modo de conclusión tras haber analizado la trayectoria comentada anteriormente.

Control de calidad: Con el fin de lograr una revisión que sea precisa y consistente se deberían de implementar controles de calidad a lo largo de las diferentes etapas del proceso. De esta forma, una vez que existe duda sobre un documento, que exista la posibilidad de marcarlo para poder realizar una segunda revisión sobre su codificación. Además, es conveniente que de manera diaria se puedan identificar los problemas relacionados con la revisión o con la comprensión de la documentación, con el objetivo de identificar y solventar lo antes posible.

2.2.8. Análisis

El análisis de las evidencias supone el comienzo por parte del equipo de *eDiscovery,* en la determinación de la estrategia y toma de decisiones fundamentada en datos sólidos. Se trata de una etapa que se puede implementar a lo largo de las distintas fases que involucra el descubrimiento electrónico. En este sentido, para tener un pleno conocimiento de los hechos y documentación recolectada o inclusive posible de obtener, sería recomendable incorporarla desde el inicio del proceso.

Por un lado, se realiza un análisis de contenido, en el que se estudia el contexto en que se han producido los hechos. Por lo tanto, será necesario comprender los sistemas de información de las empresas, teniendo en cuenta las políticas de retención de documentos.

Por un lado, es conveniente realizar revisiones sobre litigios anteriores o hechos relacionados pertenecientes al mismo sector, con el fin de determinar qué recursos proporcionan más información en el proceso de descubrimiento. Así, como establecer una serie de métricas con el fin de comprobar el tamaño de los datos, custodios que cumplen con la retención…

Posteriormente, realizar un análisis de los datos, con respecto a determinar qué datos deben mantenerse, para el posterior procesamiento, determinar el coste total de este trabajo y qué conclusiones se obtendrían de los mismos, a través de las entrevistas con los custodios, mapas de datos, listas de seguimiento, inventario de dispositivos….

En la actualidad, existen herramientas que permiten revisar los datos con el fin de comprobar si existen ciertos vacíos de contenido en los documentos, ordenar los documentos en base a las fechas o custodios.

Por consiguiente, el proceso se puede relacionar con el objetivo de lograr una mejora en la búsqueda de información. Es decir, la realización de análisis en tiempo real permite determinar la precisión real de los datos que surgen durante el descubrimiento. Para ello, es conveniente, la creación de métricas que relacionen los resultados obtenidos a través de distintas búsquedas, los elementos que se han ido eliminando, así como, la posibilidad de crear revisiones de mejora.

En esta misma línea, es necesario tener presente que la garantía de calidad durante el proceso de descubrimiento electrónico no debería olvidar en ninguna de sus etapas. Por tanto, tener presente desde un primer momento una buena calidad del análisis de la

información asegurará éxito en las decisiones basadas en fundamento y en la validación de los distintos métodos que el equipo ejecutará.

2.2.9. Producción

Hoy en día, la cantidad de información que se almacena de manera electrónica ha aumentado de forma considerable. De tal forma, que preparar las fuentes y evidencias en un formato adecuado y eficiente supone un requisito para contribuir en el proceso de descubrimiento electrónico.

Según establece la Regla 26 de las Reglas Federales de Procedimiento Civil es necesario que las partes lleguen a un acuerdo sobre cuál va a ser la forma de producción, de manera que resulte eficiente.

Cabe mencionar que existe un tipo de producción denominada producción rodante, que consiste en realizar un cronograma en el que se determinan las distintas etapas en las que se van a producir los datos, en vez de que se produzcan todos a la vez.

En otro orden de cosas, otro de los factores para tener en cuenta durante la fase de producción es seleccionar el formato en el que se van a producir los datos, con el fin, de realizar un análisis exhaustivo de la información de estos. Por lo tanto, se pueden distinguir diferentes formas de producción:

Tabla 4 Tipologías de producción

Tipo	Descripción	Ventajas	- Inconvenientes
Formato de archivo nativo	Producción de los archivos en el formato origen. Por ejemplo, archivos *Word* o *Excel*.	- Reduce costes y tiempo de conversión. - Recomendable en archivos de cálculo y base de datos pequeñas. - Se puede buscar los archivos. •	- No se pueden enumerar las páginas de forma individual. - No se puede marcar con endoso de confidencialidad. - Los metadatos pueden estar ocultos. - Se pueden alterar.
Formatos casi nativos	Archivos que se convierten en un formato de texto con una estructura, como *HTML*. Por ejemplo, los correos electrónicos.	- Reduce costes y tiempo de conversión. - Los archivos se encuentran en un formato adecuado para la revisión. - Se pueden buscar los archivos.	- No se pueden enumerar las páginas de forma individual. - No se puede marcar con endoso de confidencialidad. - Se pueden alterar.
Formatos de imagen	Consiste en convertir una fuente *ESI* o un papel, en un archivo digital. De tal forma, que no sea editable. (Es necesario consultar la fuente y el riesgo potencial).	- Permite numerar las páginas de forma individual. - Se pueden marcar las páginas con endoso de confidencialidad. - Reduce el riesgo de alteración de documentos.	- Existe un coste y un mayor tiempo de conversión de la imagen. - Hay archivos que no son propicios a este formato. - Existe riesgo de pérdida de datos durante la conversión de la imagen.

Papel	La fuente se mantiene en papel si era originalmente así o se imprime y produce en papel.	- Permite numerar las páginas de forma individual. - Se pueden marcar las páginas con endoso de confidencialidad. - Reduce el riesgo de alteración de documentos.	- Existe coste de conversión e impresión. - Aumenta el tiempo de respuesta en el procesamiento. - Hay archivos que no son propicios a este formato. - Existe riesgo de pérdida de datos durante la conversión. - No se puede buscar a partir de texto o base de datos. - No se puede regresar al archivo nativo.

Fuente: Elaboración propia

2.2.10. Presentación

La última fase del modelo EDRM se corresponde con la presentación, es decir, una vez encontrados los hallazgos, es necesario presentar dicha información ante audiencias judiciales, con el fin de validad los hechos y esclarecer los acontecimientos que han tenido lugar.

A la hora de identificar las pruebas durante la celebración del juicio, pueden presentarse en varios formatos como información en papel o en formato nativo. Asimismo, la parte anexa a los mismos puede encontrarse en cajas o en su defecto, en sistemas automatizados de soporte de litigios. De esta forma, se permite una mayor eficacia en la identificación y etiquetación de las pruebas. Estas pruebas sirven de base para apoyar o refutar los sucesos del caso.

En este sentido, es conveniente conocer el término de evidencia admisible. Se trata de cualquier prueba que se puede presentar en este caso a un juez o un jurado, con el fin de respaldar una parte del procedimiento presentado. Por consiguiente, debe de probar o desmentir un hecho que se discute, siendo lo suficientemente confiable.

Además de la autenticidad de las pruebas, resulta esencial el término referente a la cadena de custodia, de tal forma, que las pruebas durante todo el proceso que concierne el descubrimiento electrónico sean tratadas de manera adecuada, manteniendo la integridad de la información. Por consiguiente, se deberá de realizar una documentación sobre las condiciones bajo las que se recopilan las pruebas, así como las personas encargadas de estas, el tiempo de custodio y cómo ha sido el almacenamiento y el mantenimiento de estas.

Esta serie de pruebas van a contribuir en la reconstrucción de la escena del crimen, con el fin de desarrollar hipótesis y, finalmente concluir con sobre el delito. Por tanto, se distinguen tres áreas que se emplean para realizar el dibujo de los acontecimientos ocurridos. Por un lado, la reconstrucción de los incidentes específicos, en lo referente a la naturaleza del suceso que ha ocurrido. Por otro lado, la reconstrucción de los eventos, que se centra en establecer las conexiones entre los sucesos, la cronología y las personas involucradas en estos. Y, por último, la reconstrucción de la evidencia física, con el fin de determinar pruebas en base a los objetos que se encuentran en un estado físico.

En ocasiones, es necesario recurrir a declaraciones en las que se interroga (normalmente queda grabado en video) a aquellas partes que se encuentran estrechamente relacionadas con el proceso de investigación, y que, por tanto, pueden revelar información importante para incorporar en el caso.

Asimismo, desde el comienzo del proceso de descubrimiento electrónico hasta el momento en el que tiene lugar el caso, es primordial contar con un procedimiento bien definido en lo referente a las copias de seguridad y redundancia.

Por último, una vez que haya tenido lugar la audiencia y se haya obtenido un veredicto, es conveniente desarrollar una serie de pautas para proceder al archivado y almacenamiento de la información. En el caso de que se apelara, esta materia debe de permanecer de forma accesible y no enviarlo a una instalación de almacenamiento.

En otra instancia, se realizan informes periciales a través de los cuales un perito informático expone las investigaciones y los resultados obtenidos en relación con las evidencias digitales que ha encontrado. Se utiliza, por tanto, para demostrar o refutar los hechos acontecidos que suponen una elevada complejidad técnica; documentando el razonamiento elegido para fundamentar los hechos, así como las pruebas informáticas que lo respaldan.

2.2.2. Estándares ISO

La informática-forense también se encuentra estrechamente relacionada con la familia de estándares ISO. En concreto, en este apartado se centrará el foco en el estándar ISO 27001 e ISO 27037. Por un lado, la normativa ISO 27001 se especializa en la seguridad de la información, de tal forma, que establece un marco general con el fin de implementar una serie de controles para proteger la información en las fases definidas anteriormente de adquisición, preservación, análisis y presentación de las evidencias digitales. No obstante, presenta más utilidades más allá de la propia informática-forense, en este sentido, es utilizada por las empresas para consolidar su gestión de la seguridad de la información aplicada a los distintos ámbitos que componen el ciclo de negocio.

Por otro lado, la normativa ISO 27037 se centra en aspectos más específicos correspondientes a la informática-forense, guiando desde etapas tempranas hasta el final en el proceso de investigación. Por ejemplo, en la identificación de las fuentes de evidencias digitales, así como su preservación y mantenimiento. Realizando especial hincapié en la formación y capacidades del personal que se encarga de realizar el análisis que concierne en la investigación.

Bien es cierto, que ambos estándares presentan como objetivo garantizar la integridad y confiabilidad de los sistemas de la información, así como las posibles evidencias digitales. A continuación, se profundizará más sobre la relevancia y los aspectos que conciernen dichas normativas.

2.2.2.1. ISO 27001

La norma ISO 27001 [15] es el estándar internacional para la gestión de la seguridad de la información en las organizaciones, de tal forma, que se incluye tanto la información física como digital. Se trata de un estándar que incluye los requisitos establecidos para la identificación y tratamiento provocados por los sistemas de seguridad de la información.

La última versión de la 27001 se corresponde con el año 2015, sin embargo, en la Asociación Española de Normalización (UNE) aprobó una actualización en 2017. De este modo, se denomina UNE-ISO/IEC 27001.

En la actualidad, las empresas hacen frente a una serie de riesgos y vulnerabilidades que pueden tener diversos orígenes. En este sentido, la información que

manejan, y que, por consiguiente, supone su principal activo, se encuentra expuesta a una serie de amenazas. Por consiguiente, garantizar la seguridad de la información se corresponde de forma directa con la gestión correcta de una serie de cuestiones como son la elaboración de un plan de respuesta a incidentes, la realización de análisis de riesgos, la segregación funcional dentro de las empresas, la implicación de la dirección, la planificación y realización de controles, entre otros.

La normativa ISO 27001 tiene como objetivo la protección de la información bajo tres principios, la integridad, la disponibilidad y la confidencialidad. Por tanto, las empresas deben de realizar una evaluación de riesgos para detectar el origen de estos e impedir que se materialicen. Por tanto, la norma se estructura por un lado en la evaluación de riesgos, y por otro, en la aplicación de las medidas de seguridad adecuadas.

En lo que concierne la evaluación de riesgos, las empresas tienen definidos una serie de políticas, procedimientos y equipos de *software*. No obstante, en ocasiones no se utilizan o en su defecto, se aplican de forma segura. Es conveniente que tengan establecidas una serie de reglas para evitar los incidentes de seguridad. Estas reglas conciernen el ámbito de la tecnología, sin embargo, también incluyen el entorno de los recursos humanos, la protección física y jurídica, así como la gestión de los procesos. A través del plan de tratamiento de riesgos, podrán establecer una clasificación de estos bajo una serie de criterios como podría ser el impacto y la sensibilidad.

Por consiguiente, cabe mencionar que dicha normativa se enfoca en el ciclo de mejora continua, basado en Planificar-Ejecutar-Verificar-Actuar. Con el objetivo de que tras realizar las correspondientes evaluaciones de amenazas y riesgos que provoquen el peligro de la información, se apliquen las medidas y controles necesarios para mitigar o reducir las consecuencias de estos.

Tabla 5 Fases establecidas por la norma ISO 270001

Planificación	Ejecución	Verificación	Actuación
Definición de la política de seguridad	Implantación del plan de gestión de riesgos	Revisión de forma interna del Sistema de Seguridad de la Información	Adopción de las acciones correctivas
Establecimiento del alcance del Sistema de Seguridad de la Información	Aplicación del Sistema de Seguridad de la Información	Realización de auditorías internas del Sistema de Seguridad de la Información	Aplicación de las acciones de mejora
Realización de análisis de riesgos y amenazas	Implantación de los controles definidos	Establecimiento de indicadores y métricas	-
Selección de los controles a implementar	-	Realización de una revisión por parte de la alta dirección	-
Definición de competencias, mapa de procesos, autoridades y responsabilidades	-	-	-

Fuente : Elaboración propia

En esta misma línea, tomando como referencia los ejemplos referentes a los controles propuestos por el estándar ISO27001 en el Anexo A (del susodicho estándar), los controles que resultarían primordiales en el proceso de descubrimiento electrónico serían los siguientes.

- Adquisición, desarrollo y mantenimiento del sistema, entendidos como los controles que definen las pautas de seguridad durante el proceso de recopilación de las evidencias digitales, así como su soporte.
- Seguridad operativa, en lo que concierne los procedimientos y responsabilidades, las copias de seguridad de los dispositivos, el registro y monitorización de la actividad de estos, así como en los temas relacionados con el *malware* y explotación de vulnerabilidades.
- Criptografía, relacionada con el cifrado y establecimiento de controles de gestión de claves. Resulta esencial que los empleados cuiden los datos sensibles de sus dispositivos, no teniendo en un lugar accesible las contraseñas, información confidencial en espacios compartidos, destrucción de la información sensible de forma adecuada, así como la aplicación de contraseñas seguras en sus dispositivos bajo las políticas de buenas prácticas establecidas por la compañía.
- Gestión de incidentes de seguridad de la información, es decir, la definición de controles para identificar eventos anómalos, como la materialización de amenazas, definiendo las responsabilidades, realizando una evaluación del incidente. Así como, el procedimiento de respuesta y recuperación de las evidencias.
- Cuestiones de la Seguridad de la información en la gestión de la continuidad de las operaciones. En este sentido, se trata de realizar una planificación, implantación y revisión de un Plan de Continuidad Negocio, relacionado con la protección de la información de las empresas, así como asegurar la continuidad de las operaciones en el caso de que surja un incidente.
- Relación con los proveedores, es decir, establecer los acuerdos y políticas con los proveedores determinando qué aspectos se pueden incluir y supervisando los servicios de estos. Hoy en día, muchas empresas tienen externalizados algunos servicios de su actividad de negocio. Por tanto, conviene conocer al detalle la involucración en los procesos de negocio a la hora de conocer la información confidencial que tienen a su alcance.
- Cumplimiento de los controles exigidos por las leyes y el resto de los reglamentos que apliquen. En el tratamiento de la información de los sistemas de las entidades, resulta esencial proteger la propiedad intelectual de la misma, así como los datos personales, y, por ende, la información personal. Por tanto, en el tratamiento de los dispositivos y los datos de los custodios, es importante tener en cuenta este factor por la cantidad de información sensible manejada.

La certificación de las entidades bajo esta normativa supone una garantía a los clientes en la protección de los datos personales. Asimismo, a través de su aplicación correcta y la definición de los procedimientos adecuados permite evitar que las entidades sufran brechas de seguridad, suponiendo un mayor ahorro ante los incidentes que la inversión que supone la aplicación de los controles y las prácticas adecuadas.

2.2.2.2. ISO 27037

La normativa ISO/IEC 27037:2012 [10] se encuentra relacionada con las tecnologías de la información y seguridad. De esta forma, establece las pautas para el desarrollo de las actividades que implican la utilización de evidencias digitales, tales como el proceso de adquisición, almacenamiento, recopilación, preservación… con fines probatorios, con el objetivo de mantener la integridad de estas.

En este sentido, sirve como orientación a los equipos y organizaciones en el procedimiento disciplinar del manejo de las evidencias digitales obtenidas de los

siguientes dispositivos: medios de almacenamiento digital como discos duros, dispositivos electrónicos personales, ordenadores portátiles, redes basadas en TCP/IP u otros protocolos digitales, así como con aquellos dispositivos que presenten funciones similares a las mencionadas anteriormente.

Cabe destacar que la evidencia digital es gobernada bajo tres principios fundamentales: relevancia, confiabilidad y suficiencia. Dichos elementos definen la calidad de la evidencia digital en cualquier investigación. Por otro lado, los equipos involucrados en el proceso del manejo de las evidencias potencialmente digitales deben agruparse en base a los conocimientos y habilidades definidas, por tanto, se dividen en los especialistas de evidencias digitales de primera intervención (*Digital Evidence First Responder* / DEFRs), en especialistas en evidencia digital (*Digital Evidence Specialist* (DESs), especialistas en respuestas a incidentes y, en directores de laboratorios forenses.

Otro de los conceptos que la norma presenta es el término de cadena de custodia que se tratará en detalle más adelante; en lo relacionado a los requisitos mínimos establecidos para el mantenimiento de esta como, por ejemplo, el identificados unívoco de la evidencia, le personal que tiene acceso a la misma, así como el procedimiento establecido para su preservación.

Asimismo, resulta fundamental conocer el tipo de evidencia que se puede recopilar digitalmente. Dentro de este grupo se encuentran los documentos de los ordenadores, mensajes de texto, imágenes, correos electrónicos y sus correspondientes ficheros adjuntos, historiales de internet, metadatos, ubicaciones de dispositivos gracias a la publicación en redes sociales etc. Tal y como se comentó en profundidad anteriormente en el Modelo EDRM.

Con respecto a la recopilación de los dispositivos digitales, resulta fundamental determinar el entorno en el que han ocurrido los hechos, y, en consecuencia, en el momento en que la autoridad legal confirme el permiso para proceder a la confiscación de la evidencia, recolectar todos los dispositivos involucrados, así como sus correspondientes contraseñas, cargadores, cables periféricos y manuales correspondientes asociados.

En esta misma línea, existen una serie de pautas o recomendaciones a la hora de tratar los diferentes dispositivos para garantizar que no se produzca ninguna modificación en los datos almacenados en los mismos. Por ejemplo, en el caso de los móviles resulta fundamental realizar el apagado y proceder a retirar la batería en el caso de que fuera posible, para conservar la información de la ubicación, así como los registros de llamadas, evitando así la utilización del móvil, así como la activación de los comandos de destrucción remota.

De esta forma, resulta fundamental el tratamiento especial de los dispositivos, recurriendo a su aislamiento colocándolos en una bolsa *Faraday* u otro material de bloqueo, teniendo en cuenta que todos los sistemas de comunicaciones deben de estar desactivados. Además, deben de situarse en envases antiestáticos como, por ejemplo, bolsas de papel o sobres y cajas de cartón. Por tanto, se recomienda evitar el plástico debido a que puede transportar electricidad estática o permitir una acumulación de condensación o humedad.

Además, en el momento de enviar la información correspondiente al investigador se debe indicar por cada uno de los dispositivos el tipo de información que se busca, por

ejemplo, números de teléfono e historiales de llamadas, correos electrónicos u otro tipo de documentos.

La normativa establece una serie de pautas a la hora de realizar la exploración de los datos en el laboratorio, los analistas encargados de la recuperación y análisis de los datos deberán tener, por tanto, en cuenta estas consideraciones con el fin de evitar cualquier suceso que pueda interrumpir o perjudicar el proceso de investigación.

- Prevenir la contaminación. Estableciendo una analogía con respecto a la posible contaminación de la escena de un crimen, las evidencias digitales pueden presentar problemas similares relacionados con su proceso de recopilación.

En este sentido, como primera acción antes de proceder a realizar un análisis sobre la misma, es necesario realizar una imagen o copia del dispositivo, almacenada en otro medio para mantener su estado original. Además, los medios de almacenamiento deberán ser nuevos o en caso, de que se reutilicen debe de eliminarse toda la información que contenían previamente.

- Aislar los dispositivos inalámbricos. Tal y como se comentó anteriormente, conviene analizar los dispositivos en una cámara de aislamiento si fuera posible. En caso contrario, resulta primordial la utilización de una bolsa *Faraday*, así como activar el modo avión del dispositivo móvil, para evitar recibir cualquier intento de comunicación con el mismo.
- Instalar un *software* de bloqueo de escritura, con el objetivo de evitar cualquier modificación en los dispositivos o medios de almacenamiento, por tanto, el analista será el encargado de instalar el programa para que los datos únicamente se puedan visualizar, sin poder realizar ningún cambio.
- Seleccionar los métodos de extracción. Una vez que se ha realizado una copia de los dispositivos el analista determinará en función de las características del dispositivo (modelo, sistema operativo etc.) el software de extracción de información adecuado para analizar de forma más detallas los datos y su correspondiente contenido.
- Continuar con la investigación. Durante este punto, el analista comenzará con las labores de investigación, analizando los diferentes archivos, áreas ocultas o archivos que hayan sido eliminados. Asimismo, el analista puede recurrir a evidencias que residan en Internet, tales como salas de chat sitios web u otras redes de almacenamiento de información. [3]

2.3. Principales herramientas forenses

A continuación, en esta sección se van a definir las herramientas forenses más utilizadas hoy en día y varias de ellas las se van a utilizar en el caso práctico. Se van a diferenciar, por un lado, en herramientas de adquisición, herramientas de análisis y herramientas con las que se pueden adquirir y analizar evidencias. Sobre las herramientas de adquisición, se va a utilizar una u otra dependiendo del dispositivo que se vaya a querer adquirir. Para las adquisiciones de ordenadores y portátiles se va a utilizar la siguiente:

Logicube Forensic Falcon[11]: Es una clonadora forense de discos duros. Tal y como se puede ver en la imagen. El disco duro que se desea copiar se conecta en la parte

[3] Para más información: https://www.iso27001security.com/html/27037.html

izquierda de la clonadora, y en la parte derecha se colocan 2 discos duros destino, que son las copias forenses resultantes del disco origen.

Figura 6: Logicube Forensic Falcon

Fuente: Falcon®-Neo - Logicube [11]

Además, Falcon ofrece la posibilidad de ejecutar su software desde un dispositivo externo en el ordenador que se quiera adquirir. Esto se utiliza para los casos en los que sea imposible desmontar el ordenador y sacar su disco duro, ya sea porque lo tiene soldado o porque sea inaccesible. Un ejemplo de éstos pueden ser las *Microsoft Surface*. En caso de que algún custodio tuviera ese tipo de ordenadores, la opción que ofrece Falcon para adquirir su contenido es usar lo que se conoce vulgarmente en el mundo informático forense como "*Falconetti*". Esto es, *bootear* el ordenador con un USB que contine el software de la herramienta Falcon. Una vez conectado el USB al ordenador objetivo de adquirir, se requiere acceder a la BIOS de este para realizar el *booteable* y poner en marcha la adquisición del equipo.

Para la adquisición de dispositivos móviles, una de las herramientas más utilizadas en el mercado, y con la que se realizará el proyecto práctico es la siguiente:

***Cellebrite*:** Es una solución forense móvil integral, que permite a las fuerzas policiales, militares y de inteligencia, extraer datos de evidencia con solidez forense. La herramienta *Cellebrite* permite realizar varios tipos de adquisiciones de los dispositivos móviles [7]:

Tabla 6 Tipos de adquisiciones Cellebrite

SISTEMA OPERATIVO: Android	
TIPO DE EXTRACCIÓN	DESCRIPCIÓN
Física	Para permitir el análisis más completo y detallado del dispositivo, la capacidad de extracción física de *Cellebrite* accede a las capas de datos adicionales, que construyen la memoria física del teléfono. Estas capas incluyen tres grupos diferentes: 1) Contenido "lógico" no disponible a través de la API (por ejemplo, registros de llamadas. 2)Contenido borrado 3) Contenido que el teléfono recoge sin ninguna acción del usuario. Por ejemplo: redes *Wi-Fi*, ubicaciones GPS, historial web, etcétera

Lógica	La extracción lógica de los datos se realiza, en su mayor parte, a través de una API designada, disponible en el proveedor del dispositivo, la cual permite la extracción de datos desde el punto de vista forense. Tras la conexión, el UFED carga la API del proveedor correspondiente en el dispositivo. A continuación, el UFED realiza llamadas a la API de sólo lectura para solicitar datos al teléfono, como mensajes de texto (SMS), entradas de la agenda telefónica, imágenes, etc.
File System	Una extracción del sistema de archivos utiliza diferentes métodos específicos del dispositivo para copiar el sistema de archivos. Aunque estos son comparables a la API utilizada en los métodos lógicos, utilizan diferentes conjuntos de protocolos incorporados, dependiendo del sistema operativo. La combinación de protocolos a menudo difiere de una familia de dispositivos a otra.
SISTEMA OPERATIVO: iOS	
Física	Misma descripción que en la sección de *Android*
Lógica	Es posible que las extracciones de dispositivos *iOS* difieran entre la interfaz *UFED Touch*/*UFED 4PC* y el Analizador Físico *UFED*. Esto se debe a que el *UFED Touch*/*UFED 4PC* obtiene la interfaz de copia de seguridad de Apple *iTunes* utilizando su API, la Conexión de Archivos de *Apple* (AFC), la misma interfaz que se utiliza para hacer una copia de seguridad del dispositivo en un ordenador.
Lógica avanzada	*UFED Physical Analyzer* posibilita tres tipos diferentes de extracciones de copias de seguridad de *iTunes* ("*Advanced Logical*"). El método 1, como el *UFED Touch*, se basa en la copia de seguridad de *iTunes* utilizando la infraestructura de copias de seguridad de *Apple*. El método 2 extrae los datos de la copia de seguridad si el dispositivo está encriptado y el operador del *UFED* no conoce el código de acceso del dispositivo. El método 3 se recomienda tanto para los dispositivos encriptados como para los no encriptados con *jailbreak*

Fuente: Elaboración propia

Una vez realizada la adquisición o extracción de la información del dispositivo electrónico en un disco destino. Se procesa toda esa información con el programa ***Cellebrite Physical Analyzer*** [3], [4] que permite descifrar, decodificar, analizar y validar todos los datos digitales de una forma rápida y efectiva. Se verá con detalle su funcionamiento en el ejemplo práctico.

Después de haber llevado a cabo la fase del procesamiento de los datos, *Cellebrite* ofrece un programa para pasar a la fase de análisis y revisión del contenido, este programa es ***Cellebrite Reader***[5] **[4]**, el cual permite capturar todas las ideas y organizarlas de manera adecuada con el objetivo de generar informes personalizados con los hallazgos encontrados.

[4] Información sobre Cellebrite Physical Analyzer: https://bit.ly/3OoNzxn
[5] Información detallada sobre Cellebrite Reader: https://bit.ly/3NR4Mhe

Figura 7: Cellebrite Reader

Fuente: Sun-Denshi [18]

Existe otra herramienta de *Cellebrite* muy conocida cuya funcionalidad es la adquisición de ordenadores *Mac* de *Apple*. Para este tipo de ordenadores no se puede utilizar la herramienta *Logicube Falcon*, anteriormente descrita ya que éstos, presentan bastantes peculiaridades y son muy diferentes a los ordenadores con sistema operativo *Windows*. A continuación, se procede a describir las características de la herramienta:

Cellebrite Digital Collector* o *MacQuisition [2]: Es la única herramienta actualmente en el mercado que permite crear imágenes físicas descifradas de los últimos modelos de los ordenadores *Mac* de *Apple*, que utilizan el chip T2. Esta herramienta se ejecuta en el sistema operativo *MacOS X*, en el que realiza la adquisición de forma segura de diferentes modelos de computadora *Mac* en su entorno nativo. Sus principales características son[6]:

Recopilación de datos dirigida:

- Permite adquirir de forma selectiva contenido del correo electrónico, mensajes instantáneos y otros datos de usuario.
- Permite crear imágenes físicas de *Mac* con el chip T2 de *Apple*
- Permite autenticar los datos recopilados con las funciones hash MD5, SHA-1 o SHA-256

Recopilación de datos en vivo (*Live Systems*):

- Permite adquirir contenidos volátiles (Memoria RAM)
- Captura datos en vivo como contenido de internet, mensajes y archivos multimedia.

Creación de imágenes forenses

- Ofrece soporte para imágenes de unidades *APFS* (formato típico de archivos con sistema operativo *MacOS*) en discos *Fusion*
- Si el ordenador tiene FileVault2, con el uso de la contraseña o clave de recuperación, se puede montar el volumen en modo lectura.

[6] Características Digital Collector: https://bit.ly/3rpuxO5

También existen herramientas que permiten adquirir y analizar la información. Se van a presentar las más conocidas y más adelante en el caso práctico se verá el funcionamiento de alguna de ellas.

***Magnet Axiom Forensics*[7]:** *Magnet AXIOM [12]* está diseñado para recuperar, procesar y analizar pruebas digitales de diversas fuentes:

- **Dispositivos móviles:** Permite recuperar los datos de los dispositivos *IOS* y *Android* con el enfoque *artifact first* de *AXIOM* para obtener las pruebas más relevantes de las aplicaciones más populares.
- **Ordenadores/Laptops:** Permite recuperar datos borrados y analizar pruebas de dispositivos *Windows*, *Mac*, *Chrome* y *Linux*, incluyendo el historial del navegador y los archivos eliminados.
- **Plataformas *Cloud*:** Permite procesar y examinar los datos de las devoluciones de las órdenes judiciales, los archivos generados por los usuarios y los servicios en la nube en vivo, con artefactos de más de 50 de los servicios en la nube más populares.

Para llevar a cabo la fase de adquisición de la evidencia digital, dentro del paquete de *Magnet*, se utiliza la herramienta ***Magnet Acquire***.

Por otro lado, para la fase de procesamiento, se utiliza el programa ***Axiom Process***.

Finalmente, para la fase de análisis y revisión de las evidencias, se utiliza el programa ***Axiom Examine***. Todos estos programas se usarán en el caso práctico.

***FTK Imager AccessData*[8]:** *FTK Imager* [8] es una herramienta de *software* de previsualización de datos y creación de imágenes forenses que permite evaluar rápidamente las pruebas electrónicas para determinar si se justifica un análisis posterior con una herramienta forense como *Forensic Toolkit* (*FTK*). Por tanto, lo que realiza son imágenes forenses de diversas fuentes tales como: discos duros locales, CDs y DVDs, unidades de disco duro u otros dispositivos USB, carpetas enteras o archivos individuales. Además, genera el código *hash* de la imagen forense que nos será útil para la cadena de custodia de la evidencia.

***Encase Forensic*:**[9] *EnCase Forensic* [6] es una plataforma software de investigación y su función es recolectar datos digitales, realizar análisis, e informar sobre descubrimientos. Además, los preserva en un formato válido a efectos legales y siendo validado por los tribunales.

***Autopsy Digital Forensics*[10]:** *Autopsy* [1]es la principal plataforma forense de código abierto que es capaz de analizar todo tipo de dispositivos móviles y medios digitales. Presenta una arquitectura de *plug-in* que permite la extensibilidad de los módulos desarrollados por la comunidad o construidos a medida. Además, evoluciona para satisfacer las necesidades de cientos de miles de profesionales de las fuerzas del orden, la seguridad nacional, el apoyo a los litigios y la investigación corporativa.

[7] Características Magnet Forensics: https://bit.ly/43qocPR
[8] Información sobre la herramienta FTK: https://bit.ly/3JTSDH1
[9] Información sobre herramienta Encase: https://bit.ly/43ryzTi
[10] Información sobre herramienta Autopsy: https://bit.ly/3Dg5rEg

Para analizar un tipo de fichero, el *NTUSER.DAT*, que proporciona información acerca de la actividad reciente del usuario en un ordenador se utiliza la siguiente herramienta:

***ReggRipper*[11]: [13]** Es una herramienta portable cuya funcionalidad es la apertura de secciones de registro y analizar las mismas, produciendo un resumen legible en un fichero de texto. Este programa se suele utilizar para la apertura de ficheros como el *NTUSER*, para analizar la actividad reciente del usuario. Se analizará posteriormente en el ejemplo práctico.

Por otro lado, las herramientas más utilizadas del mercado para procesar la información adquirida de las evidencias digitales y su posterior revisión documental son las siguientes:

***Nuix Forensic*[12]:[17]** Es una plataforma de procesamiento de datos. El motor *Nuix* extrae los datos de las fuentes a nivel binario, los "unos y ceros", e indexa, analiza el texto y los metadatos de la evidencia. Es especialmente eficaz en el procesamiento de datos desordenados, no estructurados, junto con fuentes estructuradas y semiestructuradas. El motor *Nuix* utiliza tecnologías patentadas de procesamiento en paralelo para llegar al corazón de los datos con velocidad, escala y precisión forense. Aborda más de 1.000 tipos de datos y formatos de archivo en 10 dimensiones: comunicaciones, bases de datos, análisis forense digital y móvil, sistemas empresariales y en la nube, contenido generado por el ser humano, archivos de registro, multimedia, capturas de red, fuentes de medios sociales y en tiempo real, y comportamiento de usuarios.

***Relativity*[13]:** [14] Es una plataforma completa de *eDiscovery* que ayuda a los equipos jurídicos a resolver problemas de datos complejos durante los litigios, la investigación y los proyectos de cumplimiento. Viene con un conjunto de herramientas que ejecutan cada paso del proceso en las instalaciones y en la nube. También se integra con soluciones de terceros, permitiendo la creación de flujos de trabajo personalizados. Permite que varios usuarios reúnan, accedan y analicen estos datos desde diferentes fuentes, agilizando así el proceso legal. Tras la revisión, el software automatiza el proceso de producción en el que las partes implicadas intercambian datos no privilegiados, relevantes y que responden. Una vez adquirida, y procesadas las evidencias, *Relativity* es la plataforma donde se lleva a cabo la fase de revisión de la información para encontrar evidencias digitales para presentar en un juicios y litios entre otros.

[11] Información sobre herramienta Regripper: https://regripper.softonic.com
[12] Información sobre la herramienta Nuix: https://bit.ly/44tB21c
[13] Información sobre herramienta Relativity: https://bit.ly/46QDL6s

CAPÍTULO 3: DEFINICIÓN DEL PROCEDIMIENTO INFORMÁTICO

En consonancia con lo mencionado en los anteriores epígrafes, el procedimiento informático forense ha de realizarse manteniendo el foco en las guías de buenas prácticas. Muchas de estas recomendaciones están muy vinculadas a la confidencialidad de los datos manejados en las investigaciones forenses y las posibles repercusiones para las empresas y sus terceros.

Asimismo, cabe destacar que son varias las herramientas que pueden prestar los servicios necesarios. En este epígrafe también se comentarán las características intrínsecas de las distintas herramientas *software* y *hardware* y las ventajas aportadas a nuestro procedimiento informático-forense particular.

En paralelo a esto, cabe destacar que el procedimiento se va a realizar de la misma forma y bajo el mismo enfoque para cualquiera de los dispositivos que se realice, salvando las diferencias que conlleven las conforman. Este procedimiento poseerá una estructura similar respecto a las fases establecidas por el modelo EDRM [5] de referencia, ya que este estándar ha de ser seguido en toda investigación, diferenciado claramente las fases de identificación, preservación, adquisición, procesamiento, revisión, análisis y presentación de los resultados. Asimismo, se caracterizarán las actividades específicas, herramientas, técnicas y metodologías a emplear en cada una de las fases previamente mencionadas.

A continuación, se adjunta una tabla cuyo fin es organizar la información que ha sido extraída del estándar EDRM y cuál ha sido definida para este procedimiento específico.

Tabla 7: Tabla comparativa Modelo EDRM y procedimiento definido

Objeto	Común	Distinto
Fases	Se establece la misma agrupación de las fases	Describe cómo han de realizarse de manera específica, estableciendo herramientas, metodologías y buenas prácticas específicas
Herramienta	No se especifica la necesidad de establecimiento de una herramienta de gestión.	Se ha establecido una herramienta que ayuda a la gestión, tanto de personas, cómo de casos. Asimismo, también servirá de soporte técnico para validar el procedimiento.
Legal	No se basa en un marco legal específico.	Centrado en marco legal español.
Expertise	El *expertise* que sustenta el procedimiento es una organización de sobrenombre.	Se añade el *expertise* y buenas prácticas establecidas en el estándar EDRM, así como pequeñas especificaciones técnicas y tácticas basada en la breve experiencia de los responsables de la realización del procedimiento.

Fuente: Elaboración propia

3.1. Propuesta de procedimiento informático-forense

Antes de comenzar con el establecimiento de las fases, se van a destacar tres factores fundamentales durante todo el proceso y que van a apoyar y validar todas las conclusiones obtenidas. Sin estos mecanismos, no se podrían aportar como pruebas

válidas las obtenidas durante toda la investigación, puesto que no se podría garantizar la integridad e inalterabilidad de los datos adquiridos.

- Cadena de Custodia. Ya mencionada anteriormente, permite garantizar que los datos no han sido modificados ni eliminados por terceros. Permite asegurar la integridad, completitud y adecuación de los datos. Entre estos mecanismos se incluyen la presencia de notario en la adquisición, una correcta auditoría del laboratorio que contiene la información (asegurando así que se cumplimenta lo establecido en la ISO 27001 y buenas prácticas de almacenamiento de la información).
- GDPR y la Protección de Datos. Gracias a esta norma establecida a nivel europeo se garantiza la protección de los datos en el ámbito penal. En lo relativo a la adquisición, cabe destacar que hay ciertos automatismos que se realizan para no vulnerar los derechos de las personas.

Se van a realizar búsquedas por palabras clave, para sólo revisar los documentos relacionados con los ámbitos de la investigación, alejándose así de posibles conversaciones privadas. En paralelo a esto, cabe destacar el carácter de los equipos manejados por la empresa, que son prestados a los trabajadores con el fin exclusivo de realizar las funciones necesarias en el día a día. Esto debe quedar reflejado en un papel en el momento de la entrega de los dispositivos para asegurar el conocimiento de este factor por parte de los empleados.

Por último, la "empresa encargada de la investigación", también deberá contar con mecanismos que garanticen que los empleados realicen sus funciones con la debida confidencialidad para unos datos de dicha sensibilidad.

A continuación, se procede a documentar los pasos establecidos en nuestro procedimiento informático-forense. Si bien es cierto que la mayoría de las investigaciones tendrán muchas directrices coincidentes, los resultados dependerán de muchos matices desarrollados en el proceso.

3.1.1. Identificación de las evidencias

Se trata de conocer cuáles son los medios informáticos potencialmente vinculados a contener los datos relevantes para la investigación y que demuestren la culpabilidad/inocencia de cada uno de los actores. Para un mayor entendimiento de las cuestiones relativas a esta fase, se deberá consultar con anterioridad el apartado *2.2.3 Identificación* explicado anteriormente.

En este caso, y tras el correcto entendimiento del diagrama de la empresa, así como su parque tecnológico, los dispositivos a adquirir variarán en cada una de las investigaciones. Es de vital importancia la capacidad crítica del investigador de cara a identificar las fuentes relevantes, sin ser necesario analizar todo dispositivo informático que este encuentre (ya que conllevará una gran cantidad de esfuerzos monetarios y temporales), pero asegurando que ninguna fuente relevante se queda fuera del alcance de la organización.

Un ejemplo ilustrativo de este aspecto podría ser un ordenador para el que se desea analizar una posible fuga de información. Si el empleado posee algún disco electrónico extraíble, es muy interesante identificar este como posible evidencia ya que puede aportar mucha información adicional a la conseguida tras el análisis del propio ordenador del empleado.

Un correcto entendimiento de la estructura de la organización, así como su parque tecnológico se obtendrá tras múltiples reuniones de entendimiento con el empleado. De

nuevo la capacidad crítica ha de ser empleada en esta fase de cara a identificar y escoger la información relevante transmitida en las múltiples reuniones de cara a agilizar el proceso y evitar pérdidas de eficiencia.

Cómo estándar, previo al comienzo de la investigación, se identificarán los actores potencialmente involucrados en la investigación y se mantendrán conversaciones con el equipo técnico de la empresa para conocer cómo esta se encuentra conformada y los dispositivos que el usuario posee para realizar las tareas que conlleva su puesto. Siendo así potenciales fuentes de información, cualquier medio físico o virtual en el que se pueda almacenar datos de cualquier tipología.

3.1.2. Recolección y preservación de la evidencia

Una vez recolectados los dispositivos informáticos tras la determinación de su potencial importancia para la investigación, es de vital importancia una correcta preservación de la evidencia para mantener y asegurar la cadena de custodia. En caso de realizar este paso de manera errónea, los datos no se podrán considerar válidos ni probatorios de cara a un juicio o cualquier proceso relacionado.

Esta preservación da comienzo en el mismo instante que el comité de expertos informáticos identifica las evidencias. Es por ello por lo que en el momento de la recolección de los dispositivos se ha de realizar una correcta identificación de todos los dispositivos, los custodios a los que estos pertenecen, la fecha en la que se realiza esta acción, incluir fotografía y argumentar la importancia de la recolección del dispositivo. Esto permitirá aclarar todos estos conceptos en un futuro y es necesaria para la correcta identificación del dispositivo en todo momento del análisis.

En la mayoría de las ocasiones, en vez de llevarse tras la identificación el dispositivo al laboratorio forense, se realizará una copia de estos, que ayudará a que el manejo sea más sencillo.

Los mecanismos establecidos en nuestro procedimiento para garantizar de manera efectiva la preservación de la evidencia y así una correcta cadena de custodia son los siguientes:

- Realización de las copias forenses ante notario. El papel de esta figura es fundamental para demostrar que los datos trabajados son idénticos a los obtenidos el día de la adquisición. El notario toma un papel de tercero que valida todo el proceso.
- Realización de dos copias forenses en el momento de la adquisición. Al realizarlo de esta manera, se puede dejar una en depósito y obtener otra para trabajar en ella, garantizando así en todo momento que una copia original de los documentos se encuentra inalterada y bajo la custodia de un notario. En todo momento se podría volver a obtener las conclusiones obtenidas al final del análisis de la copia inalterada almacenada en el notario.
- Cálculo del código Hash para todos los contenidos adquiridos. Pese a que a nivel técnico es un identificador único que demuestra la validez de todo el proceso de adquisición, hoy en día, no obtiene la importancia necesaria en los juzgados. En nuestro caso particular se tendrá en cuenta los códigos hash MD5 y el SHA1, esto se realiza ya que la combinación de ambos ha demostrado ser una de las técnicas de *hashing* más probadas a nivel informático. Si bien la elección de ambos puede aumentar los requerimientos de procesamiento, la elección exclusiva de un solo algoritmo podría concluir con algunas colisiones acontecidas por el algoritmo MD%, del que múltiples estudios aseguran no ser fiable al cien por cien tras el amplio crecimiento del sector informático.

Sin todos estos mecanismos todo el análisis podría verse negado de validez. Un simple ¿Y cómo puede usted demostrar que toda esa información pertenece al equipo que comenta y no es una prueba inventada? Podría arruinar todo el trabajo realizado.

Cabe añadir que, si bien el proceso de preservación comienza en el mismo momento de la adquisición y acompaña durante todo el proceso de la investigación informático-forense, este puede llegar a terminar mucho más tarde de finalizar los estudios de los dispositivos realizados.

Para la correcta gestión y preservación de todo el material, es muy importante que todo el contenido empleado esté correctamente inventariado y que todo este proceso esté correctamente documentado. Para ello se definen las siguientes prácticas esenciales en nuestro procedimiento informático-forense.

La aplicación que sustenta este procedimiento permitirá, una vez terminado el análisis y entrega de resultados del procedimiento, el archivado del caso Cuando un procedimiento se archiva, se continúa almacenando su información y todo lo asociado al mismo, aunque la investigación ya haya finalizado.

En el ámbito judicial, esto es de vital importancia ya que, en caso de eliminar toda la información relativa al caso, en caso de haber una reapertura del expediente por la fiscalía, se podría haber pedido trazabilidad de todo el proceso previo llevado a cabo.

3.1.3. Adquisición

En esta fase se van a copiar las fuentes encontradas en la fase de identificación de las evidencias. Como bien se ha comentado en epígrafes anteriores, la realización de la copia es estrictamente dependiente de la tipología de la memoria que se desea adquirir.

Para este momento, es de vital importancia documentar fotográficamente todo el proceso. La adquisición puede resultar fallida y supondría una falta probatoria de cara al juicio una mala documentación de todo el proceso llevado a cabo. Habitualmente el principal soporte para validar el proceso es la realización de la copia ante notario, acompañado de la correcta documentación tanto de la copia, como de los códigos hash correspondientes.

Para este procedimiento se va a realizar un diagrama que engloba la distinta casuística que se puede encontrar el perito informático a la hora de realizar la adquisición y como ha se ha de proceder en cada caso.

Antes de comenzar, es necesario conocer determinados conceptos para poder comprender el diagrama adjunto:

- Copia en frío, el sistema origen permanece apagado, una ventaja de este tipo de copiado es que se resguardan los datos y no se corre el riesgo de alterar la información. Es usado como estándar durante un análisis forense informático.
- Copia en caliente, el sistema origen sigue encendido, es una práctica que se realiza en la mayoría de los casos sobre discos cifrados y, por tanto, existe el riesgo de que se altere la información, es por ello por lo que se realiza solo en casos especiales o extraordinarios. Con este tipo de adquisición o copia se puede realizar un volcado de la memoria volátil.

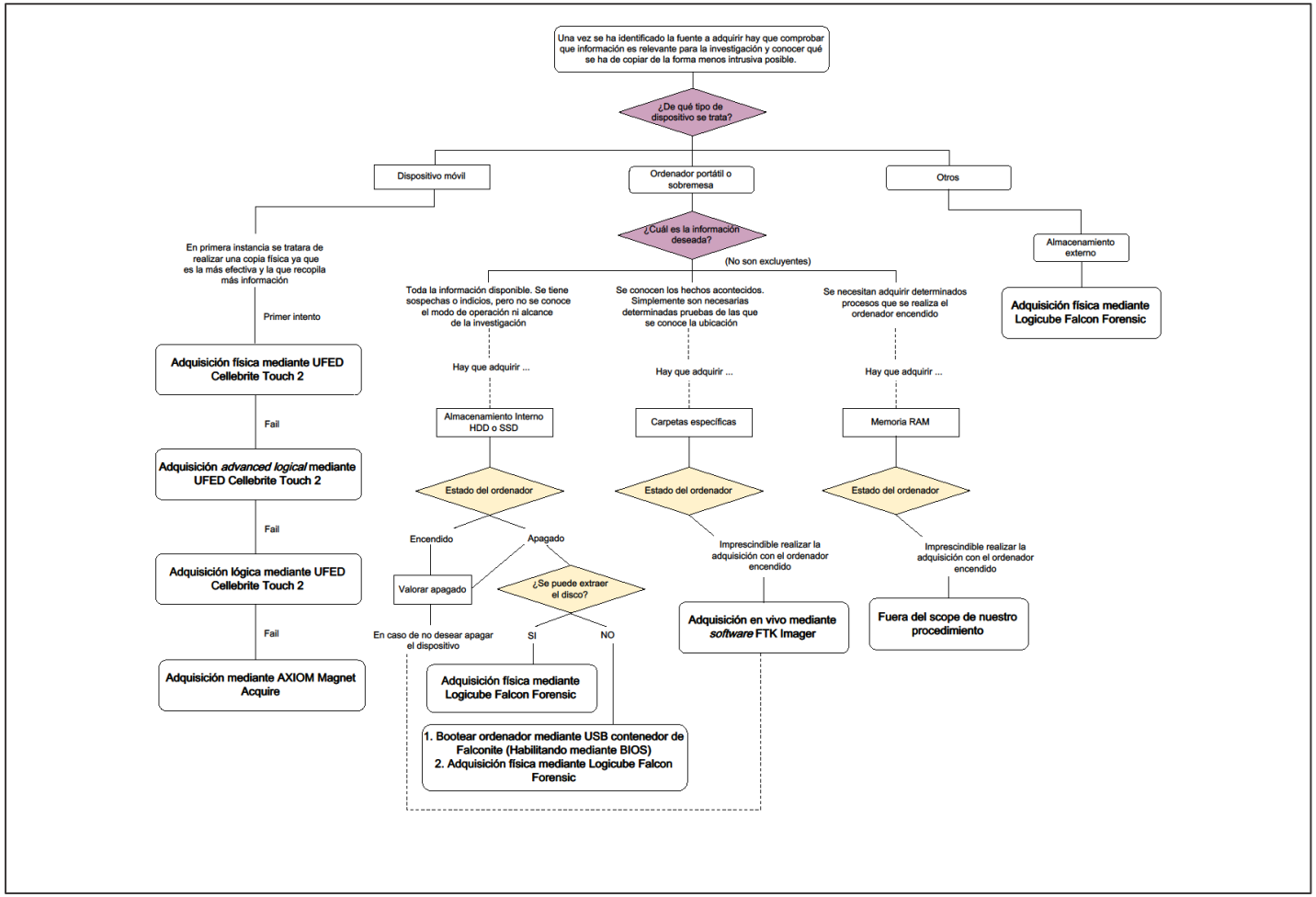
Una evidencia digital puede ser modificada muy fácilmente, dañar o destruir, durante un análisis forense es indispensable crear una copia exacta del dispositivo que resguarda la información que se desea analizar. Para esto existen algunos tipos de copiados.

- Copia *bitstream* o *bit-stream*; también conocido como *binary sequence* o secuencia de binarios, es una copia que va bit a bit tomando el contenido, es una copia fidedigna y exacta.
- Imagen *bit-stream*; a diferencia de la copia *bitstream*, la imagen contiene "una instantánea a modo de imagen". Hay varios formatos que pueden contener esta imagen, siendo el más conocido el denominado E01. Asimismo, esto se puede realizar sobre el disco entero o una partición específica. Tras esto se obtiene una imagen forense, que ha de ser "montada" con cualquier software específico (i.e. FTK Imager) para poder observar la estructura de archivos contenidas en la imagen forense.

Asimismo, cabe mencionar que la copia, en función de los requisitos iniciales, se puede realizar mediante *software* o *hardware*, siendo la segunda la preferible de las dos por cuestiones del tiempo que se tarda en realizar el proceso, así como la sencillez y métodos de comprobación del proceso posteriores.

A continuación, se adjunta un diagrama de las tomas de decisiones a seguir en caso de encontrarse ante una adquisición en base a nuestro procedimiento informático-forense. Esto dictaminará cómo se ha de actuar en base al tipo de tecnología de la que se quiere extraer la información.

Figura 8: Diagrama de decisión del procedimiento informático forense



Fuente: Elaboración propia

Añadiendo una mayor información al diagrama mostrado anteriormente, las adquisiciones se van a dividir en dos subgrupos mayoritarios en función de los tipos de dispositivos que se van a adquirir (dejando a un lado el resto de las casuísticas). Estos pueden ser:

- **Dispositivos móviles.** La primera opción siempre será la adquisición mediante la herramienta *Cellebrite UFED Touch* 2. Este dispositivo es capaz de extraer prácticamente toda la información de los dispositivos móviles y más aún si estos son de última generación. La información contenida en los dispositivos móviles suele estar almacenada en base de datos y de forma encriptada, por lo que su extracción a veces presenta dificultades. Este aparato recolecta toda la información almacenada en el dispositivo móvil y su herramienta de procesamiento es capaz de relacionar las distintas bases de datos con las aplicaciones correspondientes y desencriptar de manera efectiva toda la información.
    - Esta herramienta es utilizada por los cuerpos militares, fuerzas militares y cuerpos de inteligencia para realizar el análisis de dispositivos móviles y por eso ha sido la seleccionada para este procedimiento. Sus mejores características que la diferencian de la competencia son su portabilidad y velocidad para todo el proceso. Existen algunos problemas que pueden imposibilitar la adquisición con esta herramienta:
        - No se conocen las credenciales de acceso al dispositivo móvil y este posee una configuración que imposibilita la lectura de los datos. La herramienta tratará de *crackearlo,* pero en ocasiones no lo realiza de manera exitosa o no consigue extraer la información de todas las aplicaciones.
        - El dispositivo es muy antiguo y la base de datos encargada de adquirir la información no es capaz de reconocer la estructura de carpetas existente en el teléfono.

Adicionalmente, en caso de no poderse adquirir mediante esta herramienta o que la adquisición no se haya podido ejecutar de manera completa, se realizará una segunda adquisición mediante el *software AXIOM Acquire* del proveedor *Magnet Forensics*.

- **Ordenadores (portátiles y sobremesa).** Este tipo de adquisiciones se tratará de realizar con el equipo apagado siempre que los requisitos *hardware* lo permitan, es decir, el disco no esté soldado a la placa y se pueda extraer de manera efectiva para conectar directamente a la clonadora forense *Forensics Falcon* de *Logicube [11]*.
    - La realización de esta técnica es la más efectiva existente hoy en día. Su característica fundamental es la velocidad y permite dejar el dispositivo adquiriendo sin necesidad de estar atentos a fenómenos como que el ordenador no se bloquee, no se le acabe la batería, etc.
    - En caso de que no se pueda realizar dicha tarea, será necesario acceder con una cuenta de administrador al ordenador e instalar la herramienta *FTK Imager* [8]. Desde esta se podrá adquirir la información contenida en el disco completa o distintos directorios que fueran de interés para la investigación.

Independientemente de la técnica empleada en cualquiera de las adquisiciones llevada a cabo, será muy importante almacenar de manera adecuada los códigos *hash* resultantes tras la adquisición. Este será el mecanismo que permita comparar la

información de la fuente origen o dispositivo electrónico a adquirir, con la información contenida en el disco duro destino, es decir la imagen o copia forense. Este proceso es de suma importancia y ha de estar correctamente documentado.

Cae mencionar, que, dado el panorama actual de la informática respecto a la legalidad, un código *hash* no es reconocido como única prueba para que una adquisición ha sido realiza de manera adecuada y completa. Si bien el código *hash SHA256* (*MD5 + SHA1*) es inalterable con la tecnología existente hoy en día a nivel técnico, y obteniendo un *hash* del contenido del disco origen y otro para el disco destino, en caso de ambos coincidir se puede afirmar que ambos contenidos son idénticos, hoy en día la justicia no acepta este fenómeno como prueba suficiente para validar el proceso y continúa siendo necesario la existencia de la figura del notario.

3.1.4. Procesamiento

En esta etapa sucede lo mismo que en la anterior y en función de la metodología aplicada para extraer los datos y la imagen forense correspondiente, habrá que procesar con una herramienta u otra.

El procesado se realiza con el objetivo de extraer toda la información contenida en el ordenador y que se ha copiado del dispositivo. Hay diversas herramientas capaces de realizar este proceso, pero de nuevo se realiza una agrupación.

- **Dispositivos móviles**. Si la información se ha adquirido empleando la herramienta *hardware Cellebrite UFED Touch 2* será necesario el procesado de la imagen resultante en un *software* realizado por la misma empresa denominado *Cellebrite Physical Analyzer*. Esta herramienta es capaz de leer la información contenida en las bases de datos encriptadas que se encuentran dentro del teléfono y que han sido adquiridas en formato *"ufdr"*, convirtiendo está información en legible de cara a su posterior análisis.
    - Ya que cada dispositivo móvil y programa contenidos en estos poseen una variedad inmensa, es de vital importancia siempre mantener actualizado este *software* para que sea capaz de leer de manera efectiva la información almacenada por las distintas aplicaciones. De no realizar este proceso de forma efectiva es muy probable que se obtenga menos información de la realmente adquirida (i.e. faltan conversaciones con ciertos participantes, ausencia de mensajes dentro de conversaciones existentes, etc.)
    - Por otro lado, si la copia no se ha podido realizar con la herramienta mencionada y en su defecto se ha realizado con el *software AXIOM Acquire* de la marca *Magnet Forensics [12]*, se ha de realizar su procesado con la herramienta *AXIOM Process* de la misma marca.
- **Ordenadores (portátiles y sobremesa).** En la mayoría de las ocasiones, la información obtenida tras la adquisición de esta tipología de dispositivos será de un elevado tamaño, por lo que la sofisticación del procedimiento se dota de una mayor importancia.
    - En primer lugar, se realizará una pequeña fase de *"*preprocesamiento*"* que se realizará de una forma ligera mediante la herramienta *Encase Forensics* de *Opentext [6]*. En esta fase inicial se recuperarán todos los documentos contenidos en la imagen forense adquirida y se realizará la recuperación de los ficheros borrados del dispositivo mediante técnicas automáticas implementadas por la aplicación de *data carving*.

En esta fase se obtiene la totalidad de los ficheros contenidos y recuperables de un ordenador. En caso de que de algunos documentos borrados sólo quede la cabecera disponible derivado de un pisado de los datos, será posible visualizar el título de estos.

Derivado de la obtención de un elevado número de documentos, será necesario crear un *script* de filtrado de documento para obtener exclusivamente los ficheros deseados y descartar documentos correspondientes a archivos de sistema o sin información legible. Para nuestro procedimiento se aprovecharán las opciones de filtrado de la herramienta empleada para el "preprocesamiento" y se obtendrán sólo ficheros cuyo contenido no sea vacío, no se correspondan con ficheros de sistema y los documentos posean extensiones relevantes para la búsqueda.

Tras el filtrado de los documentos y la obtención del *scope* de documentos deseado para la investigación, se exportarán toda la información bajo una imagen forense cuyo formato será el denominado "*.L01*" compatible con la siguiente herramienta de procesado que se utilizará.

- Una vez obtenida dicha imagen se realizará el procesamiento de manera más exhaustiva mediante el *software Nuix* de *OnData [17]*. En este paso, se realizará un nuevo procesamiento de manera que se extraigan todos los "subdocumentos" obtenidos en el "documento padre". (i.e. se obtienen todas las imágenes contenidas en un PDF, o adjuntos contenidos en una conversación de correo).

Posteriormente y en dicha herramienta se realizará otro filtrado de documentos, con el objetivo de limpiar los datos de nuevo, mediante la exclusión de ficheros extraídos de los documentos padre y que se conocen que no poseen valor para la investigación.

Por último, se emplean técnicas de indexación de los contenidos para poder realizar búsquedas inteligentes, así cómo se aplicarán técnicas de Reconocimiento Óptico de Caracteres (OCR) a aquellos documentos que no poseen un texto plano asociado. Esto se realiza para que las imágenes y PDF mayoritariamente también puedan ser encontrados mediante técnicas de búsqueda masiva (i.e. buscar contenidos dentro de un PDF que posee el texto almacenado como imagen, realizar una búsqueda en los correos que posean adjuntos una firma correspondiente insertada como imagen, etc.).

- Tras esto, se pueden visualizar todos los documentos de una manera adecuada, habiendo conseguido una limpieza exhaustiva y una recuperación de datos en base a fuentes de conocimiento de inteligencia del ámbito.
- Por otro lado, y en lo referente a la actividad llevada a cabo por el sistema operativo en los comúnmente denominados artefactos forenses se va a realizar un procesamiento mediante la herramienta *Magnet AXIOM Process*. Este proceso extraerá los distintos *hives* del sistema en los que se almacena información de vital importancia para el análisis (i.e. fechas de modificación y creación de documentos contenidos en el sistema, actividad llevada a cabo por los usuarios, registro de los eventos de *Windows)*.

Por ello se puede apreciar de nuevo las dos grandes vertientes contenidas en la informática forense como son el *eDiscovery,* cuya finalidad más destacada es la revisión de una gran cantidad de documentos, así como la técnica denominada *Computer Forensics* que se centra más en extraer información de los artefactos contenidos por los sistemas operativos para su análisis en profundidad y el planteamiento de los hechos acontecidos.

En función de lo que se desea extraer del procesado y el volumen de documentos manejados, se configurará el programa con unas condiciones u otras. Para el correcto entendimiento de las condiciones utilizadas en nuestro procedimiento informático forense, consultar *ANEXO 5: PROCESAMIENTO EN NUIX DE LOS PORTÁTILES*

Asimismo, es de vital importancia establecer una metodología correcta de actualizaciones de los sistemas y una correcta configuración de estos. En caso contrario la información analizada será parcial y este suceso no será notificado por los revisores, por lo que el análisis final estará sesgado a la información parcialmente extraída.

3.1.5. Revisión y análisis

Esta sección es de vital importancia y dota de valor a todo el trabajo previo realizado. En este momento se analiza el contenido de todas las fuentes de información adquiridas y procesadas previamente.

Cómo se anticipa en el epígrafe anterior, este análisis tiene dos grandes subapartados en función del objetivo de análisis y los mecanismos empleados para ello. Esto son:

- ***eDiscovery.*** Esta técnica está muy ligada a la gestión documental y el análisis masivo de documentos. Al extraer toda la información contenida de los dispositivos electrónicos fruto del análisis se obtiene una gran magnitud de documentos los cuales se encuentran repetidos entre los distintos dispositivos o incluso uno mismo.

En esta parte es necesaria una correcta gestión de las expectativas del cliente (ya que esto fijará cuanto se ha de cerrar el *scope* de documentos a revisar) así como un correcto entendimiento de qué se busca realmente para realizar un filtrado adecuado de los documentos.

Los *scripts* realizados en la etapa de procesado facilitan este análisis con una limpieza general, pero se ha de afinar aún más en la búsqueda efectiva de información en los documentos ya que en cada investigación se han de revisar una tipología de documentos concretos.

Las dos grandes técnicas empleadas para esto son:

  - Deduplicación automática de documentos. Dado que los ficheros se encuentran en numerosas ocasiones tanto en un dispositivo (pero distintas ubicaciones o con distinto nombre) cómo en los documentos del resto de compañeros, es de vital importancia una correcta deduplicación basada en el contenido.

Para ello, el propio programa de *Nuix*, que será donde se realice el análisis de documentos, posee la funcionalidad de deduplicación de los ficheros por código *hash,* haciendo así que cada documento sea revisado sólo una vez.

En paralelo a esto, cabe destacar la existencia del término familias. Una familia de documentos está formada por un fichero “padre” que contiene otros

documentos en sí mismo (sus adjuntos). El ejemplo más claro de esta situación es un correo en el que se han adjuntado dos archivos. Es importante tener estos documentos juntos para su mejor análisis (un ejemplo sería una hoja de cálculo adjunta mandado al contable. El fichero adjunto no tiene contexto suficiente, ni el mensaje puede aportar valor completo a la investigación) y la deduplicación ha de tener en cuenta estas familias para no romper estas y que no se pierda información en el camino.

    - Búsquedas por palabras clave. Esto permitirá garantizar la privacidad del investigado ya que sólo se revisarán los documentos que atañen a la investigación, así como que se revisarán algunos documentos y no la totalidad de ellos.

Una correcta elaboración de una lista de palabras clave hará que los documentos analizados sean los justos y necesarios. Es importante no pasarse por defecto ni por exceso ya que cuanto más complejas sean las búsquedas, más precisos serán los documentos analizados, pero también habrá una menor cantidad de ficheros.

Las búsquedas por palabras clave se realizan mediante el *plugin SearchModule* contenido en dicha aplicación y que permite realizar búsquedas por palabras clave mediante el uso de búsquedas *booleanas* (i.e. factura AND fraude, modific* ficheros, etc.).

- ***Computer Forensics.*** En diferencia a la técnica mencionada anteriormente, este proceso trata de recomponer los hechos acontecidos a través de la reconstrucción de determinados artefactos que poseen los distintos Sistemas Operativos y que arrojan alguna de la información registrada. Si bien las anteriores labores son realizadas por equipos multidisciplinares, esta fase va a ser realizada por un equipo técnico, que ha de saber adaptarse a múltiples entornos y poseer una gran visión en esta materia.

Las capacidades de adaptación del equipo son esenciales ya que hay que saber adaptarse y conocer a un nivel experto cualquier dispositivo que pueda ser revisado. Cada dispositivo, aplicativo o sistema operativo registra la información de la actividad acontecida de una manera totalmente distinta.

Uno de los principales artefactos analizados habitualmente en estas investigaciones y que son quizás las más conocidas por todos los usuarios técnicos son los registros de eventos en los sistemas operativos *Windows.* De estos registros se puede extraer una gran cantidad de información.

Sin embargo, este no es el único artefacto de interés con el que cuenta el equipo de análisis. Si bien cada uno será analizado en función de la tipología de investigación que se ha de llevar a cabo, los más comunes a analizar en un sistema *Windows* (tipo de dispositivos más empleados en el mundo empresarial) son los siguientes:

- *Master File Table* o MFT que funciona a modo de índice del contenido alojado en el dispositivo y se puede ver entre otros el nombre, fecha de creación, fecha de modificación de todos los dispositivos.
- Archivos *Prefetch*. Configurados por defecto en los sistemas personales y no en los servidores recoge las preferencias de los usuarios y algunas configuraciones habituales realizadas en este. Estos aspectos pueden añadir valor a la investigación.

- Papelera de reciclaje. Almacena los ficheros eliminados recientemente en el sistema.
- *Jumplist.* Arrojan información de los accesos rápidos creados en el sistema, así como todos los iconos de aplicaciones.

Pese a todo lo comentado anteriormente, uno de los factores más importantes y que comúnmente no se presta la atención que merece es la elección de un correcto equipo encargado del análisis. En función de la tipología de empresa que se esté analizando, es importante que los expertos encargados posean unos conocimientos u otros.

Por ejemplo, si el caso estudiado compete a un fraude acontecido en las cuentas de la empresa, es de vital importancia que los revisores del caso sean expertos en la materia y que conformen un equipo junto al soporte y equipo técnicos encargado del análisis de los dispositivos.

3.1.6. Producción y preservación

Cabe destacar que para esta última fase de nuestro procedimiento se pueden arrojar determinados conocimientos al respecto, pero no será posible realizarlo de manera efectiva en el caso práctico ya que no se poseen los medios necesarios para ello.

En primer lugar y respecto a la producción final, es el documento que realizan los analistas y dónde se reflejan tanto las conclusiones tras el análisis, cómo algunas sugerencias de mejora que se pueden arrojar a la empresa con el objetivo de aportar un valor a la investigación. Existen múltiples formas de presentar todos los resultados, la más destacada de ellas por su complejidad es el informe pericial. Este documento se caracteriza por la finalidad de este que es aportar determinadas pruebas de cara a un juicio y explicar cómo se han obtenido estas.

Pero esta no es la única metodología de presentar las conclusiones, se puede por un lado reportar de manera directa mediante un comunicado por correo electrónico o emplear cualquier tipología de documento existente en el que se pudiera arrojar una información adicional.

De cara a la preservación, si el caso termina en juicio hay un mínimo de tiempo que los datos han de estar accesibles y custodiados por la empresa que se encarga del análisis que variará en función de la jurisdicción aplicada.

En nuestro procedimiento se tratará de simular un reporte de la manera más profesional posible, pero la obtención de un informe presentable de cara a un juicio requiere de una mayor cantidad de recursos, así como profesionales de distintas áreas. En lo que se refiere a la preservación de la evidencia ocurre lo mismo. Se comentarán algunas acciones que se han de llevar a cabo según lo que dictaminan los estándares, pero estas medidas se escapan del alcance de nuestro procedimiento.

Algunas de las medidas que dictaminan los estándares de cara a una correcta preservación de las evidencias son el almacenamiento de las copias realizadas sobre los sistemas ante notario en la medida de lo posible y de manera repetida, almacenamiento en habitaciones securizadas que garanticen el acceso exclusivo por quién se determine esencial (política de menos privilegios) y el establecimiento de un lugar no húmedo y en correctas condiciones para el correcto almacenado de dispositivos electrónicos.

Cabe destacar que una parte de la correcta gestión de las evidencias se realiza en la adquisición con una correcta nomenclatura (identificable, pero a su vez confidencial. Esto quiere decir que se arroja la información suficiente para relacionarlo con la evidencia

a las personas que deben ser capaces de realizar esta tarea, y no arroja información de más a un desconocido que pudiera visualizar este disco en caso de error). En nuestro procedimiento se va a tratar de establecer ciertos mecanismos como identificación de número de serie, marca del dispositivo, uso de bolsas de evidencias numeradas y otras medidas que puedan ayudar a llevar a cabo la preservación de la evidencia de manera efectiva.

Esto es importante ya que, en un campo tecnológico con miles de discos, la incorrecta gestión de estos puede terminar con la pérdida de datos cuya importancia es muy elevado, suponiendo así una brecha de seguridad de cara a la protección de los datos.

Adicionalmente, todo esto se verá apoyado por la herramienta desarrollada, que permitirá gestionar y ayudar con las labores de preservación de las copias de los dispositivos. Todo esto aportará valor a la cadena de custodia, permitirá a los empleados conocer en qué estado se encuentra todas las evidencias y poder gestionar de manera sencilla un equipo en un ambiente dinámico, confidencial y volátil como son las investigaciones de fraude en empresas.

Las funciones de la herramienta se comentan en el siguiente epígrafe donde se verá las ventajas aportadas y el valor añadido que obtiene el procedimiento gracias a su uso por parte del equipo de investigación.

CAPÍTULO 4: DESARROLLO DE LA HERRAMIENTA

Con el objetivo de validar y respaldar todo el proceso descrito anteriormente y sustentado en el caso práctico descrito en los anexos, se ha creado una herramienta cuyo objetivo es el otorgar el apoyo adecuado a los analistas con menor experiencia (mediante guías de ayuda para los usuarios) y gestión de los distintos casos, así como los diferentes usuarios involucrados en estos.

Cabe destacar que actualmente, a pesar de poseer interfaz gráfica web, no se ha publicado en internet, de manera que las ejecuciones se realizarán en local, para evitar exponer esta información a un entorno público.

Una de las principales mejoras de la herramienta se obtendrá cuando se haga pública la web y se permita el acceso remoto a todos estos recursos. Derivado de esto, surge el principal de los puntos a destacar relativo a los trabajos futuros del proyecto.

4.1. Tecnologías empleadas

En primer lugar, se ha de contar con un dispositivo que posea *Python* instalado en el sistema, ya que este será el lenguaje de programación empleado para la realización de la herramienta.

Asimismo, en el directorio de la aplicación, se ha configurado un entorno virtual, que permitirá la instalación de distintos *frameworks*, sólo a nivel de aplicación, sin ser necesario que se cuente con dichos recursos en el sistema.

El siguiente requisito para el correcto funcionamiento de la aplicación, será la inclusión de la librería *pip*, empleada como tubería para la descarga de los recursos necesarios de la web, mediante consola de comandos. Será incluida por defecto en los entornos virtuales, pero se ha de asegurar que se encuentre en el sistema ya que, si no, no funcionará de manera adecuada.

Asimismo, serán necesarias los frameworks *flask*, que según define su autor: *"es un microframework para Python basado en Werkzeug que permite crear aplicaciones web de todo tipo"* y *SQLAlchemy*, que es un *kit* de herramientas que permite el manejo de bases de datos relacionales.

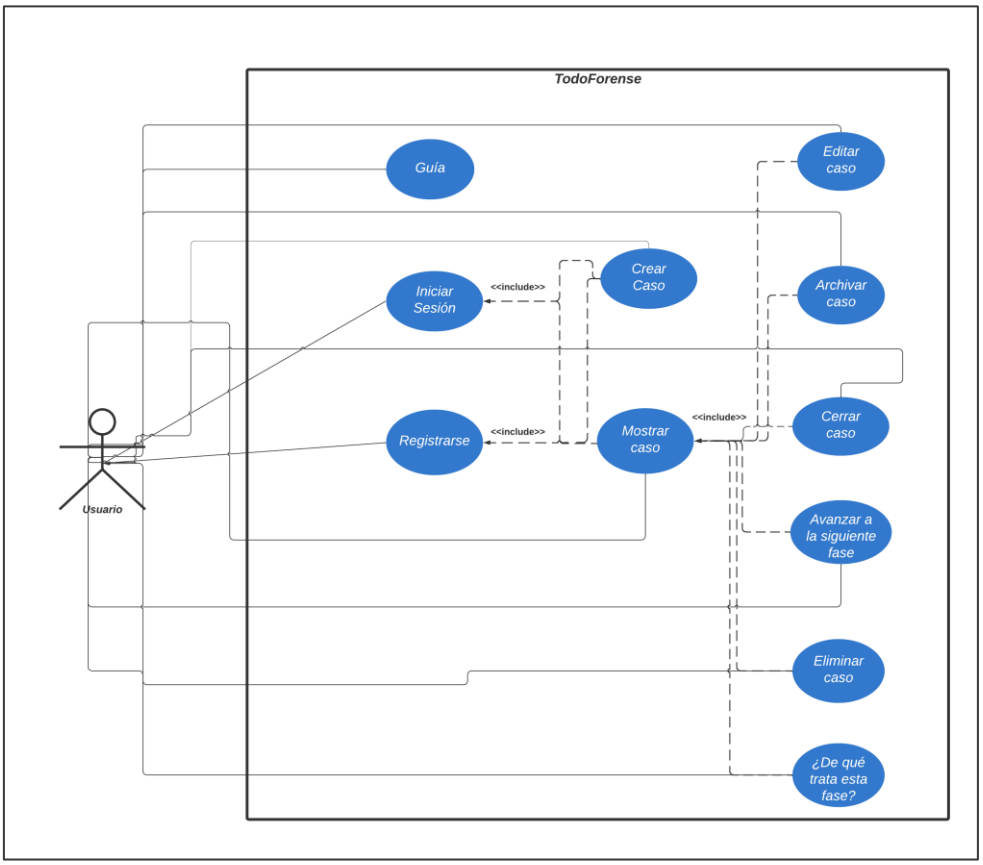
Estos *frameworks* han sido escogidos por la escalabilidad que posee el tipo de base de datos escogido, velocidad de consulta, alta integración con el lenguaje de programación *Python* y la facilidad de configuración para los distintos entornos.

4.2. Actores y captación de requisitos

Previamente al desarrollo de la herramienta, ha sido necesario determinar los actores implicados en el funcionamiento de esta, así como los diferentes casos de uso una vez establecidas las principales funciones o servicios que ofrece.

A continuación, se adjunta el diagrama de casos de uso, en el que se puede observar que el actor principal que interactuará con la herramienta será el propio usuario. Por otro lado, se muestran las funcionalidades de dicha herramienta que serán las siguientes: registrarse, inicio de sesión, guía, crear caso, mostrar caso, editar caso, archivar caso, cerrar caso, avanzar a la siguiente fase, eliminar caso y ¿de qué trata esta fase?, que se detallarán más adelante.

Figura 9: Diagrama de casos de uso y actores de la herramienta



Fuente: Elaboración propia

En los siguientes epígrafes, se procederá a detallar los requisitos exigidos para cada uno de los casos de uso observados en el anterior diagrama. En el caso de Guía, el usuario puede acceder a esta opción en cualquier momento, inclusive sin haber iniciado sesión o registrarse, por tanto, no ha sido necesaria su inclusión del diagrama, al no presentar una serie de requisitos específicos.

4.2.1. Registrarse

A continuación, se adjunta el flujo de eventos del caso de uso “Registrarse y sus correspondientes caminos alternativos:

Tabla 8: Flujo de eventos del caso de uso "Registrarse"

ACTOR: USUARIO	SISTEMA
1. Selecciona la opción de registrarse. 3. Introduce los datos requeridos para crear un usuario. 4. Pulsa al botón crear caso.	2. Solicita los datos para la creación de un usuario. 5. Recibe los datos introducidos y comprueba la validez con la BBDD. 6. Usuario creado con éxito y fin del caso de uso.
Post-requisito: La creación de un nuevo usuario en el sistema,	

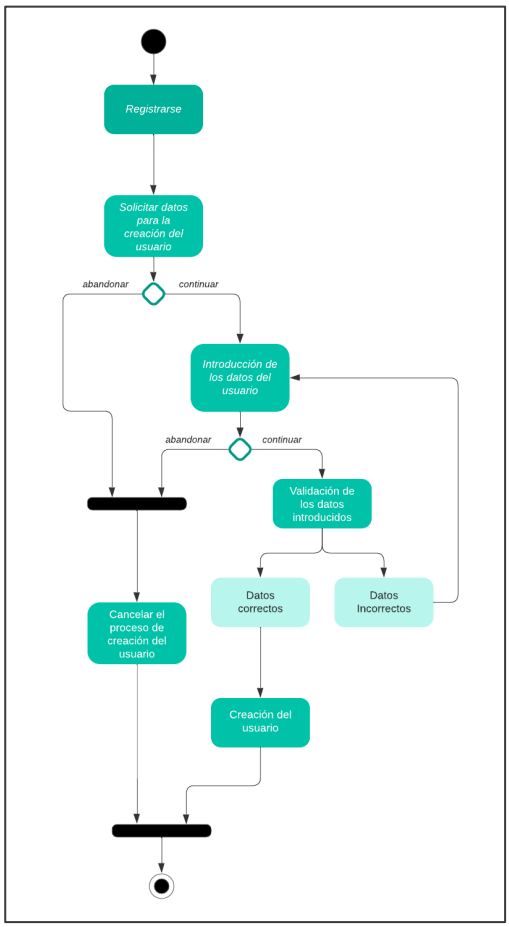
Fuente: Elaboración propio

Caminos alternativos:

Evento 3: El usuario cancela la creación de su cuenta.

Evento 4: Los datos no son válidos (usuario ya registrado/ha dejado campos vacíos).

Figura 10: Diagrama de actividad Registrarse



Fuente: Elaboración propia

4.2.2. Iniciar sesión

En paralelo a lo mencionado anteriormente, se adjunta el flujo de eventos del caso de uso “Iniciar Sesión” y sus correspondientes caminos alternativos:

Tabla 9: Flujo de eventos del caso de uso “Iniciar Sesión”

ACTOR: USUARIO	SISTEMA
1. Selecciona la opción de iniciar sesión. 3. Introduce los datos correspondientes a su usuario. 4. Pulsa al botón iniciar sesión.	2. Solicita los campos requeridos para el inicio de sesión. 5. Recibe los datos introducidos y comprueba la validez con la BBDD. 6. Usuario inicia sesión con éxito y fin del caso de uso.

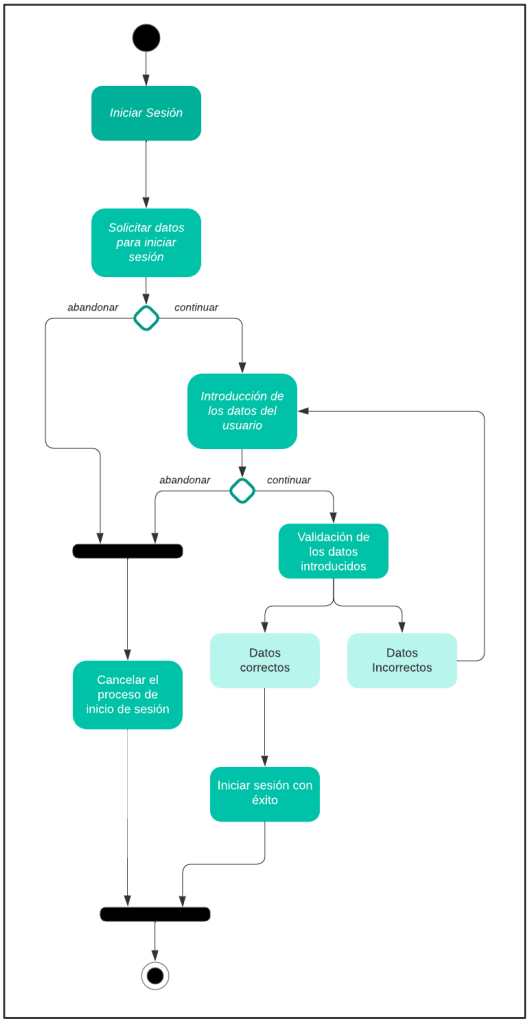
Fuente: Elaboración propia

Caminos alternativos:

Evento 3: El usuario cancela el inicio de sesión.

Evento 5: Los datos no son válidos (usuario no encontrado en la base de datos/ha dejado campos vacíos).

Figura 11: Diagrama de actividad Iniciar Sesión



Fuente: Elaboración propia

4.2.3. Crear caso

A continuación, se adjunta el flujo de eventos del caso de uso "Crear Caso" y sus correspondientes caminos alternativos:

Tabla 10: Flujo de eventos del caso de uso "Crear Caso"

Prerrequisito: El usuario debe haber iniciado sesión/ registrarse antes de poder crear un caso	
ACTOR: USUARIO	SISTEMA
1. Selecciona la opción de crear caso. 3. Introduce los datos requeridos para crear un caso. 4. Pulsa al botón crear caso.	2. Solicita los datos para la creación de un caso. 5. Recibe los datos introducidos y comprueba la validez con la BBDD. 6. Caso creado con éxito y fin del caso de uso.
Post-requisito: El usuario ha creado un nuevo caso, que se ha almacenado en la base de datos.	

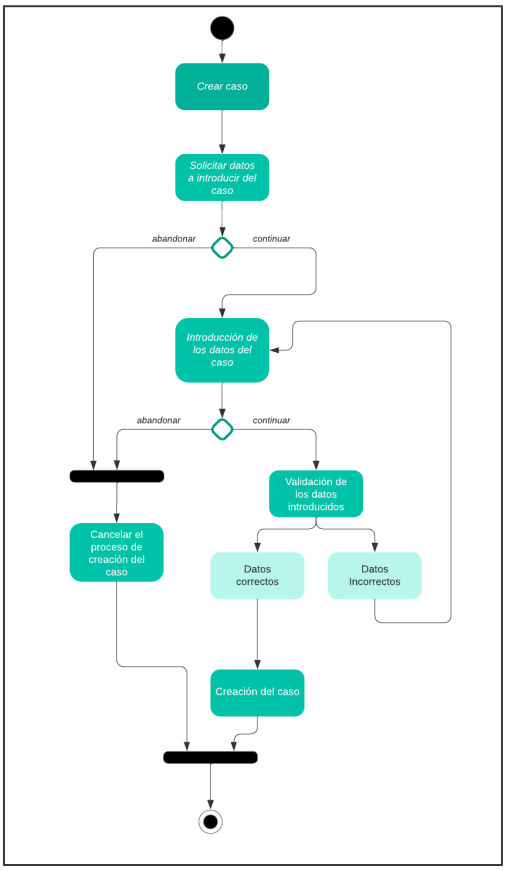
Fuente: Elaboración propia

Caminos alternativos:

Evento 3 y 4: Usuario puede cancelar.

Evento 5: Los datos introducidos no son correctos o existe el caso en la base de datos.

Figura 12: Diagrama de actividad Crear Caso



Fuente: Elaboración propia

4.2.4. Mostrar caso

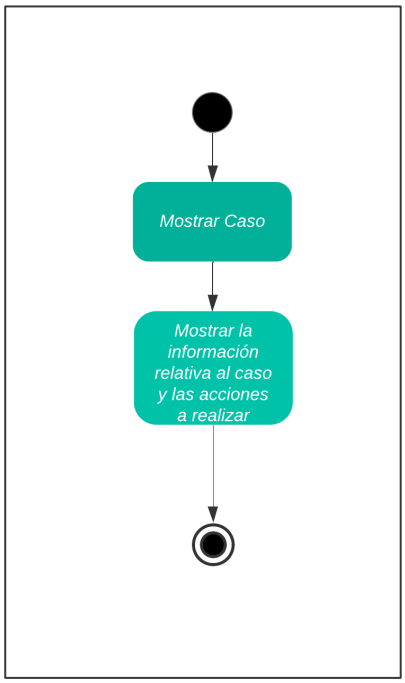
Asimismo, se adjunta el flujo de eventos del caso de uso "Mostrar Caso":

Tabla 11: Flujo de eventos del caso de uso "Mostrar Caso"

Prerrequisito: El usuario debe haber iniciado sesión para poder acceder a la opción de mis casos, y por tanto, ver la lista de casos que tiene.	
ACTOR: USUARIO	SISTEMA
1. Selecciona la opción de mostrar más del caso que desee visualizar más información.	2. Muestra todos los campos con la información almacenada para ese caso, y el resto de las acciones que se podrían realizar en dicho caso.

Fuente: Elaboración propia

Figura 13: Diagrama de actividad Mostrar caso



Fuente: Elaboración propia

4.2.5. Editar caso

Continuando con los distintos casos de usos contemplados por la herramienta, se adjunta el flujo de eventos del caso de uso "Editar Caso" y sus correspondientes caminos alternativos:

Tabla 12: Flujo de eventos del caso de uso "Editar Caso"

Prerrequisito: El usuario debe haber iniciado sesión para poder ver la vista de mostrar sus casos y por tanto, editar un caso, además, de tener casos iniciados.	
ACTOR: USUARIO	SISTEMA

1. Selecciona la opción de editar caso. 3. Edición de los datos deseados. 4. Guardar cambios.	2. Muestra todos los campos editables y no editables. 5. Recibe los datos cambiados y valida con la BBDD. 6. Caso actualizado con éxito y fin del caso de uso.
Post-requisito: Se guardarán los cambios introducidos en el caso seleccionado por el usuario.	

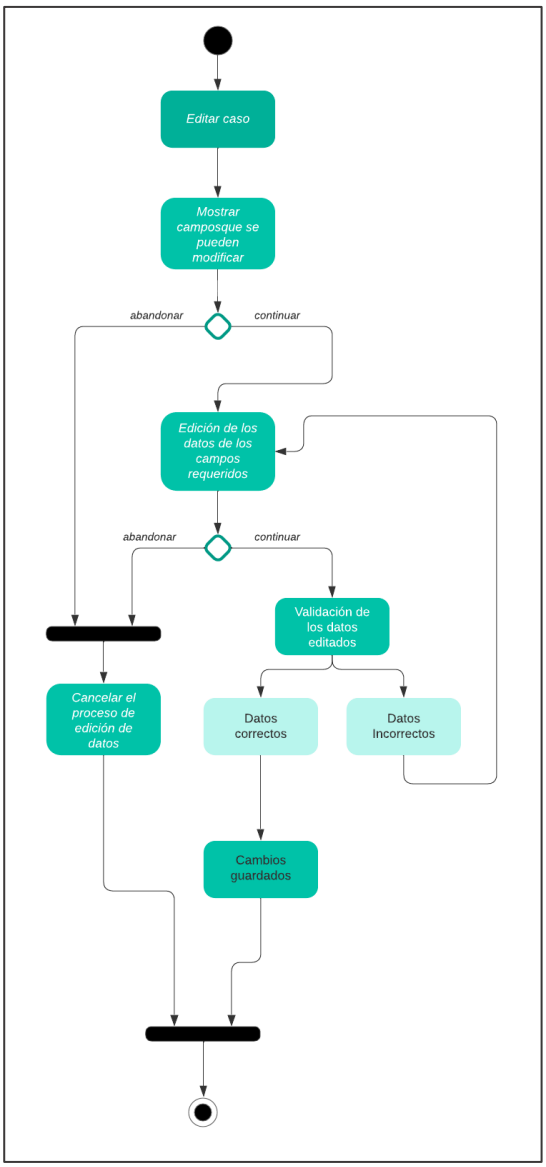
Fuente: Elaboración propia

Caminos alternativos:

Evento 3 y 4: Usuario puede cancelar.

Evento 5: Los datos introducidos pueden estar mal porque se actualiza a un estado o fase que no está permitido.

Figura 14: Diagrama de actividad Editar Caso



Fuente: Elaboración propia

4.2.6. Archivar caso

A continuación, se adjunta el flujo de eventos del caso de uso "Archivar Caso" y sus correspondientes caminos alternativos:

Tabla 13: Flujo de eventos del caso de uso "Archivar Caso"

Prerrequisito: El usuario debe haber iniciado sesión para poder ver sus casos, y por consiguiente, poder archivar el caso.	
ACTOR: USUARIO	SISTEMA
1. Seleccionar la opción de archivar caso 3. Pulsar aceptar el archivo del caso.	2. Solicitar confirmación al archivo del caso. 4. Recibe la información y la valida con la base de datos. 5. Caso archivado con éxito y fin del caso de uso.
Post-requisito: El archivado del caso seleccionado por el usuario.	

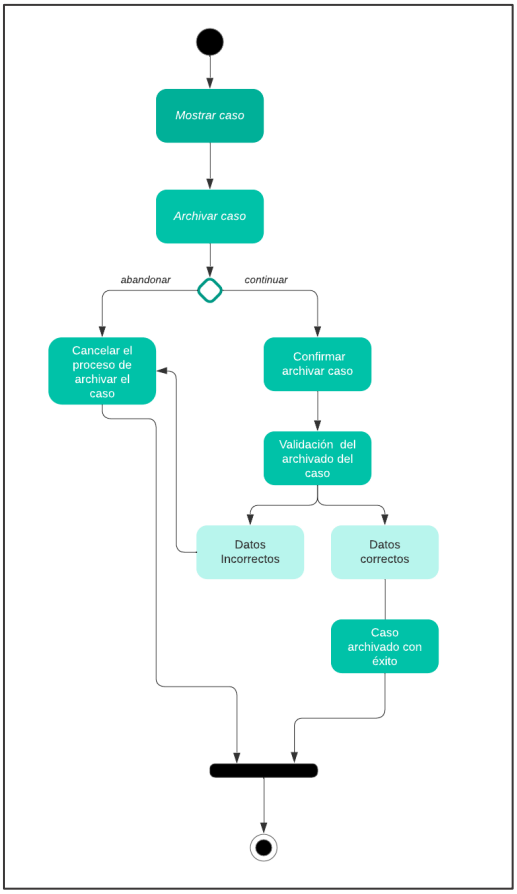
Fuente: Elaboración propia

Caminos alternativos:

Evento 2: Usuario puede cancelar el proceso de archivo del caso.

Evento 6: El caso no se puede archivar ya que no se ha llegado a la etapa del informe.

Figura 15: Diagrama de actividad Archivar Caso



Fuente: Elaboración propia

4.2.7. ¿De qué trata esta fase?

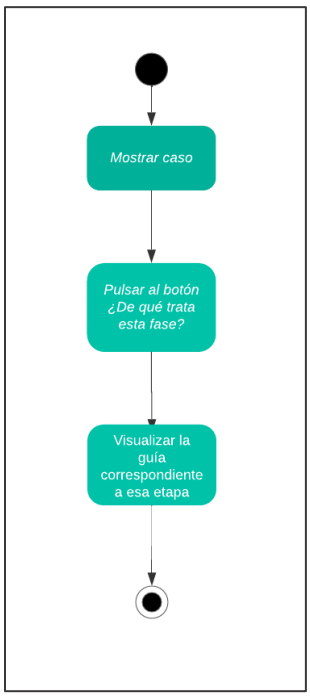
Asimismo, se adjunta el flujo de eventos correspondiente al caso de uso "¿De qué trata esta fase?:

Tabla 14: Flujo de eventos del caso de uso ¿De qué trata esta fase?

Prerrequisito: El usuario debe de haber iniciado sesión, para poder acceder a la vista de uno de sus casos, y, por consiguiente, pulsar el botón de ¿De qué trata esa fase?	
ACTOR: USUARIO	SISTEMA
1. Seleccionar la opción de ¿de qué trata esta fase?	2. Redirige a la página de guía con la etapa correspondiente y fin del caso de uso.

Fuente: Elaboración propia

Figura 16: Diagrama de actividad "¿De qué trata esta fase?"



Fuente: Elaboración propia

4.2.8. Avanzar a la siguiente fase

Además, se adjunta el flujo de eventos del caso de uso "Avanzar a la siguiente fase" y sus correspondientes caminos alternativos:

Tabla 15: Flujo de eventos del caso de uso "Avanzar a la siguiente fase"

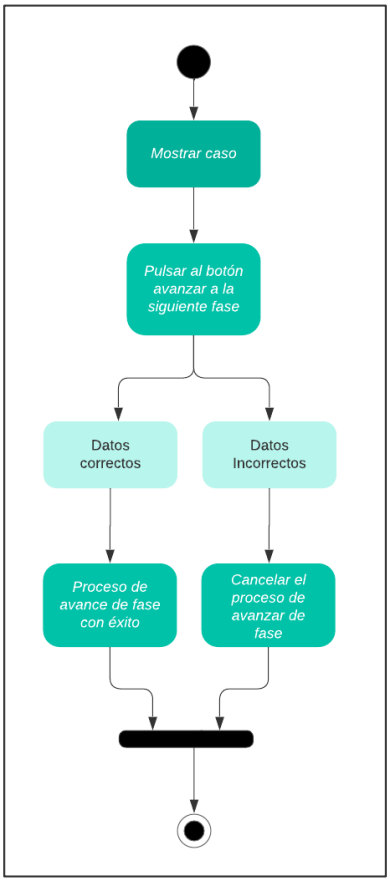
Prerrequisito: El usuario debe de haber iniciado sesión, para poder acceder a la vista de uno de sus casos, y por consiguiente, pulsar el botón de Avanzar a la siguiente fase	
ACTOR: USUARIO	SISTEMA
1. Seleccionar la opción de avanzar a la siguiente fase.	2. Valida con la base de datos si la etapa en la que se encuentra permite avanzar. 3. Caso avanza a la siguiente etapa con éxito y fin del caso de uso.

Fuente: Elaboración propia

Caminos alternativos:

Evento 2: El caso no puede pasar a la siguiente etapa ya que faltan acciones por realizar / ya se encuentra en la etapa final

Figura 17: Diagrama de actividad Avanzar a la siguiente fase



Fuente: Elaboración propia

4.2.9. Cerrar caso

En paralelo a esto, se adjunta el flujo de eventos del caso de uso "Cerrar Caso" y sus correspondientes caminos alternativos:

Tabla 16:Flujo de eventos del caso de uso "Cerrar caso"

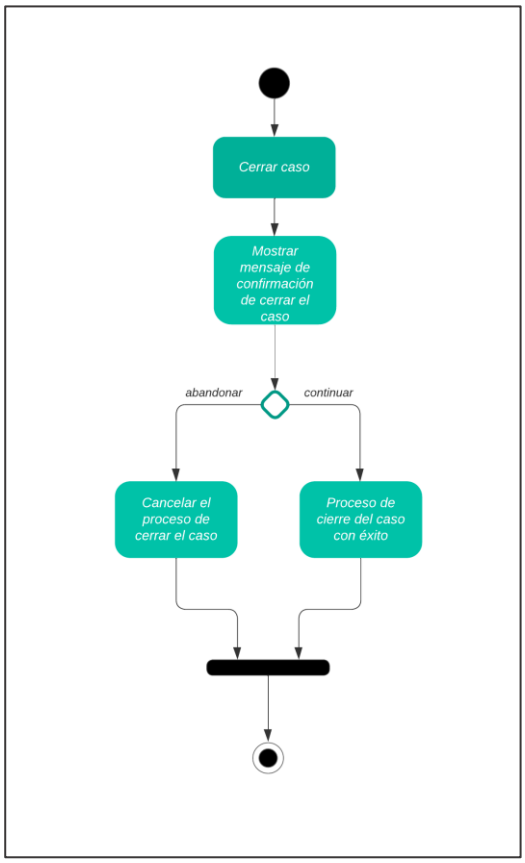
Prerrequisito: El usuario debe de haber iniciado sesión, para poder acceder a la vista de uno de sus casos, y, por consiguiente, pulsar el botón de Avanzar a la siguiente fase	
ACTOR: USUARIO	SISTEMA
1. Seleccionar la opción de cerrar caso. 3. Pulsa el botón de confirmar para cerrar el caso.	2. Muestra un mensaje de confirmación para proceder a cerrar el caso. 4. Caso cerrado y actualizado en la base de datos con éxito y fin del caso de uso.

Fuente: Elaboración propia

Caminos alternativos:

Evento 3: El usuario decide cancelar el proceso de cerrar el caso.

Figura 18: Diagrama de actividad Cerrar Caso



Fuente: Elaboración propia

4.2.10. Eliminar caso

Continuando con lo mencionado anteriormente, se adjunta el flujo de eventos del caso de uso "Eliminar Caso", y sus correspondientes caminos alternativos:

Tabla 17: Flujo de eventos del caso de uso "Eliminar Caso"

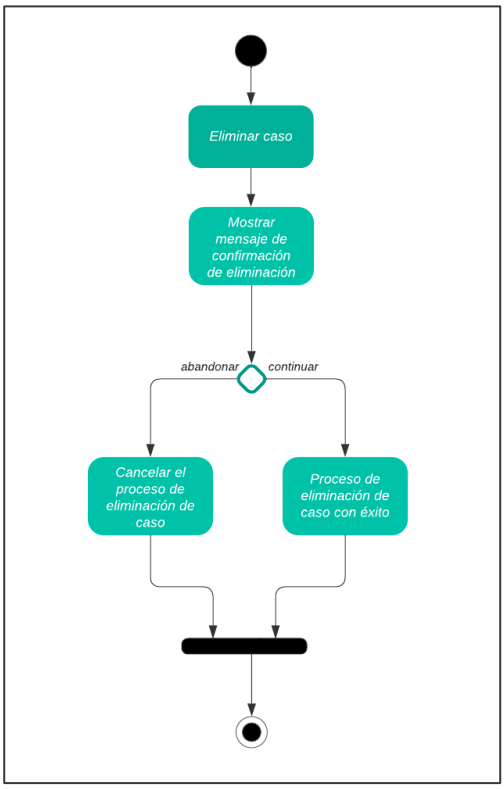
Prerrequisito: El usuario debe de haber iniciado sesión, para poder acceder a la vista de uno de sus casos, y, por consiguiente, pulsar el botón de eliminar caso.	
ACTOR: USUARIO	SISTEMA
1. Seleccionar la opción de borrar caso. 3. Pulsa el botón de confirmar eliminación.	2. Solicita confirmación de eliminar el caso. 4. Valida la eliminación con la base de datos. 5. Eliminación realizada con éxito y fin del caso de uso.
Post-requisito: La eliminación del caso seleccionado por el usuario.	

Fuente: Elaboración propia

Caminos alternativos:

Evento 3: El usuario cancela la eliminación del caso.

Figura 19: Diagrama de actividad Eliminar Caso



Fuente: Elaboración propia

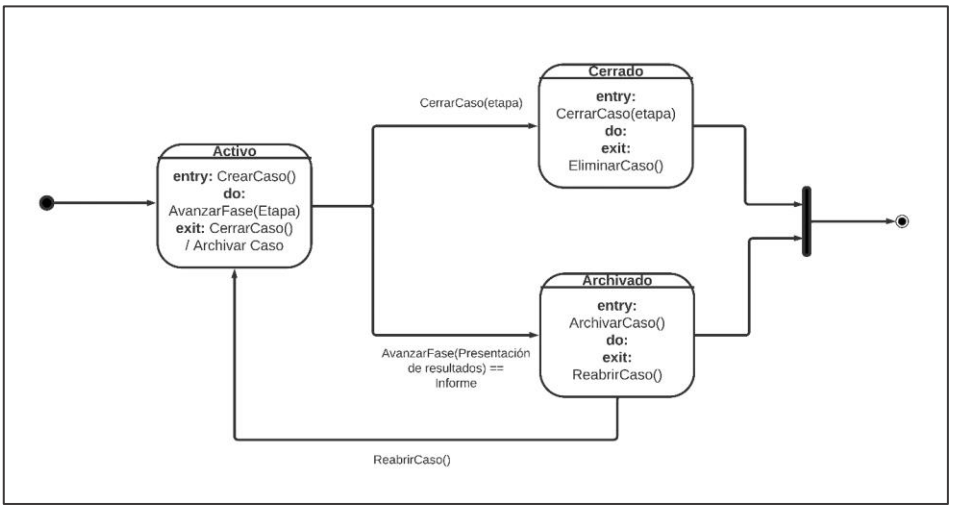
4.2.11. Diagrama de estados Caso

Los casos tienen una serie de atributos, entre los cuales se encuentran la etapa y el estado. Las etapas se corresponden con las fases definidas en el procedimiento: adquisición, procesamiento, análisis, filtrado y presentación de resultados. De esta forma, cada uno de los casos deberá de seguir ese orden, y hasta que no se complete la fase anterior no se podrá pasar hasta la siguiente fase.

Por otro lado, los estados de los casos pueden ser los siguientes: abierto, cerrado o archivado. A continuación, se detallarán las condiciones que presentan cada uno, así como la transición que se puede producir entre ellos.

- Abierto: Este estado se inicia cuando se encuentra en alguna de las etapas mencionadas anteriormente, ya que se está recopilando y analizando la información requerida para el caso. Para salir de este estado se pueden producir dos casuísticas: por un lado, que el caso se vaya a cerrar y por otro, que el caso vaya a ser archivado ya que se ha llegado al final de la investigación con la presentación de resultados a través del informe.
- Cerrado: Este estado puede comenzar en cualquiera de las etapas que conforman el caso, con motivo de un desistimiento de análisis de información, o cualquier otra causa que indica que se finaliza la investigación pudiendo haberla terminado o no.
- Archivado: Este estado se puede inicializar en el momento de que el caso se encuentre en la última etapa (presentación de resultados), y se haya generado el informe resultante. Por consiguiente, se ha finalizado la investigación y se procede a conservar esa información por si fuera necesaria utilizarla en un futuro.

Figura 20: Diagrama de estados Caso



Fuente: Elaboración propia

4.3. Navegación e Interfaz gráfica

Para la navegación por la interfaz gráfica, se separan a continuación en base a distintos casos de uso realizados previos al diseño de la página web. Asimismo, se destacarán algunos de los errores obtenidos en estas circunstancias, observándose las circunstancias que podrían terminar sin éxito en base al caso de uso realizado, obteniendo distintos mensajes de error, en lugar de afectando al rendimiento de la aplicación.

4.3.1. Pantalla de bienvenida

La primera de las páginas observadas en los instantes que cualquier agente navega hasta la dirección donde se aloja la página web se trata de un diseño de bienvenida, que podrá visualizar cualquier actor, se encuentre *logueado* en el entorno o no.

Cómo se puede observar en las imágenes adjuntas a continuación, desde aquí se pueden realizar las tareas básicas de registrar un usuario, iniciar sesión con una cuenta ya existente o navegar hasta las guías.

Figura 21: Pantalla de bienvenida de la aplicación (I)

Fuente: Elaboración propia

Figura 22: Pantalla de bienvenida de la aplicación (II)

Fuente: Elaboración propia

Cabe destacar que en caso de pulsar en *"*Seguimiento*"* sin encontrarse registrado en la herramienta, se redigirá directamente al actor a la ventana de iniciar sesión.

4.3.2. Registro de usuarios

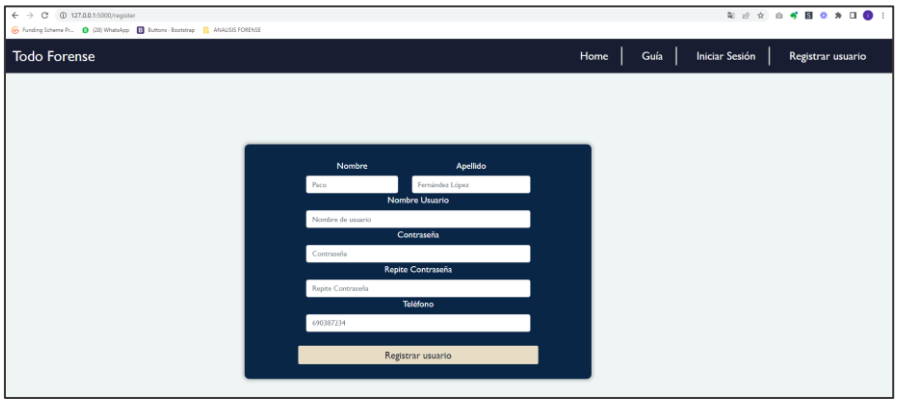
Para comenzar el caso de uso de registrar un usuario, se ha de pulsar en la barra de navegación (sin estar logueado como usuario en la herramienta) en *"*Registrar usuario*"*.

Figura 23: Barra de navegación de la interfaz (usuario no logueado)

Fuente: Elaboración propia

Una vez el actor ha realizado tal acción, se redigirá al mismo a una plantilla que posee un formulario, en el que se debe rellenar todos los campos para proceder. La información solicitada en este caso será Nombre, Apellido, Nombre de usuario (que ha de ser único en la herramienta) contraseña (introducida en dos ocasiones y que ha de coincidir en ambas) y Teléfono.

Figura 24: Barra de navegación de la interfaz (usuario no logueado)



Fuente: Elaboración propia

A continuación, se adjunta una imagen de un ejemplo completando todo el formulario y su apariencia.

Figura 25: Formulario registrar un usuario (II)

Fuente: Elaboración propia

Al pulsar en el botón de registrar usuario, en caso de encontrarse todos los campos con información válida y adecuada, se redirigirá al actor a la ventana de iniciar sesión.

Figura 26: Vista de inicio de sesión

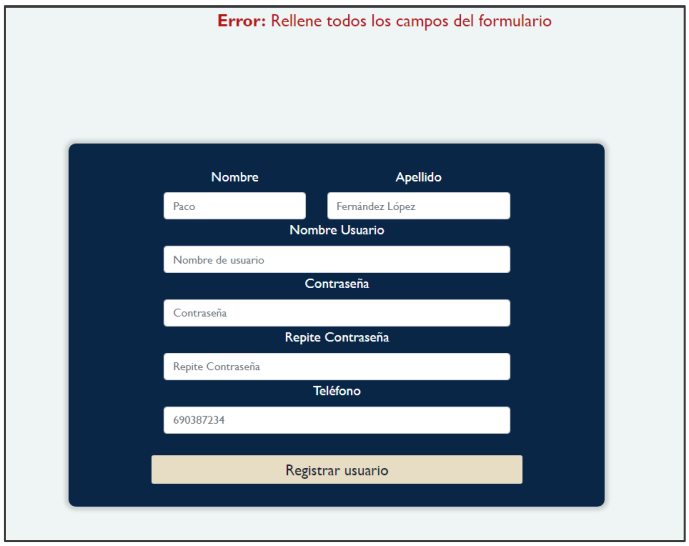
Fuente: Elaboración propia

4.3.2.1. Posibles escenarios de error

Se ha creado una serie de mecanismos destinados a evitar errores en las operaciones que se realizarán sobre la base de datos. Mediante esto, se excepcionarán determinados comportamientos por parte del actor que pudieran derivar en conflictos futuros en la herramienta. A continuación, se detallan algunos de los escenarios de error contemplados.

En primer lugar, en caso de que alguno de los campos del formulario de registrar usuario se encuentre vacío, en vez de crear un usuario, se imprimirá por pantalla el mensaje de error "*Error: Rellene todos los campos del formulario",* eliminando del formulario toda la información introducida.

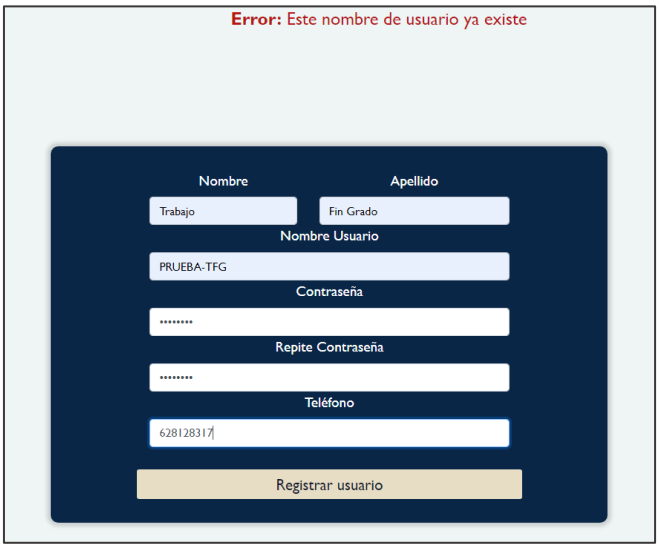
Figura 27: Escenario de error registrar usuario (I)



Fuente: Elaboración propia

Asimismo, en caso de que el actor introduzca un nombre de usuario ya existente, se procederá a no crear dicho usuario en la base de datos, excepcionando por pantalla el mensaje *"Error; Este nombre de usuario ya existe"*.

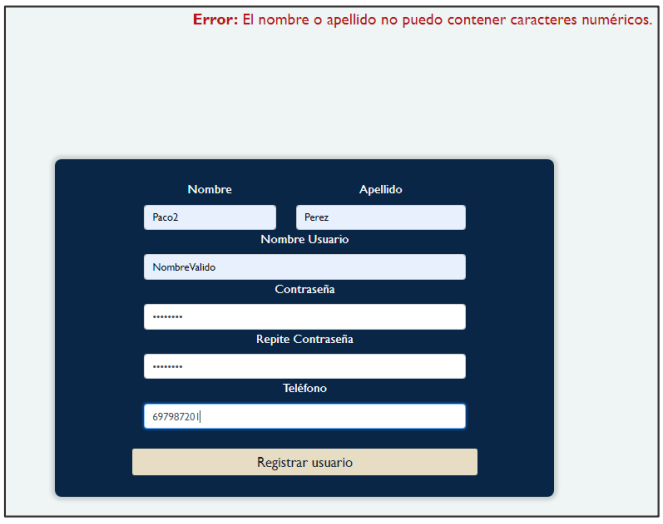
Figura 28: Escenario de error registrar usuario (II)



Fuente: Elaboración propia

Asimismo, la herramienta se asegurará de que tanto nombre, como apellidos, solo posee valores alfabéticos. En caso contrario, se imprimirá "*Error: El nombre o apellido no puede contener caracteres numéricos*"

Figura 29: Escenario de error registrar usuario (III)



Fuente: Elaboración propia

Por último, se puede dar la casuística de que las dos contraseñas introducidas sean distintas entre sí, obteniendo el mensaje de error *"Error: Introduzca contraseñas iguales en los dos campos"*.

Figura 30: Escenario de error registrar usuario (IV)

Fuente: Elaboración propia

4.3.3. Inicios de sesión

Para comenzar el caso de uso de iniciar sesión de un usuario, se ha de pulsar en la barra de navegación (sin estar logueado como usuario en la herramienta) en *"*Iniciar Sesión*"*.

Figura 31: Barra de navegación de la interfaz (usuario no logueado)

Fuente: Elaboración propia

Una vez el actor ha realizado tal acción, se redirigirá al mismo a una vista en la que se debe rellenar todos los campos para acceder. La información solicitada en este caso será el usuario y su correspondiente contraseña.

Figura 32: Vista de inicio de sesión con datos introducidos

Fuente: Elaboración propia

Una vez que el usuario ha introducido sus datos de manera correcta, a continuación, se redigirá de nuevo a la página de inicio. En la que, la barra de navegación habrá cambiado de tal forma que aparecerán las opciones de acceso a "Mis casos" y de "Cerrar Sesión", así como el contenido disponible previo al inicio de sesión.

Figura 33:Pantalla de inicio tras iniciar sesión

Fuente: Elaboración propia

4.3.3.1.Posibles escenarios de error

A la hora de iniciar sesión se han contemplado una serie de casuísticas con el fin de prevenir errores habituales que puedan interrumpir el funcionamiento de la herramienta. Por consiguiente, se han implementado una serie de alertar con el fin de remediar los posibles comportamientos del actor que pudieran alterar el correcto trabajo de gestión de la herramienta.

A continuación, se procede a detallar los posibles eventos anómalos que se han identificado:

En primer lugar, el campo usuario y el campo contraseña son obligatorios. En el caso de que el usuario no rellene alguno de los dos aparecerá un cuadro de diálogo indicando que es necesario completar el campo. A continuación, se adjunta a modo de ejemplo el mensaje que aparecería en el caso de que el usuario no complete el campo de la contraseña:

Figura 34: Vista de inicio de sesión con el campo contraseña obligatorio

Fuente: Elaboración propia

En segundo lugar, puede ocurrir que el usuario se equivoque introduciendo sus credenciales, que serán validadas con la base de datos, que almacena el registro de los usuarios. Por consiguiente, aparecerá el siguiente mensaje de error, otorgando al usuario la posibilidad de introducirlas de nuevo.

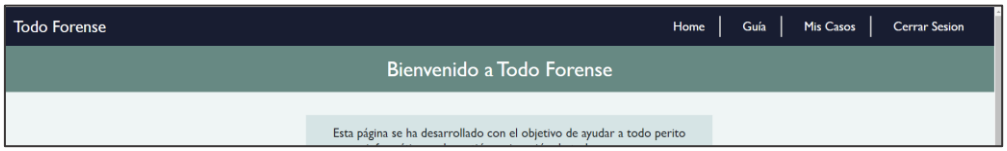
Figura 35: Vista inicio de sesión con mensaje de error por las credenciales introducidas

Fuente: Elaboración propia

4.3.4. Cerrar sesión

En caso de que un actor se encuentre *logueado* en la herramienta, se puede abandonar dicha sesión en todo momento, pulsando el botón *"*Cerrar Sesión*"* contenido en la barra de navegación superior.

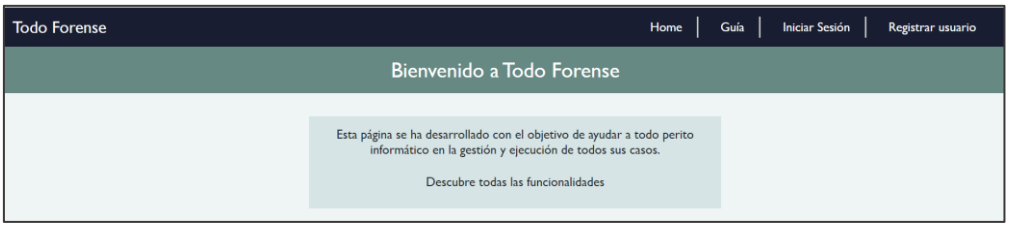
Figura 36: Barra de navegación usuario logueado



Fuente: Elaboración propia

Una vez se ha cerrado sesión, la barra de navegación volverá al estado que se encontraba previo al inicio de sesión del actor.

Figura 37: Barra de navegación usuario sin loguear



Fuente: Elaboración propia

4.3.5. Guía para usuarios

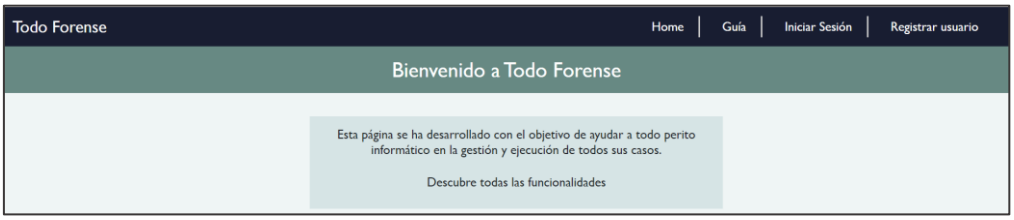
Para acceder a esta funcionalidad, se han creado múltiples formas. En primer lugar, desde la ventana de bienvenida, se podrá pulsar en *"*Ver más*"* dentro del recuadro Guía.

Figura 38: Acceso a guía desde pantalla de bienvenida

Fuente: Elaboración propia

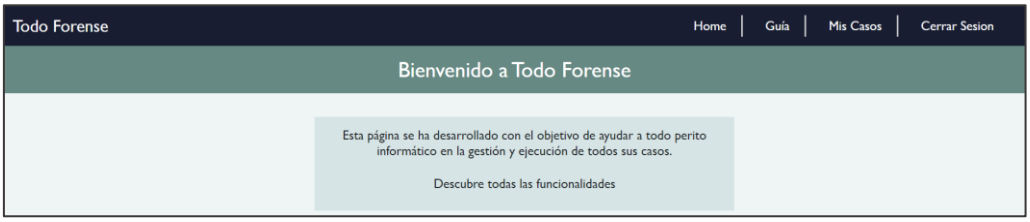
Asimismo, desde la barra de navegación, se puede acceder encontrándose el actor *logueado* en el sistema o no.

Figura 39: Acceso a guía barra de navegación usuario sin loguear



Fuente: Elaboración propia

Figura 40: Acceso a guía barra de navegación usuario logueado



Fuente: Elaboración propia

Una vez el actor se encuentra en guía, son múltiples las cuestiones que puede consultar, acerca de las distintas fases recogidas por el procedimiento informático-forense. Desde esta ventana se podrán resolver todas las dudas referentes a cualquiera de las partes contempladas por el procedimiento.

Figura 41: Bienvenida a sección guía

Fuente: Elaboración propia

A continuación, se procede a agrupar la distinta información recogida para cada una de las fases del procedimiento.

4.3.5.1. Guía adquisición

En primer lugar, en lo referente a adquisiciones, se han establecido dos epígrafes distintos, que serán consultados en función de la información requerida por el actor. En primer lugar, el denominado *"*Descripción*"* recoge una breve introducción al concepto de adquisición.

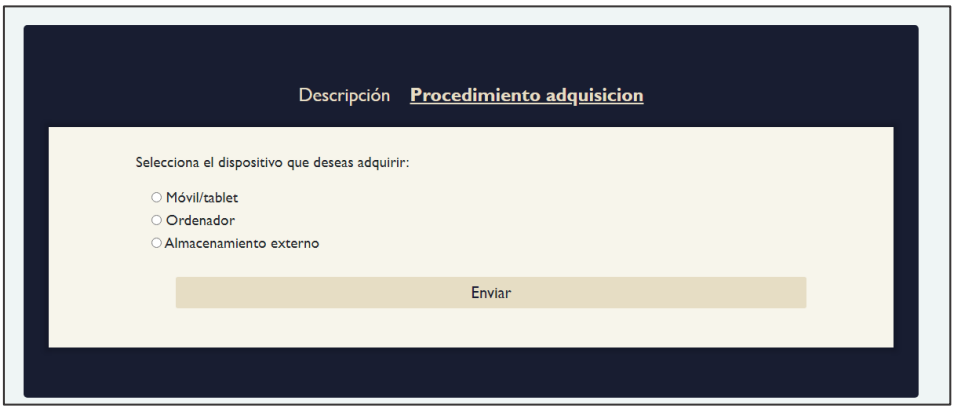
Figura 42: Descripción fase de adquisición

Fuente: Elaboración propia

En contraposición, en la sección *"*procedimiento adquisición*"* se han creado múltiples navegaciones, que, en base a la respuesta aportada por el usuario, la herramienta conducirá a determinadas circunstancias. En primer lugar, el usuario ha de elegir el tipo de dispositivo que desea adquirir, teniendo como posibilidades Móvil/Tablet, ordenador y almacenamiento externo.

Cabe destacar, que es requisito indispensable que se elija exclusiva y obligatoriamente una de las tres opciones. Para evitar fallos por parte del usuario, se ha configurado de tal forma que, en esta pantalla, no pueda elegirse dos opciones simultáneamente.

Figura 43: Guía del procedimiento de adquisición genérico



Fuente: Elaboración propia

- Adquisición móvil

En caso de seleccionar Móvil/Tablet como dispositivo que se desea adquirir, se poseen las opciones "Dispositivo muy antiguo (anterior a 2017)", "se posee el cable para conectar a *Cellebrite UFED Touch* 2", "Auto detectado por la *Tablet Cellebrite UFED Touch* 2" y "Se ha probado con *Cellebrite* y ha fallado".

Como bien se anticipaba en el procedimiento, se priorizará el uso de la herramienta de *Cellebrite*. Sin embargo, algunas casuísticas en los dispositivos pueden concluir en que la mejor opción para la adquisición sea el *software Magnet Axiom Acquire*.

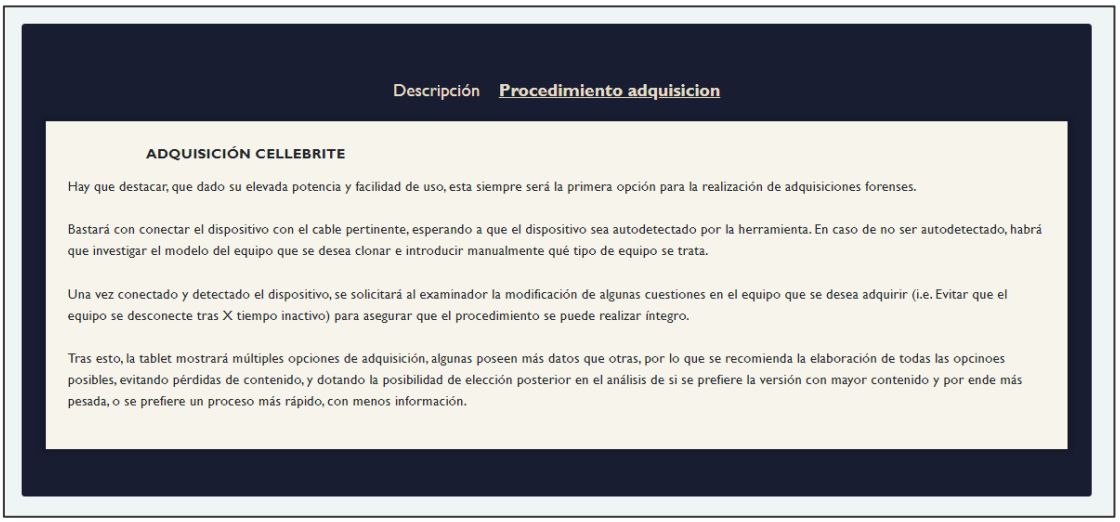
Figura 44: Guía del procedimiento de adquisición móvil

Fuente: Elaboración propia

La herramienta, siguiendo los conocimientos arrojados por el procedimiento, evaluará la mejor situación para cada escenario y redirigirá al usuario al procedimiento más adecuado.

A continuación, se muestra el texto informativo que aporta la herramienta tras evaluar que el procedimiento de adquisición óptimo es mediante la herramienta de *Cellebrite UFED Touch* 2.

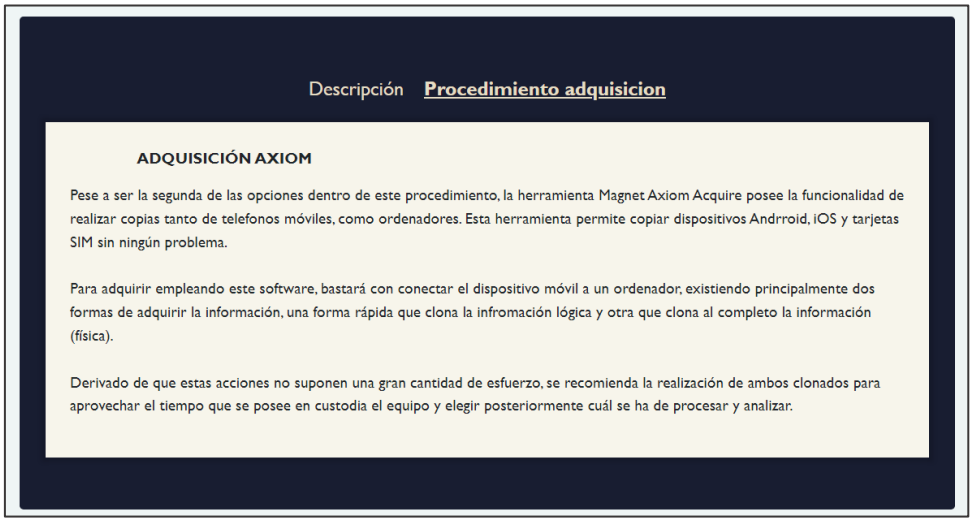
Figura 45: Procedimiento de adquisición mediante Cellebrite



Fuente: Elaboración propia

En contraposición, si tras la evaluación se determina que el procedimiento óptimo es la adquisición mediante el *software Magnet Axiom Acquire*, se redigirá al usuario a una vista con el siguiente contenido.

Figura 46: Procedimiento de adquisición mediante Axiom



Fuente: Elaboración propia

Esto aportará alguna información relevante del proceso al examinador respecto a la forma óptima de realizarlo, no obstante, si se desea obtener información adicional y detallada de cómo realizar el proceso de adquisición, se recomienda la consulta de manuales especializados para tales acciones.

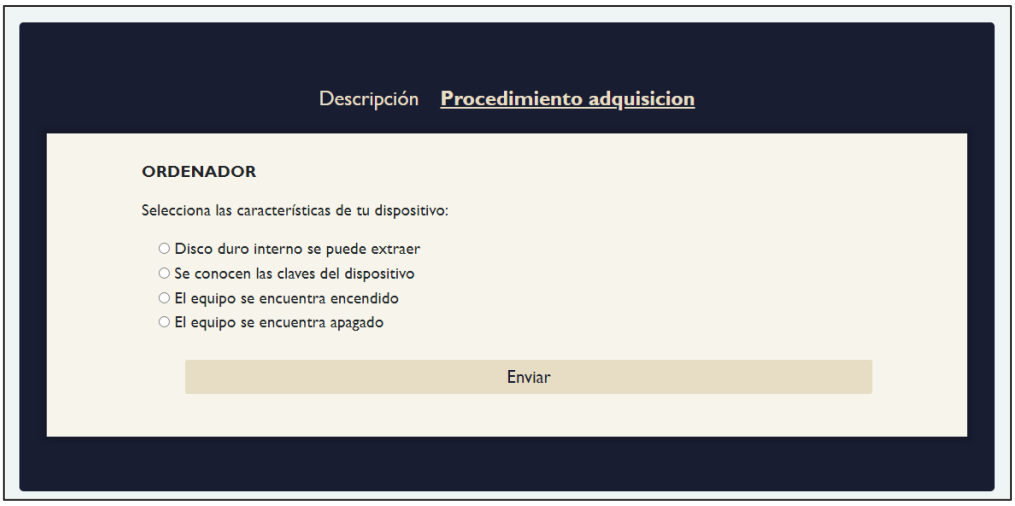
- Adquisición ordenador

En paralelo a lo mencionado anteriormente, otro tipo de fuentes que pueden ser adquiridas contempladas por el presente procedimiento y apoyado en esta herramienta son los ordenadores.

De igual manera que se mencionaba anteriormente, una vez se elige ordenadores como fuente a adquirir, y se pulsa el botón enviar, se redirige a una ventana en la que se deberá elegir entre las opciones *"Disco duro interno se puede extraer"*, *"Se conocen las*

claves del dispositivo”, *“El equipo se encuentra encendido”* y *“El equipo se encuentra apagado”*.

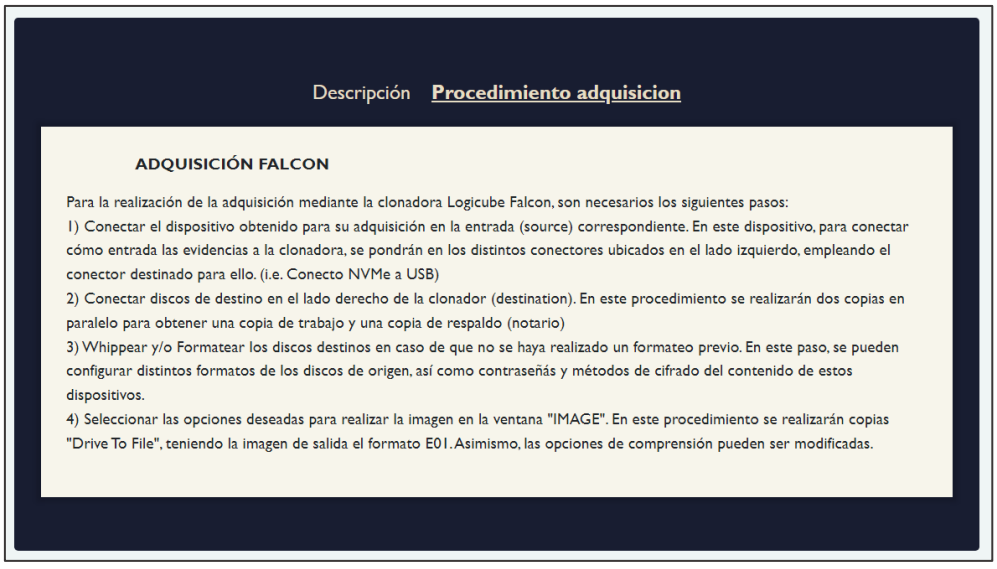
Figura 47: Guía del procedimiento de adquisición ordenador



Fuente: Elaboración propia

De igual manera que ocurre con los dispositivos móviles, una vez se ha evaluado la opción óptima entre todas las contempladas por la herramienta, se procede a redireccionar al usuario. En caso de que lo más adecuado sea la adquisición mediante la clonadora forense *Falcon*, se mostrará lo siguiente.

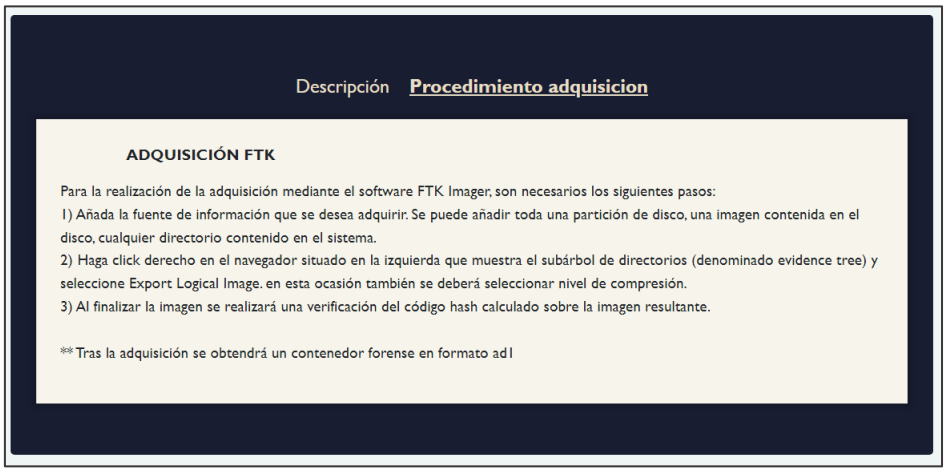
Figura 48: Procedimiento de adquisición mediante Falcon



Fuente: Elaboración propia

En contraposición, si no se puede realizar de dicha forma derivado de las características del sistema, y el resultado óptimo es la adquisición del equipo mediante el *software FTK Imager*, el contenido de la vista se adjunta a continuación.

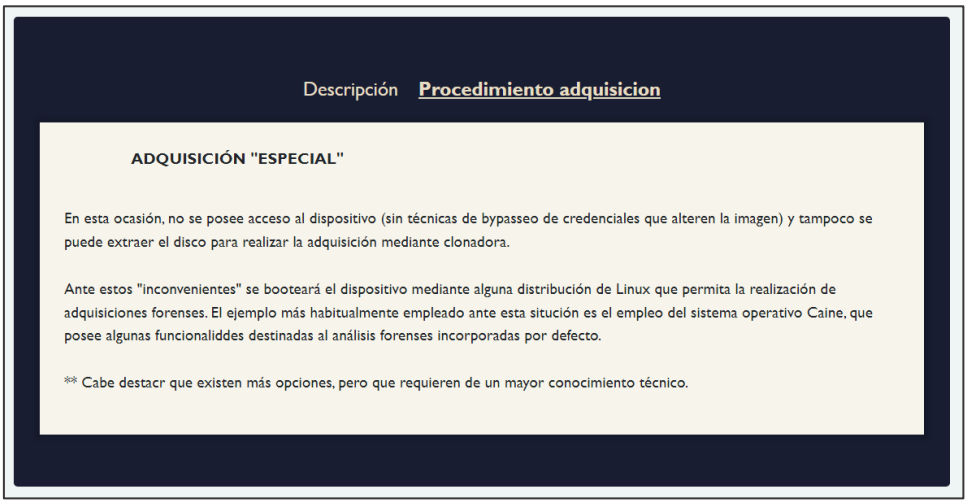
Figura 49:Procedimiento de adquisición mediante FTK



Fuente: Elaboración propia

Por último, si ninguna de las dos opciones anteriores es viable, se procede a adquirir el equipo de una manera un tanto especial, ya que es más complicada y requiere de personal más técnico o con un cierto grado de experiencia. El contenido de este último tipo de adquisiciones es el siguiente.

Figura 50: Procedimiento de adquisición mediante "adquisición especial"

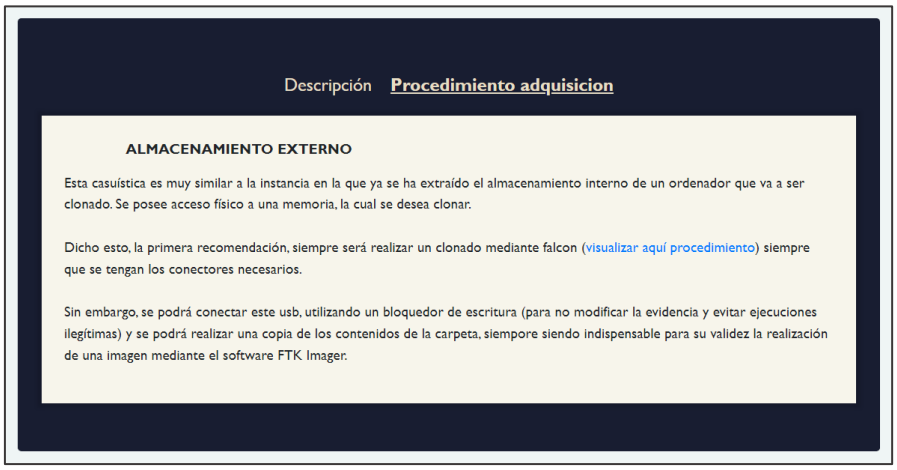


Fuente: Elaboración propia

- Adquisición almacenamiento externo

Por último, si la fuente a adquirir se trata de un almacenamiento externo, la casuística será muy similar a las anteriores. Sin embargo, para realizar la adquisición de una unidad extraíble, se procederá siempre a realizar la adquisición de la misma forma, por lo que no será necesario elegir entre múltiples opciones.

Figura 51:Guía del procedimiento de adquisición almacenamiento externo



Fuente: Elaboración propia

4.3.5.2.Guía procesamiento

Una vez se ha realizado toda la adquisición, como bien se específica en el procedimiento, el próximo paso será procesar la información obtenida. Con el objetivo de guiar al usuario a dicha tarea, se ha agrupado de igual forma que la adquisición. Por un lado, se posee un epígrafe de descripción genérico del procesamiento de las distintas fuentes de información.

Figura 52: Descripción fase de procesamiento

Fuente: Elaboración propia

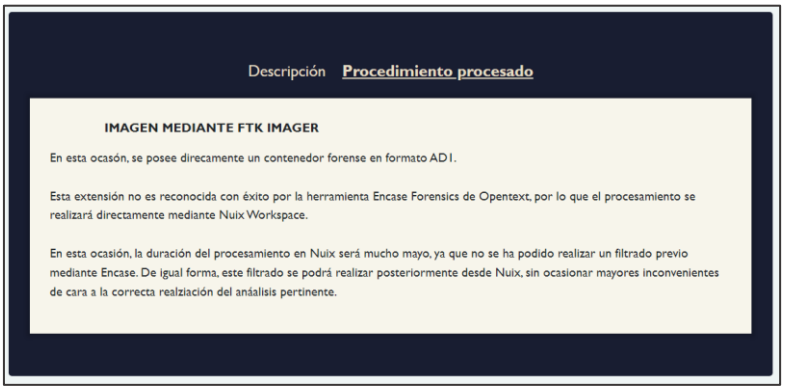
Y, por otro lado, existe una segunda vista, en la que se recogen distintas casuísticas que se deben contemplar para conocer qué tipo de procesamiento será el más adecuado. En este caso, sólo se podrá seleccionar una entre todas las opciones, ya que no pueden ocurrir de manera simultánea, ya que dependen del tipo de adquisición realizado previamente.

Figura 53: Guía del procedimiento de procesado

Fuente: Elaboración propia

En caso de que la opción seleccionada sea *"Copia en vivo mediante software FTK Imager"*, la vista que se mostrará será la siguiente.

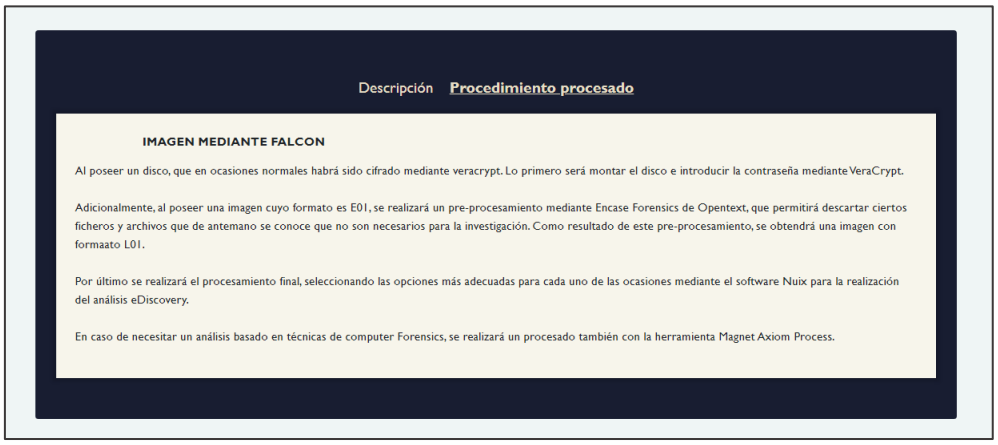
Figura 54: Guía del procedimiento de procesamiento mediante FTK



Fuente: Elaboración propia

En caso de que la opción seleccionada sea *"Copia mediante Logicube Falcon"*, la vista que se mostrará será la siguiente.

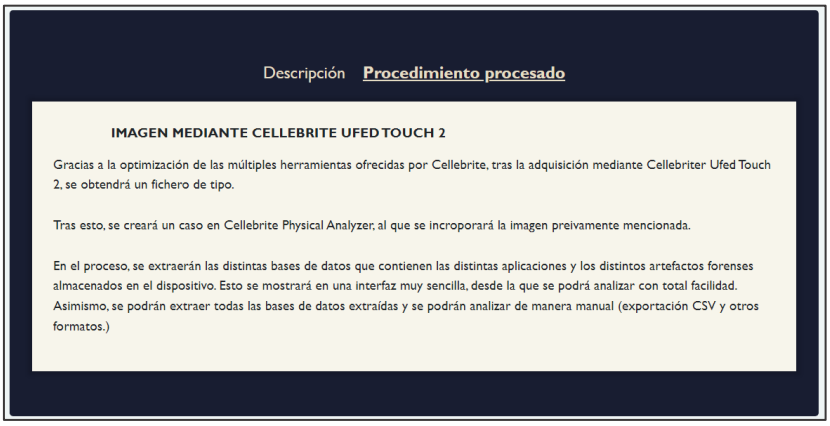
Figura 55: Guía del procedimiento de procesamiento mediante Falcon



Fuente: Elaboración propia

En caso de que la opción seleccionada sea *"Copia empleando Cellebrite UFED Touch 2"*, la vista que se mostrará será la siguiente.

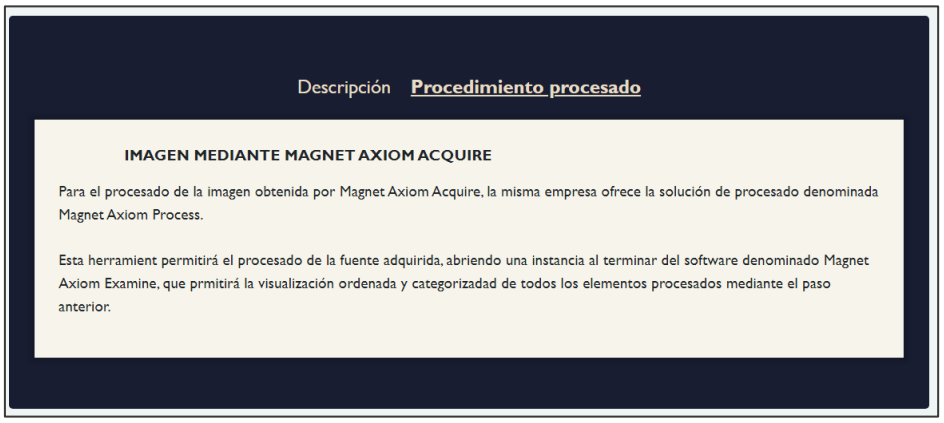
Figura 56: Guía del procedimiento de procesamiento mediante Cellebrite



Fuente: Elaboración propia

En caso de que la opción seleccionada sea *"Copia empleando software Magnet Axiom Acquire"*, la vista que se mostrará será la siguiente.

Figura 57: Guía del procedimiento de procesamiento mediante Axiom



Fuente: Elaboración propia

4.3.5.3.Guía filtrado

De igual manera que ocurre en las circunstancias anteriores, el primer contenido mostrado en la vista de filtrado es una descripción genérica que explica de manera general en qué consiste el proceso de filtrado y la importancia de una correcta planificación y realización de dichas tareas.

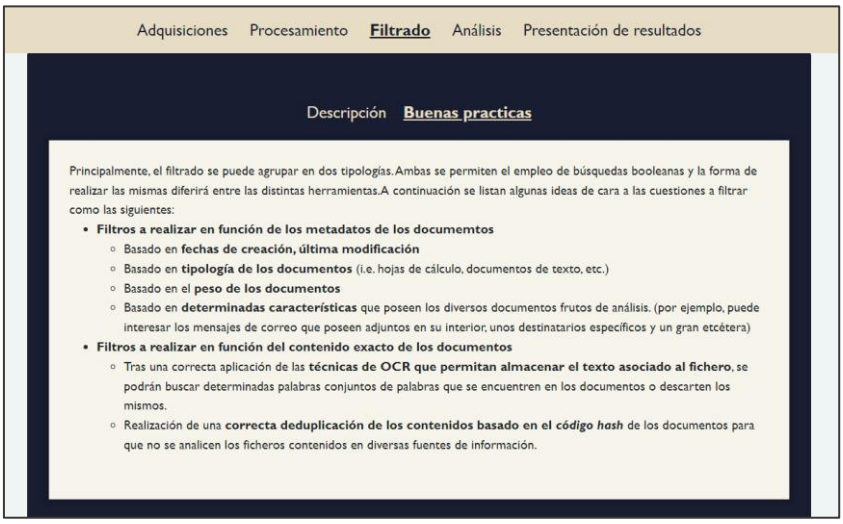
Figura 58: Descripción fase de filtrado

Fuente: Elaboración propia

En esta ocasión, el filtrado y las técnicas de filtrado para cada una de las casuísticas observadas dependerá del tipo de investigación, el contexto que se tenga de la misma y una serie de patrones que han de ser observados por analistas más experimentados.

Derivado de la imposibilidad de guiar a un usuario en una forma estática óptima de cómo realizar y aplicar las distintas técnicas de filtrado, se ha realizado una sección de buenas prácticas que sirva de soporte para comprender algunas cuestionas que no han de perderse de vista por parte del equipo resolutor.

Figura 59: Buenas prácticas fase de filtrado

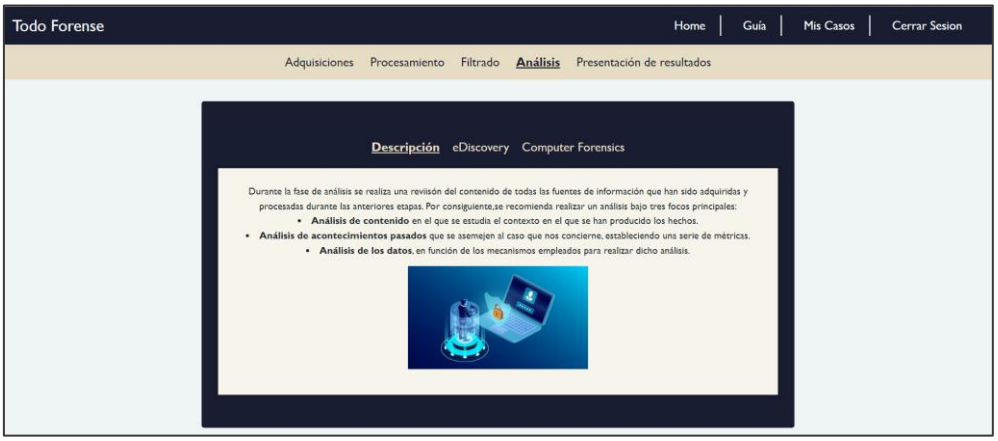


Fuente: Elaboración propia

4.3.5.4.Guía análisis

De nuevo, la primera vista mostrada, será una descripción de la fase de análisis del procedimiento desarrollado.

Figura 60: Descripción fase de análisis



Fuente: Elaboración propia

Por otro lado, se ha agrupado en dos grandes bloques en función del tipo de investigación que se va a llevar a cabo. En primera instancia, si la investigación que se va a realizar se trata de un *eDiscovery*, basado en la gestión de grandes volúmenes de información y un análisis del contenido de los documentos contenidos en el dispositivo, la información mostrada en la vista es la siguiente.

Figura 61: Guía análisis eDiscovery

Fuente: Elaboración propia

Por otro lado, si la investigación que se va a realizar se encuentra más ligada a la técnica *Computer Forensics*, la vista creada para documentar dicha tarea será similar a la adjunta en la siguiente imagen.

Figura 62: Guía análisis Computer Forensics

Fuente: Elaboración propia

Cabe destacar que para el análisis no se puede aportar unos conocimientos únicos, siendo indispensable una adaptación de la investigación al escenario observado. Por ello, siempre se recomienda la supervisión de superiores en todas las fases, ya que la experiencia es un factor diferenciador para el correcto entendimiento y gestión de una investigación informático-forense.

4.3.5.5.Guía presentación de resultados

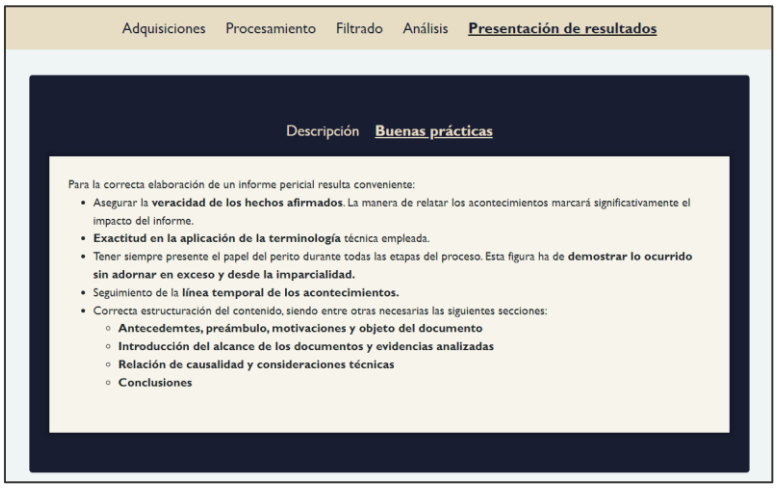
Por último, en lo relativo a la fase de presentación de resultados, se ha creado una vista denominada descripción, que mostrará a grandes rasgos en qué consiste esta fase del procedimiento.

Figura 63: Descripción fase de presentación de resultados

Fuente: Elaboración propia

Por otro lado, se cita alguna de las buenas prácticas existentes en materia de presentación de resultados, ya que un mal desarrollo de esta fase puede terminar en un mal entendimiento de lo ocurrido, así como una mala impresión por parte del juez/cliente o cualquiera que sea la entidad contratadora de estos servicios.

Figura 64: Buenas prácticas fase de presentación de resultados



Fuente: Elaboración propia

4.3.5.6.Posibles escenarios de error

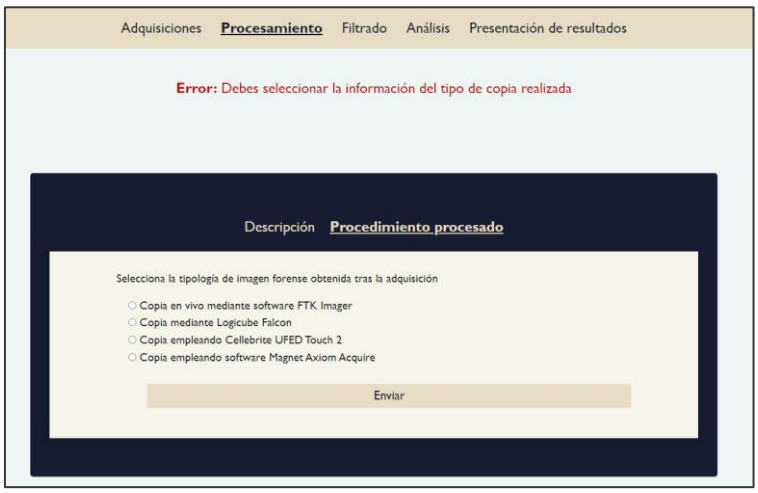
En primer lugar, como bien se ha anticipado anteriormente, en esta sección es requisito fundamental la elección de un tipo de dispositivo de manera obligatoria. Por ello, en caso de proceder sin haber seleccionado ninguno de los campos del formulario, se procede a excepcionar un mensaje de error que afirme *"Error: Debes seleccionar la información del tipo de dispositivo."*

Figura 65: Posibles escenarios de error fase de adquisición

Fuente: Elaboración propia

De igual forma que ocurre anteriormente, se ha de seleccionar al menos una de las opciones en la pestaña procedimiento procesado, obteniendo el mensaje *"Error: Debes seleccionar la información del tipo de copia realizada"* en caso de que esto no suceda de tal forma.

Figura 66:Posibles escenarios de error fase de adquisición



Fuente: Elaboración propia

Si bien no se ha adjuntado imagen de todos los formularios, en caso de no rellenar ninguna de las opciones en algún cuestionario, mostrará un mensaje de error por pantalla.

4.3.6. Revisión de mis casos

Una vez que el usuario ha iniciado sesión, como se ha mencionado anteriormente tiene la posibilidad de acceder a la vista de sus casos propios a través del botón "Mis casos", que se encuentra en la barra de navegación.

Figura 67: Barra de navegación tras iniciar sesión, "Mis casos"

Fuente: Elaboración propia

4.4.1.1. Creación de casos

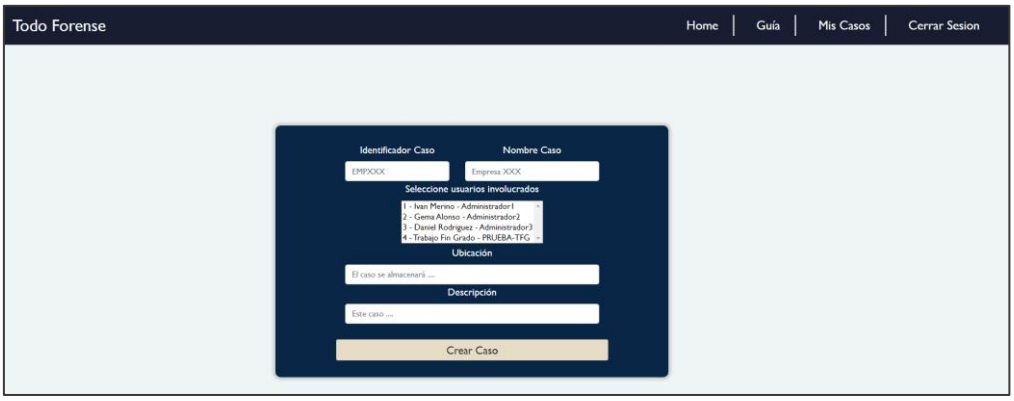
Una vez que el usuario ha accedido a "Mis Casos", se le redigirá a una vista en la que aparecerán todos sus casos abiertos, así como la opción de "Crear caso", "Ver casos cerrados" y "Ver casos archivados". Por tanto, para crear un caso deberá de seleccionar el botón disponible "Crear un caso".

Figura 68:Vista de "Mis Casos" con las opciones disponibles - Crear caso

Fuente: Elaboración propia

A la hora de crear el caso aparecerá el siguiente formulario con una serie de campos a rellenar por el usuario como es el caso del identificador, nombre, seleccionar los usuarios involucrados, la ubicación y una breve descripción; y acto seguido, pulsar el botón de crear caso.

Figura 69: Formulario a rellenar al Crear Caso



Fuente: Elaboración propia

4.4.1.2. Casos abiertos

Tal y como se ha mencionado anteriormente, una vez que el usuario pulse el botón de "Mis Casos" de la barra de navegación, se redigirá a una pantalla en la que se visualicen sus casos abiertos, así como tendrá la opción de crear un caso nuevo, archiva y cerrar un caso. A continuación, se adjunta a modo de ejemplo la pantalla para el usuario en el que se puede observar que tiene cuatro casos abiertos y las principales características (ID, Nombre, Descripción en formato resumido sobre estos y Estado)

Figura 70: Vista de "Mis Casos", con los casos abiertos y las distintas opciones

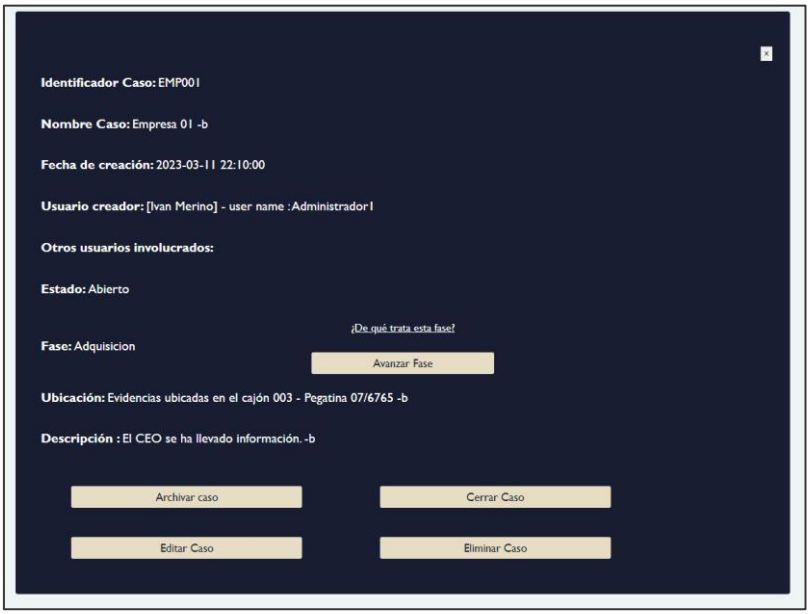
Fuente: Elaboración propia

- Mostrar más

Asimismo, tal y como se puede observar en la anterior pantalla, para cada uno de los casos que se encuentran abiertos existe la opción de hacer clic al botón *"Mostrar Más"*. Dicha acción permite el despliegue de una ventana en la que se detallan las características de los casos, incorporando información referente a la Fecha de Creación, Usuario Creador, Otros usuarios involucrados, Fase, Ubicación.

Por otro lado, permite al usuario realizar una serie de acciones que serán detalladas en otros puntos, como es el caso de obtener más información de la fase actual, de avanzar de fase, cerrar, archivar o editar el caso.

Figura 71: Vista "Mostrar Más" con toda la información relativa a un caso



Fuente: Elaboración propia

- ¿De qué trata esta fase?

En esta misma línea, en el caso de que el usuario pulse a la opción *"De qué trata esta fase?*, en función de la fase en la que se encuentre el caso, el usuario será redirigido

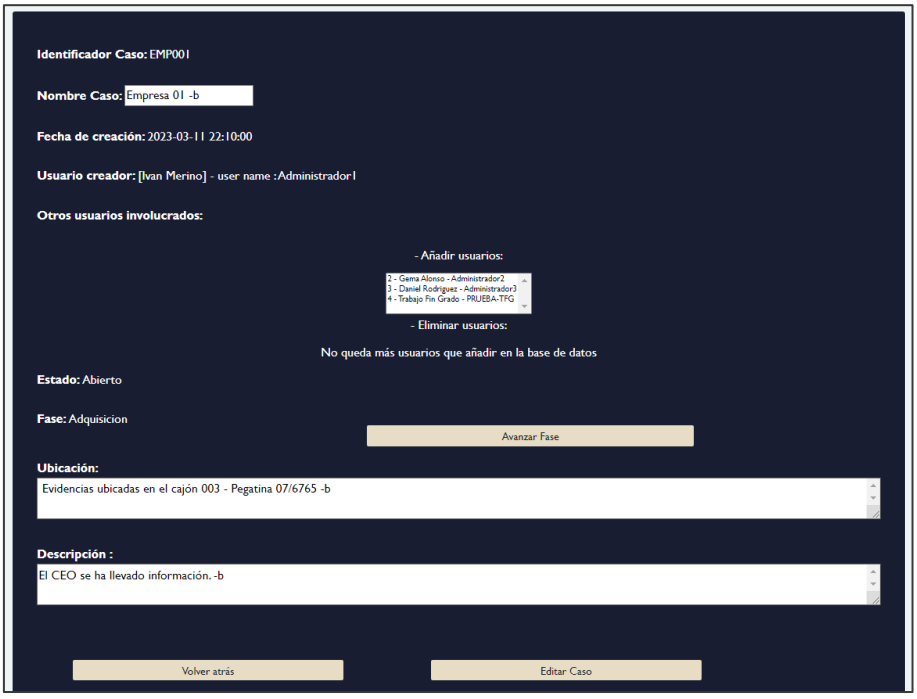
a Guía, en concreto en la fase en la que se encuentre. Por ejemplo, el caso que nos concierne se encuentra en la fase de Adquisición, si el usuario hace uso de esta funcionalidad será llevado a la parte de Adquisición que ha sido explicada anteriormente.

- Editar caso

Por otro lado, si se produce la casuística de que el usuario desea modificar alguna información relativa al caso, tiene la posibilidad de pulsar el botón *"*Editar Caso*"*, en consecuencia, se le actualizará la misma ventana, sin embargo, con una serie de campos disponibles para realizar los cambios convenientes. Los campos permitidos para que se puedan realizar modificaciones son el Nombre Caso, Otros Usuarios Involucrados, Ubicación y Descripción.

Una vez que el usuario haya realizado los pertinentes cambios tendrá la opción de confirmarlos pulsando al botón de *"*Editar Caso*"*, o si por el contrario desea retroceder, tendrá la opción de *"*Volver atrás*"*.

Figura 72:Vista de Editar Caso, con los campos editables para un caso de ejemplo



Fuente: Elaboración propia

Una vez el botón de editar caso haya sido accionado, se enviará el formulario, siendo estrictamente necesaria la confirmación de nuevo por parte del usuario, de la forma que se ha realizado en otras de las operaciones más importantes que se realizan sobre la base de datos.

- Avanzar de fase

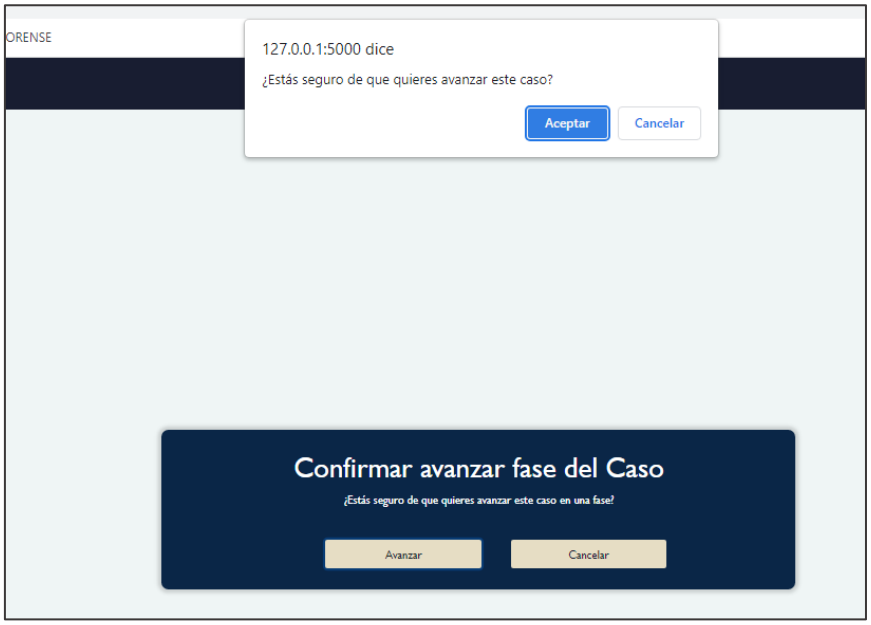
Por otro lado, otra de las funcionalidades comentadas anteriormente para el usuario es la posibilidad de Avanzar Fase, una vez que se haya completado los aspectos requeridos para la etapa en la que se encuentra. Para ello, tras pulsar a dicho botón aparecerá una ventana solicitando la confirmación del usuario para dicha acción. Por tanto, podrá pulsar "Avanzar" para seguir adelante con el propósito, o por el contrario "Cancelar" la operación regresando a la ventana detalla de dicho caso.

Figura 73: Ventana confirmación avance de fase de un caso

Fuente: Elaboración propia

Una vez que se ha confirmado el avance de la fase, el propio navegador *Chrome* solicita de nuevo la confirmación para continuar a la siguiente etapa. De tal forma, que aparece la ventana emergente que se observa a continuación, y, es necesario volver a indicar si se avanza o por el contrario se cancela este proceso.

Figura 74: Ventana confirmación Chrome avance de fase

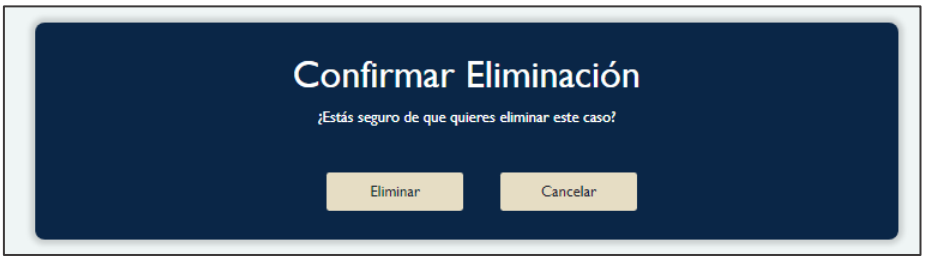


Fuente: Elaboración propia

- Eliminar caso

Otra de las opciones que el usuario podría realizar es la de *"*Eliminar Caso*"*. Para ello, se seguirá un procedimiento análogo al avance de fase que se ha observado anteriormente. Por tanto, una vez que el usuario haga clic a *"*Eliminar Caso*"*, aparecerá una ventana emergente solicitando la confirmación o cancelación del proceso, tal y como se aprecia a continuación:

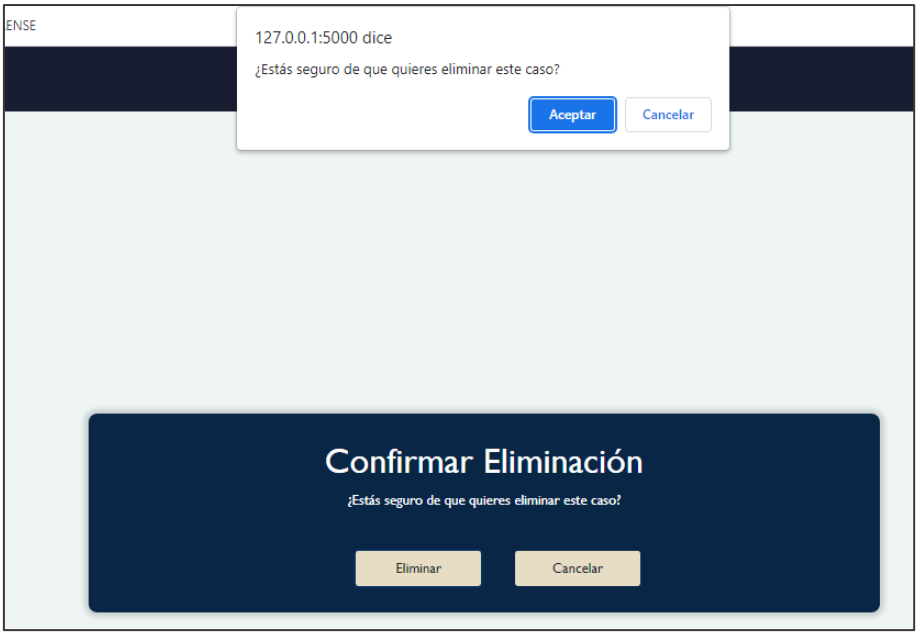
Figura 75: Ventana confirmación eliminación caso



Fuente: Elaboración propia

Cuando el usuario pulse el botón de "Eliminar", de nuevo, desde el navegador aparecerá otra ventana emergente, solicitando la confirmación de dicha eliminación. Al tratarse de acciones que realizan modificaciones en la base de datos del sistema, y con el riesgo de la pérdida de información, es conveniente tener esta doble confirmación, con el fin de asegurarnos que el usuario no borra por error dichos datos.

Figura 76: Ventana de Chrome confirmación eliminación de un caso



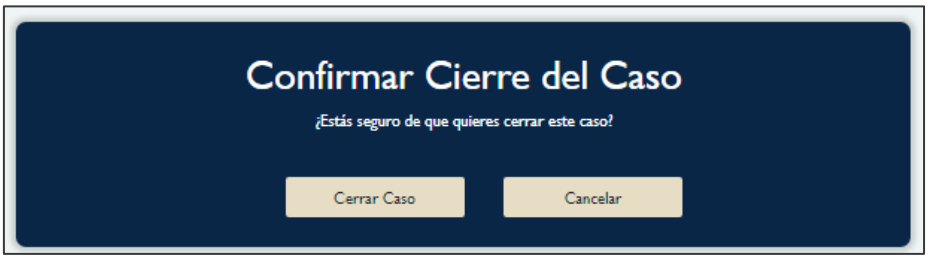
Fuente: Elaboración propia

- Cerrar caso

El usuario podrá cerrar cualquier caso que se encuentre abierto, en de las etapas que conforman procedimiento, debido a la renuncia del análisis de información, o cualquier otra causa que indica que se finaliza la investigación pudiendo haberla terminado o encontrándose en cualquiera de las fases.

De esta forma, se solicitará al usuario la confirmación del cierre del caso o en su defecto, la cancelación de este proceso, tal y como se puede observar a continuación:

Figura 77: Ventana confirmación cierre de un caso

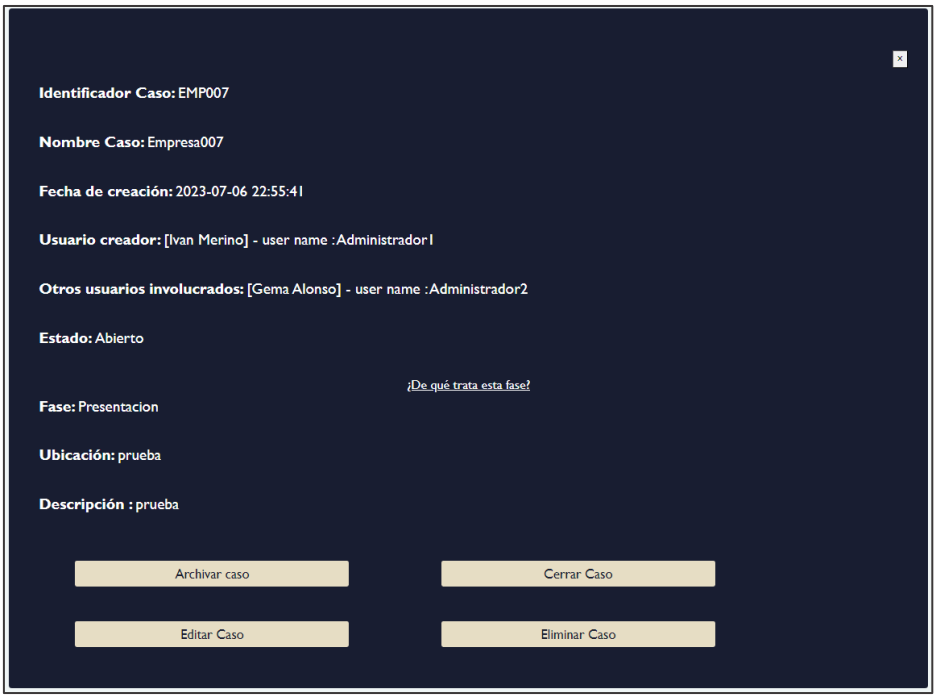


Fuente: Elaboración propia

- Archivar caso

El proceso de archivado del caso únicamente tendrá lugar cuando el estado de este sea Presentación, es decir, ya se han recorrido las distintas etapas y se han obtenido las evidencias y realizado el análisis necesario, cumpliendo con el procedimiento definido informático-forense. De tal manera, que por ejemplo el caso que se adjunta a continuación ya se encuentra en esa fase por lo que podría ser archivado. Para ello, el usuario dentro del caso que le concierne debe de pulsar el botón *"*Archivar Caso*"*.

Figura 78: Vista detalle de un caso con Fase "Presentación"



Fuente: Elaboración propia

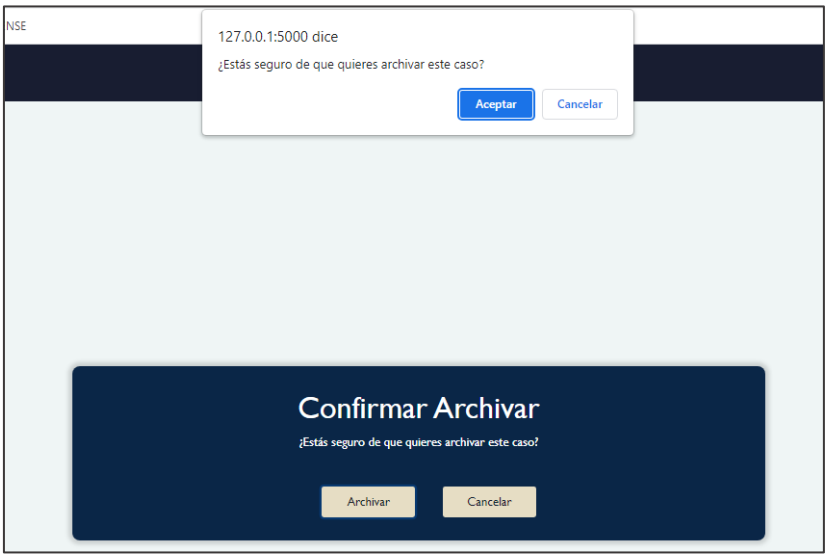
Al igual que se ha comentado en los anteriores casos de uso (cerrar caso, eliminar caso) a la hora de archivar un caso, al usuario se le mostrará una ventana emergente en la que deberá decidir la continuación o interrupción del proceso, tal y como se puede observar en la siguiente imagen:

Figura 79: Ventana emergente confirmación archivar caso

Fuente: Elaboración propia

En esta misma línea, desde el navegador *Google Chrome* solicitará al usuario de nuevo la confirmación del archivado del caso, apareciendo una ventana emergente tal y como se puede visualizar a continuación:

Figura 80: Ventana emergente Chrome confirmación archivado del caso



Fuente: Elaboración propia

4.4.1.3. Casos cerrados

Otra de las casuísticas que presenta la herramienta, es que a través de *"*Mis Casos*"*, el usuario puede acceder a la lista de los casos cerrados, que el usuario ha debido cerrar anteriormente por diversas causas. Para ello, pulsando al botón *"*Ver casos cerrados*"*, se le redirige a la siguiente pantalla, donde puede observar la información relativa al mismo. Por ejemplo, a continuación, se puede comprobar que el usuario únicamente tendría un caso cerrado. Además, cabe mencionar que se tendrían de nuevo las opciones disponibles relativas a *"*Mostrar Más*"* y *"*Eliminar Caso*"*.

Figura 81: Pantalla de visualización de los casos cerrados del usuario

Fuente: Elaboración propia

4.4.1.4. Casos archivados

En analogía con los casos abiertos y cerrados, el usuario desde "Mis Casos", tendrá la posibilidad de visualizar los casos que ha finalizado anteriormente, y, por lo tanto, han sido archivados. De esta forma, pulsando al botón *"*Ver casos archivados*",* se le redirige hacia la siguiente vista, en la que puede observar la información relativa a los mismos. Por ejemplo, en este caso únicamente el usuario tendría un caso archivado. Además, al igual que ocurre con los casos abiertos o cerrados el usuario tendría de nuevo las opciones que se corresponden con *"*Mostrar Más*"* y *"*Eliminar Caso*"*.

Figura 82: Visualización casos archivados

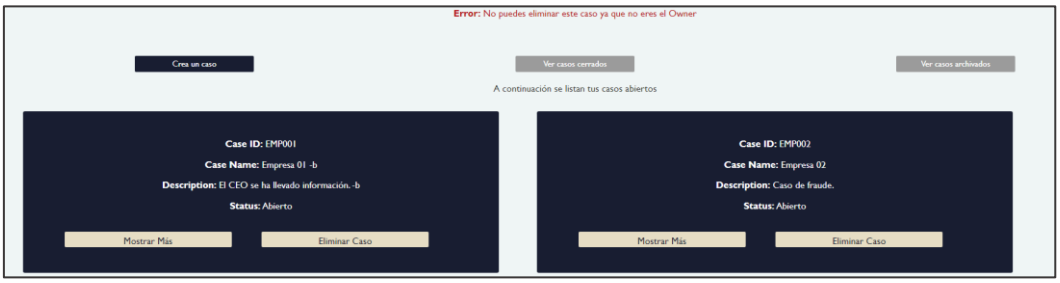
Fuente: Elaboración propia

4.4.1.5. Posibles escenarios de error

Se han desarrollado una serie de casuísticas para las cuales supondrían escenarios de error para el usuario en caso de que no se cumplan los requisitos establecidos a la hora de poder ejecutar las distintas funcionalidades que dispone la herramienta, en este caso desde la ventana de *"*Mis Casos*"*.

En primer lugar, cabe mencionar que para eliminar el caso es necesario que el usuario sea el *Owner* del mismo, es decir, no serviría con el que usuario se encuentre involucrado en este, sino que debe ser el propietario. Por tanto, si intenta realizar la eliminación de un caso del cual no es administrador aparecerá un mensaje de error tal y como se puede observar a continuación, interrumpiendo, por tanto, dicho proceso:

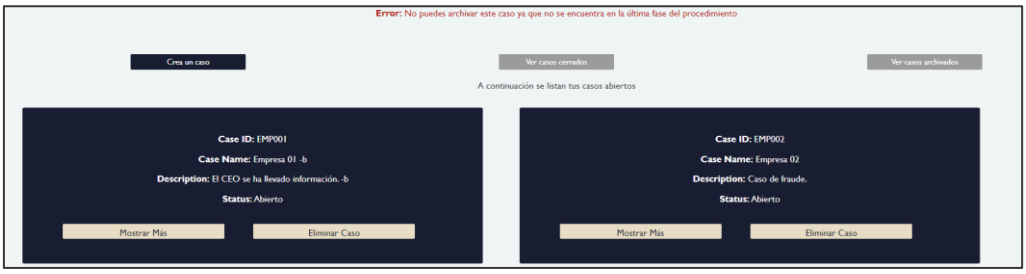
Figura 83: Error eliminación de caso, no siendo Owner de este



Fuente: Elaboración propia

Asimismo, tal y como se mención con anterioridad para poder archivar un caso, debe de encontrarse en la última fase del procedimiento (Presentación), por tanto, al tratar de archivar un caso que no se encuentre en dicha etapa, aparecerá el siguiente mensaje de error cancelando de forma automática el proceso:

Figura 84: Error archivado de caso por no encontrarse en la última etapa



Fuente: Elaboración propia

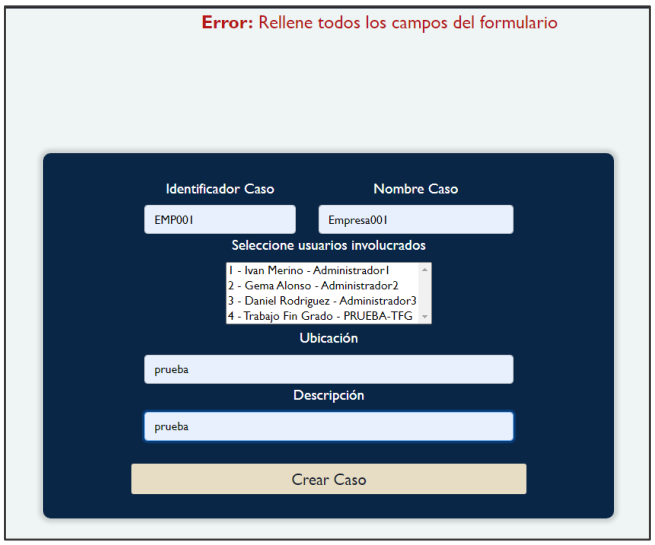
En esta instancia, existiría otro requisito a la hora de archivar un caso, el usuario también deberá ser *Owner* del mismo para poder realizar la acción. En caso contrario, aparecerá un mensaje de error indicando que dicha acción no se puede realizar y, se interrumpirá el proceso tal y como se adjunta a continuación en la imagen:

Figura 85: Error archivado de caso, no siendo el Owner de este

Fuente: Elaboración propia

Por otro lado, en el momento de crear un nuevo caso será necesario cumplimentar el formulario con todos los campos requeridos, ya que son obligatorios. En caso de que esto no se cumpla aparecerá un mensaje de error indicando la obligatoriedad de la información, tal y como se observa en la siguiente imagen:

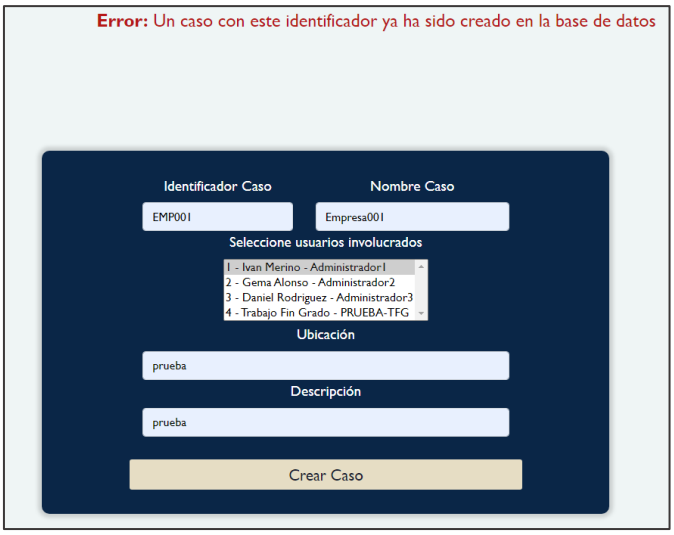
Figura 86: Error al no cumplimentar todos los campos en Crear Caso



Fuente: Elaboración propia

Además, en la funcionalidad de Crear Caso, el sistema realizará una validación con la base de datos, con el fin de determinar si el ID del caso ha sido ya introducido anteriormente por el usuario. De esta forma, si se comprueba que ya existe ese caso, se mostrará un mensaje de error indicando dicha información, posibilitando que el usuario introduzca de nuevo identificador.

Figura 87: Error en Crear Caso, identificador duplicado



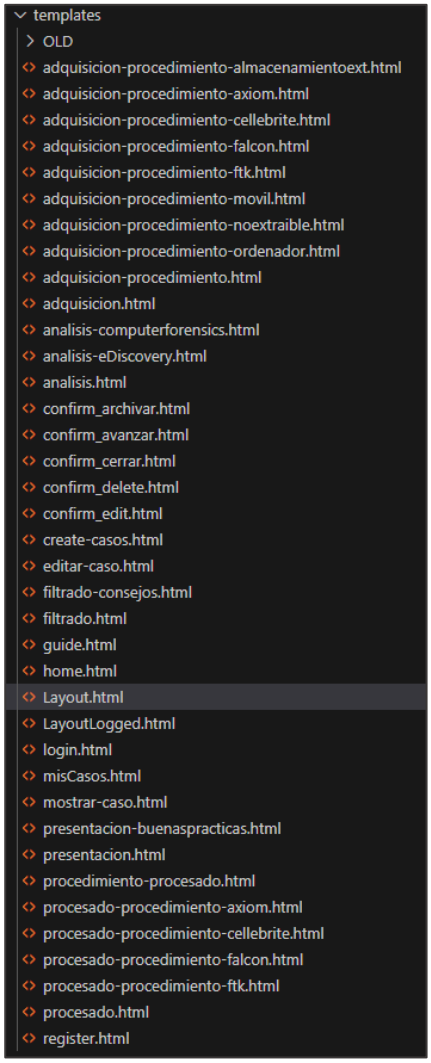
Fuente: Elaboración propia

4.4. Diseño interfaz gráfica (*front-end*)

En lo relativo al diseño de la interfaz gráfica, se han empleado plantillas de *HTML*, aportando formato a las mismas mediante hojas de estilos *css*. Asimismo, con el objetivo de no tener que crear todos los estilos desde cero, se ha incluido las utilidades del *framework Bootstrap*.

Todas las plantillas de *HTML* empleadas para dar funcionamiento a la aplicación se adjuntan a continuación. Cabe destacar que todas ellas están contenidas en el directorio *templates*.

Figura 88: Todas las plantillas HTML contenidas por la aplicación



Fuente: Elaboración propia

De entre todas ellas, se destaca la presencia de *Layout.html* y *LayoutLogged.html*, donde se ha configurado la inclusión de *css* y *Bootstrap* ya que estarán presente en todo el resto de las plantillas. Si bien ambas tienen prácticamente el mismo contenido, una de ellas será renderizada siempre que el usuario este logueado (y por ende en la barra de navegación se ve Home, Guía, Mis casos y Cerrar sesión), mientras que la otra será renderizada cuando el *logueo* no se haya realizado aún (Home, Guía, Iniciar Sesión y Registrar Usuario). La inclusión de los *frameworks* mencionados anteriormente se realiza de la siguiente forma.

Figura 89: Contenido template Layout.html (I)

```
<head>
  <style>
    body{
      background-color: #EFF5F5 !important;
    }
  </style>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Todo Forense</title>
    <!-- BOOTSRAP -->
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap@4.3.1/dist/css/bootstrap.min.css" integrity="sha384-ggOyR0iXCbMQ
    <!-- CUSTOM CSS -->
    <link rel="stylesheet" href="{{ url_for('static', filename='css/main.css')}}"></link>
</head>
```

Fuente: Elaboración propia

Asimismo, la barra de navegación de *Layout.html* se adjunta a continuación (siendo la de *LayoutLogged.html* similar, pero con los campos pertinentes). Cómo se puede observar, este código hace referencia a la barra de navegación renderizada en el resto de *templates* de la aplicación. Esta barra de navegación se incluye en el resto de las plantillas gracias al siguiente código.

Figura 90: Contenido template Layout.html (II)

```
{% with messages = get_flashed_messages() %}
  {% if messages %}
    <ul class=flashes>
  {% for message in messages %}
    <li>{{ message }}</li>
  {% endfor %}
  </ul>
  {% endif %}
{% endwith %}
<!--AQUÍ SE SITÚA NUESTRO CÓDIGO -->
{% block  content %}
{% endblock %}
```

Fuente: Elaboración propia

Como se observa en la anterior imagen, en las primeras líneas se crea un código que cargará mensajes mediante la función *get_flashed_messages()*, que permitirá cargar mensajes cuando sea necesario (especialmente relevante para enviar mensajes de error). En paralelo a esto, el código *"{% block content%}"* configura un bloque de contenido, dónde se cargarán el resto de las plantillas, aprovechando la barra de navegación y no teniendo que codificar estas cuestiones en todas las plantillas.

Asimismo, a continuación, se muestra cómo ejemplo la plantilla de registro. Como bien se comentaba anteriormente, nada más comenzar se extiende el funcionamiento de las plantillas *Layout.html* y *LayoutLogged.html*. En caso de estar el usuario *logueado*, se extenderá de la plantilla *layoutLogged.html*, mientras que, en su defecto, se renderizará *layout.html* en consonancia con lo mencionado anteriormente.

En paralelo a lo mencionado anteriormente, también se mostrará los mensajes de error en caso de haberlos. Los errores serán enviados desde *index.py*, donde se realizan las operaciones, para posteriormente renderizar las distintas plantillas.

Figura 91: Contenido template register.html (I)

```
{% if CurrentUser == -1 or currentUser == None %}
  {% extends "layout.html"%}
{% else %}
  {% extends "layoutLogged.html"%}
{% endif %}

{% block content %}
{% if error %}
    <p class="error color-rojo letra-20-2"><strong>Error:</strong> {{ error }}
{% endif %}
```

Fuente: Elaboración propia

En paralelo a esto, se ha escogido esta plantilla como ejemplo con el objetivo de mostrar uno de los múltiples métodos *POST* que se emplean para aportar la información contenida en un formulario y enviarlo al "gestor" de la base de datos.

Figura 92: contenido template register.html (II)

```
<form method="POST" action="/register" class="row" id="contenedor-registro">
    <div class="col-md-4">
      <label for="inputName" class="letra-15-izq form-label color-blanco">Nombre</label>
      <input class="form-control" id="nombre" placeholder="Paco" name="nombre">
    </div>
    <div class="col-md-5">
      <label for="InputApellido" class="letra-15-izq form-label color-blanco">Apellido</label>
      <input class="form-control" id="apellido" placeholder="Fernández López" name ="apellido">
    </div>
    <div class="col-md-9">
      <label for="inputEmail" class="letra-15-izq form-label color-blanco">Nombre Usuario</label>
      <input class="form-control" id="inputuserName" placeholder="Nombre de usuario" name="userName">
    </div>
    <div class="col-md-9">
      <label for="inputPassword" class=" letra-15-izq form-label color-blanco" >Contraseña</label>
      <input class="password form-control" id="inputPassword" placeholder="Contraseña" name="password" type="password">
    </div>
    <div class="col-9">
      <label for="inputRepeatPassword" class="letra-15-izq form-label color-blanco" type="password">Repite Contraseña</label>
      <input class="password form-control" id="repeatPassword" placeholder="Repite Contraseña" name="repeatPassword" type="password">
    </div>
    <div class="col-9">
      <label for="inputPhone" class=" letra-15-izq form-label color-blanco">Teléfono</label>
      <input class="form-control" id="inputPhone" placeholder="690387234" name="telefono">
    </div>
    <div class="col-12">
      <button type="submit" class="btn boton-crema-3">Registrar usuario</button>
    </div>
  </form>
  {% endblock%}
```

Fuente: Elaboración propia

Mediante este formulario, se podrán rellenar los distintos campos, y en caso de que todas las comprobaciones se realicen con éxito, se introducirá esta información en la base de datos. Este método se activará cuando el botón de tipo *submit* sea accionado. Asimismo, la acción que realizará el formulario al ser enviado es la denominada "/*register*". Para ver el manejo y la obtención de los datos contenidos en esta plantilla cuando se realiza el método *post*, consultar el apartado siete de este mismo epígrafe.7

Una vez han sido documentadas algunas de las principales plantillas empleadas en la herramienta, se prosigue a comentar la plantilla de mis casos, que será invocada cuando un usuario logueado, desee consultar cualquier información relativa a las investigaciones en las que se encuentra involucrado.

Para ello, desde el fichero *index.py*, serán enviadas una serie de variables, que contienen la información de los distintos casos codificada como listas de objetos *JSON*. Dejando de lado algunas de las cuestiones contenidas por la plantilla como son las plantillas del frontal explicadas anteriormente, se adjunta a continuación el código responsable de la comprobación de los casos en los que se encuentra involucrado un usuario, permitiendo navegar entre casos abiertos, cerrados o archivados en caso de encontrarse involucrado en estos.

Figura 93: Contenido template misCasos.html (I)

```
{% if sizeCasos == 0 %}
  <p class="color-gris letra-20-2">No se encuentra en ningún caso. Crea tu propio caso pulsando el botón.</p>
{% endif %}
{% if estadoAux == "Abierto" %}
  <div class = "row-2">
    <div class="col-md-4">
      <button class="boton-azul-2 " onclick="location.href='/create-casos'">Crea un caso</button>
    </div>
    {% if sizeCerrados != 0 %}
    <div class="col-md-4">
      <button class="boton-azul-2 " onclick="location.href='/misCasosCerrados'">Ver casos cerrados</button>
    </div>
    {% else %}
    <div class="col-md-4">
      <button class="boton-gris disabled" >Ver casos cerrados</button>
    </div>
    {% endif %}
    {% if sizeArchivados != 0 %}
      <div class="col-md-4">
    <button class="boton-azul-2 " onclick="location.href='/misCasosArchivados'">Ver casos archivados</button>
    </div>
    {% else %}
      <div class="col-md-4">
      <button class="boton-gris disabled" >Ver casos archivados</button>
      </div>
    {% endif %}
  </div>
<br>
<p class="color-gris letra-20-2">A continuación se listan tus casos abiertos</p>
{% endif %}
```

Fuente: Elaboración propia

Como se puede observar, si la variable "*estadoAux*" se encuentra iniciada al valor abierto, esto significa que el usuario desea conocer los casos en los que se encuentra involucrado cuyo estado es abierto. Por ello, no existe un botón con el texto ver casos abiertos, ya que esto es lo que se estaría mostrando por pantalla gracias al código existente tras el adjunto anteriormente.

Cabe destacar que este código ha debido ser diseñado de distinta forma para cada uno de los posibles estados en los que se encuentra un caso.

Una vez se ha seleccionado que tipo de casos se desea observar por parte del usuario, se procede a listar con ayuda del siguiente fragmento de código de *javascript*, todos los casos en los que el usuario se encuentra involucrado. Esto se conseguirá recorriendo y *parseando* la lista de objetos *JSON* que recibe esta plantilla, y creando un objeto de clase *jumbotron* por cada caso observado.

Figura 94: Contenido template misCasos.html (II)

```
<div id="case-list"></div>
  <script>

    const todosCasos = {{ (todosCasos | tojson) | safe }};

    console.log(todosCasos);
    const caseList = document.getElementById('case-list');
    aux=1;
    row=1;
    const caseBox1 = document.createElement('div');
    caseBox1.className = 'row-2';
    todosCasos.forEach(caso => {
      const caseBox = document.createElement('div');
      if (row % 2 == 1){
        caseList.appendChild(caseBox1);
      }
      if(aux % 2 == 1){
        caseBox.className = 'jumbotron ml-5 letra-20-2 color-blanco col-md-5 mr-5 mb-3';
      } else {
        caseBox.className = 'jumbotron letra-20-2 color-blanco col-md-5 mb-3 ml-5';
      }
        caseBox.innerHTML+=`
          <p><strong>Case ID:</strong> ${caso.idCaso}</p>
          <p><strong>Case Name:</strong> ${caso.nombreCaso}</p>
          <p><strong>Description:</strong> ${caso.descripcion}</p>
          <p><strong>Status:</strong> ${caso.estado}</p>
          <div class="row-2">
          <div class="col-md-5 mr-4">
          <button class="btn boton-crema-2" onclick="location.href='/mostrarCaso/${caso.idCaso}'">Mostrar Más</button>
          </div>
          <div class="col-md-5">
          <button class="btn boton-crema-2" onclick="location.href='/eliminarCaso/${caso.idCaso}'">Eliminar Caso</button>
          </div>
          </div>
        `;
```

Fuente: Elaboración propia

Figura 95: Contenido template misCasos.html (III)

```
        aux ++;
        row ++;
        caseBox1.appendChild(caseBox);

      });
    </script>
```

Fuente: Elaboración propia

Aplicando la lógica explicada anteriormente, se puede afirmar que cada *JSON*, se corresponde con un caso, por lo que la cantidad de casos mostrados por pantallas será equivalente a la lista de objetos *JSON* recibida por esta plantilla. Cómo se puede observar en los campos del objeto de clase jumbotron, no toda la información contenida por el caso se mostrará por pantalla, correspondiéndose esto con un resumen de las principales características del caso.

Para observar más información, se deberá pulsar en el botón que posee el texto Mostrar Más, que redirigirá a */mostrarCaso/*idCaso**, permitiendo que el fichero *index.py* ejecute la función pertinente y muestre por pantalla la información consultada sobre la base de datos respecto a uno de los casos específicos.

La plantilla donde se muestra un solo caso, o se permite la edición de este, actúa siguiendo estos conceptos, aunque con las modificaciones necesarias para su correcta operativa.

Pasando a otras de las plantillas realizadas, se ha implementado la denominada *guide.html*, que permite realizar tareas vinculadas con la guía de usuarios en la aplicación. En primer lugar, se ha realizado una barra de navegación similar a la observada en las plantillas, cambiando el color y dónde se establecerán los distintos valores (fases del procedimiento) disponibles en la guía.

Figura 96: Contenido template guide.html (I)

```
<ul class="nav color-crema1 justify-content-center">
    <li class="nav-item active">
        <a class="nav-link color-negro letra-20" href="/adquisicion">Adquisiciones</a>
      </li>
    <li class="nav-item active">
        <a class="nav-link color-negro letra-20" href="/procesado">Procesamiento</a>
      </li>
    <li class="nav-item active">
        <a class="nav-link color-negro letra-20" href="/filtrado">Filtrado</a>
      </li>
    <li class="nav-item active">
        <a class="nav-link color-negro letra-20" href="/analisis">Análisis</a>
    </li>
    <li class="nav-item active">
        <a class="nav-link color-negro letra-20" href="/presentacion">Presentación de resultados</a>
    </li>
</ul>
```

Fuente: Elaboración propia

Asimismo, esta plantilla se trata de la pantalla de bienvenida de las guías, donde se describen brevemente cada una de las falles, pudiendo acceder a información más detallada de cada una de ellas.

Figura 97:Contenido template guide.html (II)

```
<section>
    <div class="containerCentro">
      <div class="presentationCentro">
        <div class="presentation__text color-grisoscuro">
        <h4>El procedimiento está formado por las siguientes etapas </h4>
          </p>
        </div>
      </div>
    </div>
  </section>
    <section>
        <div class="containercaja2">
          <div class="actions">
            <div class="actions__box2 color-grisoscuro">
              <h2>Adquisición </h2>
              <p>Conoce la información relativa a la correcta extracción de los datos contenidos en las distintas fuentes electrónicas.</p>
              <a href="/adquisicion">Ver más</a>
            </div>
            <div class="actions__box2 color-grisoscuro">
              <h2>Procesamiento</h2>
              <p>Extrae toda la información contenida en las adquisiciones de los dispositivos identificados como relevantes para la investigac
              <a href="/procesado">Ver más</a>
            </div>
            <div class="actions__box2 color-grisoscuro">
              <h2>Filtrado</h2>
              <p>Reconoce los principales acontecimientos del caso y elimina los datos menos relevantes para la investigación.</p>
              <a href="/filtrado">Ver más</a>
            </div>
            <div class="actions__box2 color-grisoscuro">
              <h2>Análisis</h2>
              <p>Identifica la información primordial para reconstruir los hechos acontecidos.</p>
              <a href="analisis">Ver más</a>
            </div>
            <div class="actions__box2 color-grisoscuro">
              <h2>Presentación de resultados</h2>
              <p>Culmina el procedimiento mediante la elaboración del informe pericial o presenta de manera organizada tus resultados.</p>
              <a href="presentacion">Ver más</a>
            </div>
          </div>
        </div>
      </section>
```

Fuente: Elaboración propia

Una vez el usuario acciona una de las fases que desea consultar, se renderiza una nueva plantilla. En este caso, se ha escogido de ejemplo la plantilla donde se renderiza el procedimiento de adquisición de ordenadores. Como se observa a continuación, se observarán múltiples *checkbox*, que podrán ser elegidos en función de las características del dispositivo que va a ser adquiridos.

Al existir opciones que no pueden ser elegidas de manera simultánea se han agrupado por grupos con el objetivo de que sólo un elemento de cada grupo pueda ser elegido. Por ejemplo, las opciones “el ordenador se encuentra encendido” y “el ordenador se encuentra apagado” se sitúan dentro del grupo 3, dónde en caso de seleccionar las dos a la vez, sólo se mostrará seleccionada la última que ha sido pulsada.

Asimismo, cualquier error acontecido a la hora de accionar el botón de tipo submit, será enviado a esta plantilla desde el gestor de la aplicación, mostrándose el error al renderizarse esta plantilla.

Figura 98:Contenido template adquisicion-procedimiento-ordenador.html (I)

```
{% if error %}
    <p class="error color-rojo letra-20-2"><strong>Error:</strong> {{ error }}
{% endif %}
<br>
<div class="jumbotron-container">
  <div class="jumbotron">
    <form method="POST" action="/adquisicion-procedimiento-ordenador">
    <div class="btn-group">
      <a href="/adquisicion" class="btn color-crema letra-20" >Descripción</a>
      <a href="/adquisicion-procedimiento" class="btn subrayado-crema color-crema letra-20" aria-current="page" >Procedimiento adquisicion</a>
    </div>
    <p></p>
    <div class="contenedor-claro texto-contenedor">
      <div class="letra-15 margen-contenedor"> <b>ORDENADOR</b>
        <p></p>
      </div>
      <div class="letra-15 margen-contenedor"> Selecciona las características de tu dispositivo:
        <p></p>
      </div>
        <div class="form-check letra-15 margen-contenedor">
          <input type="radio" value="1" name="group1"> Disco duro interno se puede extraer
        </div>
        <div class="form-check letra-15 margen-contenedor">
          <input type="radio" value="2" name="group2"> Se conocen las claves del dispositivo
        </div>
        <div class="form-check letra-15 margen-contenedor">
          <input type="radio" value="3" name="group3"> El equipo se encuentra encendido
        </div>
        <div class="form-check letra-15 margen-contenedor">
          <input type="radio" value="4" name="group3"> El equipo se encuentra apagado
        </div>
        <input class="boton-crema" type="submit">
    </div>
  </div>
</div>
</form>
```

Fuente: Elaboración propia

Cabe destacar que al haber escogido botones de tipo "*radio-button*", una vez se ha escogido un valor en una celda, este no puede ser desactivado pulsando encima de el de nuevo. Esta funcionalidad ha sido añadida en la herramienta mediante el siguiente código de *javascript*. Esto ha sido realizado para evitar que una equivocación al pulsar en un botón pudiera llevar consigo una peor experiencia por parte del usuario.

Figura 99: Contenido template adquisicion-procedimiento-ordenador.html (II)

```
<script>
  var radioBtns = document.querySelectorAll('input[name="group1"]');
  var checked1;

  radioBtns.forEach(function(radioBtn) {
    radioBtn.addEventListener('click', function() {
      if (checked1 === this) {
        this.checked = false;
        checked1 = null;
      } else {
        checked1 = this;
      }
    });
  });

  </script>
  <script>
    var radioBtns = document.querySelectorAll('input[name="group2"]');
    var checked2;

    radioBtns.forEach(function(radioBtn) {
      radioBtn.addEventListener('click', function() {
        if (checked2 === this) {
          this.checked = false;
          checked2 = null;
        } else {
          checked2 = this;
        }
      });
    });

    </script>
```

Fuente: Elaboración propia

Una vez se ha explicado la funcionalidad de guía, se procede a documentar el contenido del fichero denominado *editar-caso.html*. Este ha sido incluido en la memoria por ser uno de los códigos más complejos implementado para la herramienta.

La variable de tipo caso, que ha sido enviada al renderizar la plantilla, se muestra por pantalla dentro de un formulario. Los campos que son editables se muestran dentro de un campo de tipo input, mientras que los no editables aparecen directamente escritos. Esto evitará que determinadas características de la base de datos no puedan ser modificadas, evitando conflictos.

Asimismo, al poder añadir y eliminar usuarios, se ha de crear dos listas, que serán mostradas en pantalla, en función de usuarios que ya están en el caso (y podrán ser eliminados) o usuarios que no se encuentran involucrados (y, por ende, pueden ser añadidos). Los usuarios serán mostrados en un objeto de tipo *select*, donde cada una de las opciones será un usuario de la herramienta, pudiendo el actor elegir cero, uno o más usuarios que desea involucrar o sacar de un caso.

Figura 100: Contenido template editar-caso.html (I)

```
<div class="jumbotron-container-2">
<div class="jumbotron">
  <div class="col-md-12">
    <p class="letra-20-izq form-label color-blanco"><strong>Identificador Caso: </strong> {{ caso.idCaso }} </p>
  </div>
  <br>
  <div class="col-md-12">
    <p class="letra-20-izq form-label color-blanco"><strong>Nombre Caso: </strong>
      <input id="nombreCaso" name="nombreCaso" value="{{ caso.nombreCaso }}"> </p>
    </p>
  </div>
  <br>
  <div class="col-md-12">
    <p class="letra-20-izq form-label color-blanco"><strong>Fecha de creación: </strong> {{ caso.fecha }} </p>
  </div>
  <br>
  <div class="col-md-12">
    <p class="letra-20-izq form-label color-blanco"><strong>Usuario creador: </strong> {{ caso.usuarioOwner }} </p>
  </div>
  <br>
  <div class="col-md-12">
    <p class="letra-20-izq form-label color-blanco"><strong>Otros usuarios involucrados: </strong> {{ caso.listaUsuarios }} </p>
  </div>
  <br>
  <div class="col-md-12">
    <p class="letra-20-med form-label color-blanco">- Añadir usuarios:</p>
      {% if notIncludedUsersSize == 0 %}
      <p class="letra-20-med form-label color-blanco">No queda más usuarios que añadir en la base de datos</p>
      {% endif %}
      {% if notIncludedUsersSize != 0 %}
      <select id="include-users" name="selected-users" multiple>
      <p class="letra-20-med form-label color-blanco">notIncludedUsersSize</p>
        {% for user in notIncludedUsers %}
          <option value="{{ user.id }}">{{ user.id }} - {{ user }} {{ user.apellido }} - {{ user.nombreUsuario }}</option>
        {% endfor %}
      </select>
      {% endif %}
```

Fuente: Elaboración propia

Otras de las características permitidas en la ventana de edición es avanzar de fase la investigación. Este botón será mostrado exclusivamente cuando la fase en la que se encuentre sea distinta a "presentación" ya que esta es la última, no siendo posible avanzar la fase. Una vez se pulsa el botón, se procede a modificar la *URL* a *localhost/avanzarFase/*casoId**, gestionándose la petición y siendo necesaria una confirmación para realizar esta actividad en la base de datos.

Figura 101: Contenido template editar-caso.html (II)

```
<div class="row-2">
  <p class="col-md-4 letra-20-izq form-label color-blanco"><strong>Fase: </strong> {{ caso.fase }}
    {% if not (caso.fase == "Presentacion") %}
    <div class="col-md-6">
      <button type="submit" class="btn boton-crema-3" id="avanzarFase">Avanzar Fase</button>
    </div>
    {% endif %}
    <script>
      const avanzarFaseBtn = document.getElementById('avanzarFase');
      avanzarFaseBtn.addEventListener('click', () => {
        window.location.href = '/avanzarFase/{{caso.idCaso}}';
      });
    </script>
  </p>
</div>
<br>
```

Fuente: Elaboración propia

Cómo ejemplo de ventana de confirmación creada, se adjunta a continuación el código implementado para a plantilla *confirm_edit.html*. Como se puede observar, se solicitará una aprobación por parte del usuario, pudiendo este aprobar la operación o volver a la página anterior.

Una vez el botón confirmar sea accionado, se procederá a codificar los datos recibidos, para enviar de manera codificada a través de la *URL*. Esta información será recibida por el gestor de la aplicación, obteniendo los nuevos datos introducidos y realizando la modificación pertinente en la base de datos.

Figura 102: Contenido template confirm_edit.html (I)

```
{% block content %}
    <script>
      function confirmEdit() {
        if (confirm("¿Estás seguro de que quieres editar este caso?")) {
          const ubicacionval = "{{ubicacion}}";
          const descripcionval = "{{descripcion}}";
          const nombreval = "{{nombre}}"
          const addUsersval = "{{addUsers}}"
          const deleteUsersval = "{{deleteUsers}}"
          const url = '/editarCaso/{{caso.idCaso}}?ubicacion=' + encodeURIComponent(ubicacionval.trim()) + '&descripcion=' + encodeURIComponent(
          form.action = url;
          document.getElementById("edit-form").submit();
        }
      }
    </script>
    <div class="contenedor">
        <div class="contenedorcentrado">
            <div class="confirmDelete">
                <h1 class="color-blanco">Confirmar Editar Caso</h1>
                <p class="color-blanco">¿Estás seguro de que quieres editar este caso?</p>
                <form id="edit-form" method="POST">
                <div class="row-2">
                    <div class="col-6">
                        <button class="btn boton-crema-2" type="submit" onclick="confirmEdit()">Editar</button>
                    </div>
                    <div class="col-6">
                        <button class="btn boton-crema-2" type="button" onclick="window.history.back()">Cancelar</button>
                    </div>
                </div>
                </form>
            </div>
        </div>
    </div>
{% endblock%}
```

Fuente: Elaboración propia

4.5. Diseño y gestión de la base de datos (back-end)

Si bien anteriormente, se han mencionado todos los mecanismos empleados para la construcción de la propia interfaz gráfica, muchas de las operaciones realizan operaciones CRUD (*Create*, *Read*, *Update and Delete*) sobre una base de datos. Estas operaciones se encuentran controladas todas mediante el fichero *index.py*, que se encarga de gestionar todas las operaciones realizadas en la herramienta (tanto redirecciones de la interfaz gráfica, como asegurar la adecuación de las operaciones sobre la base de datos y distintos algoritmos necesarios para el correcto funcionamiento de la herramienta)

Cabe destacar que se han creado dos ficheros de *Python* para la configuración de la base de datos. En primer lugar, el denominado *bd.py*, donde se establecen algunos de las importaciones de distintas librerías necesarias, inicialización y configuración de distintas variables para el correcto funcionamiento de la base de datos.

Figura 103: Contenido del fichero bd.py

```
from sqlalchemy import create_engine
from sqlalchemy.ext.declarative import declarative_base
from sqlalchemy.orm import sessionmaker

engine = create_engine('sqlite:///mydatabase.db', connect_args={'check_same_thread': False})

Base = declarative_base()

Base.metadata.create_all(engine)
Session = sessionmaker(bind=engine)
session = Session()
```

Fuente: Elaboración propia

En contraposición, se cuenta con el fichero denominado *models.py* donde se definirá la estructura de las distintas tablas contenidas en la base de datos, así como algunas de las operaciones básicas necesarias para el correcto funcionamiento de la herramienta. A continuación, se adjuntan las importaciones necesarias para este módulo de la herramienta.

Figura 104: Contenido del fichero models.py (I)

```
import db
from datetime import datetime
from enum import Enum


from sqlalchemy import Column, Integer, String, DateTime, Enum
```

Fuente: Elaboración propia

Asimismo, la tabla denominada usuario, tendrá las columnas id, nombreUsuario, nombre, apellido, *password* y teléfono. La base de datos ha sido configurada de tal forma que la clave primaria es el *id* (número entero) y ninguna de las columnas podrá ser inicializada sin valor.

En paralelo a esto, se observan algunas de las funciones básicas como son *__init__*, implementada para inicializar nuevos objetos en la tabla usuario o *__repr__* y *__str__* para representar o imprimir los distintos objetos de la tabla usuario.

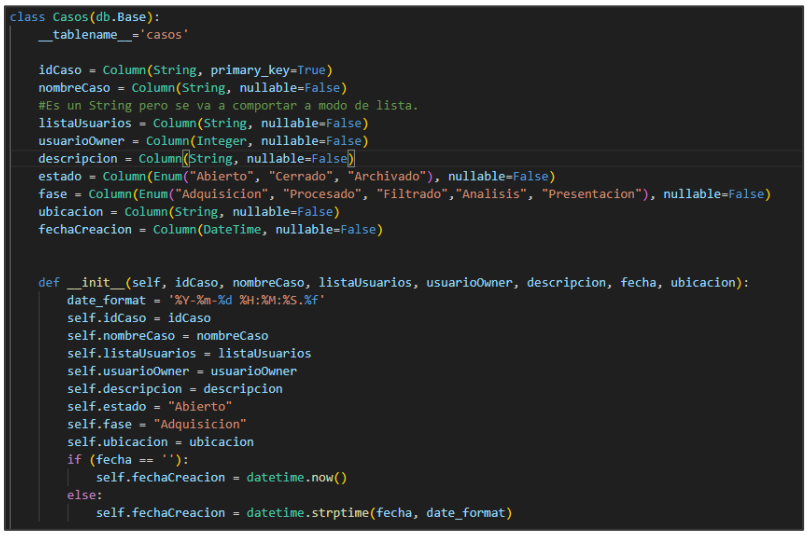
Figura 105: Contenido del fichero models.py (II)

```
class Usuario(db.Base):
    __tablename__='usuario'

    id = Column(Integer, primary_key=True)
    nombreUsuario = Column(String, nullable=False)
    nombre = Column(String, nullable=False)
    apellido = Column(String, nullable=False)
    password = Column(String, nullable=False)
    telefono = Column(Integer, nullable=False)

    def __init__(self, nombre, apellido, nombreUsuario, password, telefono):
        identificador = db.session.query(Usuario).count() + 1
        self.nombre = nombre
        self.apellido = apellido
        self.nombreUsuario = nombreUsuario
        self.password = password
        self.id = identificador
        self.telefono = telefono

    def __repr__(self):
        return f'Usuario({self.id}, {self.nombre}, {self.apellido}, {self.nombreUsuario}, {self.password}, {self.telefono})'

    def __str__(self):
        return self.nombre
```

Fuente: Elaboración propia

De igual manera que en la tabla usuario, la tabla denominada casos posee las columnas idCaso (clave primaria), nombreCaso, listaUsuarios, usuarioOwner, descripción, estado, fase, ubicación y fechaCreación. En este caso, de igual manera que ocurría anteriormente, ninguno de los valores de las distintas columnas podrá ser inicializado vacío. Asimismo, cabe destacar la peculiaridad de las columnas fase y ubicación, que funcionan a modo de set de texto predefinidos, que permitirán que los datos posibles para esas variables estén siempre inicializados a valores correctos.

Figura 106: Contenido del fichero models.py (III)



```python
class Casos(db.Base):
    __tablename__='casos'

    idCaso = Column(String, primary_key=True)
    nombreCaso = Column(String, nullable=False)
    #Es un String pero se va a comportar a modo de lista.
    listaUsuarios = Column(String, nullable=False)
    usuarioOwner = Column(Integer, nullable=False)
    descripcion = Column(String, nullable=False)
    estado = Column(Enum("Abierto", "Cerrado", "Archivado"), nullable=False)
    fase = Column(Enum("Adquisicion", "Procesado", "Filtrado","Analisis", "Presentacion"), nullable=False)
    ubicacion = Column(String, nullable=False)
    fechaCreacion = Column(DateTime, nullable=False)


    def __init__(self, idCaso, nombreCaso, listaUsuarios, usuarioOwner, descripcion, fecha, ubicacion):
        date_format = '%Y-%m-%d %H:%M:%S.%f'
        self.idCaso = idCaso
        self.nombreCaso = nombreCaso
        self.listaUsuarios = listaUsuarios
        self.usuarioOwner = usuarioOwner
        self.descripcion = descripcion
        self.estado = "Abierto"
        self.fase = "Adquisicion"
        self.ubicacion = ubicacion
        if (fecha == ''):
            self.fechaCreacion = datetime.now()
        else:
            self.fechaCreacion = datetime.strptime(fecha, date_format)
```

Fuente: Elaboración propia

En paralelo a esto, en la imagen adjunta anteriormente se puede observar la función *__init__* empleada para crear las distintas filas necesarias para crear un "objeto".

A continuación, se adjuntan algunas de las funciones implementadas relativas a la tabla Casos, que permitirán entre otras avanzar la fase en la que se encuentra un caso, añadir un usuario como analista y eliminar un usuario entre los que se encuentran involucrados en un caso.

Figura 107: Contenido del fichero models.py (IV)

```python
def __str__(self):
    return self.nombreCaso

def avanzarCaso(self):
    if self.fase == "Adquisicion":
        self.fase = "Procesado"
    elif self.fase == "Procesado":
        self.fase = "Filtrado"
    elif self.fase == "Filtrado":
        self.fase = "Analisis"
    elif self.fase == "Analisis":
        self.fase = "Presentacion"
    return self

def addUsuarios (self, addUsers):
    if (addUsers != '' and addUsers != ' ' and addUsers != None):
        self.listaUsuarios += '·'+ addUsers
    return self

def deleteUsuarios (self, deleteUsers):
    if (deleteUsers != '' and deleteUsers != ' ' and deleteUsers != None):
        if ('·' in deleteUsers):
            listaUsuariosToDelete = [int(x) for x in deleteUsers.split('·')]
        else:
            listaUsuariosToDelete = []
            listaUsuariosToDelete.append(int(deleteUsers))
        listaUsuariosAux = [int(x) for x in self.listaUsuarios.split('·')]
        for item in listaUsuariosToDelete:
            listaUsuariosAux.remove(item)
        separador = "·"
        self.listaUsuarios = separador.join(str(num) for num in listaUsuariosAux)
    return self
```

Fuente: Elaboración propia

4.6. Gestión, comunicación front-end back-end y principales funciones.

Como se ha adelantado anteriormente, todas las redirecciones necesarias para el correcto funcionamiento del *front-end*, así como las consiguientes comprobaciones para

asegurar la ausencia de errores en el comportamiento deseado por parte del usuario y las operaciones CRUD sobre la base de datos se realizan todas en el fichero denominado *index.py*.

Este fichero será ejecutado para la puesta en marcha de la herramienta. Todo esto se realizará gracias al código que se adjunta a continuación, en el que se inicia la base de datos. En caso de que la BBDD no se encuentre configurada, se inicializará con algunos valores por defecto para asegurar que siempre hay determinados usuarios al comienzo de la aplicación. Sin embargo, si ya existen usuarios, simplemente se hará un recuento de todos los casos creados en el equipo, así como todos los usuarios ya existentes en la herramienta.

Figura 108: Contenido del fichero index.py (I)

```python
#Para hacer que nuestra apliación este escuchando siempre hacemos lo siguiente
#Validación para comprobar que estamos en el fichero principal. Este es el que va a emjecutar nuestra aplicación.
if __name__ == '__main__':
    db.Base.metadata.create_all(db.engine)
    #debug=true va a hacer que nuestra aplicación se acutoactualice a medida que se le van incorporando cambios.
    #Creamos una sola vez la abse de datos
    totalAntiguo = db.session.query(Usuario).count()
    if(totalAntiguo == 0):
        dbIni()
    users = db.session.query(Usuario).all()
    casos = db.session.query(Casos).all()
    app.run(debug=True)
```

Fuente: Elaboración propia

A continuación se adjunta la información contenida en la función *dbIni()*, que será invocada en caso de que no se encuentre el fichero *mydatabase.db* en el directorio de la herramienta.

Figura 109: Contenido del fichero index.py (II)

```python
#incializador de la base de datos
def dbIni():
    administrador1 = Usuario ('Ivan', 'Merino', 'Administrador1', [redacted], 99)
    db.session.add(administrador1)
    administrador2 = Usuario ('Gema', 'Alonso', 'Administrador2', [redacted], 96)
    db.session.add(administrador2)
    caso1 = Casos ('EMP001', 'Empresa 01', '1-2', '1', 'El CEO se ha llevado información.', '2023-03-11 22:10:00.000', '
    db.session.add(caso1)
    caso2 = Casos ('EMP002', 'Empresa 02', '1-2','2', 'Caso de fraude.', '2023-03-10 13:30:00.000', "Evidencias ubicadas
    db.session.add(caso2)
    caso3 = Casos ('EMP003', 'Empresa 03', '1-2', '1', 'Amenazas por parte de un empleado.', '2023-02-05 11:21:13.000',
    db.session.add(caso3)
    caso4 = Casos ('EMP004', 'Empresa 04', '1-2','2', 'Caso de suplantación de identidad.', '', "Evidencias ubicadas en
    db.session.add(caso4)
    db.session.commit()
```

Fuente: Elaboración propia

Las distintas importaciones de distintos *frameworks*, así como como configuraciones iniciales de la herramienta se adjuntan a continuación.

Figura 110: Contenido del fichero index.py (III)

```
#Importamos el framework Flask
from flask import Flask, render_template, request, flash, jsonify, redirect, session, url_for
#Para la creación de usuarios y todos los eventos relacionados que han de ser invocados desde aquí
from models import Usuario,Casos,CurrentUser
import db
import json


#Con esto le diremos a nuestra aplicación que ha de empezar aquí (junto a if name == main)
app = Flask(__name__)
app.secret_key = 'miClavePrivada12345678901234567890887654321'
```

Fuente: Elaboración propia

La primera de las plantillas que va a ser renderizada es la denominada *home.html*. Está página se renderizará siempre que, por URL, se obtenga algo similar a lo siguiente *http://XXXX/*, siendo XXXX el dominio sobre el que se encuentre alojada la aplicación y siendo en el caso que nos concierne, el puerto 5000 del host local.

Figura 111: Contenido del fichero index.py (IV)

```
#Con esto creamos la ruta principal
@app.route('/', methods=['GET','POST'])
def home():
    global CurrentUser
    return render_template('home.html', CurrentUser=CurrentUser)
```

Fuente: Elaboración propia

Una vez se han documentado algunas de las funciones más sencillas, se procede a listar algunas de las funciones que bien por su complejidad o importancia son más relevantes para el correcto funcionamiento de la herramienta.

- *Login()*

Esta función será renderizada cuando en la URL se redireccione a */login*. Cómo se puede observar, con esta función se pueden realizar peticiones tanto *GET*, cómo *POST*. En caso de existir una petición de tipo *POST*, se obtendrá el valor contenido en los campos usuario y *password* del formulario.

Acto seguido, se obtendrán los usuarios almacenados en la tabla Usuario, comprobando así, si existen las credenciales introducidas. En caso de existir las credenciales introducidas, se procederá a renderizar la plantilla *home.html* vinculada con la página de bienvenida de la aplicación. Por el contrario, se renderizará de nuevo la plantilla *login.html*, enviando la variable error, con el valor "Las credenciales introducidas no son correctas".

Figura 112: Contenido del fichero index.py (V)

```python
@app.route('/login', methods=['GET','POST'])
def login():
    global CurrentUser
    error = None
    if request.method == 'POST' :
        nombreAux=request.form.get('usuario')
        passwordAux=request.form.get('password')
        all = db.session.query(Usuario).all()
        for usuario in all:
            if usuario.nombreUsuario == nombreAux:
                if(passwordAux == usuario.password):
                    CurrentUser = usuario.id
                    return render_template('home.html', CurrentUser=CurrentUser)
        error = 'Las credenciales introducidas no son correctas'
    return render_template('login.html', error=error, CurrentUser=CurrentUser)
```

Fuente: Elaboración propia

- *Register()*

La función denominada *register* empleada para la creación de nuevos usuarios y accionada mediante la *URL host\register*, permite peticiones de tipo *GET* y *POST*.

De igual manera que la mencionada anteriormente, la información de los campos es recogida en caso de que el método sea de tipo *POST*. Una vez estos datos son introducidos en el frontal de la aplicación, se procede a comprobar que los valores introducidos son correctos y completos. En caso de encontrarse algún error de los contemplados por la aplicación, se procederá a dar valor a la variable denominada error.

Por último, en caso de que todo se realice de manera exitosa, se creará un objeto de tipo usuario, se incorporará a la base de datos y se renderizará la plantilla *login.html*, documentada anteriormente. En contraposición, si ha ocurrido algún error, se procede a renderizar la plantilla de registro, con la variable error enviada como parámetro.

Figura 113: Contenido del fichero index.py (VI)

```python
@app.route('/register', methods=['GET','POST'])
def register():
    error = None
    if request.method == 'POST' :
        nombreAux=request.form.get('nombre')
        nombreAux2 = nombreAux.replace(" ","")
        apellidoAux=request.form.get('apellido')
        apellidoAux2 = apellidoAux.replace(" ","")
        userNameAux=request.form.get('userName')
        passwordAux=request.form.get('password')
        repeatPasswordAux=request.form.get('repeatPassword')
        telefonoAux=request.form.get('telefono')
        all = db.session.query(Usuario).all()
        yaExistente = False
        for usuario in all:
            if usuario.nombreUsuario == userNameAux and not yaExistente:
                yaExistente = True
        if(passwordAux != repeatPasswordAux):
            error="Introduzca contraseñas iguales en los dos campos"
        elif(nombreAux == '' or apellidoAux == '' or userNameAux == '' or passwordAux == '' or repeatPasswordAux == '' or telefonoAux == ''):
            error="Rellene todos los campos del formulario"
        elif not nombreAux2.isalpha() or not apellidoAux2.isalpha():
            error="El nombre o apellido no puedo contener caracteres numéricos."
        elif yaExistente:
            error="Este nombre de usuario ya existe"
        else:
            newUser = Usuario(nombreAux, apellidoAux, userNameAux, passwordAux, telefonoAux)
            db.session.add(newUser)
            db.session.commit()
            return render_template('login.html',error=error, CurrentUser=CurrentUser)
    return render_template('register.html',error=error, CurrentUser=CurrentUser)
```

Fuente: Elaboración propia

- *createCaso()*

La función *createCaso*() puede renderizar peticiones de tipo *GET* y *POST*. En caso de ser la segunda tipología la realizada desde el frontal de la aplicación, se procede a obtener toda la información introducida en el formulario.

Para la creación de objetos en la base de datos, en primer lugar, se hará una serie de comprobaciones necesarias para garantizar la correcta introducción de información a la base de datos.

Cabe destacar, que el campo que codificar la lista de usuarios que participa en la investigación en el frontal, genera una lista de elementos, que, en función de los valores seleccionados, necesitará un *parseo* de lista a cadena de caracteres para la correcta introducción de estos valores en el *backend* de la herramienta.

Asimismo, una vez se han realizado todas las asignaciones necesarias, se procede a crear un objeto de tipo caso, incluyendo este a la base de datos y realizando un *commit* de la base de datos al final siempre, para asegurar que la información añadida se crea de manera persistente en el resto de las sesiones.

Figura 114: Contenido del fichero index.py (VII)

```
@app.route('/create-casos', methods=['GET', 'POST'] )
def create_casos():
    error = None
    global CurrentUser
    if request.method == 'POST':
        idCasoAux=request.form.get('idCaso')
        nombreCasoAux=request.form.get('NombreCaso')
        descripcionAux=request.form.get('descripcion')
        ubicacionAux=request.form.get('ubicacion')
        usersAuxList=request.form.getlist('selected-users')
        usersAux =''
        for eachUser in usersAuxList:
            if(usersAux == ''):
                usersAux += eachUser
            else:
                usersAux += "-"+ str(eachUser)
        print(usersAux)
        all = db.session.query(Casos).all()
        casoExistente = False
        if usersAux == None:
            usersAux = ''
        for caso in all:
            if caso.idCaso == idCasoAux and not casoExistente:
                casoExistente = True
        if(nombreCasoAux == '' or ubicacionAux == '' or descripcionAux == '' or usersAux == ''):
            error="Rellene todos los campos del formulario"
        #elif not estadoAux.isalpha() or not descripcionAux.isalpha():
        #    error="El estado y/o la descripción no pueden contener caracteres numéricos"
        elif casoExistente:
            error="Un caso con este identificador ya ha sido creado en la base de datos"
        else:
            listaUsuariosAux = [int(x) for x in usersAux.split('-')]
            if not (CurrentUser in listaUsuariosAux):
                usersAux += "-"+ str(CurrentUser)
            newCaso = Casos(idCasoAux, nombreCasoAux, usersAux, CurrentUser, descripcionAux, '', ubicacionAux)
            db.session.add(newCaso)
            print(newCaso)
            db.session.commit()
            return redirect('/misCasos')
    return render_template('create-casos.html', CurrentUser=CurrentUser, usersList = db.session.query(Usuario).all(), error=error)
```

Fuente: Elaboración propia

- *misCasos()*

Una vez el usuario se encuentra *logueado* en el sistema, se seleccionan todos los casos asociados a este actor. Se crearán tres listas que, en función del estado en el que se encuentran los casos, creará un objeto *JSON* con toda la información observada en la base de relativos a estos objetos, obteniendo así una serie de listas con toda la información de los casos en los que participa un usuario, agrupados en base al estado en el que este se encuentra.

Cómo variables para el renderizado de la plantilla misCasos.html, se pasa entre otras el identificador de usuario *logueado*, una lista con los identificadores de los casos abiertos, cantidad de casos abiertos, cantidad de casos cerrados, cantidad de casos archivados, lista con todos los casos cerrados, lista con todos los casos archivados y la variable de error que recogerá cualquier anomalía en las operaciones mencionadas anteriormente.

Figura 115: Contenido del fichero index.py (VIII)

```python
@app.route('/misCasos')
def misCasos():
    global CurrentUser
    error=session.pop('error',None)
    listaIdCasos = []
    todosCasos = []
    casosCerrados = []
    casosArchivados=[]
    all = db.session.query(Casos).all()
    for caso in all:
        listaUsuariosAux = [int(x) for x in caso.listaUsuarios.split('·')]
        if(CurrentUser in listaUsuariosAux and caso.estado == "Abierto"):
            todosCasos.append({'idCaso':caso.idCaso, 'nombreCaso':caso.nombreCaso, 'descripcion':caso.descripcion, 'estado':caso.estado})
            listaIdCasos.append(caso.idCaso)
        if(CurrentUser in listaUsuariosAux and caso.estado == "Cerrado"):
            casosCerrados.append({'idCaso':caso.idCaso, 'nombreCaso':caso.nombreCaso, 'descripcion':caso.descripcion, 'estado':caso.estado})
        if(CurrentUser in listaUsuariosAux and caso.estado == "Archivado"):
            casosArchivados.append({'idCaso':caso.idCaso, 'nombreCaso':caso.nombreCaso, 'descripcion':caso.descripcion, 'estado':caso.estado})
    return render_template('misCasos.html', CurrentUser=CurrentUser, listaIdCasos=listaIdCasos,
                           sizeCasos=len(listaIdCasos), todosCasos=todosCasos, error=error, estadoAux="Abierto",
                           sizeCerrados= len(casosCerrados), sizeArchivados=len(casosArchivados))
```

Fuente: Elaboración propia

- mostrarCaso(caso_id)

La función mostrarCaso, que recibirá cómo parámetros el identificadore del caso, obtendrá en primera instancia toda la información asociada al caso seleccionado consultando directamente sobre la base de datos.

En base a la información obtenida, se procederá a codificar esta información en formato *JSON*, para poder enviar a la plantilla toda la información vinculada con el objeto consultado. Esta plantilla de *HTML* dará formato a los datos contenidos en el objeto *JSON*.

Figura 116: Contenido del fichero index.py (IX)

```python
@app.route('/mostrarCaso/<caso_id>', methods=['GET','POST'])
def mostrarCaso(caso_id):
    list=[]
    global CurrentUser
    casoAux = db.session.query(Casos).get(caso_id)
    usersAux=casoAux.listaUsuarios
    owner = db.session.query(Usuario).get(casoAux.usuarioOwner)
    listaUsuariosAux = [int(x) for x in usersAux.split('·')]
    stringListaUsuarios= ''
    for user in listaUsuariosAux:
        if (user != casoAux.usuarioOwner):
            if(stringListaUsuarios == ''):
                stringListaUsuarios += "[" + db.session.query(Usuario).get(user).nombre + " " +  db.session.query(Usuario).get(user).apellido + "
            else :
                stringListaUsuarios += " | " + db.session.query(Usuario).get(user).nombre + " " +  db.session.query(Usuario).get(user).apellido +
    casoDict = {
        "idCaso": casoAux.idCaso,
        "nombreCaso": casoAux.nombreCaso,
        "usuarioOwner": "[" + owner.nombre + " " +  owner.apellido + "] - user name : " + owner.nombreUsuario ,
        "listaUsuarios": stringListaUsuarios,
        "descripcion": casoAux.descripcion,
        "estado": casoAux.estado,
        "fecha": casoAux.fechaCreacion.strftime('%Y-%m-%d %H:%M:%S'),
        "ubicacion": casoAux.ubicacion,
        "fase": casoAux.fase
    }
    casoText = json.dumps(casoDict)
    caso = json.loads(casoText)
    return render_template('mostrar-caso.html', caso=caso)
```

Fuente: Elaboración propia

- ventanaEditarCaso(caso_id)

La función ventanaEditarCaso, obtendrá como elemento adjunto en la *URL*, el identificador del caso que se desea editar. Una de las comprobaciones necesarias para la correcta gestión de esta acción, será asegurar que el usuario que está realizando estas operaciones es el *owner*, ya que en su defecto, no podrán ser realizadas modificaciones.

Una vez toda la información del caso es consultada sobre la base de datos en base al identificador recibido, se crea un objeto *JSON* para pasarle a la interfaz gráfica de la herramienta, de modo que pueda se mostrada en el frontal.

Asimismo, al tratarse de una edición y existir una lista de usuarios, se ha de distinguir entre los que se encuentran involucrados en el caso y los que no. Esto se realiza porque en el momento de la edición de un caso, desde el frontal se crea un campo del formulario de adición de usuarios al caso (entre los que se encuentran involucrados) y de eliminación de estos (entre los ya involucrados).

Figura 117: Contenido del fichero index.py (X)

```python
@app.route('/ventanaEditarCaso/<caso_id>', methods=['GET','POST'])
def ventanaEditarCaso(caso_id):
    global CurrentUser
    casoAux = db.session.query(Casos).get(caso_id)
    usersAux=casoAux.listaUsuarios
    owner = db.session.query(Usuario).get(casoAux.usuarioOwner)
    listaUsuariosAux = [int(x) for x in usersAux.split('·')]
    stringListaUsuarios= ''
    includedUsers = []
    for user in listaUsuariosAux:
        includedUsers.append(db.session.query(Usuario).get(user))
        if (user != casoAux.usuarioOwner):
            if(stringListaUsuarios == ''):
                stringListaUsuarios += "[" + db.session.query(Usuario).get(user).nombre + " " +  db.session.query(Usuario).get(user).apellido + "]
            else :
                stringListaUsuarios += " | " + db.session.query(Usuario).get(user).nombre + " " +  db.session.query(Usuario).get(user).apellido + "
    casoDict = {
        "idCaso": casoAux.idCaso,
        "nombreCaso": casoAux.nombreCaso,
        "usuarioOwner": "[" + owner.nombre + " " +  owner.apellido + "] - user name : " + owner.nombreUsuario ,
        "listaUsuarios": stringListaUsuarios,
        "descripcion": casoAux.descripcion,
        "estado": casoAux.estado,
        "fecha": casoAux.fechaCreacion.strftime('%Y-%m-%d %H:%M:%S'),
        "ubicacion": casoAux.ubicacion,
        "fase": casoAux.fase
    }
    casoText = json.dumps(casoDict)
    caso = json.loads(casoText)
    if (not casoAux.usuarioOwner == CurrentUser):
        session['error']="No puedes editar este caso ya que no eres el Owner"
    todosUsuarios = db.session.query(Usuario).all()
    todosUsuarios.remove(owner)
    notIncludedUsers = []
    for usuario in todosUsuarios:
        if not usuario in includedUsers:
            notIncludedUsers.append(usuario)
    if owner in notIncludedUsers:
        notIncludedUsers.remove(owner)
    if owner in includedUsers:
        includedUsers.remove(owner)
    return render_template('editar-caso.html', caso=caso, notIncludedUsers = notIncludedUsers , includedUsers=includedUsers, notIncludedUsersSize =
```

Fuente: Elaboración propia

- archivarCaso(caso_id)

Si bien esta función sirve como ejemplo de una modificación específica de un campo contenido por un objeto caso, hay múltiples funciones que poseen esta estructura.

En este código, en caso de tratarse del usuario creador del caso, se procede a renderizar una plantilla de confirmación. Desde esta plantilla, se recibirá una petición de tipo *POST* en caso de que se realice con éxito, pudiendo así modificar el campo estado ha archivado.

En caso de que cualquiera de las condiciones mencionadas anteriormente no sea satisfecho, se procede a mostrar por pantalla un mensaje de error que hace referencia a la incompatibilidad de realización de dicha acción.

Figura 118: Contenido del fichero index.py (XI)

```python
@app.route('/archivarCaso/<caso_id>', methods=['GET','POST'])
def archivarCaso(caso_id):
    global CurrentUser
    caso = db.session.query(Casos).get(caso_id)
    if (caso.usuarioOwner == CurrentUser and caso.fase == "Presentacion"):
        if request.method =='POST':
            caso.estado = "Archivado"
            db.session.commit()
            return redirect("/mostrarCaso/" + caso_id)
        else:
            return render_template('confirm_archivar.html', caso=caso)
    else:
        if(not caso.usuarioOwner == CurrentUser):
            session['error']="No puedes archivar este caso ya que no eres el Owner"
        else:
            session['error']="No puedes archivar este caso ya que no se encuentra en la última fase del procedimiento"
        return redirect("/misCasos")
```

Fuente: Elaboración propia

- adquisición_procedimiento_movil()

Se ha escogido un ejemplo de función relacionada con la explicación de adquisiciones en dispositivos móviles. Cabe destacar que toda la parte de guía ha sido implementada de esta forma pese a haber escogido este código como ejemplo.

Esta función será renderizada cuando la *URL* sea /adquisición-procedimiento-móvil, procediendo a recoger todos los valores contenidos en los distintos grupos de elementos de *check* e introduciéndolo en una lista.

Posteriormente, se comprobará qué valores han sido introducidos y en base a la inteligencia aplicada, relacionando las elecciones con el procedimiento informático-forense diseñado, se procederá a renderizada una de las plantillas. En función de qué *template* sea renderizado, se explicará cada uno de los procedimientos más aptos para las características de la adquisición observada.

Figura 119:Contenido del fichero index.py (XII)

```python
@app.route('/adquisicion-procedimiento-movil', methods=['GET','POST'])
def adquisicion_procedimiento_movil():
    error=session.pop('error',None)
    list2 = []
    if request.method == 'POST':
        if 'group1' in request.form:
            list2.append(request.form['group1'])
        if 'group2' in request.form:
            list2.append(request.form['group2'])
        if 'group3' in request.form:
            list2.append(request.form['group3'])
        if('1' in list2 and not '2' in list2 and not '3' in list2 and not '4' in list2):
            return redirect(url_for('adquisicion_procedimiento_cellebrite'))
        if('1' in list2 and '3' in list2 and not '2' in list2 and not '4' in list2):
            return redirect(url_for('adquisicion_procedimiento_cellebrite'))
        if('1' in list2 and not '2' in list2 and not '3' in list2 and '4' in list2):
            return redirect(url_for('adquisicion_procedimiento_axiom'))
        if('1' in list2 and '3' in list2 and not '4' in list2 and '2' in list2):
            return redirect(url_for('adquisicion_procedimiento_cellebrite'))
        if('1' in list2 and '2' in list2 and not '3' in list2 and not '4' in list2):
            return redirect(url_for('adquisicion_procedimiento_cellebrite'))
        if('1' in list2 and '2' in list2 and '4' in list2 and not '3' in list2):
            return redirect(url_for('adquisicion_procedimiento_axiom'))
        if('2' in list2 and not '1' in list2 and not '3' in list2 and not '4' in list2):
            return redirect(url_for('adquisicion_procedimiento_cellebrite'))
        if('2' in list2 and '3' in list2 and not '1' in list2 and not '4' in list2):
            return redirect(url_for('adquisicion_procedimiento_cellebrite'))
        if('2' in list2 and not '1' in list2 and not '3' in list2 and '4' in list2):
            return redirect(url_for('adquisicion_procedimiento_axiom'))
        if('3' in list2 and not '1' in list2 and not '2' in list2 and not '4' in list2):
            return redirect(url_for('adquisicion_procedimiento_cellebrite'))
        if('4' in list2 and not '2' in list2 and not '3' in list2 and not '1' in list2):
            return redirect(url_for('adquisicion_procedimiento_axiom'))
        if(not '1' in list2 and not '2' in list2 and not '3' in list2 and not '4' in list2):
            error= "Debes seleccionar al menos una casuistica"
    return render_template('adquisicion-procedimiento-movil.html', CurrentUser=CurrentUser, error=error)
```

Fuente: Elaboración propia

4.7. Instalación de las tecnologías y puesta en marcha de la aplicación

Para la puesta en marcha de todos los requisitos mencionados previamente, en primer lugar, se ha de abrir una consola de comandos, y navegar hasta el directorio en el que se encuentre la herramienta.

Posteriormente, se podrá activar el entorno virtual, que previamente ha de ser instalado como bien se ha mencionado anteriormente. Para activar dicho entorno bastará con ejecutar los comandos que se adjuntan a continuación.

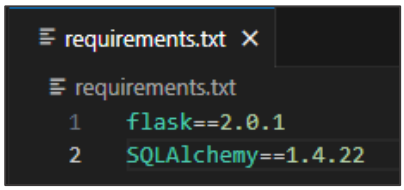
Figura 120: Comandos necesarios para activar el entorno virtual

```
PS C:\Users\ivanm\Desktop\TFG-Test\TFG-Test> cd .\env\
PS C:\Users\ivanm\Desktop\TFG-Test\TFG-Test\env> cd .\Scripts\
PS C:\Users\ivanm\Desktop\TFG-Test\TFG-Test\env\Scripts> .\activate
(env) PS C:\Users\ivanm\Desktop\TFG-Test\TFG-Test\env\Scripts>
```

Fuente: Elaboración propia

Una vez este entorno ha sido instalado, se han de instalar los requerimientos necesarios para el funcionamiento de la aplicación. Para ello, se ha creado un fichero de texto denominado *requirements.txt* y que contiene el siguiente texto.

Figura 121: Contenido del fichero requirements.txt



Fuente: Elaboración propia

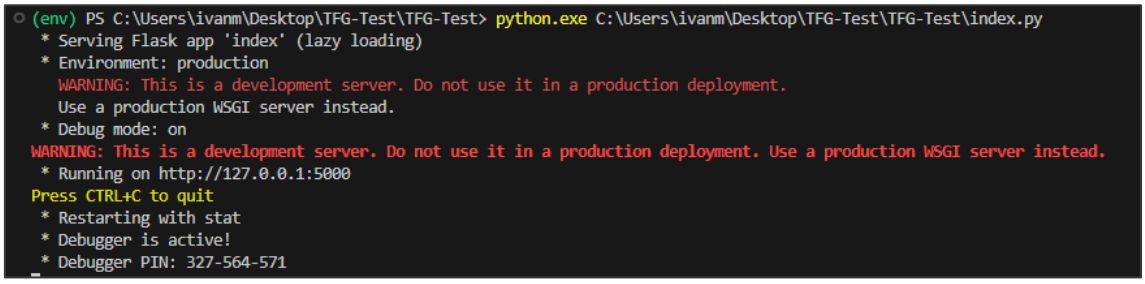
Para instalar los requisitos previamente mencionados, bastará con ejecutar el código adjunto en la imagen a continuación. Como se puede observar es necesario incluir el parámetro "*-r*", que realizará que todas las líneas sean recorridas e instaladas de manera recursiva.

Figura 122: Configuración del entorno

Fuente: Elaboración propia

Por último, una vez se ha configurado todo el entorno, se puede ejecutar la aplicación. Para ello, se ejecuta el aplicativo de *Python*, dándole como parámetro el fichero index.py, que se explicará en mayor detalle posteriormente.

Figura 123: Ejecución de la herramienta



Fuente: Elaboración propia

Cómo se puede observar, en el puerto 5000 de localhost, se puede acceder a la interfaz gráfica de la aplicación. Actualmente, la consola de comandos se quedará a la espera de recibir todas las peticiones realizadas mediante la interfaz web, procesando las mismas en base a lo configurado en el *back-end*. Todos esto será explicado en detalle en los próximos epígrafes.

CAPÍTULO 5: VALIDACIÓN DEL PROCEDIMIENTO Y DE LA HERRAMIENTA

Con el objetivo de valorar todos lo mecanismos implementados y descritos a lo largo de los anteriores capítulos, se ha diseñado un escenario ficticio que servirá para replicar múltiples de las cuestiones planteadas.

Este escenario poseerá múltiples actores, que son los realizadores de este TFG, sirviendo el mismo a modo de ejemplificación de funcionamiento de la herramienta, así como demostración de un procedimiento informático-forense válido.

Para la consecución de estas cuestiones, se han necesitado múltiples dispositivos y la correcta replicación de distintas acciones observadas en el entorno empresarial que serán descritas con mayor detalle en los próximos subapartados.

5.1. Caso práctico

El planteamiento del trabajo se inicia tras los actos de fraude ocurridos en una empresa y cometidos principalmente por el directivo (Iván Merino) y el empleado 1 (Daniel Rodríguez). Además, pretenden culpar al empleado 2 (Gema Alonso), actor no involucrado, por ello, se demostrará su inocencia en tales actos. Por su parte, las acciones realizadas por el directivo y el empleado 1 incluyen: la falsificación y modificación de documentos, importación de información confidencial de otra empresa, fuga y eliminación de documentación. Asimismo, se han mantenido conversaciones de carácter ilegítimo (cooperación en el fraude a cambio de un ascenso). En esta misma línea, el empleado 2 ha sufrido acoso por parte de estos, y, adicionalmente, ha sido culpabilizado de los actos realizados por los mismos.

En consecuencia, el empleado 2 ha realizado una denuncia tras descubrir la naturaleza de estos actos, por lo que, se incorpora la figura del inspector (papel realizado por los realizadores del presente documento). Esta figura es aquella que se va a encargar de llevar a cabo la investigación que demuestre los hechos acontecidos.

Para ello el inspector va a realizar una serie de acciones:

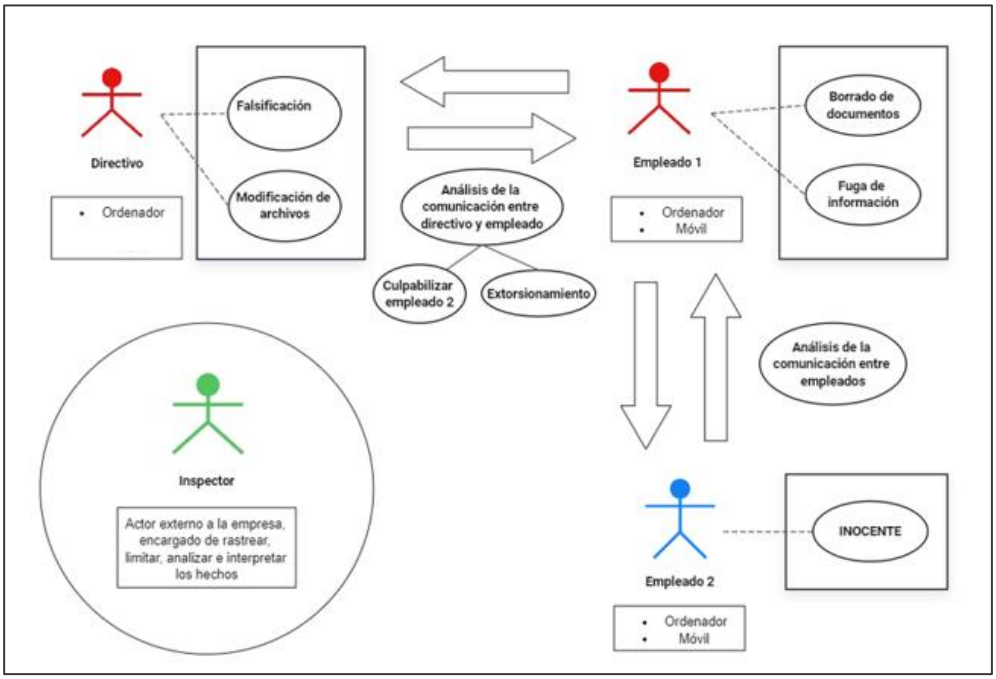
- Realización de una copia forense de todos los dispositivos localizados objeto de la investigación, garantizando la cadena de custodia y siguiendo las mejores prácticas.
- Procesado de toda la información con el objetivo de recopilar todo tipo de documentos ofimáticos, correos electrónicos, mensajería instantánea, registro de eventos, *logs*...
- Filtrado de información, para reducir el *scope* y garantizar que se cumple GDPR (protección de datos). Para ello, se emplearán búsquedas booleanas por palabras clave que aseguran no visualizar contenido de carácter personal.
- Revisión de la información obtenida mediante distintas técnicas de análisis (*eDiscovery* y *Computer Forensics*) y recomponer la historia sucedida, gracias al registro de eventos, análisis de conexiones, análisis de metadatos y documentos.

En la siguiente imagen se puede observar a los actores y los dispositivos que intervienen en el caso práctico que nos concierne. En este sentido, se identifican en rojo los actores que cometerán actos de falsificación, modificación, eliminación y fuga de información (directivo y empleado 1). Por otro lado, en azul se identifica al empleado 2

que es inocente; y por último, en verde al inspector que será el actor externo encargado de realizar la demostración e interpretación de los hechos.

Asimismo, se muestran para cada uno de los actores los dispositivos involucrados, los cuales tendrán que ser analizados, con el fin de que el Inspector pueda interpretar y concluir con los acontecimientos ocurridos.

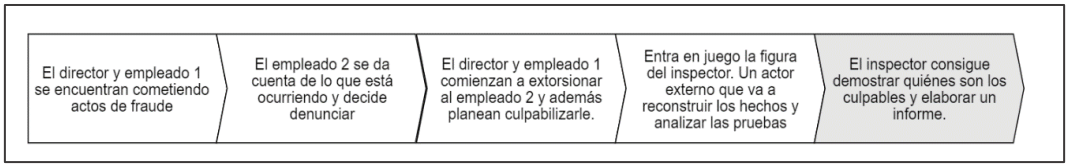
Figura 124: Caso práctico prueba del procedimiento



Fuente: Elaboración propia

De forma resumida, los sucesos se producirían de este modo:

Figura 125: Esquema acontecimientos caso práctico



Fuente: Elaboración propia

5.2. Demostración del funcionamiento de la herramienta

Una vez se ha contextualizado el caso práctico, se va a proceder a su validación dentro de la herramienta desarrollada.

En primera instancia, cabe destacar que los custodios implicados se encuentran claramente identificados. Por lo tanto, será necesario analizar los dispositivos que involucran al directivo y a los dos empleados. Se trata, por lo tanto, de cinco dispositivos que se corresponden con tres ordenadores y dos teléfonos móvil. En base a las políticas establecidas en el procedimiento, los tres involucrados deben estar dispuestos a ceder sus dispositivos con las contraseñas correspondientes, para proceder al inicio de la investigación informático-forense, o en su defecto, tratarse de dispositivos gestionados por la entidad para la que trabajan.

Gracias a la implementación de la herramienta, se permite conocer al usuario a través de la guía cuál será el procedimiento establecido, en base a las características que presentan cada una de las tecnologías que se van a analizar. En este sentido, se ha podido determinar que en el caso de las adquisiciones de los ordenadores portátiles se realizarán un clonado de los mismos a través de la herramienta *Falcon*.

Durante el clonado de los ordenadores de dichos custodios ocurrió un problema con el ordenador del empleado 2. El disco duro del dicho ordenador no era reconocido por la clonadora *Falcon*. Por consiguiente, acudiendo a la Guía de la herramienta se encontraron otras alternativas de adquisición. En este sentido, siguiendo las directrices establecidas por el procedimiento encontrado, se realizó una adquisición *FTK*, resultando de forma satisfactoria.

Por otro lado, en relación con los dispositivos móviles, acudiendo como referencia a la Guía, se especifica que se adquirirán a través de la herramienta *Cellebrite*, y bajo los pasos indicados se logró el objetivo de esta primera etapa del proceso definido. De esta forma, se permitió el avance del caso práctico hacia la siguiente fase, la etapa de procesamiento.

Tras el avance a la segunda etapa, se procederá al procesamiento de las distintas fuentes obtenidas. Para los ordenadores portátiles pertenecientes al directivo y empleado 1, al haber sido adquirido a través de *Falcon*, recurriendo a la Guía se indica que deberán de ser montados y descifrados a través de *Veracrypt*, ya que el disco duro destino de la clonación, debe estar cifrado en este formato (buenas prácticas de adquisición empleando clonadora *Falcon*).

En paralelo a esto, será conveniente hacer un preprocesamiento con *EnCase* con el fin de realizar un primer filtrado para descartar aquellos archivos que de primera mano se conoce que no van a ser útiles para la realización del análisis. Un ejemplo de estos filtros sería: eliminar archivos de sistemas (i.e. librerías dinámicas contenido de *System32*, ficheros *.msi*, entre otros); realización de filtros temporales, etc. Esto permitiría acotar el *scope* de la investigación, reduciendo significativamente los documentos que van a ser analizados.

En el caso que nos concierne, es conveniente centrarse sobre todo en correos electrónicos y sus correspondientes ficheros adjuntos, así como conversaciones entre el equipo, y otros documentos relevantes de la empresa tales como actas, cuentas, y toda aquella documentación que haya sido intercambiada por todos los miembros que componen el equipo.

Una vez que se ha realizado dicho preprocesamiento, para los dos ordenadores portátiles se realiza el correspondiente procesamiento con *Axiom* con el fin de obtener los artefactos forenses como son registros de actividad, metadatos, historial de navegación, etc.

En esta misma línea, con respecto al ordenador portátil que fue adquirido en vivo con el *software FTK*, según las directrices establecidas en la guía no es posible realizar un preprocesamiento con *EnCase*, ya que no reconoce el formato del archivo obtenido tras la adquisición. Por lo tanto, será necesario realizar el procesamiento directamente a través de *Nuix Workspace*.

Por otro lado, en relación con los dispositivos móviles no requieren de un procesamiento específico, sino que, la herramienta de adquisición *Cellebrite* se abre mediante el *software Cellebrite Physical Analyzer*, que se encargará de extraer toda la

información obtenida en la imagen forense. Una vez se completa el procesamiento, se proceden a analizar las evidencias, tal y como se indica en la guía.

En consecuencia, este hecho permite avanzar hacia la fase de filtrado con el fin de delimitar el intervalo de tiempo, y contexto de la investigación. Según establece la guía se explican una serie de buenas prácticas que facilitan y agilizan el proceso con el fin de obtener resultados óptimos y relevantes que ayuden en el avance de la investigación.

Por consiguiente, en base a dichas recomendaciones y tras contextualizarse sobre la situación el investigador ha desarrollado una serie de palabras clave que le permitirán realizar un correcto filtrado de la información y encaminar los documentos en base a las líneas de esta.

En orden a las directrices reflejadas por la guía, durante la fase de análisis resulta fundamental establecer un análisis en base a tres focos, los datos, el contenido y posibles acontecimientos pasados que hayan tenido lugar. Por lo tanto, mediante el uso de dos técnicas (*eDiscovery y Computer Forensics*) se procede a realizar el análisis en función del objetivo que se quiere obtener y las características propias de la investigación.

En el caso que nos concierne, se han empleado las dos técnicas mencionadas anteriormente de manera que las técnicas contenidas por la rama *eDiscovery* han permitido evidenciar, en base al análisis de documentos, algunas acciones ilegítimas que han sido realizadas por el empleado 1 y el director. Por otro lado, el análisis realizado mediante las técnicas contenidas por la rama *Computer Forensics*, ha permitido obtener una mayor trazabilidad de la actividad realizada por estos usuarios y su operativa.

En paralelo a todo lo mencionado anteriormente, la herramienta ha permitido a los analistas, no sólo adecuarse al procedimiento establecido, sino que han podido llevar una correcta gestión de los activos adquiridos en la aplicación. Además, también ha ayudado a la hora de conformar el equipo resolutor del presente análisis, así como no perder el objetivo de la investigación, ya que han tenido acceso continúo a la descripción y características de todos los sucesos acontecidos.

5.3. Conclusión de los resultados tras el análisis

Una vez que se ha ejecutado las pautas establecidas por la herramienta, el investigador deberá de realizar un análisis y concluir en base a los resultados obtenidos, con el fin de determinar los culpables en los hechos acontecidos y, finalmente, formular el informe resultante para concluir la investigación.

Cabe mencionar que en los sucesivos anexos del presente trabajo se puede observar en detalle la configuración de las herramientas empleadas y los dispositivos analizados, así como el resultado de las diferentes pruebas realizadas, para la obtención de las evidencias y el análisis de la información.

Con respecto a la información obtenida en base a los ordenadores portátiles móviles, se ha observado que tanto el empleado 1 como el director cometieron actos de modificación de archivos y borrado de documentos, en base a su historial de navegación, *Windows Office Alerts*, la papelera de reciclaje y el análisis de los logs de actividad de *Windows*, tal y como se puede observar en mayor detalle más adelante. *ANEXO 7: ANÁLISIS DE LOS ORDENADORES PORTÁTILES Y DISPOSITIVOS MÓVILES*

En esta misma línea, ambos han realizado actos de fuga de información. Este Hecho se ha podido corroborar a través de una serie de registros que evidencian que se

ha realizado un volcado de información confidencial de la empresa a un disco duro externo.

Asimismo, en relación con las conversaciones de *Microsoft Teams* analizadas se ha comprobado los actos de extorsión y amenazas contra el empleado 2, promovidos por el director y el empleado 1, que pretendían culparle de actos de fraude que habían cometido ellos mismos. Así como a través de la mensajería de *WhatsApp*, el empleado 2 ha sido objeto de aberraciones e insultos. *ANEXO 7: ANÁLISIS DE LOS ORDENADORES PORTÁTILES Y DISPOSITIVOS MÓVILES*

En definitiva, tras la información analizada finalmente el investigador puede concluir con que los actos delictivos han sido ejecutados por el director y el empleado 1, quedando, por tanto, demostrada la inocencia del empleado 2.

CAPÍTULO 6: CONCLUSIÓN Y TRABAJOS FUTUROS

6.1. Conclusiones

A lo largo de los años la informática forense ha tomado una mayor importancia en la investigación de delitos, que se encuentran estrechamente relacionados con las tecnologías. Por consiguiente, se ha convertido en un ámbito que resulta fundamental para hacer frente aquellos desafíos a los que se encuentra sometida la sociedad dentro del mundo digital.

Estableciendo un mayor foco en el mundo empresarial, las entidades se encuentran envueltas en complejos procesos de automatización, digitalizando los modelos de negocio y, prácticamente, toda la actividad diaria que comprenden. Son frecuentes los casos que se producen de fraude financiero, filtrado de información, entre otros. Por consiguiente, esta fuerte dependencia de los sistemas de la información, sumado al creciente aumento de los delitos informáticos promueve la necesidad de formar a los expertos en informática-forense para que se encuentren altamente capacitados.

En este sentido, se podría ejemplificar y destacar las tecnologías de comunicación emergentes y su continua evolución, ya que son las fuentes de datos que los investigadores tratarán de copiar y analizar en las investigaciones. La continua aparición de nuevas aplicaciones de mensajería y nuevas actualizaciones de las ya existentes, demuestran que el campo de la informática forense requiere de formación continua para ofrecer soluciones a los problemas y nuevos desafíos que se presenten. Ejemplo de ello son la aparición de *Telegram*, mensajes directos de *Instagram* y *Twitter*, o también una de las aplicaciones de mensajería más importantes en Asia, como es *WeChat*.

Respecto a lo comentado anteriormente referida al aumento de las fuentes de información analizables, que coloquialmente se conocen en el mundo de la informática forense como "*Emerging Data Sources*" sería conveniente mencionar la siguiente consecuencia, referida a la necesidad de tratar cada vez con mayor volumen de información y por tanto, para poder ser eficientes, se necesitan herramientas cada vez más potentes, y de la necesidad de tener mayor almacenamiento de datos.

Asimismo, cabe mencionar que actualmente el desarrollo de la informática forense se encuentra en un momento de evolución contante, como resultado de los diferentes y sofisticados métodos que se encuentran disponibles con motivo del rápido avance de la tecnología; así como del aumento de los datos generados por diferentes dispositivos electrónicos y herramientas. Sin embargo, en relación con los mecanismos de gestión como guía en los procedimientos de investigación no se encuentran fuertemente desarrollados, y, por consiguiente, sería necesario la implementación de desarrollos y controles, para garantizar la integridad y confidencialidad de la información desde el inicio hasta el final de esta.

En esta misma línea, el principal objetivo de este trabajo se fundamenta la respuesta a esa necesidad de negocio planteada, por tanto, se centra en la elaboración de un procedimiento informático-forense validado a través de un caso práctico. Sentando las bases en los principales conceptos y estándares que conforman el ámbito de la informática forense y estableciendo las mejores prácticas para el correcto desarrollo de este.

Tal y como se ha comentado a lo largo del trabajo, uno de los aspectos más presentes a la hora de comenzar el procedimiento es la delimitación de los acontecimientos y de los custodios que se encuentran implicados en la investigación.

Resulta crucial durante las primeras fases determinar e inventariar de forma adecuada las características y modelos de los diferentes dispositivos y su pertenencia, pues durante las siguientes fases se continuará con el procesamiento y análisis de la información obtenida, con el fin, de llegar hasta una presentación de los resultados.

En este caso, en el caso práctico que nos concierne se ha había delimitado desde un primer momento los dispositivos que involucraban a los diferentes usuarios con el fin de proceder a su análisis. En esta misma línea, se ha comprobado que en un entorno empresarial normalmente se provee de dispositivos con características similares lo que podría facilitar el proceso de la adquisición de estos. No obstante, tras realizar el procesamiento surgieron problemas con uno de los dispositivos, determinando finalmente, que el estado de estos y sus particularidades pueden influir en el avance de la investigación, como consecuencia de la imposibilidad de obtener información de ciertos dispositivos que presentan alguna peculiaridad.

Por tanto, en el desarrollo de la herramienta se han planteado las diferentes casuísticas a la hora de guiar en la adquisición de los dispositivos, con el fin de otorgar la mayor precisión posible, y proponer alternativas en el caso de que se produjera algún tipo de improviso.

Asimismo, conviene recordar la importancia del mantenimiento y preservación de las evidencias de tal forma, que se encuentren custodiadas y ajenas a ser manipuladas o contaminadas durante el proceso de análisis. Por lo tanto, se ha desarrollado una herramienta en la que se conoce la ubicación y la totalidad de los activos involucrados en la investigación. Además, se plantean guías y recomendaciones sobre las prácticas más adecuadas para su conservación, teniendo un registro de aquellas personas que se encuentran involucradas en el caso, tanto el responsable de este como el resto del equipo que puede acceder a dicha información y analizarla.

En esta instancia, sobre los aspectos a destacar de la gestión de las investigaciones a través de TodoForense, se traduce en el conocimiento de la etapa del caso en todo momento. Permitiendo una mayor organización e información accesible ante posibles rotaciones en los equipos, e inclusive, ya que los analistas se encuentran involucrados en distintos casos a la vez, permitiendo, por tanto, una mayor organización y eficacia en el acceso a la información.

En otro orden de cosas, con respecto a la realización del caso práctico, es necesario resaltar la importancia del filtrado de los documentos con el fin de no desviar la investigación hacia otras líneas que no se corresponden. En este sentido, resulta un papel fundamental por parte del investigador en la elección de las palabras clave adecuadas a través de las cuales se realizan las búsquedas, así como la acotación del horizonte temporal en el que han transcurrido los hechos. De esta forma, se asegura la recuperación y reconstrucción de los acontecimientos de forma precisa.

Otro de los objetivos establecidos en el desarrollo del presente trabajo se basaba la homogeneización de los casos informático-forenses. Con el fin de obtener una referencia y estándar para cualquier empresa en la elaboración de sus investigaciones. De tal manera, que, partiendo de una misma estructura permita realizar los estudios de diferentes índoles resultando una solución efectiva y eficiente. Se trata uno de los motivos, además, por los que se ha optado por incluir la información principal mostrada para cada uno de los casos, de tal manera, que se obtengan resultados óptimos ante una metodología sistemática.

6.2. Trabajos futuros

De cara a trabajos futuros, con el fin de continuar con el desarrollo de la herramienta, en relación con la adquisición y mantenimiento de las evidencias se propone la elaboración de etiquetas con localizador para los dispositivos, con el fin de tener un registro y poder realizar una trazabilidad sobre el movimiento y el transporte de estos. Inclusive, se podrían incorporar pegatinas en dichas etiquetas pegatinas con un QR, de tal manera que al escanearlo se pueda visualizar los datos correspondientes al tipo de dispositivo, custodio al que pertenece, sistema operativo, versión, y el tipo de datos que pueden almacenar, entre otras características.

Por otro lado, para la continuación de la herramienta de gestión a la hora de la presentación de los resultados también convendría la incorporación de una plantilla a modo de ejemplo del informe pericial, de tal forma, que en lo sucesivo en la investigación se incorporaran los avances y conclusiones obtenidas, y que, tras pulsar a una nueva funcionalidad de generación de informe pericial, se obtenga directamente.

En esta misma línea, al tratarse de un informe que necesita ser verídico ante una audiencia tribunal resultaría necesaria añadir la posibilidad de firma electrónica para agilizar los procesos en los que intervienen los abogados, peritos… adaptándolo al tipo de trámite que, por ejemplo, se encuentran en las distintas páginas web de los ministerios. En definitiva, proporcionar otras vías que agilicen el procedimiento judicial.

En definitiva, el sector de la informática forense continúa en creciente expansión, de tal forma, que es propulsada por el aumento de los delitos relacionados con la tecnología y con la necesidad de identificar y prevenir las amenazas que surgen en el entorno digital. Por consiguiente, su importancia radica fundamentalmente en el análisis e identificación de evidencias digitales, con el objetivo de contribuir tanto en la privacidad, protección y seguridad de la información que se encuentra digitalizada. Así como en la recomendación y asesoramiento con el fin de prevenir posibles futuros incidentes.

6.3. Distribución del trabajo

Derivado de las múltiples tareas necesarias para la realización de este proyecto, ha sido necesario un reparto de tareas que permitiera a los alumnos involucrados la participación en las múltiples cuestiones necesarias, tratando de no sobrecargar de actividad a ninguno de ellos.

En primera instancia, de cara a la documentación necesaria para la realización del procedimiento, se establecieron múltiples sesiones en las que se debatieron las mejores prácticas llevadas a cabo por cada uno de los usuarios en su actividad laboral, repartiendo las distintas fases del procedimiento entre los distintos alumnos cuyo objetivo es la realización de un procedimiento adecuado para las múltiples necesidades encontradas. Toda la documentación ha sido leída e introducida en la memoria por los tres alumnos de manera conjunta.

Por otro lado, de cara a la realización del procedimiento informático-forense específico diseñado para este proyecto, se han repartido las tareas entre los usuarios. En este sentido, la fase de adquisición ha sido desarrollada por Iván Merino Mesa, la fase de procesamiento ha sido diseñada por Daniel Rodríguez Borreguero y por último, las fases de filtrado, análisis y presentación de resultados han sido realizada por Gema Alonso Bote.

Esto ha sido realizado de tal forma, derivado de las múltiples cuestiones y casuísticas posibles encontradas en las dos primeras fases observadas para este procedimiento. Tras la implementación de las distintas etapas del procedimiento, se han establecido sesiones para garantizar la conformidad de todos los integrantes.

En paralelo a esto, el caso práctico ha sido realizado de manera presencial, por lo que los tres integrantes de este proyecto se han encontrado presentes en todo el proceso de realización del caso práctico. Si bien cada uno ha preparado sus evidencias, esto se ha realizado de manera conjunta, pudiendo organizar todo el organigrama de la empresa analizada de manera ágil.

De cara a la consecución de cada una de las fases del caso práctico, la adquisición ha sido realizada de manera presencial con motivo de la necesidad de tener todos los dispositivos electrónicos reunidos para la correcta adquisición. Asimismo, el procesamiento, análisis y filtrado ha sido realizado de igual forma de manera presencial, ya que solo se contaba con un dispositivo conectado al laboratorio forense desde el que se han utilizado todas las herramientas necesarias para el procedimiento.

Asimismo, con el objetivo de que la realización de la herramienta fuera lo más equitativa posible, se han establecido múltiples jornadas de trabajo, en las que todos los usuarios han asistido mediante videollamada, cuyo objetivo era programar las distintas funcionalidades contempladas por la herramienta.

Además, cuando uno de los alumnos se bloqueaba en la implementación del código, o terminaba su parte y solicitaba una aprobación del resto de compañeros, al estar todos en llamada, se podían resolver dichas cuestiones con facilidad.

Por esto, el grupo realizador del presente trabajo, considera que la herramienta ha sido desarrollada por todos los participantes de manera equitativa, que, si bien el reparto de tareas se ha ido realizando sobre la marcha de cara a la eficiencia en la consecución de un proyecto óptimo, se considera que todos los integrantes han participado de alguna forma en cada una de las implementaciones del código.

Por último, para la realización de la memoria, se han establecido diferentes sesiones de seguimiento entre los tres participantes, con el objetivo de comprender que tareas se encontraban pendientes de finalización y repartiendo indistintamente, ya que todos los alumnos poseen conocimientos similares de todas las ramas del trabajo realizado.

BIBLIOGRAFÍA

[1]. Basis Technology. (2023, 23 junio). *Autopsy - digital forensics*. Autopsy. https://www.autopsy.com/

[2]. *Cellebrite Digital Collector - Cellebrite*. (2023, mayo 23). Cellebrite. https://bit.ly/3rpuxO5

[3]. *Cellebrite Physical Analyzer - Cellebrite*. (2020, septiembre 2). Cellebrite. https://bit.ly/3OoNzxn

[4]. *Cellebrite Reader - Cellebrite*. (2023, mayo 23). Cellebrite. https://bit.ly/44JrQoX

[5]. EDRM Global Inc. (2023, 31 marzo). *Current EDRM Model - EDRM*. EDRM. https://bit.ly/44Ish2J

[6]. *Encase Forensic Software: características y funciones*. (s. f.). Ondata International. https://bit.ly/43ryzTi

[7]. *Endpoint Forensics - How Cellebrite works*. (s.f.). https://bit.ly/3DxxvmJ

[8]. Exterro. (2023, 3 julio). *FTK® Imager*. Exterro. https://bit.ly/3JTSDH1

[9]. Fraser-Clark, I. (2022, 22 noviembre). *eDiscovery Best Practices - Processing Guidelines Released*. https://www.altlaw.co.uk/blog/processing-guidelines

[10]. IsecT Ltd. www.isect.com. (s. f.-b). *ISO/IEC 27037 Eforensics*. Copyright © IsecT Ltd. 2023. https://bit.ly/3PTjIy7

[11]. Logicube. (2023, 8 febrero). *Falcon®-Neo - Logicube*. https://bit.ly/43svbb4

[12]. Magnet Forensics. (2023, 7 julio). *Magnet Axiom Cyber - Magnet Forensics*. https://bit.ly/43qocPR

[13]. *Regripper*. (2009, 26 enero). Softonic. https://bit.ly/43vlTee

[14]. *Relativity Ediscovery Case Study*. (s. f.). Relativity eDiscovery case study. https://bit.ly/46QDL6s

[15]. Riveros, A. (2023). Qué es la norma ISO 27001 y para qué sirve. *EALDE Business School*. https://bit.ly/44Ipua2

[16]. Robmazz. (2023, 18 marzo). *Soluciones de exhibición de documentos electrónicos de Microsoft Purview - Microsoft Purview (Compliance)*. Microsoft Learn. https://bit.ly/3rwpaNd

[17]. *Technology | NUIX*. (s.f.). https://bit.ly/44MdtjY

[18]. サン電子株式会社. (s. f.). サン電子株式会社. https://www.sun-denshi.co.jp /

ANEXO 1: GLOSARIO DE TÉRMINOS

Bloqueador de escritura: Herramienta fundamental que nos permite analizar un disco duro n modo bloqueo de escritura, es decir, sin que se pueda modificar algún sector del disco de forma accidental, por ende, se modifiquen registros de una evidencia digital.

Código Hash: Cadena de caracteres alfanuméricos resultante del cálculo de un algoritmo sobre un conjunto de datos (un fichero único, un grupo de ficheros, un disco duro entero, etc.) y que describe su contenido íntegro, pudiendo usarse como un identificador o "huella digital" de los mismos. Cabe destacar, que cualquier mínimo cambio en dichos datos alteraría por completo el *código hash* resultante. Los algoritmos de *código hash* más comúnmente utilizados en el ámbito de la Informática Forense son el *MD5, el SHA-1 y el SHA-256.*

Clonación: Copia idéntica *bit a bit* de un dispositivo origen a uno o varios dispositivos destino.

Clonadora Forense: Herramienta utilizada para realizar clonaciones forenses de discos duros. Esto se realiza con el objetivo de certificar y mantener la cadena de custodia

Copia lógica: Son réplicas de los datos lógicos que poseen los dispositivos. Por ejemplo, tablas o procedimientos almacenados en los mismos, exportados desde una base de datos y almacenados en un archivo binario, para luego volver a importarlos a una base de datos

Deduplicación: Técnica especializada de compresión de datos que nos permite eliminar copias duplicadas de datos repetidos.

Encriptación: Procedimiento de seguridad que altera mediante algoritmos, los datos que componen un fichero. [14]El objetivo principal es hacer que los datos se vuelvan ilegibles por parte de cualquier persona no autorizada.

Evidencia Digital: Registro de información guardada o difundida a través de un sistema informático que puede utilizarse como prueba de un delito judicial.

Formatos forenses: El resultado que se obtiene al finalizar la creación de una imagen forense desde un dispositivo sospechoso, generalmente es una copia exacta del dispositivo de origen. Este archivo puede recibir diferentes formatos en función de su formato. Entre los existentes se puede destacar: *E01*, *EX01*, *AD1*, *.DD*, *.RAW*.

Imagen forense: Copia exacta *bit a bit* de un dispositivo de almacenamiento.[15] Cada *bit* (1 o 0) es duplicado en otro dispositivo limpio, como por ejemplo, un disco duro. Esto se realiza porque estos dispositivos de almacenamiento pueden incluir archivos eliminados o parcialmente sobrescritos.

***Keywords*:** Palabras clave que poseen una importancia especial para el análisis de la evidencia.

***Querys*:** Consulta o sentencia lógica que un usuario escribe con el objetivo de cuando realizar un tipo de búsqueda utilizando palabras clave

[14] Definición extraída de: https://bit.ly/3Q1YPAK
[15] Definición extraída de: https://bit.ly/3Oe1LZQ

ANEXO 2: ADQUISICIONES DE PORTÁTILES

2.1. Proceso de adquisición física

A continuación, en el siguiente anexo se va a explicar cómo se ha llevado a cabo la adquisición de las evidencias de tipo laptop del proyecto asignados a los custodios Daniel Rodríguez e Iván Merino. Para ello se han adjuntado fotos de la ejecución de esta, donde se muestra todo el procedimiento llevado a cabo.

Antes de comenzar a utilizar la herramienta de adquisición, se debe identificar y extraer el disco duro origen de la evidencia.

Tabla 18: Identificación de los dispositivos

Dispositivo	Marca	Modelo	Custodio
Portátil	ACER	Aspire 1810TZ	Daniel Rodríguez
Portátil	Lenovo	Ideapad 100-15IBD	Iván Merino

Fuente: Elaboración Propia

Figura 126: Foto portátil ACER (I)

Fuente: Elaboración Propia

Figura 127: Foto portátil ACER (II)

Fuente: Elaboración Propia

Figura 128: Foto portátil ACER (III)

Fuente: Elaboración Propia

Figura 129: Foto portátil ACER (IV)

Fuente: Elaboración Propia

Una vez identificado y extraído el disco duro, se utiliza la herramienta *Logicube Forensic Falcon*, explicada en la sección de herramientas forenses de la siguiente manera:

1) Una vez encendida la herramienta se debe ir a la sección *System Settings* y poner las siguientes configuraciones: *Cipher Mode: VCRYPT* y una contraseña de encriptación para los discos duros destino.

Figura 130: Paso I adquisición con Falcon

Fuente: Elaboración Propia

2) Se cogen dos discos duros vírgenes donde se van a volcar las dos copias forenses y se conectan a la herramienta.

Figura 131: Paso II adquisición con Falcon

Fuente: Elaboración Propia

3) En la herramienta, se identifican y formatean los discos con las siguientes configuraciones: *Encryption: ON Format: Yes* y *File System: NTFS*

Figura 132: Paso III adquisición con Falcon (I)

Fuente: Elaboración Propia

Figura 133: Paso III adquisición con Falcon (II)

Fuente: Elaboración Propia

4) Se accede al modo *"Imaging"* y se conecta el disco origen a la herramienta aplicando las siguientes configuraciones:
   - *Mode: DRIVE TO FILE*: Para generar una evidencia en modo fichero.

Figura 134: Paso IV adquisición con Falcon (I)

Fuente: Elaboración Propia

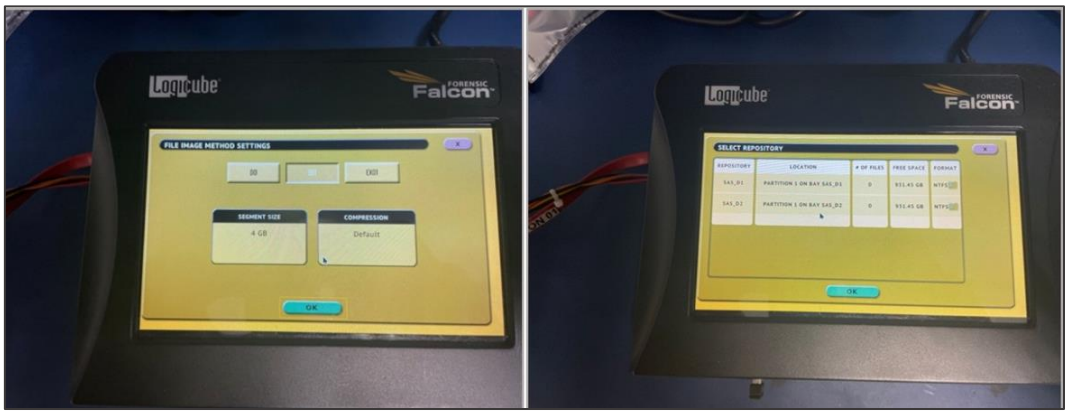
- Se conecta la evidencia y se selecciona. Por otro lado, se rellena el nombre de la evidencia, de la forma: APELLIDOINICIALNOMBRE_DISPOSITIVO_FECHA. En este caso: RODRIGUEZD_LT01_20221019.

Figura 135: Paso IV adquisición con Falcon (II)

Fuente: Elaboración Propia

- El tipo de fichero generado, del contenedor forense es *E01*. En la segunda imagen se seleccionan los discos duros destinos donde se van a realizar las dos copias y que, previamente se han formateado.

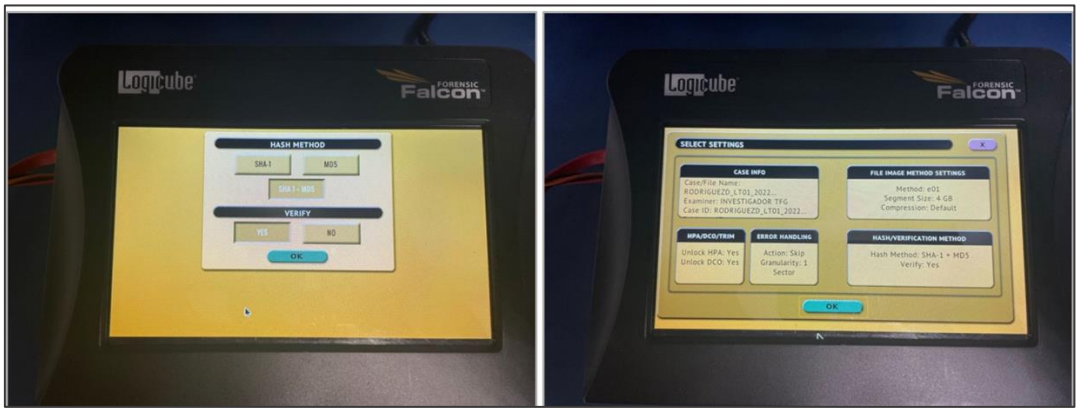
Figura 136: Paso IV adquisición con Falcon (III)



Fuente: Elaboración Propia

- Se seleccionan los tipos de *Hash* que se quiere que se calcule. En este caso se seleccionan tanto el hash *SHA1* como el *MD5* y para realizar una copia forense con las mejores garantías, también se selecciona la opción que verifique el código *hash.*

Figura 137: Paso IV adquisición con Falcon (IV)



Fuente: Elaboración Propia

5) Para terminar, con la configuración tal y como muestra la imagen, se pulsa el botón *"Start"* para que comience la copia.

Figura 138: Paso V adquisición con Falcon

Fuente: Elaboración Propia

2.2. Proceso de adquisición en vivo

A continuación, se adjunta las imágenes que demuestran la adquisición de la evidencia del portátil *Acer* perteneciente al custodio Gema Alonso siguiendo el procedimiento denominado "copia en vivo" que tiene las siguientes características:

1) No es una copia física del ordenador. Sino que se accede con las credenciales del custodio y se realiza un contenedor forense seleccionando la carpeta a copiar. Como procedimiento general y tal se procederá en el presente trabajo, se realiza un contenedor forense de toda la información en la unidad C del dispositivo.
2) Para realizar el contendor forense anteriormente mencionado, se necesita instalar en el ordenador del custodio la herramienta *FTK Imager*, la cual, permite realizar este tipo de adquisición del dispositivo.
3) Cabe destacar, que este proceso es más intrusivo que los procedimientos anteriores, sin embargo, si el custodio accede a facilitar sus credenciales, y se tiene definida la información se quiere copiar para su posterior análisis, se trata de un proceso que se lleva a cabo en menos tiempo, y por tanto, es más eficiente.

A continuación, se encuentran adjuntas las fotografías que se han tomado para documentar la adquisición forense del equipo.

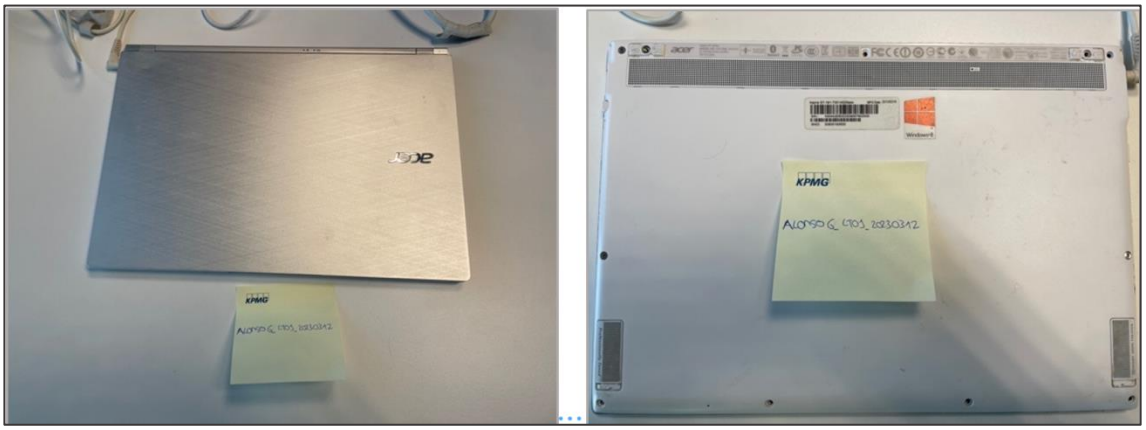
1) Identificación del equipo a adquirir con los siguientes datos:

Tabla 19: Identificación del dispositivo

Dispositivo	Marca	Modelo	Custodio
Portátil	ACER	Aspire S7-191-73514G25	Gema Alonso

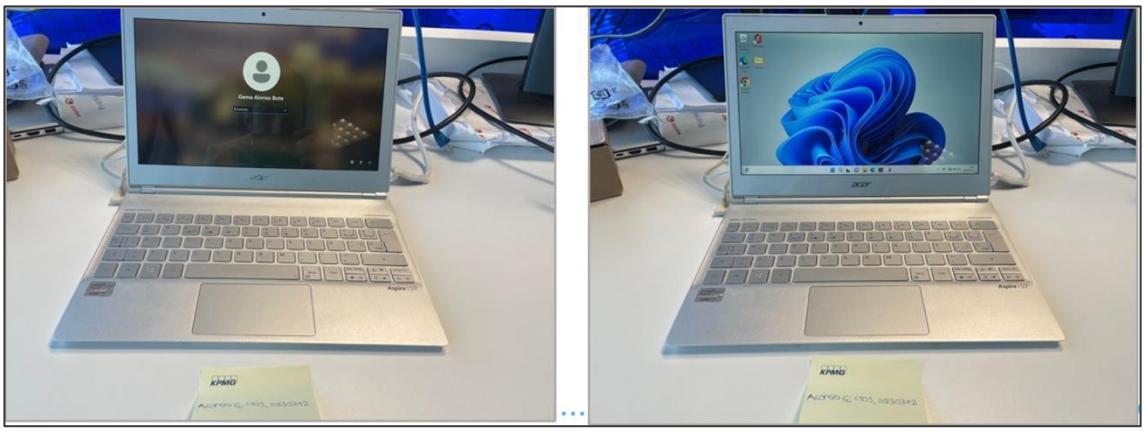
Fuente: Elaboración Propia

Figura 139: Identificación de dispositivo (I)



Fuente: Elaboración Propia

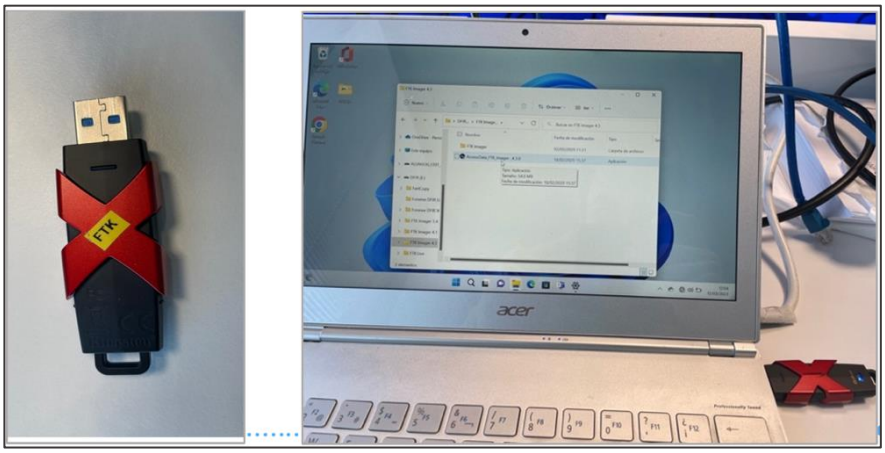
Figura 140: Identificación de dispositivo (II)



Fuente: Elaboración Propia

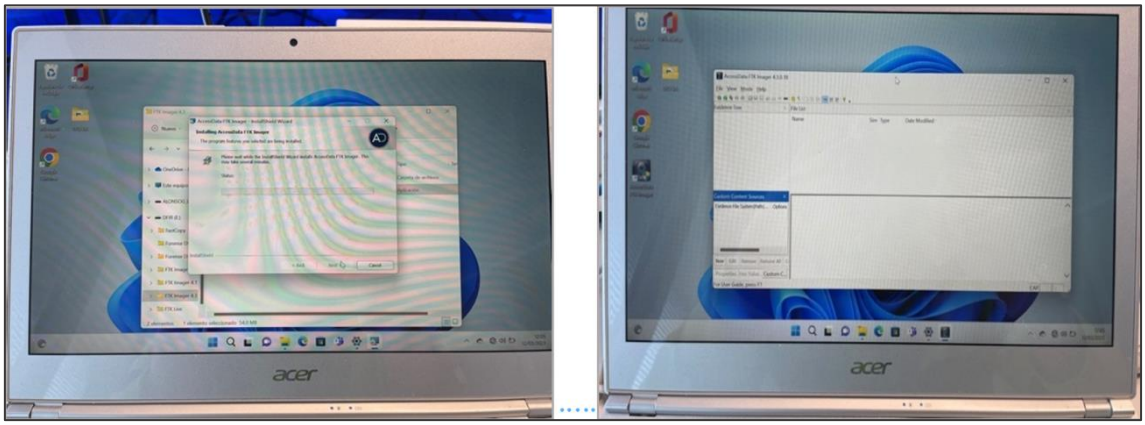
2) Se conecta el pendrive con el programa ejecutable *FTK Imager* para instalar en el dispositivo y poder realizar la adquisición forense del mismo.

Figura 141: Ejecutable herramienta FTK Imager (I)



Fuente: Elaboración Propia

Figura 142: Ejecutable FTK Imager (II)

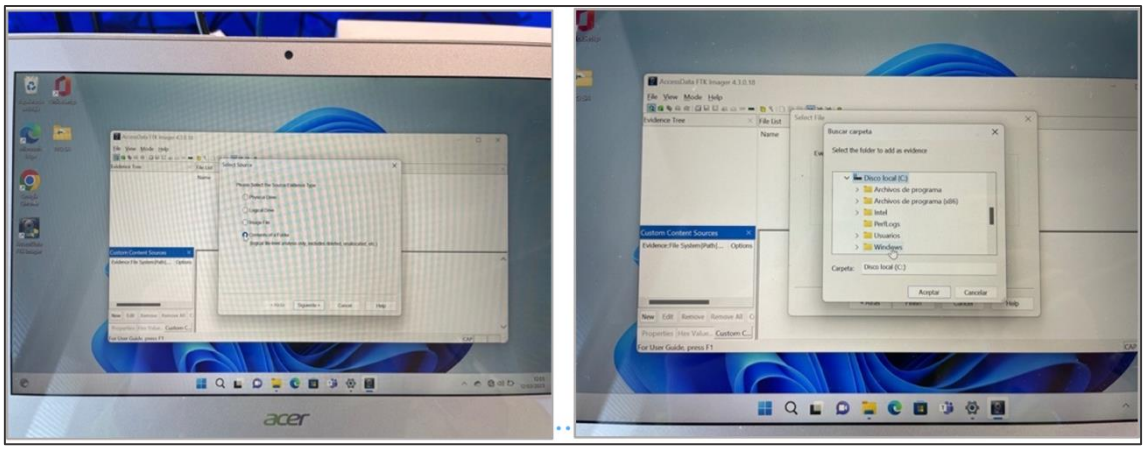


Fuente: Elaboración Propia

Una vez se tiene instalado *FTK Imager* comienza el proceso de adquisición las siguientes directrices:

3) Se añade la carpeta a la que se va a realizar el contenedor forense (fichero con extensión *.ad1*), que, en este caso, es la carpeta C\.

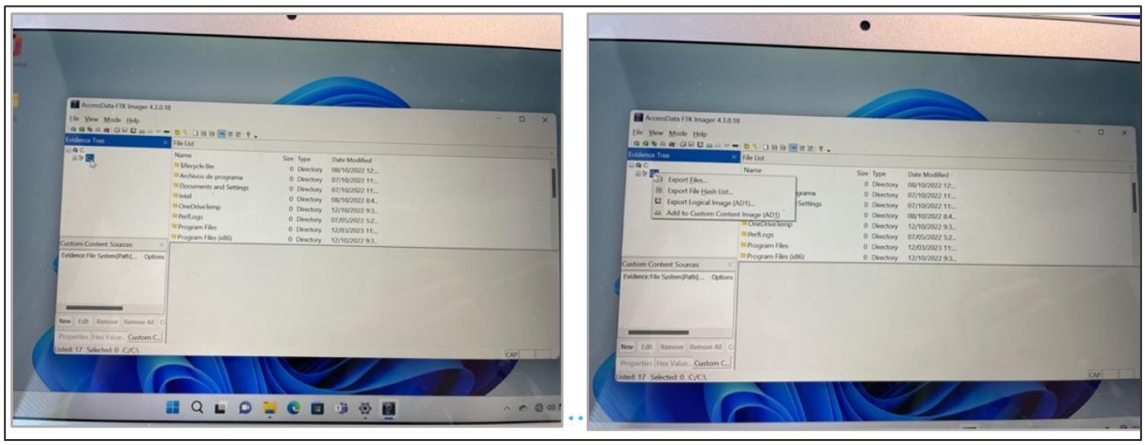
Figura 143: Selección de la carpeta de Origen



Fuente: Elaboración Propia

4) Una vez añadida, se selecciona y se clica botón derecho, con la opción de *" Export Logical Image"(AD1).*

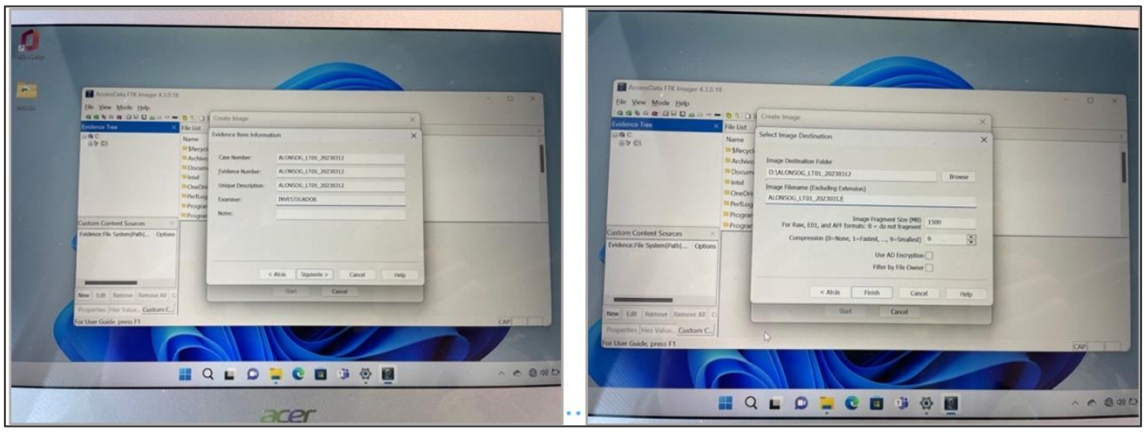
Figura 144: Creación del contenedor forense AD1



Fuente: Elaboración Propia

5) Se establece el nombre de la evidencia y la ruta destino donde se va a almacenar el contendor forense resultante de la adquisición del dispositivo.

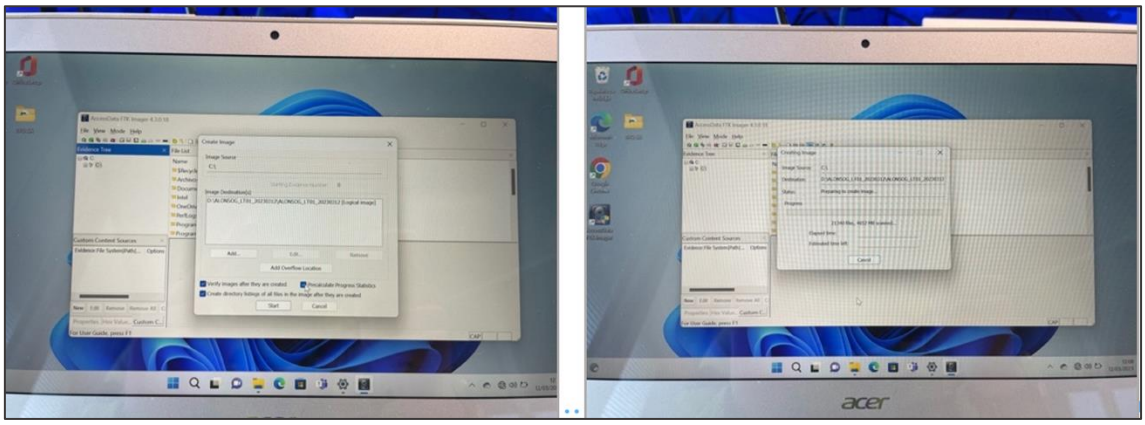
Figura 145: Nombre y ruta destino de la evidencia



Fuente: Elaboración Propia

6) A continuación, se hace clic en las tres opciones que se muestran, con las que se consigue, verificar las imágenes forenses al final el proceso, crear un directorio en el que se listan todas ellas y el último, para poder observar una barra de progreso mientras se desarrolla la adquisición.

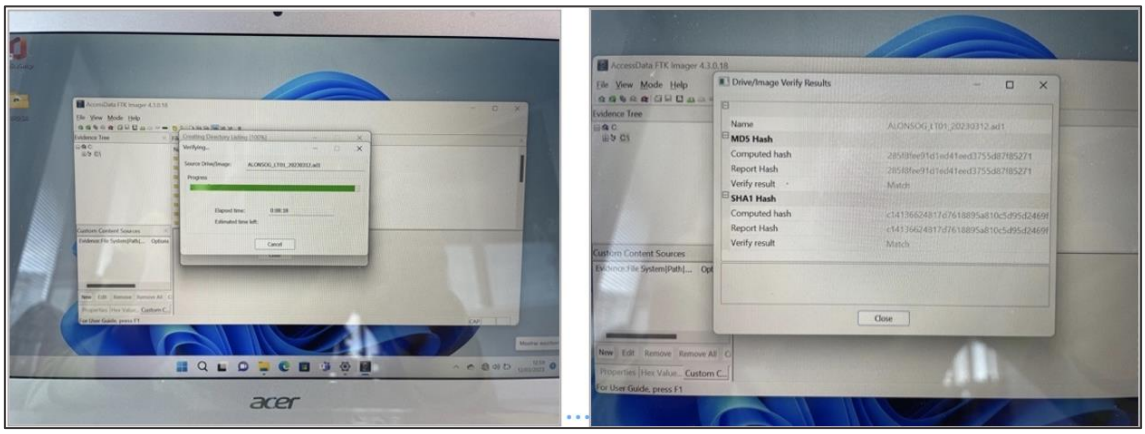
Figura 146: Ejecución del contenedor forense AD1



Fuente: Elaboración Propia

7) Una vez terminada la adquisición y verificación, se observa que se ha realizado correctamente. Esto se comprueba en *"verify result: Match"*.

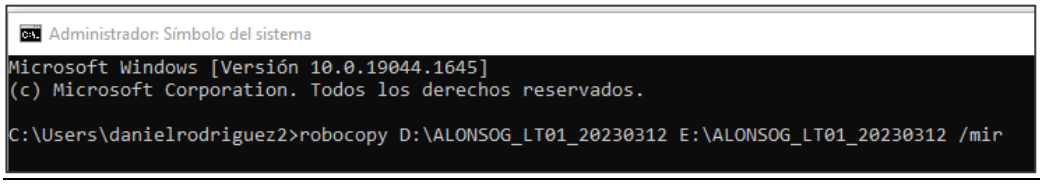
Figura 147: Verificación del contenedor forense AD1



Fuente: Elaboración Propia

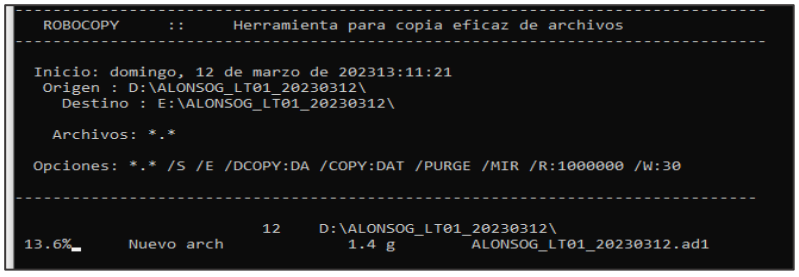
8) Por último, se realiza una segunda copia de la evidencia a otro disco duro destino, mediante el comando *"robocopy"* que se observa en las imágenes.

Figura 148: Comando Robocopy (I)



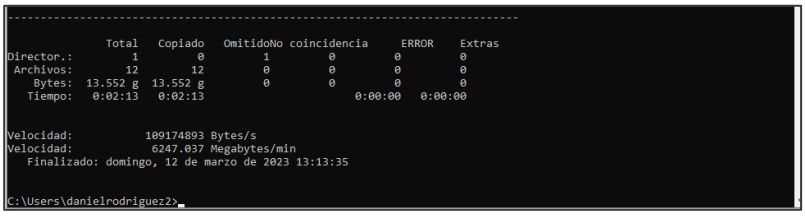
Fuente: Elaboración Propia

Figura 149: Comando Robocopy (II)



Fuente: Elaboración Propia

Figura 150: Comando Robocopy (III)



Fuente: Elaboración Propia

ANEXO 3: PREPROCESAMIENTO DE LOS PORTÁTILES

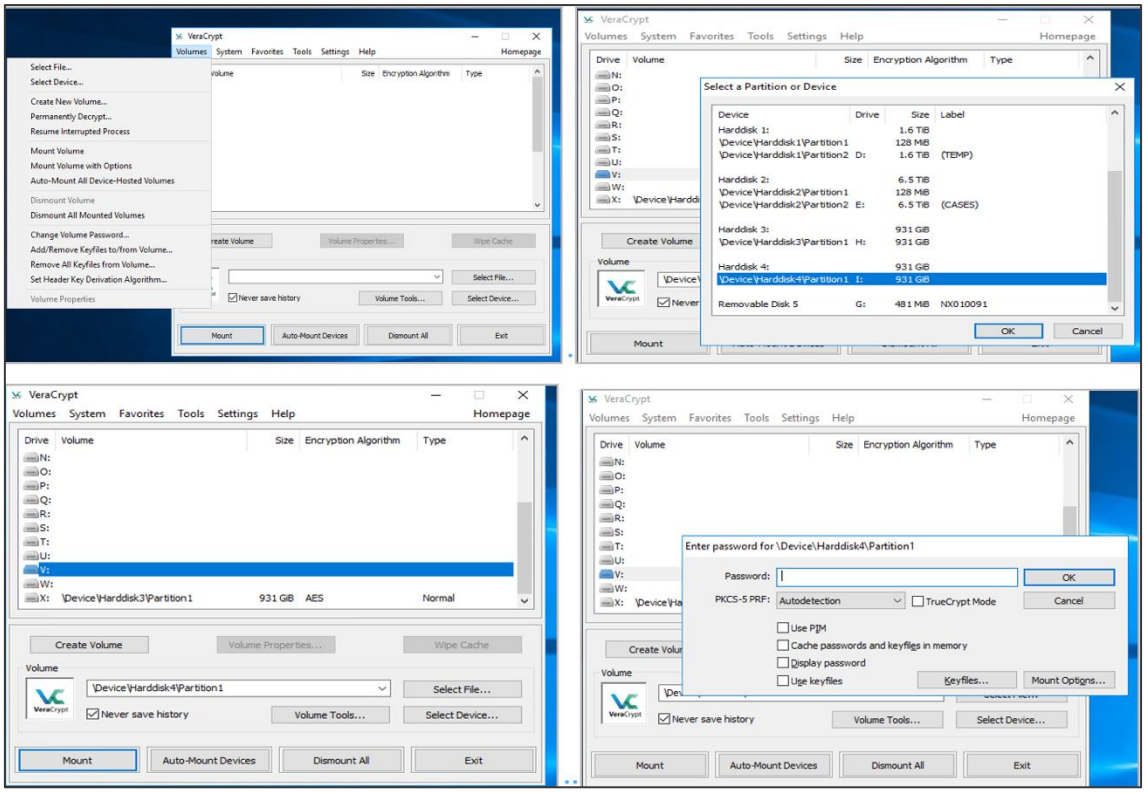
A continuación, en el siguiente anexo se va a explicar cómo se ha llevado a cabo el preprocesamiento de las evidencias de los custodios Iván Merino y Daniel Rodríguez, cuyos ordenadores portátiles fueron adquiridos por medio de la herramienta *Falcon*. Para ello se han adjuntado fotos de la ejecución de este, donde se muestra todo el procedimiento realizado.

Una vez se ha llevado a cabo el procedimiento de adquisición de las evidencias, se debe comenzar con un prefiltrado de los datos para no procesar ficheros de sistema del ordenador. Con este prefiltrado lo que se hace es limpiar de archivos inútiles lo máximo posible que permite la herramienta *EnCase Forensic*, que es la que se utilizará para desarrollar esta función.

Para ello se conecta el disco duro que va a ser nuestra copia de trabajo al ordenador donde se tiene la licencia de EnCase y se procede a lo siguiente:

Primero de todo, el disco duro de la evidencia se cifró con *Veracrypt* en el proceso de adquisición para evitar el acceso de personal no involucrado a esta evidencia. Para poder visualizar su contenido, se necesita que sea montado con dicho programa. Para ello, se selecciona el dispositivo que se desea visualizar con el *software* de *Veracrypt*, se le asigna una letra donde montarlo y se introduce la contraseña del proceso de adquisición.

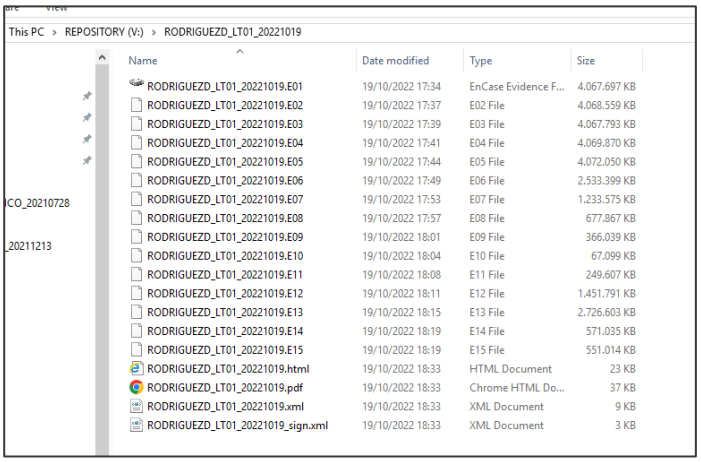
Figura 151: Activación del disco duro con Veracrypt



Fuente: Elaboración Propia

Al rellenar la contraseña que se agregó en el proceso de adquisición, finalmente se accede al contenido de la evidencia, que se trata de un contenedor forense de tipo: *E01*.

Figura 152: Visualización de la evidencia

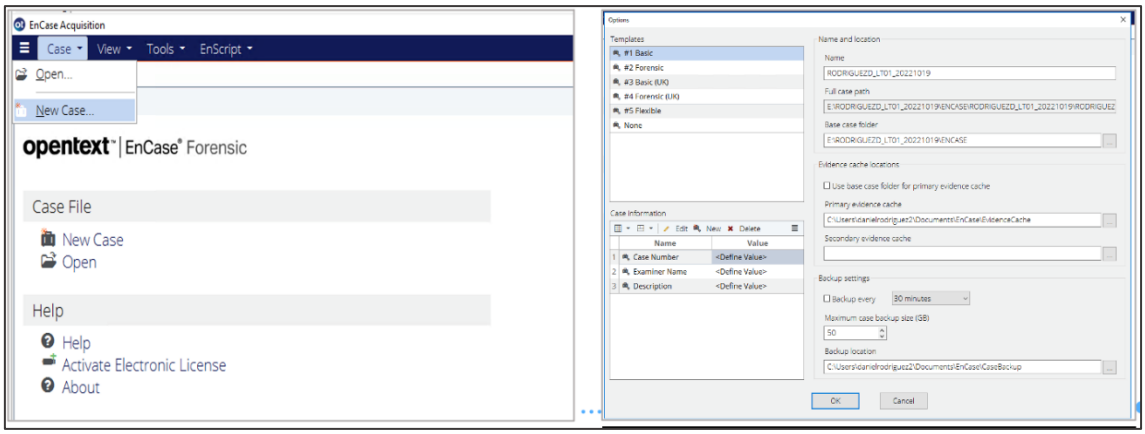


Fuente: Elaboración Propia

Una vez está disponible el contenido de la evidencia se procede a llevar a cabo el procedimiento de datos con la herramienta forense *EnCase*, tal y como se puede observar a continuación en los pasos a realizar:

1) Se crea un caso nuevo en *Encase* con el nombre de la evidencia que se va a utilizar y se introduce las rutas donde se van a guardar.

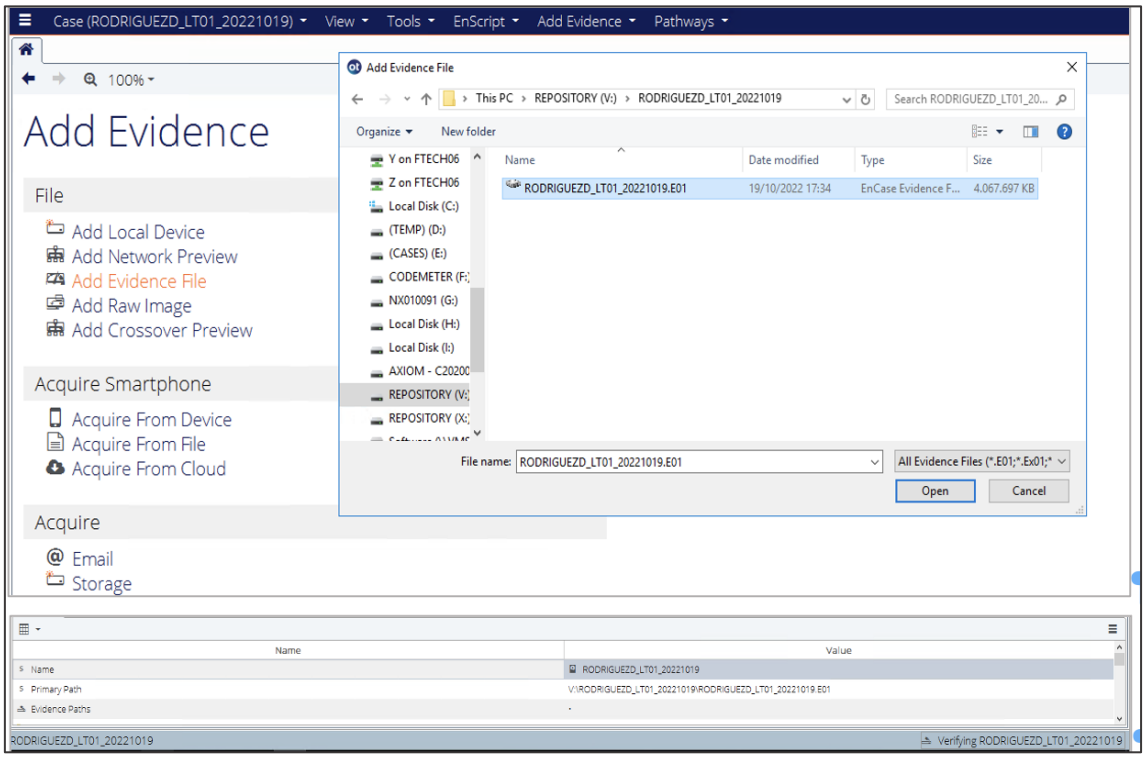
Figura 153: Paso I con herramienta Encase Forensic



Fuente: Elaboración Propia

2) Se añade la evidencia que se quiere analizar y posteriormente como se ve en la imagen, empieza la verificación, que es un proceso que tiene el objetivo de verificar los *hashes* de la evidencia.

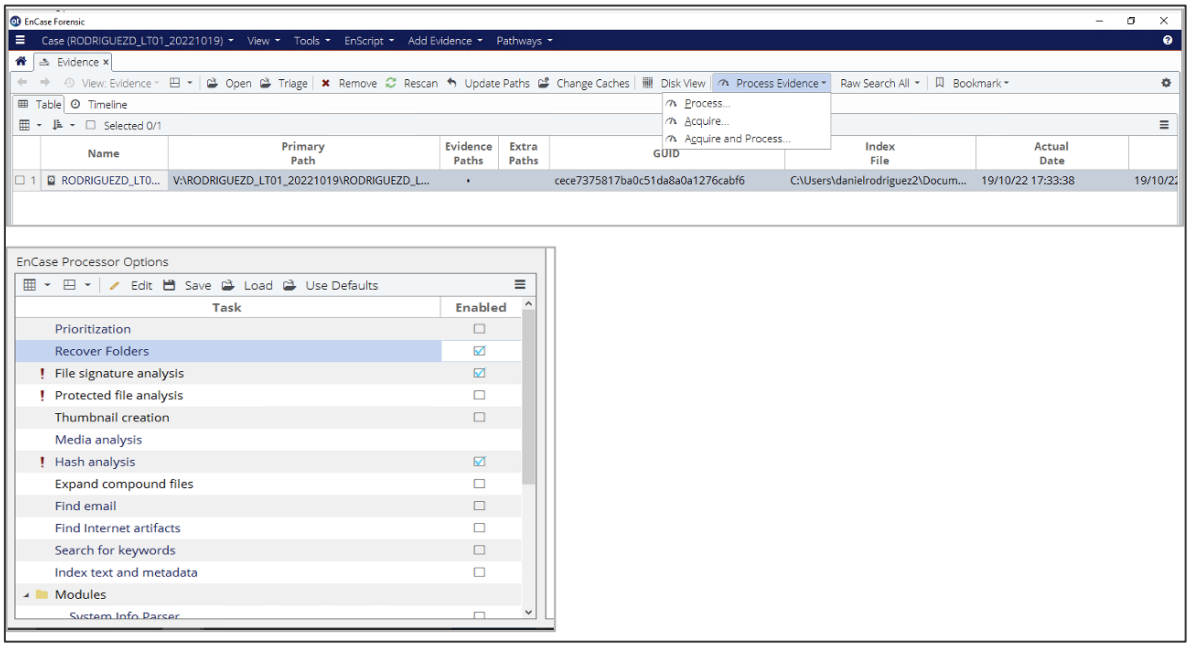
Figura 154: Paso II con la herramienta Encase Forensic



Fuente: Elaboración Propia

3) Una vez terminado el proceso de verificación, se lleva a cabo el procesamiento de la evidencia. En dicho proceso se seleccionan las opciones de: *Recover Folders*, *File signature analysis* y *Hash analysis.*

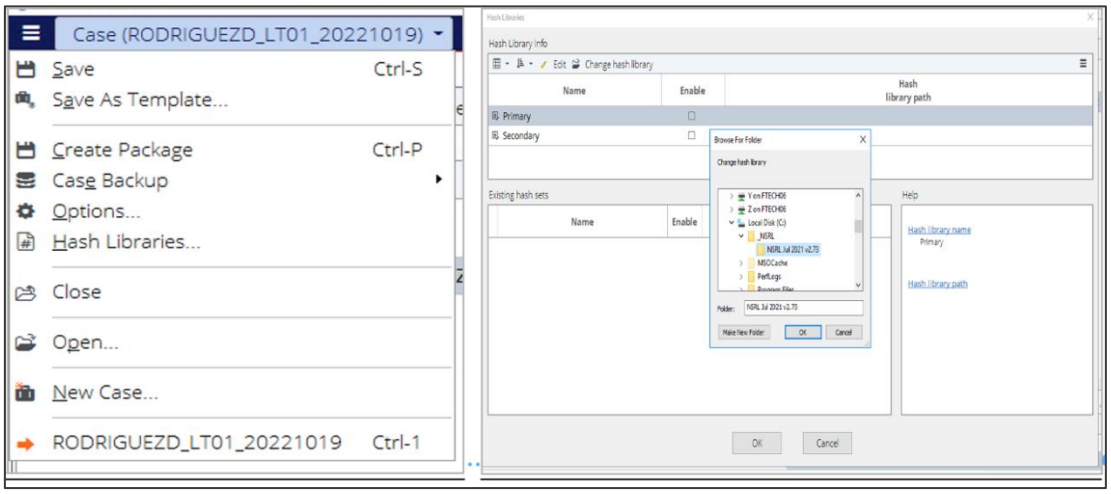
Figura 155: Paso III con la herramienta Encase Forensic



Fuente: Elaboración Propia

4) En esta sección se elige el script que permite filtrar los elementos que no son de basura del sistema ya que éstos no son de interés para la investigación.

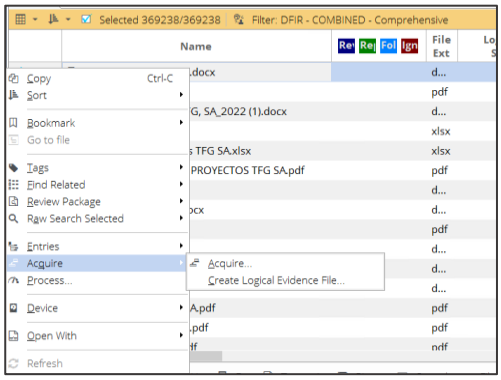
Figura 156: Paso IV con la herramienta Encase Forensic



Fuente: Elaboración Propia

5) Una vez se tienen seleccionado los elementos que se requieren, se crea el contenedor forense con los mismos.

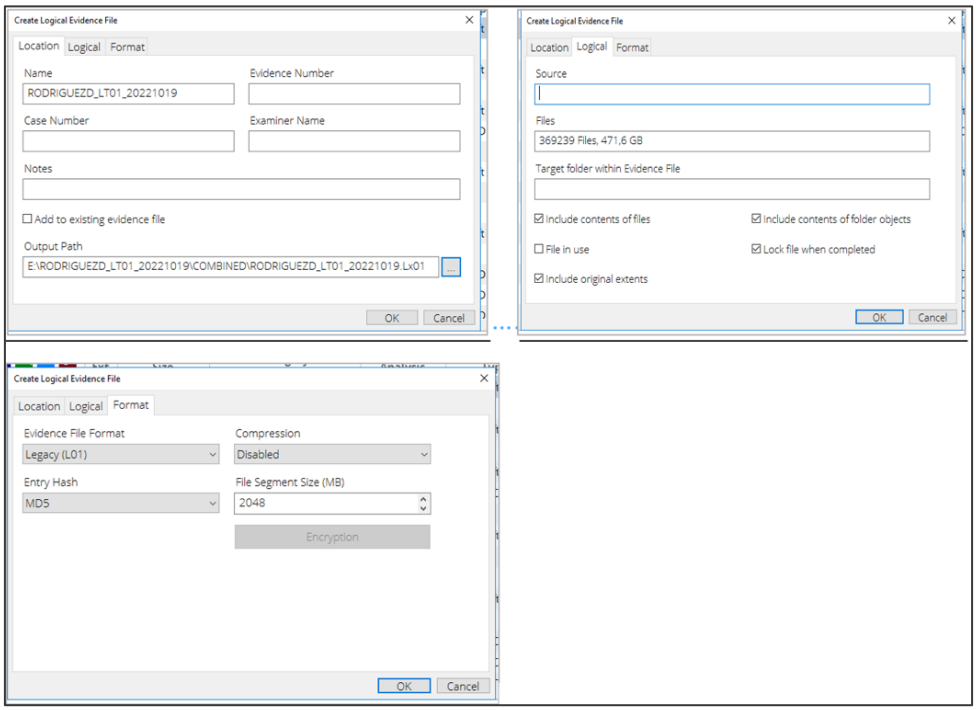
Figura 157: Paso V con la herramienta Encase Forensic



Fuente: Elaboración Propia

6) En esta última parte, se agrega el nombre de la evidencia del contenedor forense, la ruta donde se desea que se guarde y por último destacar, que el formato de este es un *L01*, que es el propio de contenedor forense de *EnCase*.

Figura 158: Paso VI con la herramienta Encase Forensic



Fuente: Elaboración Propia

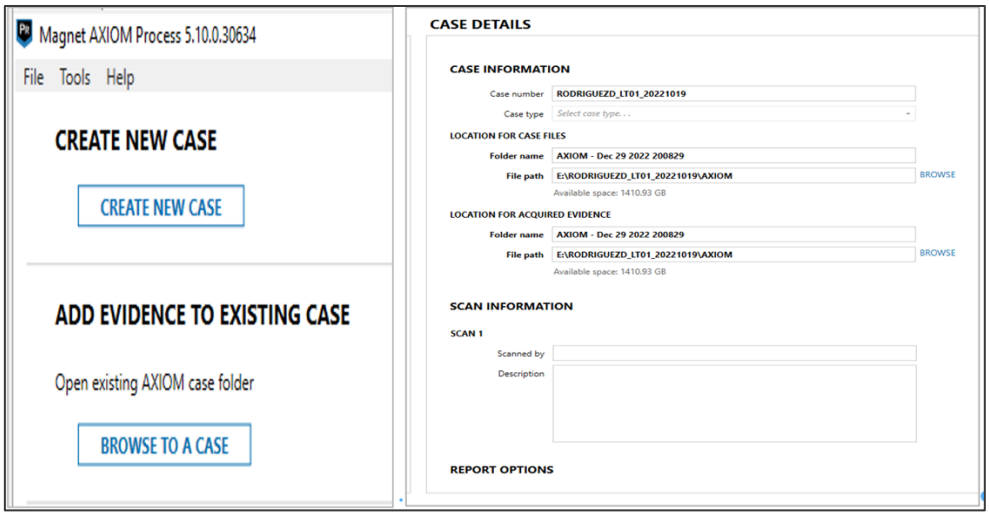
Cabe destacar que debido a que con el portátil asignado al custodio Gema Alonso Bote se ha llevado una adquisición en vivo y no física. Este hecho se debe a que no se puede realizar este tipo de procedimiento ya que su contenedor forense resultante es un fichero *.ad1*, y en consecuencia, es incompatible con dicho procedimiento.

ANEXO 4: PROCESAMIENTO EN AXIOM DE LOS PORTÁTILES

En este anexo se va a describir el procesamiento de la evidencia con la herramienta forense *Magnet Axiom*, de los portátiles asignados a los custodios Daniel Rodríguez e Iván Merino, con el objetivo de poder analizar los artefactos forenses del dispositivo que ayuden a entender y demostrar las actividades delictivas de las que se le acusan al custodio.

1) Primero de todo se abre la herramienta *Axiom Process* y se crea un nuevo caso para comenzar a procesar la evidencia:

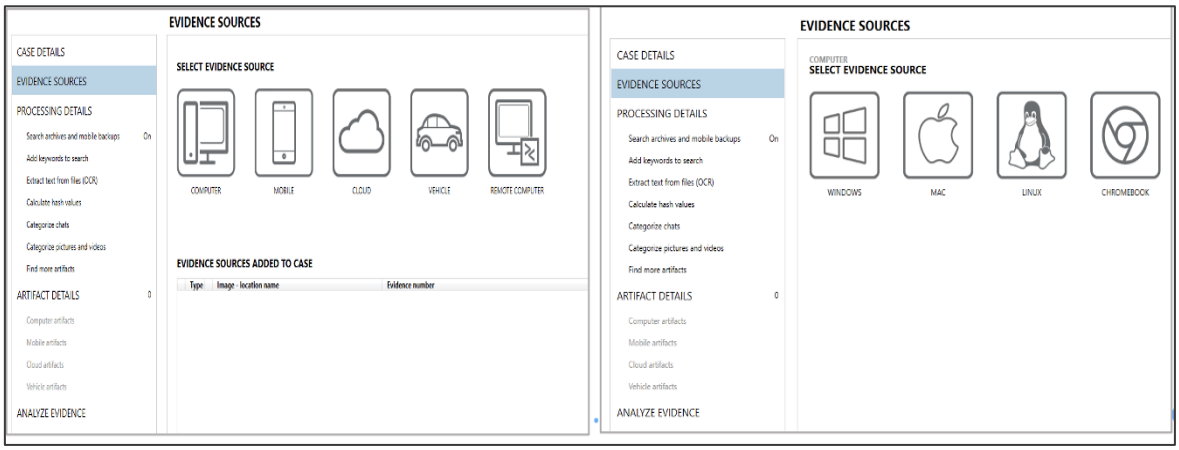
Figura 159: Paso I con la herramienta Axiom



Fuente: Elaboración Propia

2) A continuación, se siguen los pasos de la herramienta y se establece que tipo de evidencia se va a procesar, en este caso es un ordenador *Windows*.

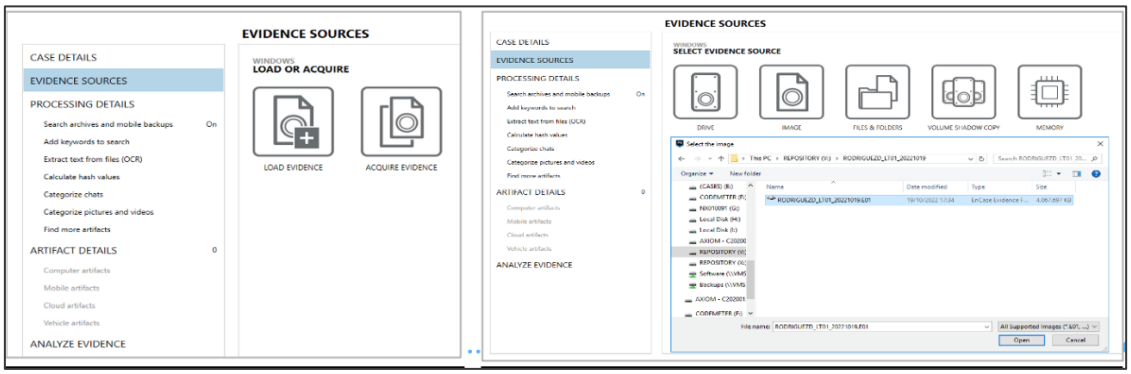
Figura 160: Paso II con la herramienta Axiom



Fuente: Elaboración Propia

3) Por otro lado, como ya está disponible la evidencia resultante de la adquisición, se selecciona la opción de *"load evidence"* y como es una imagen forense, la opción de *"image"* y se selecciona la evidencia a procesar.

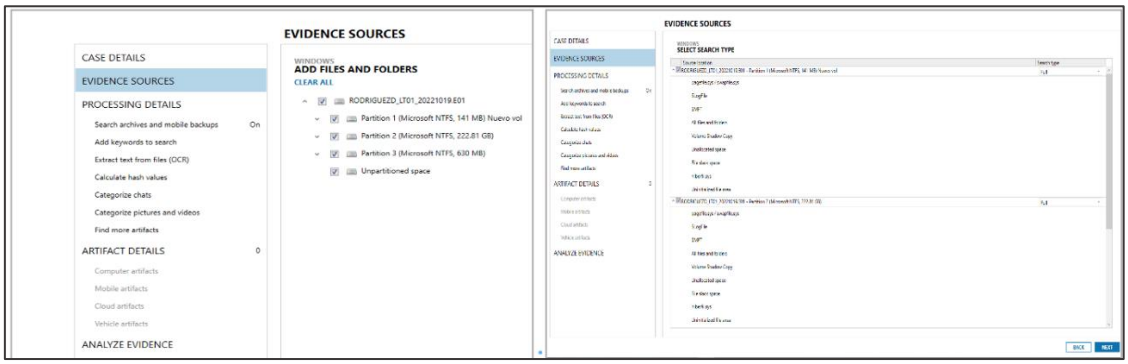
Figura 161: Paso III con la herramienta Axiom



Fuente: Elaboración Propia

4) Como se ve en la imagen, se han detectado varias particiones, y como se aprecia, la que tiene toda la información es la partición 2 con 221,8GB. Se seleccionan todas con la opción *"full"* para que se realice un procesamiento completo de todas ellas.

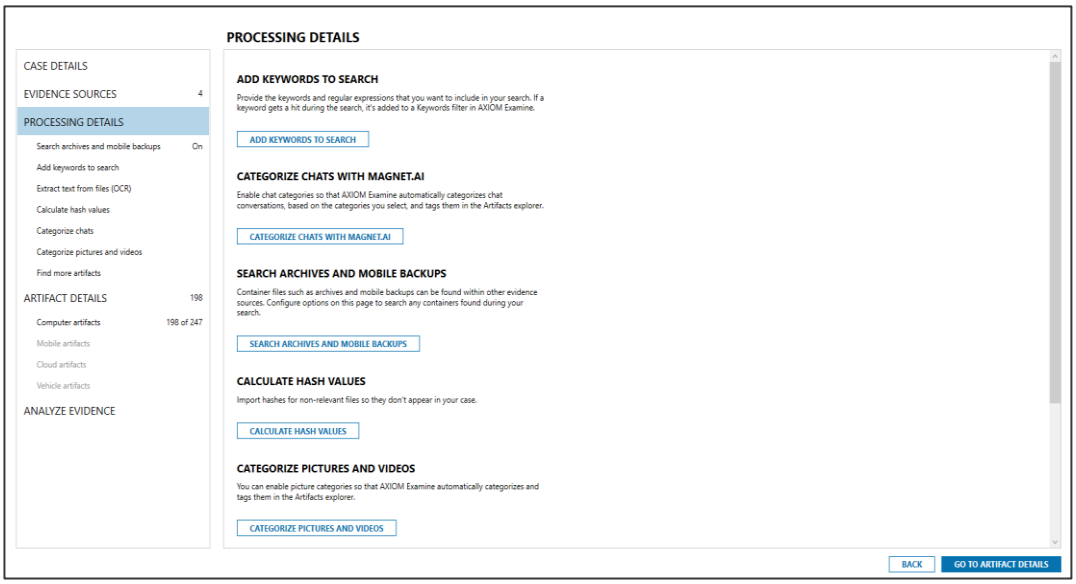
Figura 162: Paso IV con la herramienta Axiom



Fuente: Elaboración Propia

5) En la siguiente imagen se muestra la sección de *"Processing Details"* donde se puede ver todas las opciones que permite *Axiom*. En este caso en particular no se van a usar ninguna de las que aparecen en la foto.

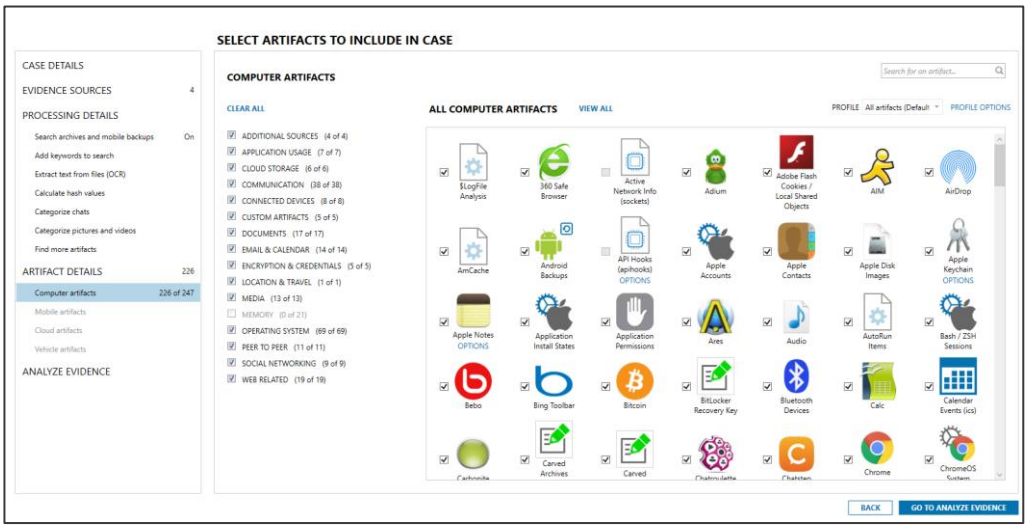
Figura 163: Paso V con la herramienta Axiom



Fuente: Elaboración Propia

6) En la siguiente sección denominada *"Computer Artifacts"* se puede seleccionar todos los artefactos forenses que se desee analizar. Se han seleccionado todos para tener una mayor completitud de información de la evidencia.

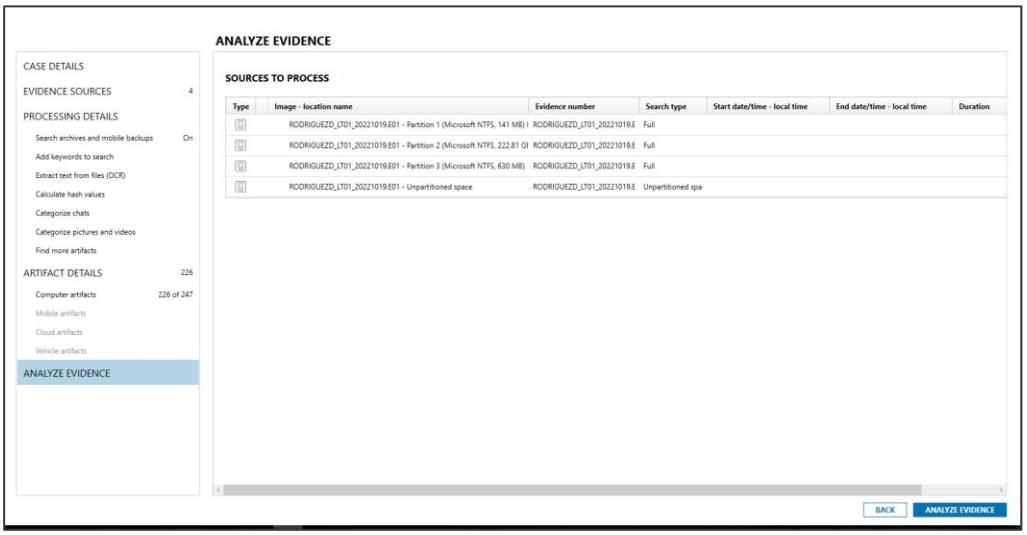
Figura 164: Paso VI con la herramienta Axiom



Fuente: Elaboración Propia

7) Por último, faltaría hacer clic al botón de *Analyze Evidence* para que comience a procesar la evidencia.

Figura 165: Paso VII con la herramienta Axiom



Fuente: Elaboración propia

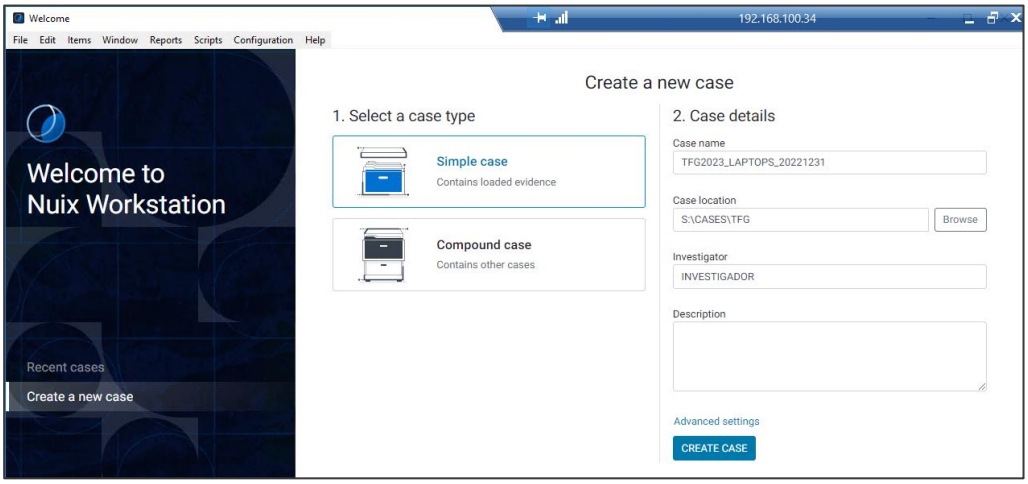
Cabe destacar de nuevo, que debido el portátil asignado al custodio Gema Alonso Bote se ha realizado adquisición en vivo y no física, no se puede realizar este tipo de procedimiento ya que su contenedor forense resultante es un fichero *.ad1*. En consecuencia, es incompatible con este procedimiento y dicha evidencia se analizará con la herramienta *FTK Imager*

ANEXO 5: PROCESAMIENTO EN NUIX DE LOS PORTÁTILES

En este anexo se va a documentar el procedimiento de procesamiento de la evidencia del portátil de los custodios con la herramienta *Nuix Forensic*.

1) Primero de todo se tiene que crear el caso de los portátiles donde se van a agregar las evidencias correspondientes a los tres custodios.

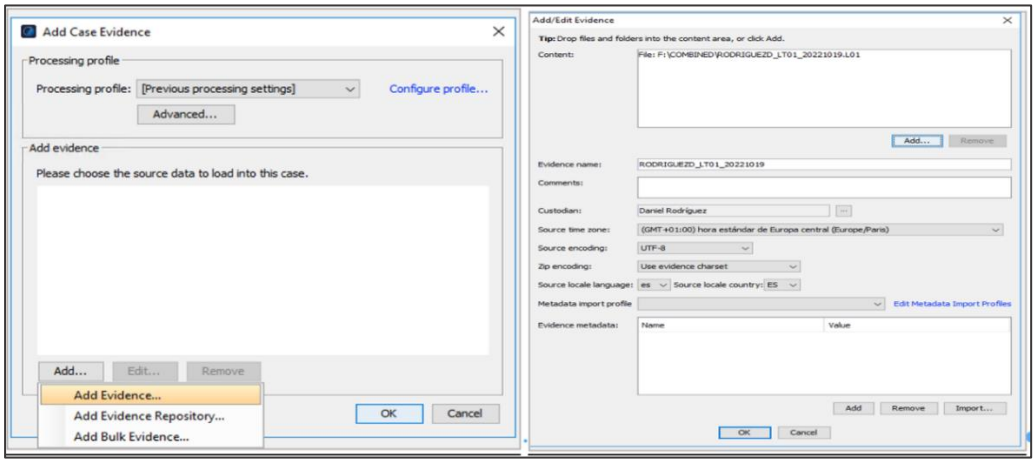
Figura 166: Paso I con la herramienta Nuix



Fuente: Elaboración Propia

2) Se va a añadir la primera evidencia que corresponde con el portátil del custodio de Daniel Rodríguez, asignando la ruta donde se encuentra la evidencia resultante del prefiltrado de *Encase*, el nombre de la evidencia, el nombre del custodio y configuraciones como *UTF-8* y la zona horaria.

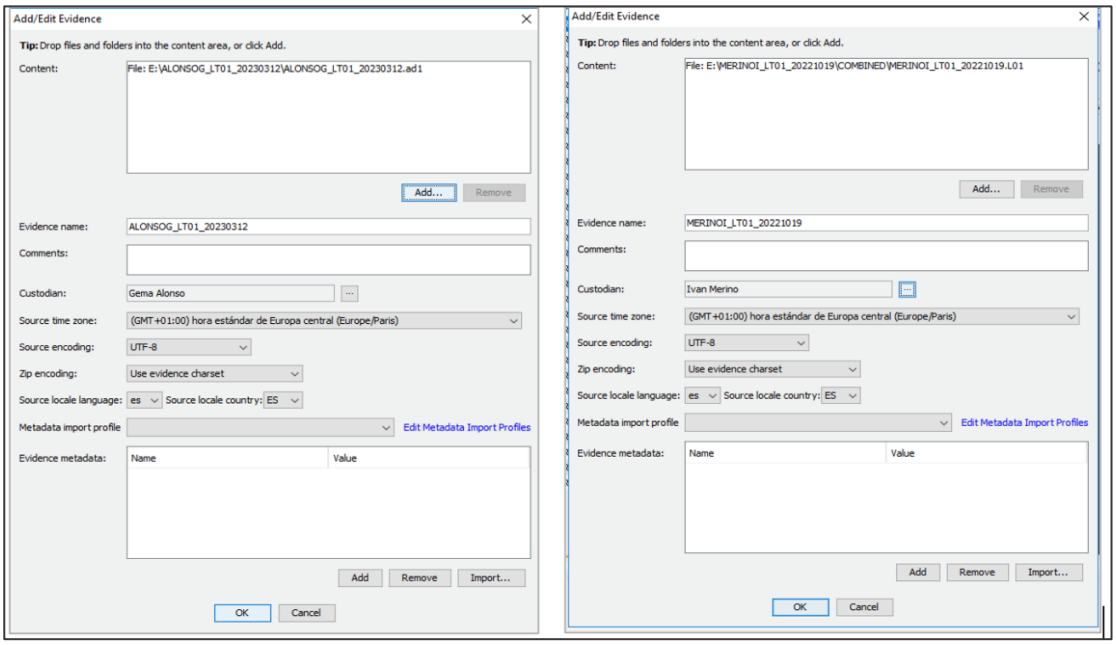
Figura 167: Paso II con la herramienta Nuix



Fuente: Elaboración Propia

3) A continuación, se añaden las otras dos evidencias que conforman el caso, que son el ordenador de Gema Alonso y de Iván Merino, tal y como se observa en las imágenes:

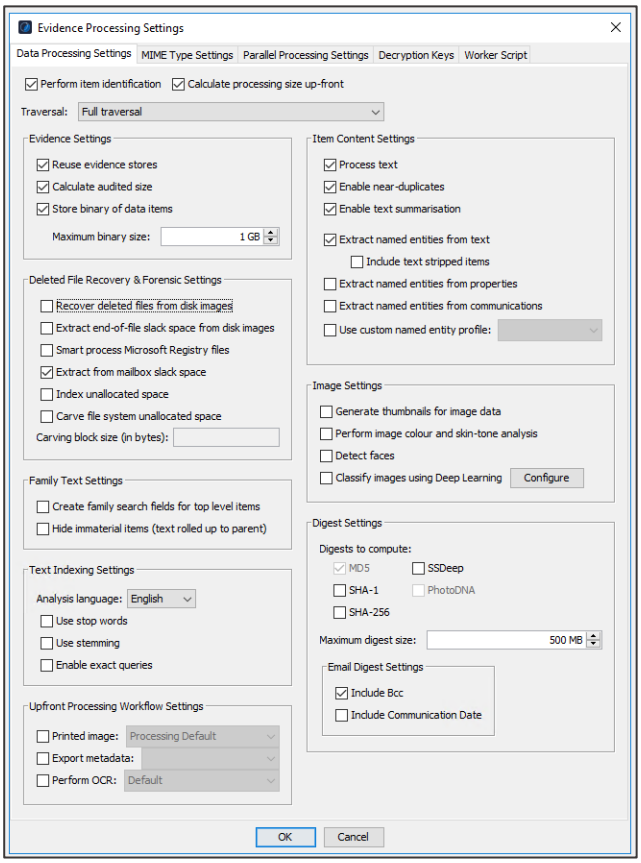
Figura 168: Paso III con la herramienta Nuix



Fuente: Elaboración Propia

4) Respecto al perfil de procesamiento se va a analizar las opciones que se pulsan y explicar el motivo de su selección.

Figura 169: Paso IV con la herramienta Nuix



Fuente: Elaboración Propia

Acerca de las opciones del perfil de procesamiento, se va a analizar el concepto de cada una de ellas[16]:

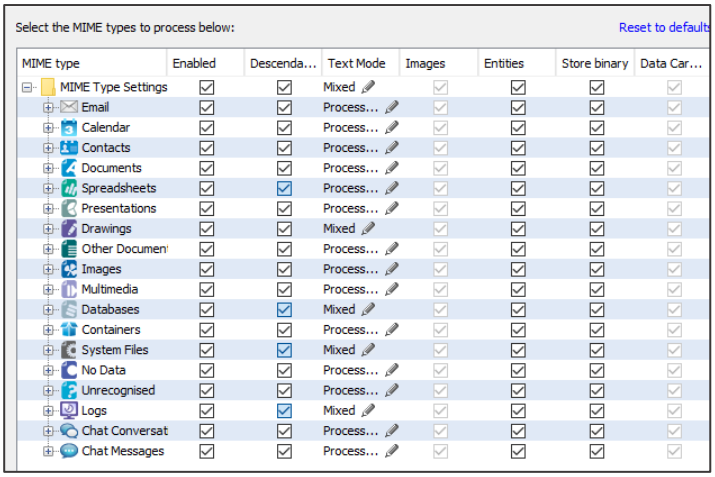
- *Perform item identification:* Permite realizar otras opciones de indexación en elementos individuales. Si esta opción no está marcada *Nuix* crea una entrada de archivo binario desconocido por cada archivo físico que encuentra.
- *Calculating processing size up-front:* Activa la barra de progreso de procesamiento del tamaño de los archivos de la evidencia.
- *Reuse evidence stores:* Permite añadir nuevas pruebas a los índices de pruebas existentes, por ello implica mayor velocidad en búsqueda y exportación de ficheros.
- *Calculate audited size:* Permite calcular el campo de auditoría de los ficheros materiales. Este valor es muy útil para las empresas, ya que, a la hora de facturar procesamiento de datos, utilizan este dato.
- *Extract from mailbox slack space:* Extrae archivos borrados de buzones *pst, ost y edb* a un nivel diferente, inferior permitiendo el acceso a los elementos de espacio libre.
- *Process text:* Permite a *Nuix* extraer el contenido de texto de las evidencias para permitir hacer búsquedas en él.
- *Enable near-duplicates:* Permite la identificación de palabras *"shingle"* que permiten identificar la detección de posibles elementos duplicados.

[16] Definiciones de opciones de procesamiento de Nuix: https://bit.ly/43s4XoQ

- Enable text summarization: Permite a *Nuix* calcular y almacenar resúmenes de texto de documentos cuando se ingieren los datos.
- *Extract named entities from text*: Permite extraer entidades con nombre del texto de las evidencias.
- *Enable Exact queries:* Esta opción almacena el contenido de texto de los elementos para permitir el uso de signos de puntuación y mayúsculas en las búsquedas, por tanto, permite una coincidencia exacta entre cadenas *String*.
- *Include Bcc:* Se selecciona esta opción para incluir este campo a los creados por defecto en los mensajes de *email*. Representa a las copias ocultas de direcciones de correo electrónico en un mensaje de correo electrónico.

5) Una vez elegido el perfil de procesamiento de las evidencias, se selecciona todos los tipos de fichero que se va a querer procesar. Para ello, se selecciona todos los que ofrece *Nuix*, como se observa en la imagen:

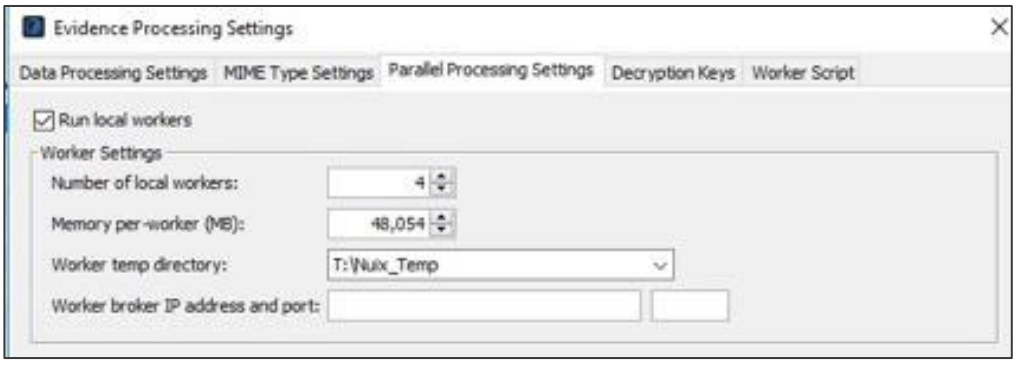
Figura 170: Paso V con la herramienta Nuix



Fuente: Elaboración Propia

6) A continuación, se seleccionan los *"workers"* que se van a usar para procesar las evidencias. A mayor número de *"workers"*, menor tiempo de procesamiento será necesario para procesar las evidencias y menor cantidad de memoria se destinará a cada uno.

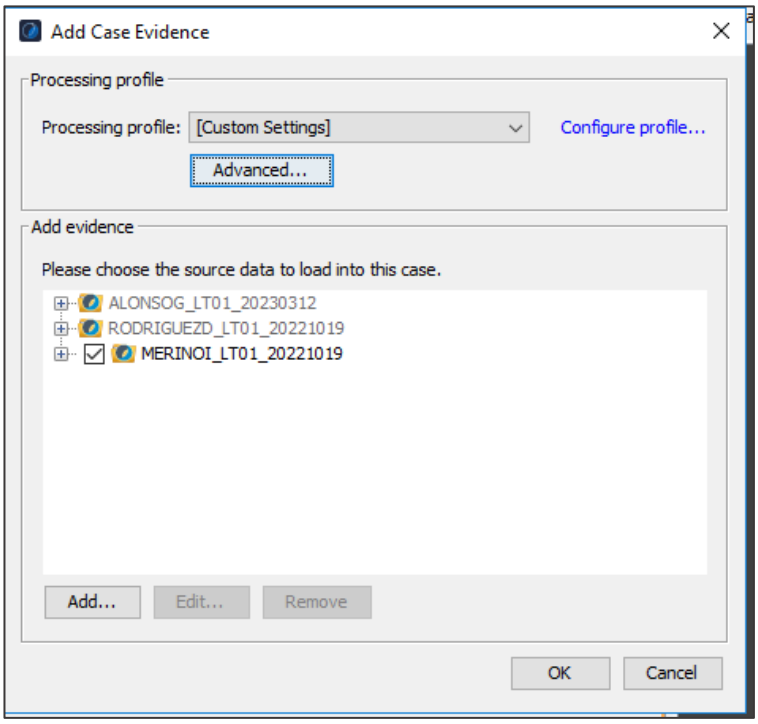
Figura 171: Paso VI con la herramienta Nuix



Fuente: Elaboración Propia

7) Finalmente, se vuelve a la ventana principal donde se encuentran las tres evidencias a procesar y se hace clic en "OK", para comenzar con el procesamiento.

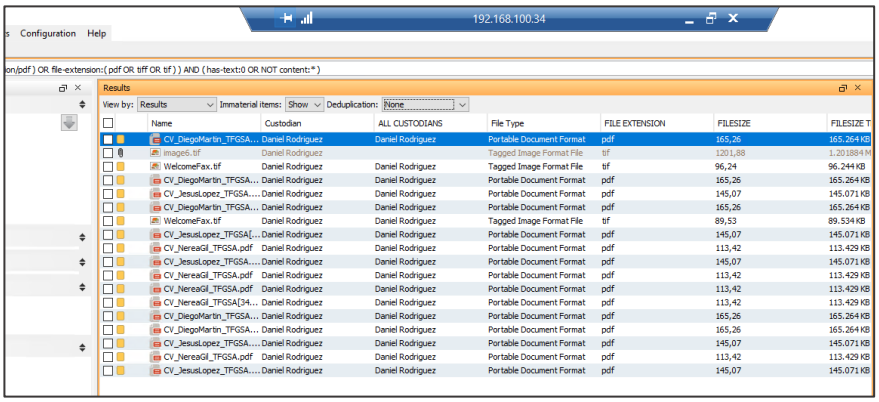
Figura 172: Paso VII con la herramienta Nuix



Fuente: Elaboración Propia

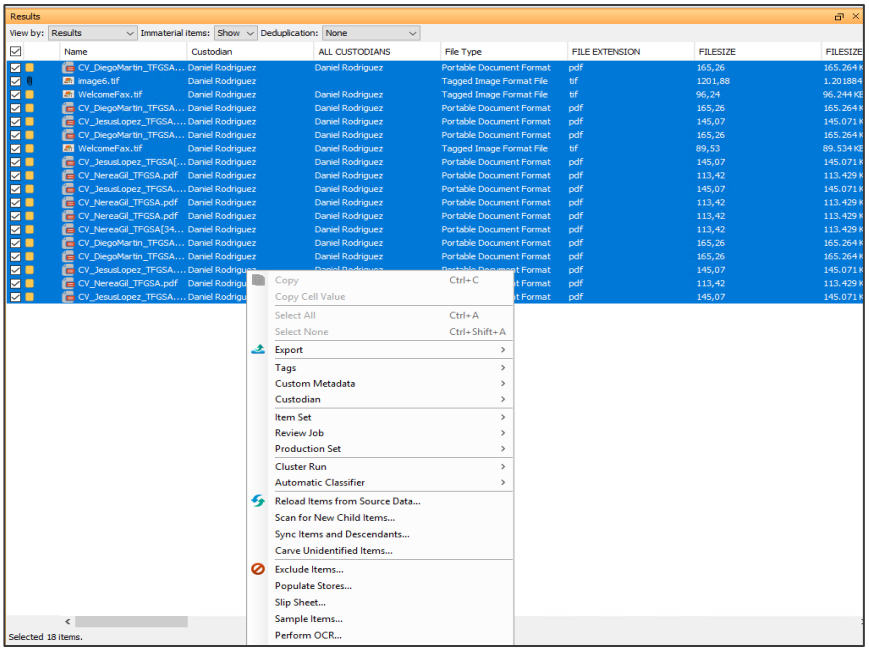
8) Una vez terminado el procesado de las evidencias y previo al análisis se deben realizar tres pasos adicionales. El primero de ellos es pasar el OCR a los archivos *.pdf, .tif* etcétera, necesario para que puedan ser legibles. Para desarrollar esto, *Nuix* posee una opción denominada *"Perform OCR"*, donde solo se tiene que identificar los elementos a los se les vaya a aplicar esta función. Para ello, se ha creado una *query*, con la que se identifican los archivos que son necesarios: (*mime-type: (image7tiff OR application/pdf) OR file-extension: (pdf OR tiff OR tif)) AND (has-text:0 OR NOT content*)*. En las siguientes imágenes se ven los ejemplos para la primera evidencia:

Figura 173: Paso VIII con la herramienta Nuix (I)



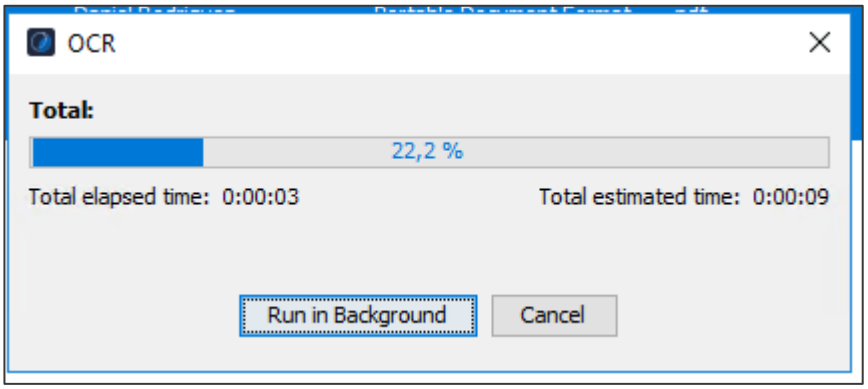
Fuente: Elaboración Propia

Figura 174: Paso VIII con la herramienta Nuix (II)



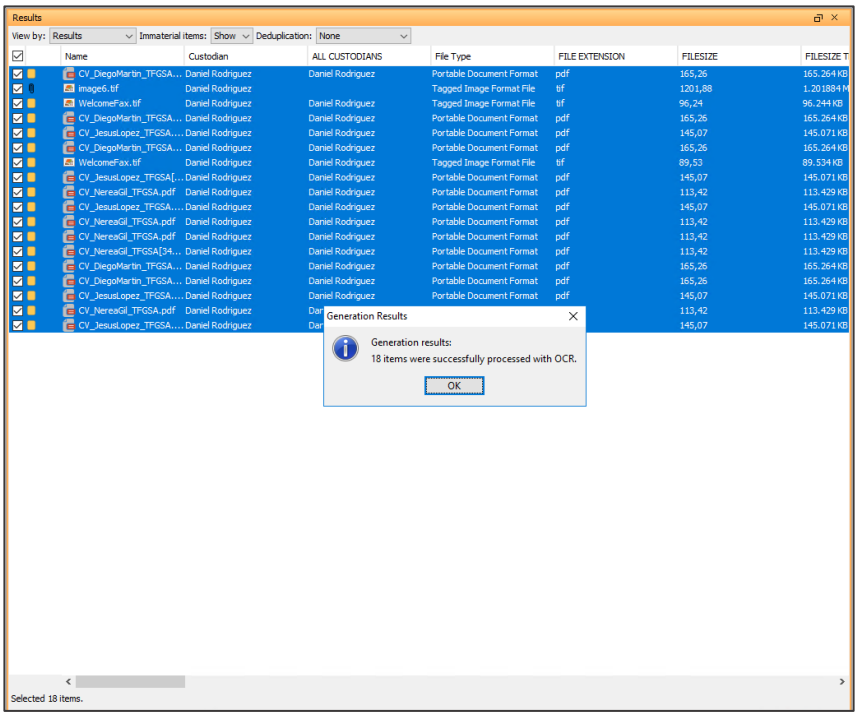
Fuente: Elaboración Propia

Figura 175: Paso VIII con la herramienta Nuix (III)



Fuente: Elaboración Propia

Figura 176: Paso VIII con la herramienta Nuix (IV)



Fuente: Elaboración Propia

9) El siguiente paso, consiste en excluir una serie de ficheros de sistema que no aportan información ni valor para la investigación. Para ello, se lanza un *script* llamado *"Annotate from CSV"*, en el que se ha desarrollado un una serie de consultas almacenadas en la columna *"Match Query"*. Por otro lado, se nombra a cada una de ellas con el nombre de la exclusión que se desea crear en la columna "*Exclude*", tal y como se observa en la imagen:

Figura 177: Paso IX con la herramienta Nuix (I)

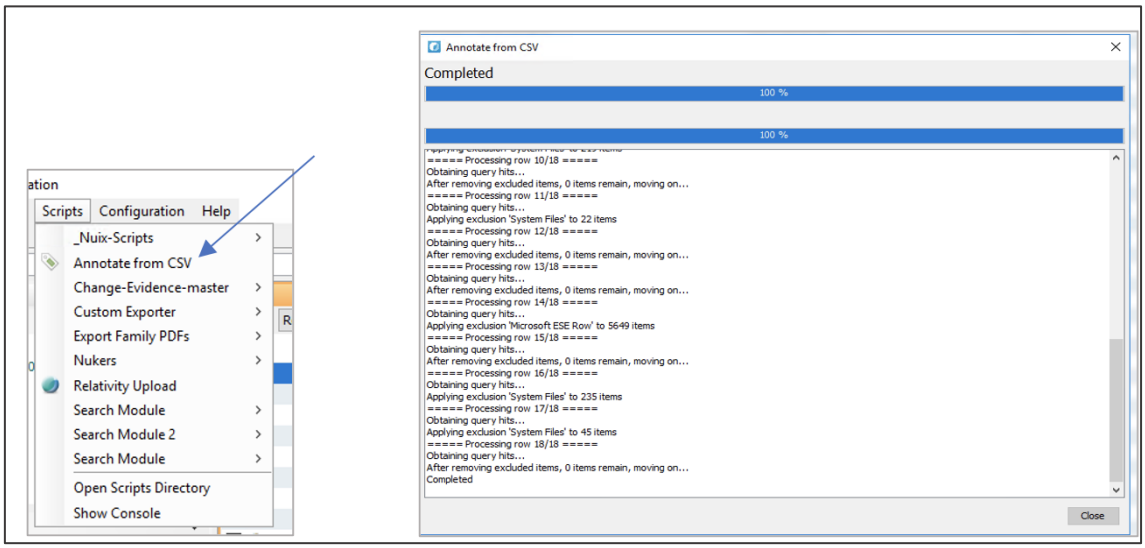
MatchQuery	Exclude
kind:multimedia	Multimedia
kind:no-data	No Data
kind:unrecognised AND NOT mime-type:text/plain	Unrecognised
kind:other-document AND !mime-type:(application/vnd.ms-outlook-task OR application/*outlook* OR application/vnd.ms-onenote OR application/vnd.ms-project OR application/*lotus*)	System Documents
mime-type:application/java-archive OR path-mime-type:application/java-archive	System Containers1
mime-type:application/vnd.ms-cab-compressed OR path-mime-type:application/vnd.ms-cab-compressed	System Containers2
mime-type:application/x-self-extracting-archive OR path-mime-type:application/x-self-extracting-archive	System Containers3
path-mime-type:application/x-thumbs-db or mime-type:application/x-thumbs-db	System Files
mime-type:text/html and not content:*	System Files
file-extension:FileSlack	System Files
mime-type:application/vnd.openxmlformats-officedocument.drawingml.chart+xml OR mime-type:application/x-database-table-row	System Files
(mime-type:application/vnd.corel-wordperfect AND path-mime-type:(application/vnd.openxmlformats* OR application/vnd.ms-excel OR application/vnd.ms-word OR application/vnd.ms-powerpoint))	System Files
file-extension:joboptions	System Files
mime-type:application/vnd.ms-ese-row AND not content:*	Microsoft ESE Row
file-extension:txt content:Created By AccessData	System Files
mime-type:text/plain AND (name:VTIMEZONE OR file-extension:(inf OR rdp OR ini OR lst OR url OR css OR js) OR path-name:Temporary Internet Files OR path-name:((Microsoft AND Windows) OR (Docume	System Files
kind:system AND NOT exclusion:'System Documents' AND NOT exclusion:'System Containers'	System Files
path-name:(personmetadata OR applicationdataroot)	O365

Fuente: Elaboración Propia

Posteriormente, se sigue el siguiente proceso para ejecutar el script:

1) Se selecciona en la pestaña de *Scripts*, el siguiente: *Annotate from CSV* y se ejecuta.

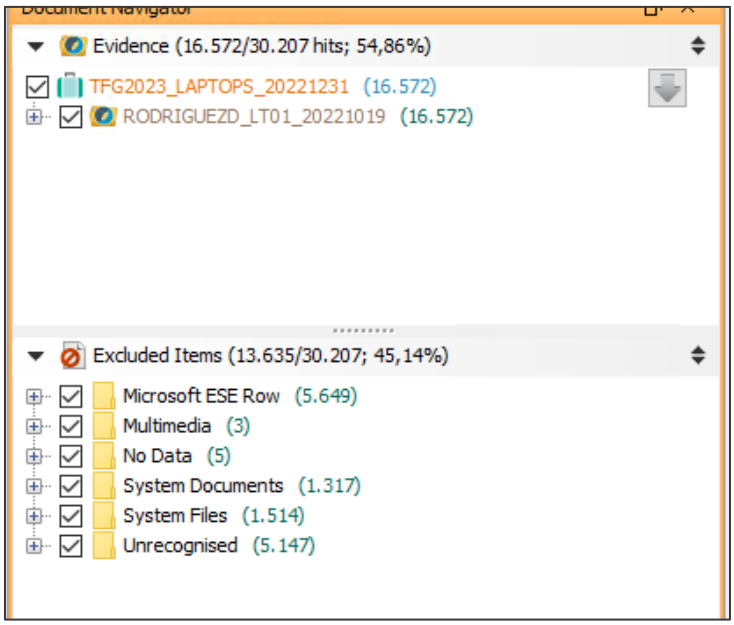
Figura 178: Paso IX con la herramienta Nuix (II)



Fuente: Elaboración Propia

2) A continuación, se ve el resultado de los elementos excluidos.

Figura 179: Paso IX con la herramienta Nuix (III)



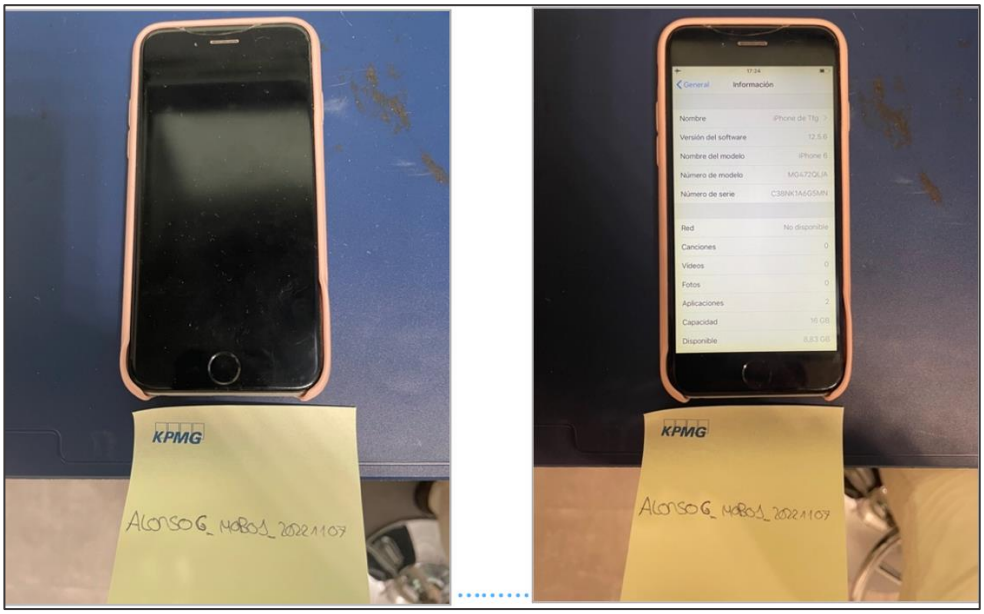
Fuente: Elaboración Propia

ANEXO 6: ADQUISICIÓN Y PROCESAMIENTO DE LOS DISPOSITIVOS MÓVILES

En este anexo se va a documentar el procedimiento de la adquisición y el procesamiento de la evidencia del móvil de los custodios con la herramienta *Cellebrite UFED.*

1) Primero de todo se coloca el móvil y se identifica con el *post-it* agregando el nombre la evidencia que se va a tratar y se anotan las características del teléfono que aparecen en la imagen de la derecha

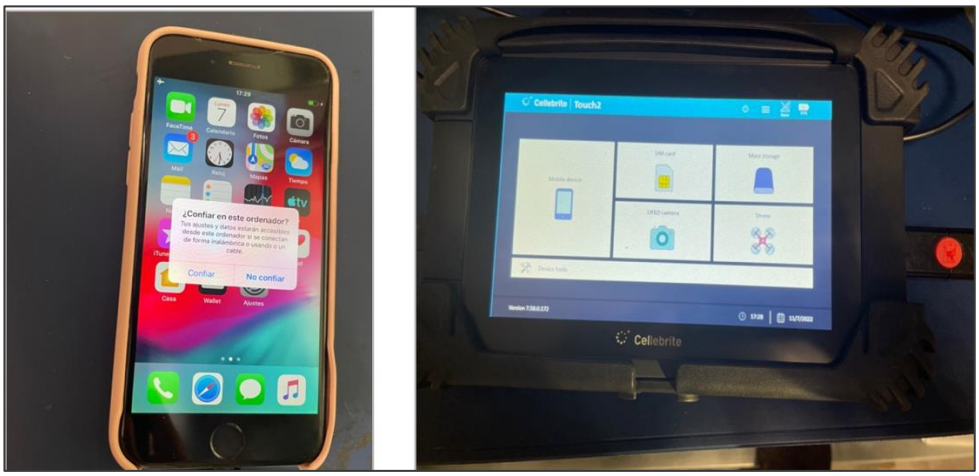
Figura 180:Paso I adquisición de móviles con Cellebrite



Fuente: Elaboración Propia

2) Después, se conecta el teléfono a la máquina *Cellebrite UFED* y aparecerá el mensaje de si se confía en este ordenador y se le clicará siempre a Sí.

Figura 181: Paso II adquisición de móviles con Cellebrite



Fuente: Elaboración Propia

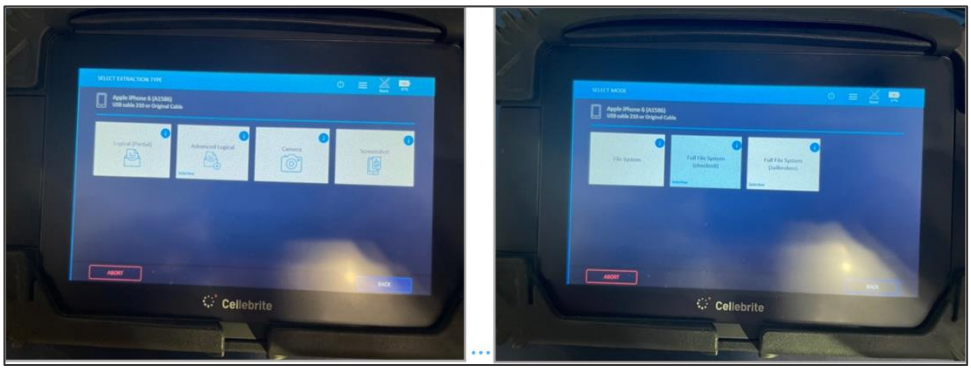
3) Una vez conectado el teléfono, se deberá clicar en la opción auto detecte para que la herramienta *Cellebrite* identifique el modelo del teléfono y posteriormente, se seleccione alguno de ellos como se puede ver en la imagen de la derecha.

Figura 182: Paso III adquisición de móviles con Cellebrite

Fuente: Elaboración Propia

4) Una vez detectada la evidencia a adquirir, se debe seleccionar el tipo de extracción/adquisición más exhaustiva posible que permita dicho modelo de teléfono. Como se puede apreciar en las imágenes, se ha procedido a realizar una adquisición *"Advanced Logical"* y la opción de *"Full File System"*.

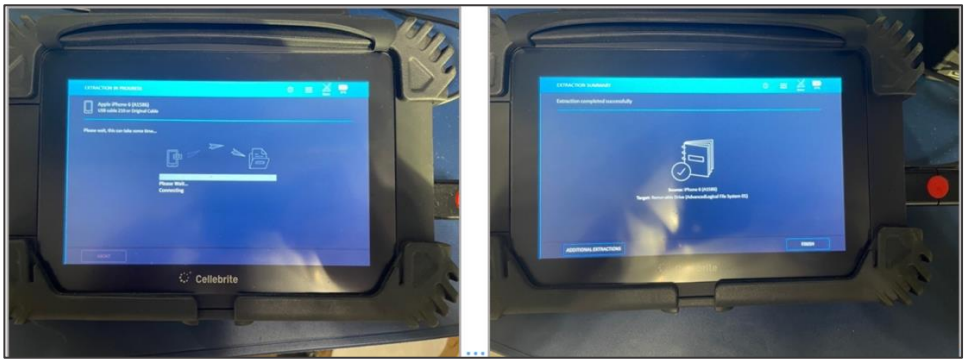
Figura 183: Paso IV adquisición de móviles con Cellebrite



Fuente: Elaboración Propia

5) Una vez seleccionado el tipo de extracción se debe conectar un dispositivo externo en el que se va a volcar la adquisición y esperar a que la misma termine correctamente como se puede ver en la imagen de la derecha.

Figura 184: Paso V adquisición de móviles con Cellebrite



Fuente: Elaboración Propia

Una vez realizada la adquisición de las evidencias, se debe abrir el fichero con extensión *ufdr* resultante. Con esto, comenzará el procesamiento de las evidencias que se realizará con la herramienta *Cellebrite Physical Analyzer*.

ANEXO 7: ANÁLISIS DE LOS ORDENADORES PORTÁTILES Y DISPOSITIVOS MÓVILES

En este anexo se va a documentar una de las partes más importantes de la investigación, que se trata del análisis de los equipos corporativos de los custodios. Esta fase es la que comprende, la identificación de las pruebas o evidencias del caso práctico. Para ello se entrará en profundidad a analizar los artefactos forenses de los equipos, que demostrarán las acciones delictivas que han tenido lugar.

Primero de todo, y siguiendo las buenas prácticas y la legalidad vigente, la búsqueda de se ha realizado por el método de búsqueda ciega o por palabras clave, con el objetivo de no analizar todo el contenido de los equipos, sino solamente los ficheros que han dado *"hit"*, es decir, las palabras claves se encuentran contenidas en dichos documentos. Estas palabras clave las ha desarrollado el investigador siguiendo el entendimiento del caso práctico y los ficheros a buscar, se han lanzado tanto en los ordenadores, como en los dispositivos móviles, y son las siguientes:

- "Pr?ximos proyectos"
- "Informe Resultados"
- "CV_*"
- "Valoraci?n W/2 TFG"
- "Acta w/2 reuni?n"
- "Listado de Clientes TFG"
- "Posici?n competidores"
- "Robar informaci?n"
- "Dejar rastro"
- "Disco duro"
- "Como se lo digas"
- "Polic?a"
- "denuncia*"
- "Prueba"
- "termin* w/2 carrera"

Una vez definido en qué consiste el anexo y las palabras clave utilizadas, se procederá a comenzar con el análisis de los ordenadores.

1. Análisis del ordenador portátil asignado al custodio Daniel Rodríguez
    - Primero de todo, se va a analizar el dispositivo utilizando la herramienta *Magnet Axiom Examine*, que nos permite analizar los principales artefactos forenses del equipo, que se aglutinan en las siguientes vertientes de la investigación:

Tabla 20: Principales categorías y artefactos analizados

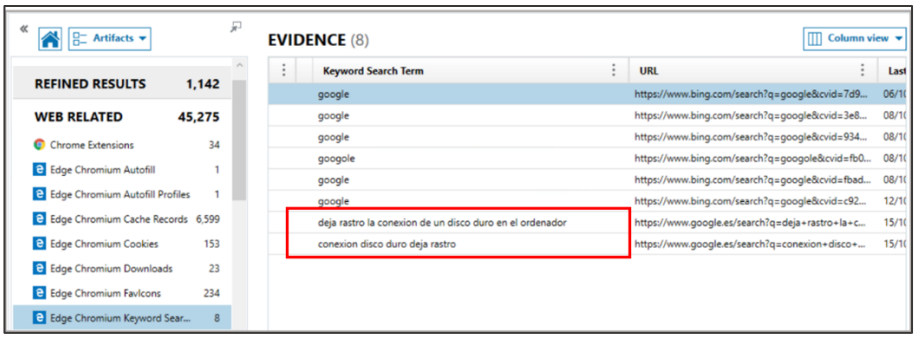
Categoría de análisis	Artefactos forenses implicados y descripción
Actividad Reciente del equipo	Se van a analizar los siguientes artefactos: *Jumplist, Shellbags, Lnks y Windows Office Alerts*. Estos nos dan información sobre la actividad del usuario en cuanto a la creación, modificación y visualización de ficheros.

Borrado de información	Se van a analizar el siguiente artefacto: *$RecicleBin*. Este nos da información acerca de los ficheros que han sido eliminados y mandados a la papelera de reciclaje.
Navegación web	Se van a analizar los siguientes artefactos: *IE, Chrome, Safari, Edge Main History, Keyword Searches.* Estos nos dan información sobre el historial de navegación del usuario en los diferentes navegadores web.
Descarga de datos en la web	Se van a analizar los siguientes artefactos: *IE, Chrome, Safari, Edge Downloads*. Estos nos dan información sobre las descargas de ficheros realizadas por el usuario
Fuga de información	Se van a analizar los siguientes artefactos: *USB Connected Devices, Windows Event Logs - Storage Device Events*. Estos nos dan información sobre las conexiones de dispositivos de almacenamiento externos en el portátil del usuario.

Fuente: Elaboración Propia

- Para comenzar el análisis, se va a analizar la sección de la navegación web (“*Web Related”)*, y se han descubierto los siguientes hallazgos que se muestran en las siguientes imágenes:
- ***Edge Chronium Keyword Searches:***

Figura 185: Búsquedas en explorador Edge



Fuente: Elaboración Propia

- Con el objetivo de mejorar la visualización de los artefactos analizados utilizando la herramienta *Axiom Examine*, se ha procedido a exportar los resultados a formato *Excel*, por lo que, a partir de ahora, se mostrará una imagen de los resultados y el consiguiente acceso a dicho fichero Excel resultado.
- Continuando con el análisis de la navegación web, en el que se tiene en cuenta también, el historial de navegación y las descargas realizadas en los diferentes navegadores, en este dispositivo no se han encontrado descargas relevantes, sin embargo, se ha observado que utilizaba el navegador Edge.

- Resultado artefacto ***Edge_Internet Explorer 10-11 Main History****:*

Figura 186: Historial de navegación en navegador Edge

URL	User	Accessed Date/Time - UTC+00:00 (dd/MM/yyyy)
file:///C:/Users/Daniel Rodríguez/Desktop/INFO DE INTERÉS	Daniel Rodríguez	19/10/2022 14:48:27
file:///E:/INFO DE INTERÉS/Valoracion_TFG_SA.xlsx	Daniel Rodríguez	15/10/2022 11:45:29
file:///E:/INFO DE INTERÉS/Informe Resultados TFG, SA_2022.pdf	Daniel Rodríguez	15/10/2022 11:46:20
file:///E:/INFO DE INTERÉS/Informe Resultados TFG, SA_2022 (1).docx	Daniel Rodríguez	15/10/2022 11:50:32
file:///E:/INFO DE INTERÉS/CV_DiegoMartin_TFGSA.docx	Daniel Rodríguez	15/10/2022 11:52:01
file:///E:/INFO DE INTERÉS/CV_DiegoMartin_TFGSA.pdf	Daniel Rodríguez	15/10/2022 11:52:21
file:///E:/INFO DE INTERÉS/CV_JesusLopez_TFGSA.docx	Daniel Rodríguez	15/10/2022 11:52:32
file:///E:/INFO DE INTERÉS/CV_JesusLopez_TFGSA.pdf	Daniel Rodríguez	15/10/2022 11:52:45
file:///E:/INFO DE INTERÉS/CV_NereaGil_TFGSA.docx	Daniel Rodríguez	15/10/2022 11:53:01
file:///E:/INFO DE INTERÉS/CV_NereaGil_TFGSA.pdf	Daniel Rodríguez	15/10/2022 11:53:10
file:///C:/Users/Daniel Rodríguez/Desktop/INFO DE INTERÉS/Listado de Clientes TFG.xlsx	Daniel Rodríguez	15/10/2022 11:17:09
file:///C:/Users/Daniel Rodríguez/Desktop/INFO DE INTERÉS/Posicion competidores TFG SA.xlsx	Daniel Rodríguez	15/10/2022 11:17:59
file:///C:/Users/Daniel Rodríguez/Desktop/INFO DE INTERÉS/Valoracion_TFG_SA.xlsx	Daniel Rodríguez	15/10/2022 11:33:29
file:///C:/Users/Daniel Rodríguez/Desktop/INFO DE INTERÉS/Informe Resultados TFG, SA_2022.pdf	Daniel Rodríguez	15/10/2022 11:34:37
file:///C:/Users/Daniel Rodríguez/Desktop/INFO DE INTERÉS/Informe Resultados TFG, SA_2022 (1).docx	Daniel Rodríguez	15/10/2022 11:35:17
file:///C:/Users/Daniel Rodríguez/Desktop/INFO DE INTERÉS/CV_NereaGil_TFGSA.pdf	Daniel Rodríguez	15/10/2022 11:36:26
file:///C:/Users/Daniel Rodríguez/Desktop/INFO DE INTERÉS/CV_NereaGil_TFGSA.docx	Daniel Rodríguez	15/10/2022 11:36:59
file:///C:/Users/Daniel Rodríguez/Desktop/INFO DE INTERÉS/CV_JesusLopez_TFGSA.pdf	Daniel Rodríguez	15/10/2022 11:37:36
file:///C:/Users/Daniel Rodríguez/Desktop/INFO DE INTERÉS/CV_JesusLopez_TFGSA.docx	Daniel Rodríguez	15/10/2022 11:38:42
file:///C:/Users/Daniel Rodríguez/Desktop/INFO DE INTERÉS/CV_DiegoMartin_TFGSA.pdf	Daniel Rodríguez	15/10/2022 11:39:05
file:///C:/Users/Daniel Rodríguez/Desktop/INFO DE INTERÉS/CV_DiegoMartin_TFGSA.docx	Daniel Rodríguez	15/10/2022 11:39:28

Fuente: Elaboración Propia

Para mayor detalle, ver en el siguiente enlace, los reportes de los artefactos forenses: PRUEBAS ORDENADOR DANI

- A continuación, se va a analizar la **actividad reciente del usuario**, analizando, por tanto, los artefactos, *Jumplists*, *Lnks*, *shellbags* y presentando atención a las acciones que refleja el artefacto *Windows Office Alerts*. A continuación, tal y como se observa en la imagen, se ha filtrado los accesos a ficheros con dispositivos externos, con el objetivo de demostrar una potencial fuga de información de ficheros confidenciales de la empresa.
- Resultados artefacto forense ***JumpList***:

Figura 187:Registros de actividad reciente del artefacto Jumplist

Linked Path	Volume Serial Number	Target File Created Date/Time - U	Target File Last Modified Date/Tim	T
E:\INFO DE INTERÉS\Valoracion_TFG_SA.xlsx	5DE33197	15/10/2022 11:45:05	15/10/2022 11:50:10	1
E:\INFO DE INTERÉS\RESUMEN PRÓXIMOS PROYECTOS TFG SA.docx	5DE33197	14/10/2022 10:05:39	14/10/2022 9:57:16	1
E:\INFO DE INTERÉS\Valoracion_TFG_SA.xlsx	5DE33197	15/10/2022 11:45:05	15/10/2022 11:54:28	1
E:\INFO DE INTERÉS\Listado de Clientes TFG.xlsx	5DE33197	14/10/2022 10:05:38	15/10/2022 11:54:06	1
E:\INFO DE INTERÉS	5DE33197	14/10/2022 10:05:38	14/10/2022 10:03:22	1
E:\INFO DE INTERÉS\RESUMEN PRÓXIMOS PROYECTOS TFG SA.pdf	5DE33197	14/10/2022 10:05:39	14/10/2022 9:21:48	1
E:\INFO DE INTERÉS\Inventario activos TFG_SA 2022.xlsx	5DE33197	14/10/2022 10:05:38	14/10/2022 10:00:48	1
E:\INFO DE INTERÉS\RESUMEN PRÓXIMOS PROYECTOS TFG SA.pdf	5DE33197	14/10/2022 10:05:39	14/10/2022 9:21:48	1
E:\INFO DE INTERÉS\CV_NereaGil_TFGSA.pdf	5DE33197	15/10/2022 11:44:47	15/10/2022 11:32:52	1
E:\INFO DE INTERÉS\CV_JesusLopez_TFGSA.pdf	5DE33197	15/10/2022 11:44:48	15/10/2022 11:32:36	1
E:\INFO DE INTERÉS\Valoracion_TFG_SA.xlsx	5DE33197	15/10/2022 11:45:05	15/10/2022 11:50:10	1
E:\INFO DE INTERÉS\CV_DiegoMartin_TFGSA.pdf	5DE33197	15/10/2022 11:44:47	15/10/2022 11:30:04	1
E:\INFO DE INTERÉS\Listado de Clientes TFG.xlsx	5DE33197	14/10/2022 10:05:38	14/10/2022 10:10:36	1
E:\INFO DE INTERÉS\Listado de Clientes TFG.xlsx	5DE33197	14/10/2022 10:05:38	14/10/2022 10:10:36	1
E:\INFO DE INTERÉS\Inventario activos TFG_SA 2022.xlsx	5DE33197	14/10/2022 10:05:38	14/10/2022 10:00:48	1
E:\INFO DE INTERÉS\RESUMEN PRÓXIMOS PROYECTOS TFG SA.docx	5DE33197	14/10/2022 10:05:39	15/10/2022 11:55:40	1
E:\INFO DE INTERÉS\Inventario activos TFG_SA 2022.xlsx	5DE33197	14/10/2022 10:05:38	14/10/2022 10:00:48	1
E:\INFO DE INTERÉS\Posicion competidores TFG SA.xlsx	5DE33197	14/10/2022 10:05:39	14/10/2022 9:22:18	1
E:\INFO DE INTERÉS\Posicion competidores TFG SA.xlsx	5DE33197	14/10/2022 10:05:39	14/10/2022 9:22:18	1
E:\INFO DE INTERÉS\CV_NereaGil_TFGSA.docx	5DE33197	15/10/2022 11:44:48	15/10/2022 11:32:44	1
E:\INFO DE INTERÉS\CV_NereaGil_TFGSA.pdf	5DE33197	15/10/2022 11:44:47	15/10/2022 11:32:52	1
E:\INFO DE INTERÉS\CV_JesusLopez_TFGSA.docx	5DE33197	15/10/2022 11:44:48	15/10/2022 11:32:28	1
E:\INFO DE INTERÉS\CV_DiegoMartin_TFGSA.docx	5DE33197	15/10/2022 11:44:47	15/10/2022 11:29:58	1
E:\INFO DE INTERÉS\Informe Resultados TFG, SA_2022 (1).docx	5DE33197	15/10/2022 11:44:47	15/10/2022 11:51:10	1
E:\INFO DE INTERÉS\Informe Resultados TFG, SA_2022.pdf	5DE33197	15/10/2022 11:44:47	15/10/2022 11:30:32	1
E:\INFO DE INTERÉS\CV_NereaGil_TFGSA.docx	5DE33197	15/10/2022 11:44:48	15/10/2022 11:32:44	1
E:\INFO DE INTERÉS\CV_JesusLopez_TFGSA.pdf	5DE33197	15/10/2022 11:44:48	15/10/2022 11:32:36	1
E:\INFO DE INTERÉS\CV_JesusLopez_TFGSA.docx	5DE33197	15/10/2022 11:44:48	15/10/2022 11:32:28	1
E:\INFO DE INTERÉS\CV_DiegoMartin_TFGSA.pdf	5DE33197	15/10/2022 11:44:47	15/10/2022 11:30:04	1
E:\INFO DE INTERÉS\CV_DiegoMartin_TFGSA.docx	5DE33197	15/10/2022 11:44:47	15/10/2022 11:29:58	1
E:\INFO DE INTERÉS\Informe Resultados TFG, SA_2022 (1).docx	5DE33197	15/10/2022 11:44:47	15/10/2022 11:30:42	1
E:\INFO DE INTERÉS\Informe Resultados TFG, SA_2022.pdf	5DE33197	15/10/2022 11:44:47	15/10/2022 11:30:32	1
E:\INFO DE INTERÉS\Posicion competidores TFG SA.xlsx	5DE33197	14/10/2022 10:05:39	14/10/2022 9:22:18	1

Fuente: Elaboración Propia

En los siguientes resultados del artefacto *Windows Office Alerts* se demuestra que el usuario tuvo interacción con los ficheros en cuestión.

- Resultados artefacto forense ***Windows Office Alerts***.

Figura 188: Registros de actividad reciente del artefacto Windows Office Alerts

Created Date/Time - UTC+00:00 (dd/MM/yyyy)	Application Name	Message
08/10/2022 12:08:14	Microsoft Word	¿Desea guardar los cambios en "Política de uso equipos corporativos"?
08/10/2022 12:08:17	Microsoft Word	¿Quiere conservar el último elemento copiado?
14/10/2022 9:57:13	Microsoft Word	¿Desea guardar los cambios en "RESUMEN PRÓXIMOS PROYECTOS TFG SA"?
14/10/2022 10:00:47	Microsoft Excel	¿Desea guardar los cambios efectuados en 'Inventario activos TFG_SA 2022.xlsx'?
14/10/2022 10:10:35	Microsoft Excel	¿Desea guardar los cambios efectuados en 'Listado de Clientes TFG.xlsx'?
15/10/2022 11:46:11	Microsoft Excel	¿Desea guardar los cambios efectuados en 'Valoracion_TFG_SA.xlsx'?
15/10/2022 11:48:59	Microsoft Word	¿Desea guardar los cambios en "Informe Resultados TFG, SA_2022 (1)"?
15/10/2022 11:50:08	Microsoft Excel	¿Desea guardar los cambios efectuados en 'Valoracion_TFG_SA.xlsx'?
15/10/2022 11:51:07	Microsoft Word	¿Desea guardar los cambios en "Informe Resultados TFG, SA_2022 (1)"?
15/10/2022 11:54:04	Microsoft Excel	¿Desea guardar los cambios efectuados en 'Listado de Clientes TFG.xlsx'?
15/10/2022 11:54:25	Microsoft Excel	¿Desea guardar los cambios efectuados en 'Valoracion_TFG_SA.xlsx'?
15/10/2022 11:55:38	Microsoft Word	¿Desea guardar los cambios en "RESUMEN PRÓXIMOS PROYECTOS TFG SA"?
19/10/2022 14:45:17	Microsoft Word	¿Desea guardar los cambios en CV_DiegoMartin_TFGSA?
19/10/2022 14:46:20	Microsoft Word	¿Desea guardar los cambios en CV_JesusLopez_TFGSA?
19/10/2022 14:46:55	Microsoft Word	¿Desea guardar los cambios en CV_NereaGil_TFGSA?
19/10/2022 14:47:39	Microsoft Word	¿Desea guardar los cambios en "Informe Resultados TFG, SA_2022 (1)"?

Fuente: Elaboración Propia

- Una vez analizada la actividad reciente del usuario, se va a analizar los ficheros que elimina del dispositivo, con el objetivo de eliminar pruebas. Para ello se va a analizar el artefacto *$RecicleBin.*
- Resultados artefacto forense: *$RecicleBin*

Figura 189: Registros de borrado de información del artefacto $RecicleBin

File Name	Deleted Date/Time	Security Identifier	Original Path
INFO DE INTERÉS	19/10/2022 14:47:59	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS
CV_NereaGil_TFGSA.pdf	19/10/2022 14:48:55	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\CV_NereaGil_TFGSA.pdf
Posicion competidores TFG SA.xlsx	19/10/2022 14:40:51	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\Posicion competidores TFG SA.xlsx
RESUMEN PRÓXIMOS PROYECTOS TFG SA.docx	19/10/2022 14:49:37	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\RESUMEN PRÓXIMOS PROYECTOS TFG SA.docx
Posicion competidores TFG SA.xlsx	19/10/2022 14:49:35	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\Posicion competidores TFG SA.xlsx
Listado de Clientes TFG.xlsx	19/10/2022 14:49:23	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\Listado de Clientes TFG.xlsx
CV_JesusLopez_TFGSA.pdf	19/10/2022 14:48:46	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\CV_JesusLopez_TFGSA.pdf
CV_JesusLopez_TFGSA.docx	19/10/2022 14:48:43	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\CV_JesusLopez_TFGSA.docx
CV_DiegoMartin_TFGSA.docx	19/10/2022 14:48:38	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\CV_DiegoMartin_TFGSA.docx
RESUMEN PRÓXIMOS PROYECTOS TFG SA.pdf	19/10/2022 14:49:39	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\RESUMEN PRÓXIMOS PROYECTOS TFG SA.pdf
CV_NereaGil_TFGSA.docx	19/10/2022 14:48:50	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\CV_NereaGil_TFGSA.docx
Valoracion_TFG_SA.xlsx	19/10/2022 14:49:40	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\Valoracion_TFG_SA.xlsx
RESUMEN PRÓXIMOS PROYECTOS TFG SA.pdf	19/10/2022 14:41:06	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\RESUMEN PRÓXIMOS PROYECTOS TFG SA.pdf
Informe Resultados TFG, SA_2022.pdf	19/10/2022 14:49:20	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\Informe Resultados TFG, SA_2022.pdf
CV_DiegoMartin_TFGSA.pdf	19/10/2022 14:48:41	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\CV_DiegoMartin_TFGSA.pdf
Informe Resultados TFG, SA_2022 (1).docx	19/10/2022 14:49:09	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\Informe Resultados TFG, SA_2022 (1).docx
INFO DE INTERÉS	19/10/2022 14:49:49	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS
Inventario activos TFG_SA 2022.xlsx	19/10/2022 14:49:25	S-1-5-21-3338402279-1744945149-2327375240-1001	C:\Users\Daniel Rodriguez\Desktop\INFO DE INTERÉS\Inventario activos TFG_SA 2022.xlsx

Fuente: Elaboración Propia

- Por último, se van a analizar los dispositivos externos conectados con su número de serie y la fecha en el que se conectan para poder trazar la actividad analizada anteriormente en la sección de actividad reciente del usuario. Para ello, se van a analizar los artefactos *USB devices* y *Windows Event Logs - Storage Device Events.*
- Resultados artefacto ***Windows Event Logs - Storage Device Events***.

Figura 190: Registros de conexiones externas del artefacto Storage Device Events

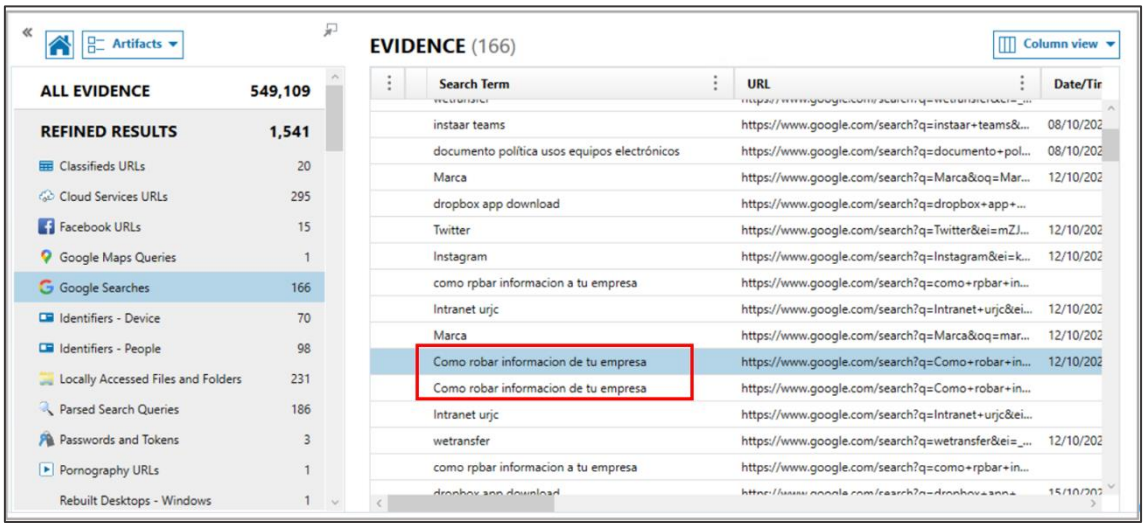
Created Date/Time	Event Description Summary	Action	Manufacturer	Model	Serial Number
14/10/2022 10:01:07	Storage Device Seagate BUP Slim Connected.	Connected	Seagate	BUP Slim	00000000NAB56A85
14/10/2022 10:59:27	Storage Device Seagate BUP Slim Disconnected.	Disconnected	Seagate	BUP Slim	00000000NAB56A85
15/10/2022 11:41:06	Storage Device Seagate BUP Slim Connected.	Connected	Seagate	BUP Slim	00000000NAB56A85
19/10/2022 14:35:13	Storage Device Seagate BUP Slim Disconnected.	Disconnected	Seagate	BUP Slim	00000000NAB56A85

Fuente: Elaboración Propia

2. Análisis del ordenador portátil asignado al custodio Iván Merino

- En la sección de navegación web del portátil corporativo asociado al usuario Iván Merino, se han encontrado los siguientes hallazgos:
- ***Google Searches*:** Búsquedas en la barra de búsqueda de *Google.*

Figura 191: Búsquedas de Google



Fuente: Elaboración Propia (Magnet Axiom)

- Resultados artefacto ***Edge_Internet Explorer 10-11 Main History***.

Figura 192: Historial de navegación en navegador Edge

URL	User	Accessed Date/Time
file:///C:/Users/Iván Merino Mesa/Desktop/FiscalYear-22/DOCUMENTOS IMPORTANTES	Iván Merino Mesa	15/10/2022 11:46:40
file:///C:/Users/Iván Merino Mesa/OneDrive/Introducción a OneDrive.pdf	Iván Merino Mesa	15/10/2022 11:47:38
file:///C:/Users/Iván Merino Mesa/OneDrive/DOCUMENTOS IMPORTANTES/CV_DiegoMartin_TFGSA.docx	Iván Merino Mesa	15/10/2022 11:48:20
file:///C:/Users/Iván Merino Mesa/OneDrive/DOCUMENTOS IMPORTANTES/CV_DiegoMartin_TFGSA.pdf	Iván Merino Mesa	15/10/2022 11:49:48
file:///C:/Users/Iván Merino Mesa/OneDrive/DOCUMENTOS IMPORTANTES/CV_JesusLopez_TFGSA.docx	Iván Merino Mesa	15/10/2022 11:51:52
file:///C:/Users/Iván Merino Mesa/OneDrive/DOCUMENTOS IMPORTANTES/CV_NereaGil_TFGSA.docx	Iván Merino Mesa	15/10/2022 11:51:57
file:///C:/Users/Iván Merino Mesa/OneDrive/DOCUMENTOS IMPORTANTES/Informe Resultados TFG, SA_2022.docx	Iván Merino Mesa	15/10/2022 11:52:00
file:///C:/Users/Iván Merino Mesa/OneDrive/DOCUMENTOS IMPORTANTES/Inventario activos TFG_SA 2022.xlsx	Iván Merino Mesa	15/10/2022 11:52:01
file:///C:/Users/Iván Merino Mesa/OneDrive/DOCUMENTOS IMPORT芟J伸デ	Iván Merino Mesa	15/10/2022 11:52:02
file:///C:/Users/Iván Merino Mesa/OneDrive/DOCUMENTOS IMPORTANTES/RESUMEN PRÓXIMOS PROYECTOS TFG SA.docx	Iván Merino Mesa	15/10/2022 11:52:03
file:///C:/Users/Iván Merino Mesa/Downloads/Posicion competidores TFG SA.xlsx	Iván Merino Mesa	15/10/2022 11:25:12
file:///C:/Users/Iván Merino Mesa/Downloads/RESUMEN PRÓXIMOS PROYECTOS TFG SA.pdf	Iván Merino Mesa	15/10/2022 11:25:33
file:///C:/Users/Iván Merino Mesa/Downloads/RESUMEN PRÓXIMOS PROYECTOS TFG SA.docx	Iván Merino Mesa	15/10/2022 11:25:45
file:///C:/Users/Iván Merino Mesa/Downloads	Iván Merino Mesa	15/10/2022 11:26:39
file:///C:/Users/Iván Merino Mesa/Downloads/Inventario activos TFG_SA 2022.xlsx	Iván Merino Mesa	15/10/2022 11:31:14
file:///C:/Users/Iván Merino Mesa/Downloads/CV_JesusLopez_TFGSA.docx	Iván Merino Mesa	15/10/2022 11:32:07
file:///C:/Users/Iván Merino Mesa/Downloads/CV_DiegoMartin_TFGSA.docx	Iván Merino Mesa	15/10/2022 11:32:11
file:///C:/Users/Iván Merino Mesa/Downloads/CV_NereaGil_TFGSA.docx	Iván Merino Mesa	15/10/2022 11:32:16
file:///C:/Users/Iván Merino Mesa/Downloads/CV_DiegoMartin_TFGSA.pdf	Iván Merino Mesa	15/10/2022 11:32:18
file:///C:/Users/Iván Merino Mesa/Downloads/Informe Resultados TFG, SA_2022.docx	Iván Merino Mesa	15/10/2022 11:32:19
file:///C:/Users/Iván Merino Mesa/Downloads/CV_JesusLopez_TFGSA.pdf	Iván Merino Mesa	15/10/2022 11:32:20
file:///C:/Users/Iván Merino Mesa/Downloads/CV_NereaGil_TFGSA.pdf	Iván Merino Mesa	15/10/2022 11:32:20
file:///C:/Users/Iván Merino Mesa/Downloads/Informe Resultados TFG, SA_2022.pdf	Iván Merino Mesa	15/10/2022 11:32:21

Fuente: Elaboración Propia

En lo que respecta a la actividad reciente del usuario se han encontrado las siguientes hallazgos:

- Resultados artefacto ***Jumplist***

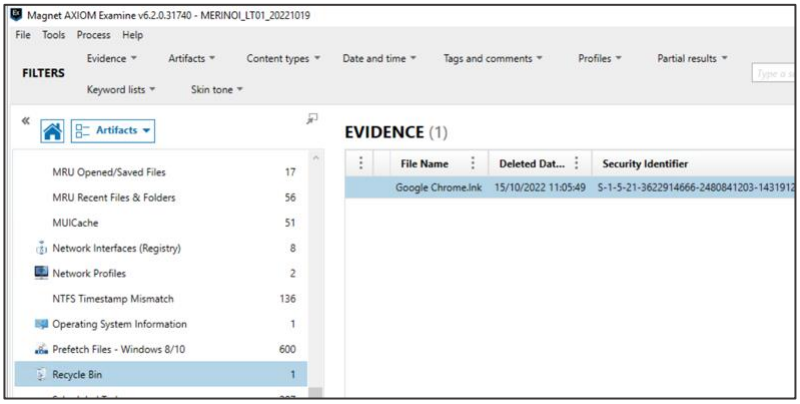
Figura 193: Registros de actividad reciente del artefacto Jumplist

Linked Path	Volume Serial Number	Target File Created D	Target File Last Mod
C:\Users\Iván Merino Mesa\OneDrive\DOCUMENTOS IMPORTANTES\RESUMEN PRÓXIMOS PROYECTOS TFG SA.docx	94D2CE7A	15/10/2022 11:48:11	12/10/2022 11:34:06
C:\Users\Iván Merino Mesa\OneDrive\Introducción a OneDrive.pdf	94D2CE7A	12/10/2022 10:17:44	08/10/2022 10:54:23
C:\Users\Iván Merino Mesa\OneDrive\DOCUMENTOS IMPORTANTES\Posicion competidores TFG SA.xlsx	94D2CE7A	15/10/2022 11:48:11	12/10/2022 12:16:34
C:\Users\Iván Merino Mesa\OneDrive\DOCUMENTOS IMPORTANTES\Inventario activos TFG_SA 2022.xlsx	94D2CE7A	15/10/2022 11:48:11	12/10/2022 11:09:24
C:\Users\Iván Merino Mesa\OneDrive\DOCUMENTOS IMPORTANTES\Informe Resultados TFG, SA_2022.docx	94D2CE7A	15/10/2022 11:48:10	12/10/2022 10:31:27
C:\Users\Iván Merino Mesa\OneDrive\DOCUMENTOS IMPORTANTES\CV_NereaGil_TFGSA.docx	94D2CE7A	15/10/2022 11:48:10	12/10/2022 10:49:30
C:\Users\Iván Merino Mesa\OneDrive\DOCUMENTOS IMPORTANTES\CV_JesusLopez_TFGSA.docx	94D2CE7A	15/10/2022 11:48:10	12/10/2022 10:49:30
C:\Users\Iván Merino Mesa\OneDrive\DOCUMENTOS IMPORTANTES\CV_DiegoMartin_TFGSA.pdf	94D2CE7A	15/10/2022 11:48:10	12/10/2022 10:49:30
C:\Users\Iván Merino Mesa\OneDrive\DOCUMENTOS IMPORTANTES\CV_DiegoMartin_TFGSA.docx	94D2CE7A	15/10/2022 11:48:09	12/10/2022 10:49:30
C:\Users\Iván Merino Mesa\OneDrive\Introducción a OneDrive.pdf	94D2CE7A	12/10/2022 10:17:44	08/10/2022 10:54:23
C:\Users\Iván Merino Mesa\AppData\Roaming\Microsoft\Templates\Normal.dotm	94D2CE7A	08/10/2022 11:19:13	15/10/2022 11:38:56
C:\Users\Iván Merino Mesa\Downloads\CV_JesusLopez_TFGSA.docx	94D2CE7A	12/10/2022 10:41:47	12/10/2022 10:49:30
C:\Users\Iván Merino Mesa\Downloads\CV_NereaGil_TFGSA.docx	94D2CE7A	12/10/2022 10:46:22	12/10/2022 10:49:30
C:\Users\Iván Merino Mesa\Downloads\Informe Resultados TFG, SA_2022.docx	94D2CE7A	12/10/2022 10:30:00	12/10/2022 10:31:27
C:\Users\Iván Merino Mesa\Downloads\CV_DiegoMartin_TFGSA.docx	94D2CE7A	12/10/2022 10:44:27	12/10/2022 10:49:30
C:\Users\Iván Merino Mesa\Downloads\RESUMEN PRÓXIMOS PROYECTOS TFG SA.docx	94D2CE7A	12/10/2022 11:33:00	12/10/2022 11:34:06
C:\Users\Iván Merino Mesa\Downloads\Inventario activos TFG_SA 2022.xlsx	94D2CE7A	12/10/2022 11:08:00	12/10/2022 11:09:24
C:\Users\Iván Merino Mesa\Downloads\Posicion competidores TFG SA.xlsx	94D2CE7A	12/10/2022 12:03:44	12/10/2022 12:16:34
C:\Users\Iván Merino Mesa\Downloads\Informe Resultados TFG, SA_2022.pdf	94D2CE7A	12/10/2022 10:30:00	12/10/2022 10:31:27
C:\Users\Iván Merino Mesa\Downloads\CV_NereaGil_TFGSA.pdf	94D2CE7A	12/10/2022 10:46:30	12/10/2022 10:49:30
C:\Users\Iván Merino Mesa\Downloads\CV_JesusLopez_TFGSA.pdf	94D2CE7A	12/10/2022 10:41:58	12/10/2022 10:49:30
C:\Users\Iván Merino Mesa\Downloads\CV_DiegoMartin_TFGSA.pdf	94D2CE7A	12/10/2022 10:44:34	12/10/2022 10:49:30
C:\Users\Iván Merino Mesa\Downloads\RESUMEN PRÓXIMOS PROYECTOS TFG SA.pdf	94D2CE7A	12/10/2022 11:33:00	12/10/2022 11:34:06
C:\Users\Iván Merino Mesa\Desktop\FiscalYear-22\IT\Política de uso equipos corporativos.docx	94D2CE7A	08/10/2022 11:35:26	08/10/2022 11:35:33
C:\Users\Iván Merino Mesa\Desktop\FiscalYear-22\Reuniones\ACTA DE LA REUNION -20221008.docx	94D2CE7A	08/10/2022 11:18:42	08/10/2022 11:18:45
C:\Users\Iván Merino Mesa\Downloads\Nuevo Logo TFG_SA.png	94D2CE7A	08/10/2022 10:57:08	08/10/2022 11:05:40
C:\Users\Iván Merino Mesa\OneDrive\DOCUMENTOS IMPORTANTES\CV_DiegoMartin_TFGSA.pdf	94D2CE7A	15/10/2022 11:48:10	12/10/2022 10:49:30
C:\Users\Iván Merino Mesa\OneDrive\Introducción a OneDrive.pdf	94D2CE7A	12/10/2022 10:17:44	08/10/2022 10:54:23
C:\Users\Iván Merino Mesa\Downloads\Informe Resultados TFG, SA_2022.pdf	94D2CE7A	12/10/2022 10:30:00	12/10/2022 10:31:27
C:\Users\Iván Merino Mesa\Downloads\CV_NereaGil_TFGSA.pdf	94D2CE7A	12/10/2022 10:46:30	12/10/2022 10:49:30
C:\Users\Iván Merino Mesa\Downloads\CV_JesusLopez_TFGSA.pdf	94D2CE7A	12/10/2022 10:41:58	12/10/2022 10:49:30
C:\Users\Iván Merino Mesa\Downloads\CV_DiegoMartin_TFGSA.pdf	94D2CE7A	12/10/2022 10:44:34	12/10/2022 10:49:30
C:\Users\Iván Merino Mesa\Downloads\RESUMEN PRÓXIMOS PROYECTOS TFG SA.pdf	94D2CE7A	12/10/2022 11:33:00	12/10/2022 11:34:06

Fuente: Elaboración Propia

- En lo que concierne a la papelera de reciclaje solo se ha encontrado un registro. Esto es debido a que posiblemente haya utilizado la técnica Ctlr + Supr, no enviando así los ficheros a la papelera de reciclaje.

Figura 194: Registros de borrado de información del artefacto $RecicleBin



Fuente: Elaboración Propia

- En lo que se refiere a la conexión de dispositivos externos no se han encontrado grandes hallazgos, solo esta conexión, pero sin actividad relevante en ese día concreto.
- Resultados artefacto ***Windows Event Logs - Storage Device Events***

Figura 195: Registros de conexiones externas del artefacto Storage Device Events

Created Date/Time -	Event Description Summary	Action	Manufacturer	Model	Serial Number
06/10/2022 16:46:19	Storage Device SanDisk Extreme Pro Connected.	Connected	SanDisk	Extreme Pro	00000000000000000000
06/10/2022 17:06:58	Storage Device SanDisk Extreme Pro Connected.	Connected	SanDisk	Extreme Pro	00000000000000000000

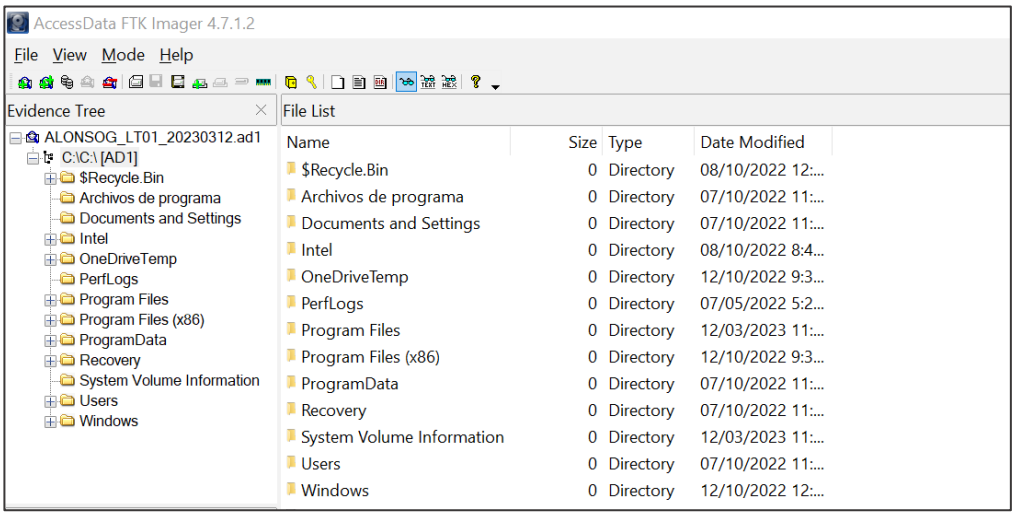
Fuente: Elaboración Propia

Para mayor detalle, ver en el siguiente enlace, los reportes de los artefactos forenses: PRUEBAS ORDENADOR IVAN

Sin embargo, en este custodio se han encontrado correos electrónicos relevantes que se analizarán más adelante.

3. Análisis del ordenador portátil al custodio Gema Alonso
   - En este apartado se va a analizar el resultado de la adquisición en vivo del portátil asignado al custodio Gema Alonso Bote. Para ello se va a utilizar la herramienta *FTK Imager*, donde se va a abrir el fichero *.ad1* resultante de la adquisición y que se muestra a continuación:

Figura 196: Evidencia sujeto de análisis con la herramienta FTK Imager

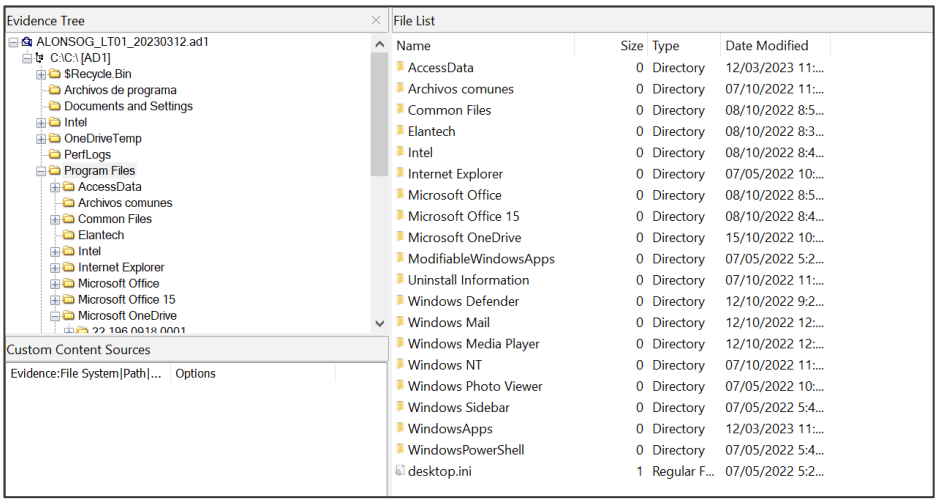


Fuente: Elaboración Propia

   - Como se puede observar, se encuentran las carpetas de la unidad C del portátil y en las que a continuación se va a analizar teniendo en cuenta la investigación, aquellas consideradas más relevantes:
   -

1) Análisis de las aplicaciones instaladas del dispositivo, en busca de posible herramienta de borrado profesional o masivo.

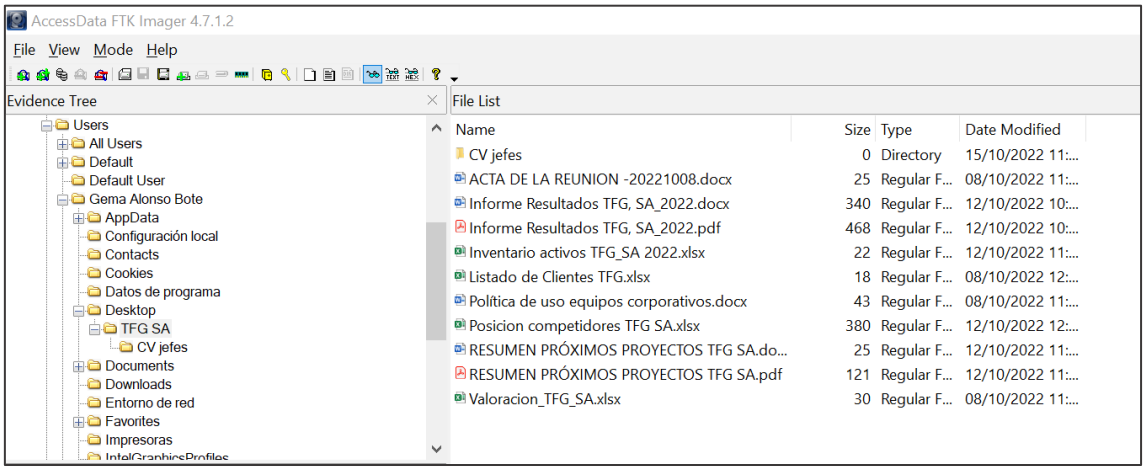
Figura 197: Aplicaciones instaladas



Fuente: Elaboración Propia

2) Análisis de la información contenida en el usuario asignado al custodio: Gema Alonso Bote.

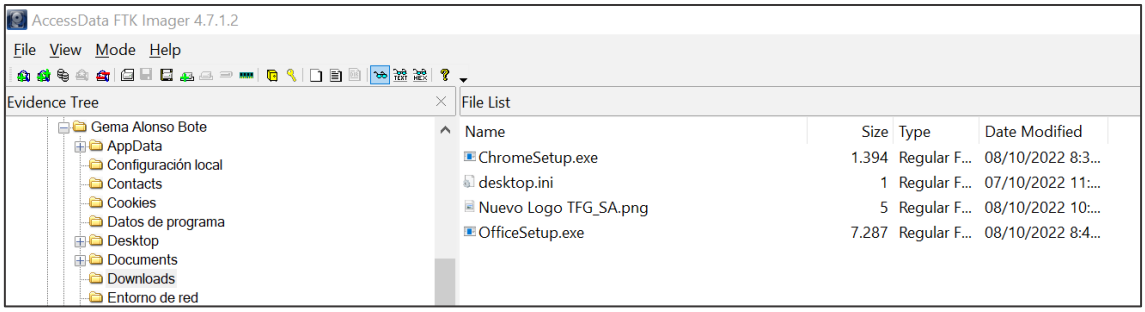
Figura 198: Información contenida en el usuario del custodio



Fuente: Elaboración Propia

3) Análisis de las descargas realizadas con el usuario asignado al custodio: Gema Alonso Bote:

Figura 199: Análisis de las Descargas realizadas



Fuente: Elaboración Propia

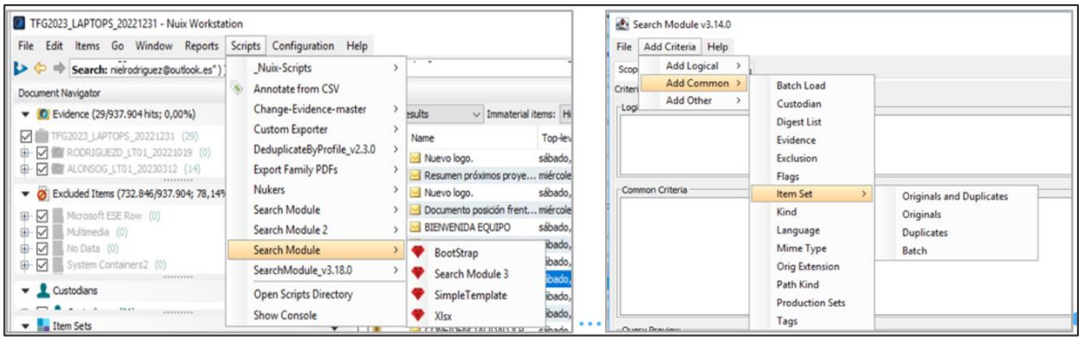
4. Análisis de comunicaciones electrónicas entre los tres custodios.

- En el siguiente apartado se va a analizar las comunicaciones mantenidas entre los tres custodios por medio de correo electrónico, *WhatsApp* etcétera. Primero de todo se van a analizar las comunicaciones vía email, donde el análisis se ha desarrollado con la herramienta forense *Nuix Forensic* y se ha procedido a realizar las siguientes acciones:

1) Lanzar en *Nuix* las palabras clave mencionadas anteriormente tal y como se muestra en las imágenes:

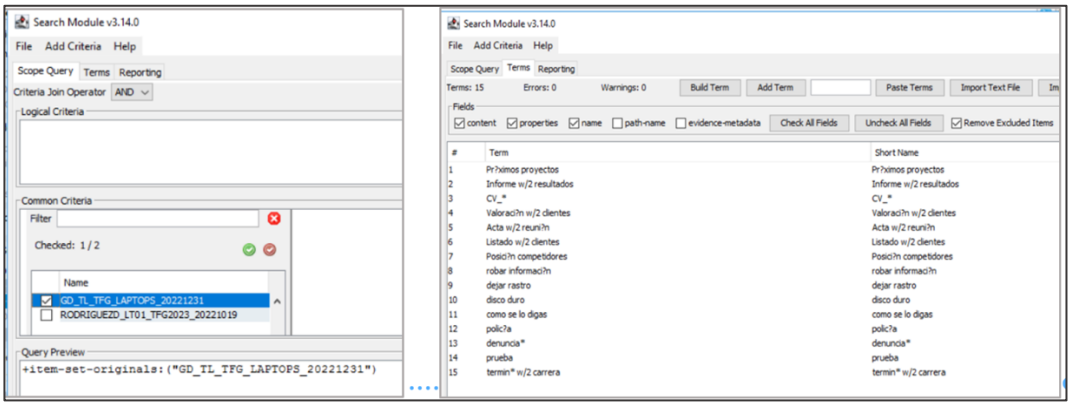
Se utiliza el script definido en *Nuix* denominado *"Search module 3*"

Figura 200: Lanzamiento palabras clave en Nuix (I)



Fuente: Elaboración Propia

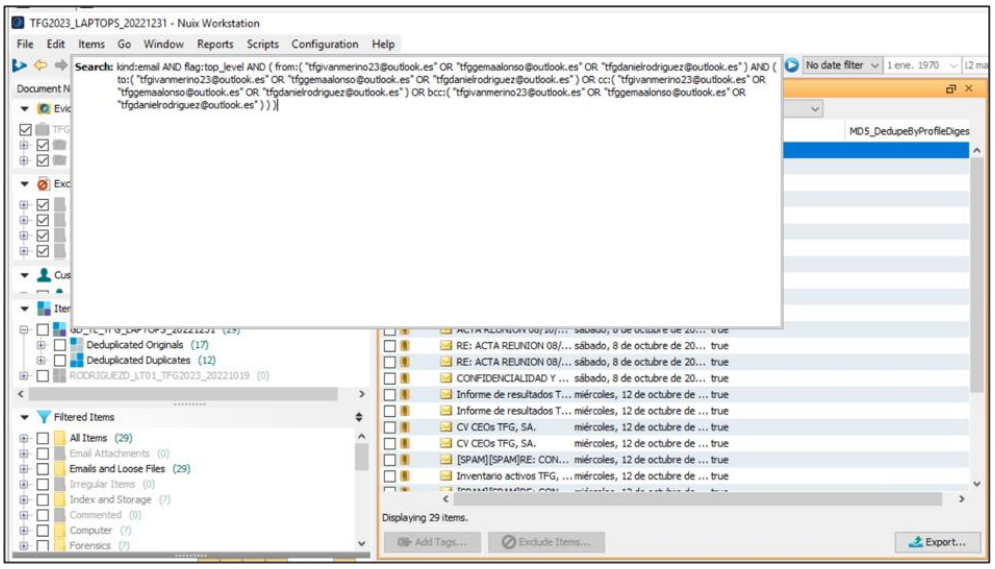
Figura 201: Lanzamiento palabras clave en Nuix (II)



Fuente: Elaboración Propia

2) Desarrollando una consulta en *Nuix Forensic* que devuelva la población de comunicaciones directas por email entre los tres custodios, tal y como se observa en la imagen:

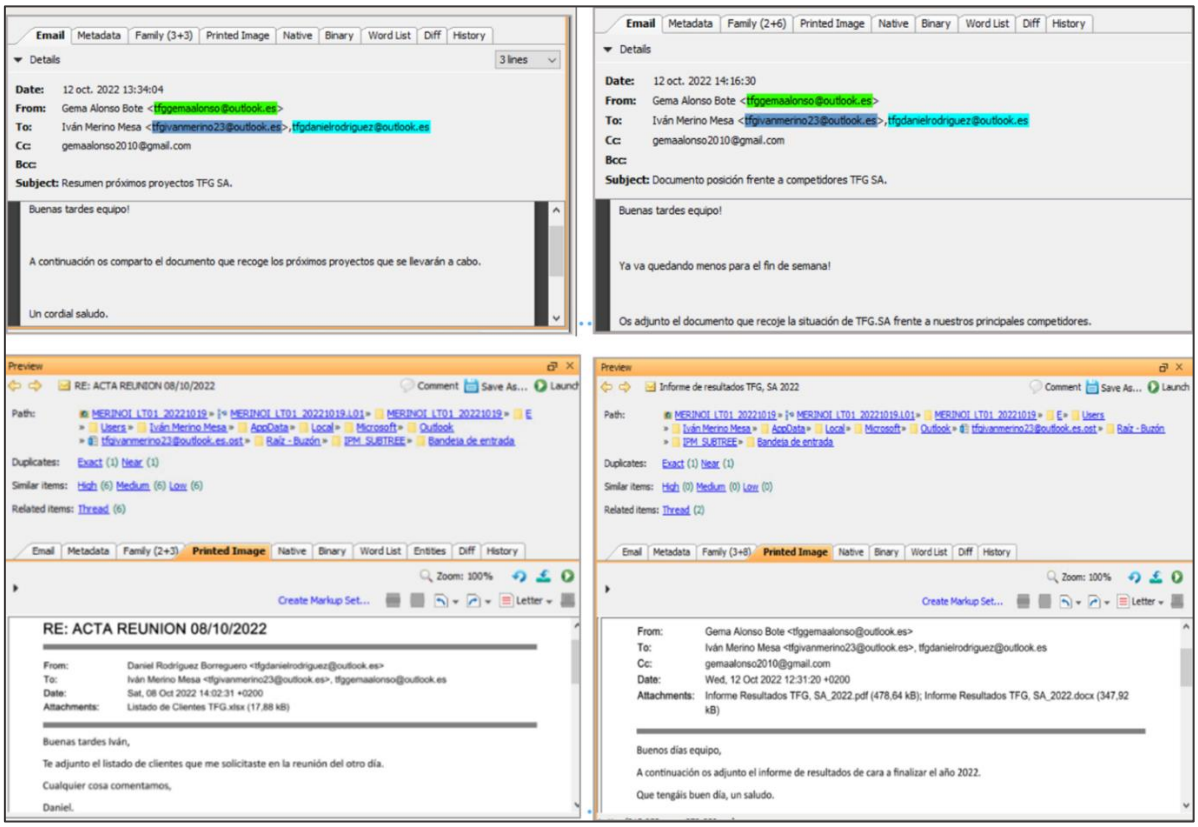
Figura 202: Consulta de análisis de comunicaciones



Fuente: Elaboración Propia

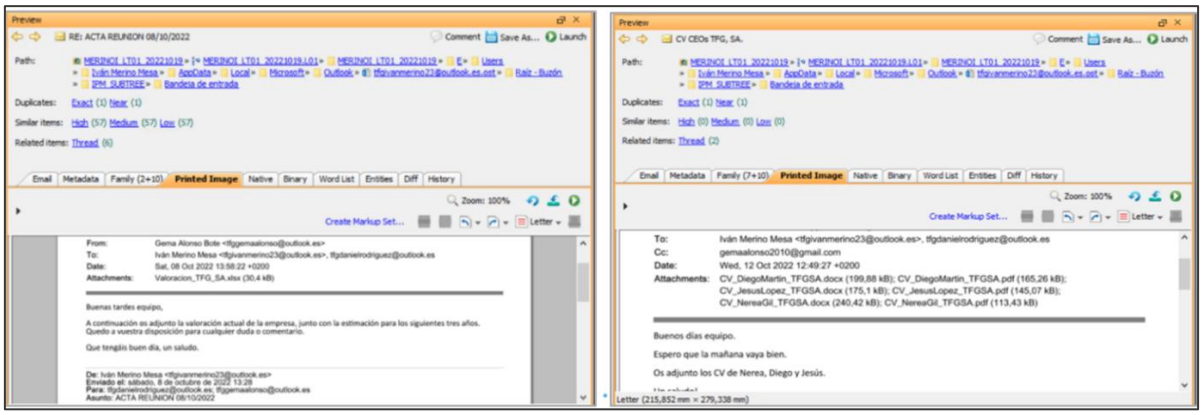
- La sentencia más diferente que se observa es la de *"flag:top_level"*. Esto quiere decir, que se busque en los emails en los que su categorización sea elementos principales, eliminando así adjuntos y otros documentos, distintos al hilo referido.
- Esto devuelve las siguientes conversaciones que se adjuntan a continuación en las siguientes imágenes:

Figura 203: Listado de emails (I)



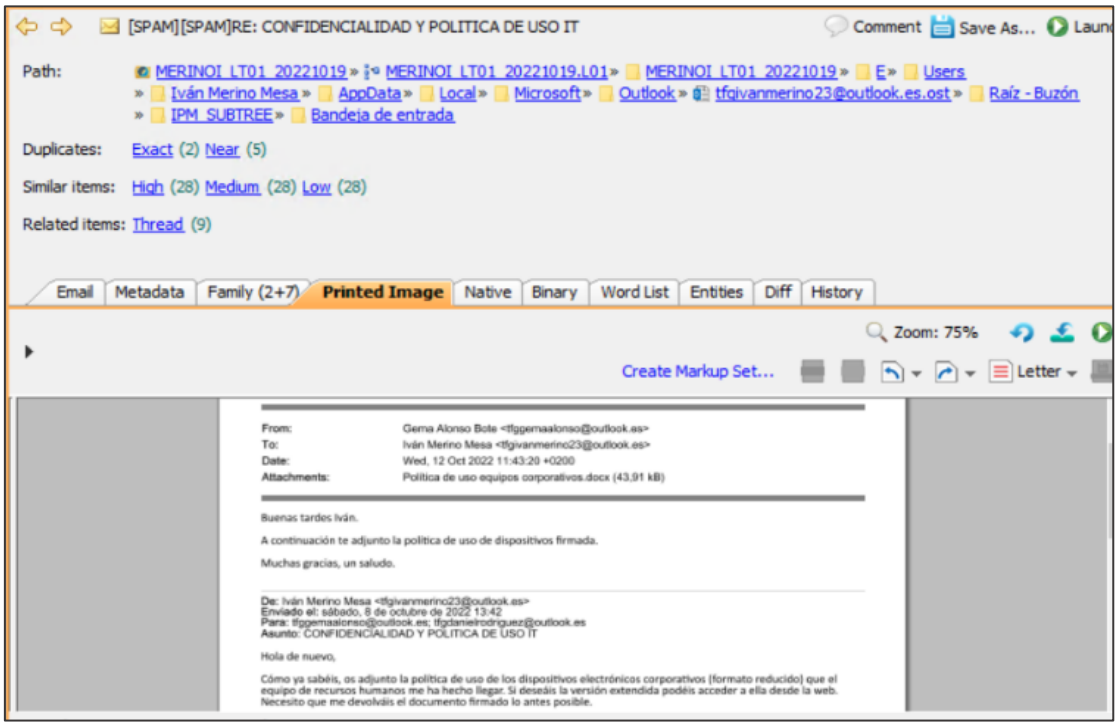
Fuente: Elaboración Propia

Figura 204: Listado de emails (II)



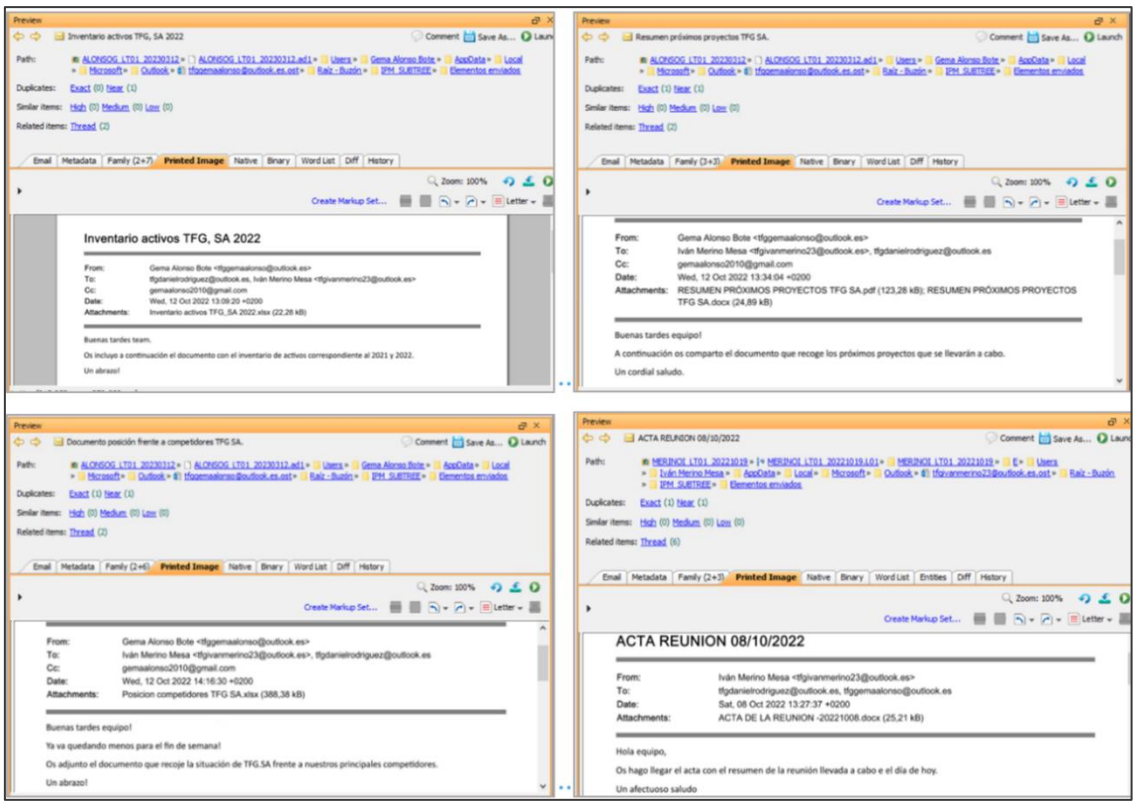
Fuente: Elaboración Propia

Figura 205: Listado de emails (III)



Fuente: Elaboración Propia

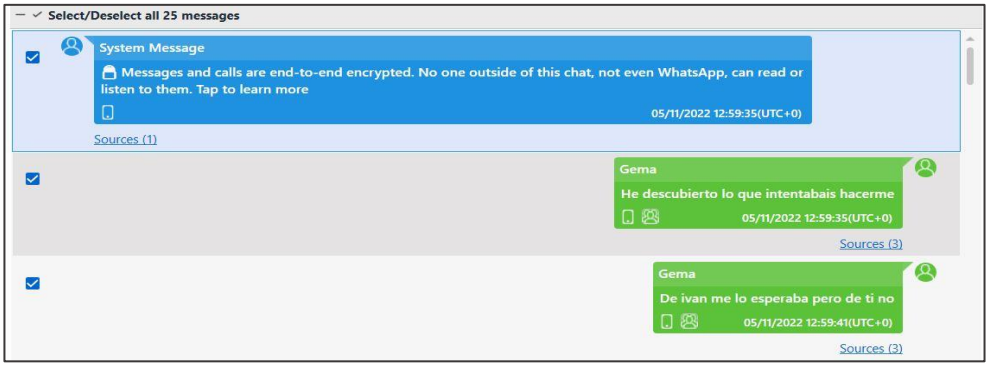
Figura 206: Listado de emails (IV)



Fuente: Elaboración Propia

5. Análisis de los dispositivos móviles corporativos de los custodios Gema Alonso y Daniel Rodríguez.
    - Después del procesamiento de los dispositivos móviles de los custodios por medio de la herramienta *Cellebrite UFED*, en esta sección se va a analizar el contenido de dichas evidencias, por medio de la herramienta *Cellebrite Physical Analyzer*.
    - A continuación, se van a adjuntar varias imágenes, numeradas del I al IV, según el orden de mensajes, donde se muestra la conversación a través de *WhatsApp*, que ha dado resultado después de aplicar la lista de palabras clave a las evidencias. Esta conversación se produce entre los custodios Gema Alonso y Daniel Rodríguez.

Figura 207: Conversación WhatsApp (I)



Fuente: Elaboración Propia

Figura 208: Conversación de WhatsApp (II)

Fuente: Elaboración Propia

Figura 209: Conversación de WhatsApp (III)

Fuente: Elaboración Propia

Figura 210: Conversación de WhatsApp (IV)

Fuente: Elaboración Propia

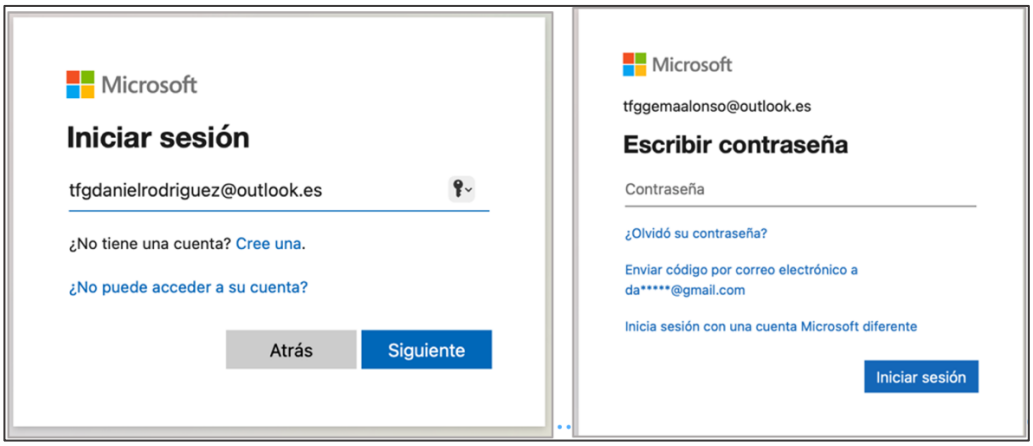
6. Procedimiento de extracción y análisis de las conversaciones de Teams de los custodios.

Para lograr la extracción de las conversaciones de *Microsoft Teams* de los custodios, se han seguido las indicaciones de *Microsoft*, en las que indica que se debe ir a la opción de privacidad de la cuenta de cada usuario: https://support.microsoft.com/es-es/office/exportar-o-eliminar-los-datos-en-microsoft-teams-gratis-1ed6ac68-5fb4-41be-9861-1a4127fecf68 y seguir el procedimiento.

A continuación, se va a mostrar el procedimiento que se ha realizado para uno de los custodios y que se replicará para cada uno de ellos.

1) Se accede a la cuenta de cada usuario utilizando las credenciales de su cuenta de correo de Outlook corporativa.

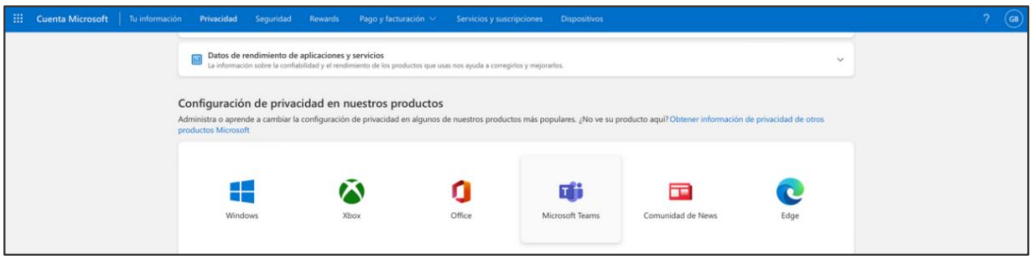
Figura 211: Paso I adquisición de Microsoft Teams



Fuente: Elaboración Propia

2) Una vez se ha accedido a la cuenta del usuario, se clica en el botón de privacidad y se busca la herramienta *Microsoft Teams*.

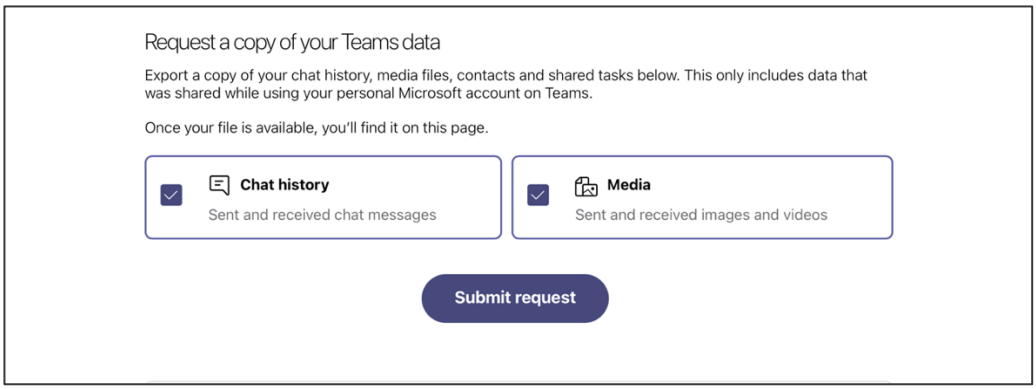
Figura 212: Paso II adquisición de Microsoft Teams



Fuente: Elaboración Propia

3) Una vez clicado, nos aparece la ventana siguiente en el que se selecciona que se desea exportar. Por tanto, se selecciona tanto el historial de chats como el contenido de media que pudieran tener,

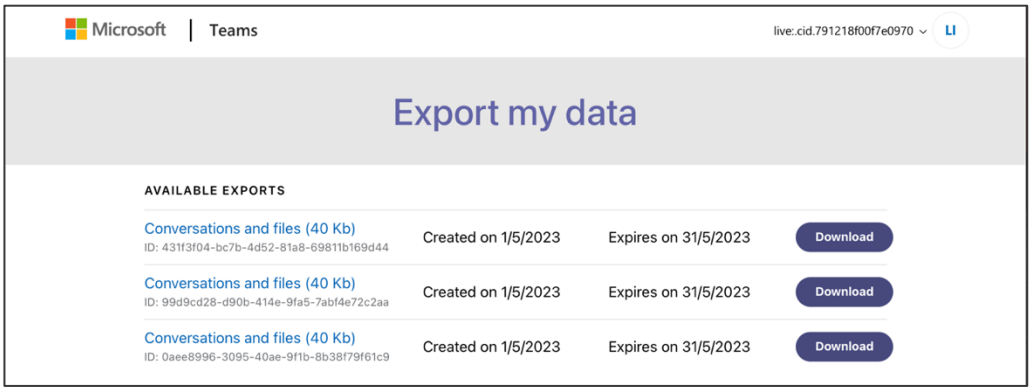
Figura 213: Paso III adquisición de Microsoft Teams



Fuente: Elaboración Propia

4) Por último, una vez se tienen las 3 conversaciones y ficheros asociados a los 3 custodios, se procede a su descarga.

Figura 214: Paso IV adquisición de Microsoft Teams



Fuente: Elaboración Propia

Una vez finalizado el proceso de extracción, ha generado unos archivos *".tar"*, los cuales se han procesado con la herramienta *Nuix Forensic* siguiendo el procedimiento de procesamiento explicado en la anterior sección y se ha renombrado, siguiendo las mejores prácticas a cada evidencia como: MERINOI_TEAMS_230501, ALONSOG_TEAMS_20230501 Y RODRIGUEZD_TEAMS_20230501.

A continuación de la fase de procesamiento, se han extraído los ficheros que contienen los mensajes de *Microsoft Teams* de cada uno de los custodios, estos son ficheros tipo *".json"* y se ha procedido a su análisis importándolo con Excel y acoplando bien el formato con *PowerQuery*.

Tras realizar el análisis de las conversaciones que aparecen en la herramienta Microsoft Teams de los 3 custodios, se procede a desglosar los hallazgos más importantes en las siguientes imágenes:

1) Conversación entre el custodio Iván Merino y Daniel Rodríguez

Figura 215: Conversación de Microsoft Teams (I)

Conversacion IMM con DRB.displayName	Conversacion IMM con DRB.originalarrivaltime	Conversacion IMM con DRB.content
	2022-10-08T10:43:48.729Z	<addmember><eventtime>1665225828729</eventtime><initiator>8:live:.cid.791218f00f7e0970</initiator><rosterVersion
Iván Merino Mesa	2022-10-08T10:43:49.322Z	Hola Dani, Bienvenido a este apasionante proyecto !
	2022-10-08T10:43:53.858Z	
Iván Merino Mesa	2022-10-08T10:44:19.055Z	Estoy seguro que este proyecto nos depara muchas cosas grandes
Iván Merino Mesa	2022-10-08T10:44:53.345Z	Tendré una llamada privada contigo, y te contaré unas ideas que tengo, creo que nos vamos a forrar jeje
Daniel Rodríguez Borreguero	2022-10-08T10:46:02.246Z	Buenos días Iván
Daniel Rodríguez Borreguero	2022-10-08T10:46:11.405Z	Perfecto, estoy deseando conocer los detalles
Iván Merino Mesa	2022-10-08T10:46:40.1Z	Tienes que prometer no contar nada ...
Daniel Rodríguez Borreguero	2022-10-08T10:47:07.163Z	Te lo prometo
Daniel Rodríguez Borreguero	2022-10-08T10:47:11.991Z	tenemos que llevar cuidado
Iván Merino Mesa	2022-10-08T10:49:57.284Z	Sobre todo es muy importante que esa tal Gema no se entere de nada ...
Iván Merino Mesa	2022-10-08T10:50:01.224Z	Confío en ti !
Iván Merino Mesa	2022-10-08T10:50:08.483Z	Por los viejos tiempos !
Daniel Rodríguez Borreguero	2022-10-08T10:51:51.82Z	Tenemos que vigilarla y tener cuidado con ella para que no sospeche
Iván Merino Mesa	2022-10-12T09:54:52.084Z	Hola Dani, ya sé como hacer para llevarnos los documentos que nos ha pedido la competencia
Iván Merino Mesa	2022-10-12T09:56:05.989Z	Voy a decir a Gema que cree los documentos que necesitamos y se los envíe a su cuenta personal
Iván Merino Mesa	2022-10-12T09:56:24.281Z	Así si nos pillan en algún momento, diremos que los documentos se los pasó Gema a su correo
Iván Merino Mesa	2022-10-12T09:56:27.064Z	Que te parece ?
Daniel Rodríguez Borreguero	2022-10-12T09:56:51.661Z	Perfecto eso es
Daniel Rodríguez Borreguero	2022-10-12T09:57:03.618Z	se la puede acusar de fuga de info a su cuenta de correo personal
Iván Merino Mesa	2022-10-12T09:57:22.546Z	Sabes donde podemos copiar
Iván Merino Mesa	2022-10-12T09:57:27.568Z	Toda esta información ?
Iván Merino Mesa	2022-10-12T09:57:37.733Z	Yo creo que me lo subiré a mi carpeta de WeTRansfer
Iván Merino Mesa	2022-10-12T09:57:44.301Z	Tu tienes forma de obtenerlo ?
Daniel Rodríguez Borreguero	2022-10-12T09:57:44.423Z	tengo una idea
Daniel Rodríguez Borreguero	2022-10-12T09:57:58.625Z	creo que tengo un disco duro externo que no está registrado en la empresa
Iván Merino Mesa	2022-10-12T09:58:14.829Z	Eso será genial
Iván Merino Mesa	2022-10-12T09:58:28.564Z	Seguro que si no está inventariado
Iván Merino Mesa	2022-10-12T09:58:35.8Z	No lo pueden registrar de ninguna forma
Daniel Rodríguez Borreguero	2022-10-12T09:58:42.446Z	podemos usarlo para llevarnos los archivos
Daniel Rodríguez Borreguero	2022-10-12T09:59:42.622Z	eso es
Daniel Rodríguez Borreguero	2022-10-12T09:59:58.286Z	perfecto pues lo hacemos así
Iván Merino Mesa	2022-10-15T12:15:50.762Z	Hola Dani !
Iván Merino Mesa	2022-10-15T12:16:59.034Z	Ya tengo todos los documentos en OneDrive
Iván Merino Mesa	2022-10-15T12:17:22.439Z	<img itemscope="" itemtype="http
Daniel Rodríguez Borreguero	2022-10-15T12:17:35.943Z	Buenas Iván!
Daniel Rodríguez Borreguero	2022-10-15T12:17:37.438Z	perfecto
Daniel Rodríguez Borreguero	2022-10-15T12:17:46.107Z	yo ya tengo todos los documentos en el disco duro
Daniel Rodríguez Borreguero	2022-10-15T12:17:56.881Z	el plan sigue adelante! <img itemscope="" itemtyp
Iván Merino Mesa	2022-10-15T12:23:07.102Z	Genial tio ! Con todo !!

Fuente: Elaboración Propia

2) Conversación grupal entre los tres custodios por medio de un chat denominado *"Chat Future"*.

Figura 216: Conversación de Microsoft Teams (II)

Conversacion PROYECTO FUTURE.displayName	Conversacion PROYECTO FUTURE.originalarrivaltime	Conversacion PROYECTO FUTURE.content
	2022-10-08T11:58:13.12Z	<addmember><eventtime>1665230293120</eventtime><initiator>8:live:.cid.791218f00f7e0970</initiator><rosterVersion>1665230292983</rosterVersion><target>8:live:.cid.79
	2022-10-08T11:58:13.189Z	<topicupdate><eventtime>1665230293189</eventtime><initiator>8:live:.cid.791218f00f7e0970</initiator><value>CHAT PROYECTO FUTURE</value></topicupdate>
	2022-10-08T11:58:13.318Z	<joiningenabledupdate><eventtime>1665230293318</eventtime><initiator>8:live:.cid.791218f00f7e0970</initiator><value>True</value></joiningenabledupdate>
Iván Merino Mesa	2022-10-08T11:58:14.855Z	Hola equipo, cree un grupo para poder conversar los tres
Iván Merino Mesa	2022-10-08T11:58:32.948Z	Voy a cerrar ya que tengo comida, recordad pasarme lo que os pedí
Daniel Rodríguez Borreguero	2022-10-08T11:58:41.145Z	Un saludo, hablamos estos días !
Gema Alonso Bote	2022-10-08T12:01:00.46Z	Hola Iván!
Gema Alonso Bote	2022-10-08T12:01:09.553Z	Estupendo te lo acabo de enviar
Gema Alonso Bote	2022-10-08T12:01:17.85Z	Que tengáis buen día
Iván Merino Mesa	2022-10-12T10:02:47.896Z	Hola equipo
Iván Merino Mesa	2022-10-12T10:02:50.974Z	Que tal estáis ?
Iván Merino Mesa	2022-10-12T10:03:09.684Z	Cómo bien sabéis el tiempo que tenemos para la realización del proyecto es bastante escaso
Iván Merino Mesa	2022-10-12T10:03:18.14Z	Gema, Daniel ahora mismo está muy liado
Iván Merino Mesa	2022-10-12T10:03:22.808Z	Necesito que me eches una mano
Iván Merino Mesa	2022-10-12T10:03:38.107Z	Necesito que me realices los siguientes documentos
Iván Merino Mesa	2022-10-12T10:07:10.582Z	- Resumen de siguientes proyectos de la empresa - Cuadro de posición frente a competidores - Inventario de activos de la er
Iván Merino Mesa	2022-10-12T10:07:25.229Z	Cuando me lo pases, pon en copia tu correo electrónico personal
Iván Merino Mesa	2022-10-12T10:07:35.75Z	Que quiero mandarte una cosa posteriormente
Iván Merino Mesa	2022-10-12T10:07:38.753Z	Gracias !
Gema Alonso Bote	2022-10-12T10:07:47.98Z	<blockquote itemscope="" itemtype="http://schema.skype.com/Reply" itemid="1665569018107">Iván Merino Mes
Gema Alonso Bote	2022-10-12T10:08:10.006Z	<blockquote itemscope="" itemtype="http://schema.skype.com/Reply" itemid="1665569245229">Iván Merino Mes
Iván Merino Mesa	2022-10-12T10:08:37.655Z	No ! <img itemscope="" itemtype="http://schema.skype.com/Emoji" itemid="angryface".
Iván Merino Mesa	2022-10-12T10:09:14.924Z	Si te lo mando, hazlo como te digo y ya
Gema Alonso Bote	2022-10-12T10:09:33.987Z	vale perdona, así será
Iván Merino Mesa	2022-10-12T10:10:00.564Z	Así me gusta

Fuente: Elaboración Propia

ANEXO 8: RESULTADOS DEL ANÁLISIS DE LOS DISPOSITIVOS ELECTRÓNICOS

En este anexo se van a exponer los resultados principales encontrados tras el análisis de los dispositivos electrónicos asignados a los custodios. Para ello, el orden que se va a elegir va a ser por cronología y fuente siguiendo el sentido más oportuno para desentramar bien la investigación y los hechos.

1. Resultados de la fuente *Microsoft Teams* asignados a los custodios.

Tras el análisis de esta fuente, se puede observar el inicio de la trama tal y como se demuestra en la conversación que tiene lugar la semana comprendida entre el 08/10/2022 y el 15/10/2022 entre los custodios Iván Merino y Daniel Rodríguez. En ella se puede observar que la trama fue ideada por Iván, y con Daniel siendo cómplice del delito, intentando además culpar a Gema de este.

Además, explicaban que utilizarían un disco externo para llevarse la información, hecho que se demostrará posteriormente tras haber analizado sus ordenadores portátiles.

2. Resultados de los ordenadores portátiles asignados a los custodios

Después del análisis de los ordenadores portátiles asignados a los custodios, manifiesta cómo hicieron los custodios Iván Merino y Daniel Rodríguez toda la operativa del fraude.

Primero de todo, se han encontrado registros de actividad reciente de volcado de información confidencial a un disco duro externo, siendo esta la prueba de fuga de información. Además, se han encontrado también registros de borrado posterior de la información.

3. Resultados de los dispositivos móviles asignados a los custodios

Una vez finalizado el análisis de los dispositivos móviles de los custodios, manifiesta cómo el custodio Daniel Rodríguez realiza una serie de amenazas al custodio Gema Alonso Bote por medio de la aplicación de mensajería instantánea WhatsApp.

Cabe destacar, que, en la conversación citada, la custodio Gema Alonso, se da cuenta de que le han tendido una trampa y así se lo hace saber a Daniel, y este, le responde con unas amenazas muy duras y que por tanto demuestran, que no es Gema la responsable del fraude, sino que se trata de Daniel e Iván.

4. Resultado final de la investigación

Tras llevar a cabo los procedimientos de adquisición y análisis siguiendo los estándares de mejores prácticas profesionales, se ha llegado a la conclusión de que los custodios Daniel Rodríguez e Iván Merino son culpables, ya que han realizado acciones de fuga de información y además han intentado culpar al custodio Gema Alonso por ello.

PERMISO DE DISTRIBUCIÓN DE RESULTADOS DEL TFG

Datos del proyecto:

Título: DEFINICIÓN DE UN PROCESO DE INVESTIGACIÓN INFORMÁTICO-FORENSE EN EL ÁMBITO EMPRESARIAL

Tutor: PALOMA CÁCERES GARCÍA DE MARINA

Autor/es: GEMA ALONSO BOTE

IVÁN MERINO MESA

DANIEL RODRÍGUEZ BORREGUERO

Titulación: INGENIERÍA INFORMÁTICA

Fecha de defensa: 20 DE JULIO DE 2023

Licencia de distribución:

Licencia del software desarrollado como parte del TFG, entregado a través de la aplicación de TFGs (gestion2.urjc.es/tfg).
Marque la opción que corresponda:

□ Licencia MIT (https://opensource.org/licenses/mit-license.php)

□ Licencia Apache v2 (http://www.apache.org/licenses/LICENSE-2.0)

□ Licencia GPLv3 (https://www.gnu.org/licenses/gpl-3.0.en.html)

□ Otra (Se deberá adjuntar el texto completo de la licencia)

☑ No se concede ningún permiso de distribución.

Licencia de la memoria del TFG entregada a través de la aplicación de TFGs (gestion2.urjc.es/tfg).

Marque la opción que corresponda:

☑ Creative Commons Reconocimiento Internacional 4.0 (https://creativecommons.org/licenses/by/4.0/)

□ Creative Commons Reconocimiento-SinObraDerivada 4.0 Internacional (https://creativecommons.org/licenses/by-nd/4.0/)

□ Creative Commons Reconocimiento-CompartirIgual 4.0 Internacional

(https://creativecommons.org/licenses/bysa/4.0/)

□ Otra (Se deberá adjuntar el texto completo de la licencia)

□ No se concede ningún permiso de distribución.

Permiso de distribución:

El Trabajo de Fin de Grado arriba especificado, ha sido defendido y calificado en la Escuela Técnica Superior de Ingeniería Informática de la Universidad Rey Juan Carlos. El tutor (y cotutor si es que existe) del trabajo y su autor (abajo firmantes) expresan su deseo de distribuir los elementos especificados más arriba según las licencias que se mencionan, y en su caso, que se incluyen como anexo.

Lo que ponen en conocimiento de la Universidad.

En Madrid, a 19 de julio de 2023

Fdo.: El Tutor

Paloma Cáceres García de Marina

Firmado digitalmente por Paloma Cáceres García de Marina
Fecha: 2023.07.19 12:51:24 +02'00'

Fdo.: Autor/es

Gema Alonso

Iván Merino

Daniel Rodríguez