

INFORME TÉCNICO

ADQUISICIÓN FORENSE DE
DATOS DE DISPOSITIVOS

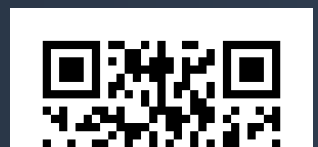
NÚMERO DE SOLICITUD
45818104

NÚMERO DE LEGAJO
M-005766/2022

UNIDAD FISCAL
UNIDAD FISCAL DE INVESTIGACION Y
ENJUICIAMIENTO ESP EN DELITOS C/LA
PROPIEDAD Y C/LA INTEG FISICA

ESPECIALISTA
Alberto Daniel Pérez

DIRECCION
Prosecretario Edgar J. Aranda



MPF

DEPARTAMENTO DE INFORMÁTICA FORENSE
EQUIPO CIENTÍFICO DE INVESTIGACIONES FISCALES
MINISTERIO PÚBLICO FISCAL DE TUCUMÁN

Introducción

Objetivos

- Mantener la cadena de custodia de los elementos probatorios, desde su recepción hasta su entrega, garantizando la integridad de los datos adquiridos.
- Estandarizar el conjunto de actividades y tareas a desarrollar, estableciendo criterios unificados de trabajo, y mayor seguridad.

Marco legal

El informe técnico tiene como referencia básica el Código Procesal de Tucumán, la ley nacional de protección de datos personales, la ley de propiedad intelectual y la ley de delitos informáticos. Ante la ausencia de regulación específica se ha tenido especialmente en cuenta la normativa constitucional y los aportes provenientes de líneas jurisprudenciales firmes y del derecho comparado.

Roles

- El rol del director consiste en realizar el control de calidad de los diferentes informes y procesos llevados a cabo, garantizando que se respeten los objetivos y marco legal del presente informe.
- El rol del especialista es el de recolectar, identificar, preparar, adquirir, extraer, analizar y/o presentar la evidencia, según sea necesario. Sin perjuicio de ello, existen examinadores especializados en diferentes áreas.

Técnicas de estudio

El trabajo realizado ha utilizado el modelo PURI (Proceso Unificado de Recuperación de Información), el cual es un proceso teórico de las tareas involucradas en la aplicación de técnicas y herramientas forense disponibles. La extracción de evidencias en esta rama podría diagramarse como una composición de etapas, no necesariamente todas imprescindibles, representado por el siguiente esquema.

Relevamiento e identificación

Identificación de dispositivos, del caso, de la documentación legal y los participantes durante cualquier etapa del desarrollo del informe.

Preparación y adquisición

Preparación del lugar del trabajo, evitando contaminantes digitales y/o físicos; y la posterior adquisición de los datos contenidos en los dispositivos por intermedio de los programas y herramientas disponibles en este Departamento de Informática Forense.

Extracción y análisis

Extracción de los datos adquiridos y su validación, realizando un examen general y específico de acuerdo a los presupuestos indicados por el solicitante. Se realizará una interpretación de la evidencia, dentro del marco de incumbencia y en los términos de los puntos de pericia que hubieren sido indicados.

Presentación

Redacción del informe, la presentación de la evidencia obtenida, la forma de su preservación, entre otros factores. El mismo será generado digitalmente bajo constancia de doble firma electrónica, con el fin de asegurar la integridad de su contenido. Dicha firma electrónica tendrá un cifrado con algoritmo clave RSA 1024-bits, la cual cumple con los requisitos de validez del artículo 1 y 9 de la Ley Nacional n° 25.506.

INFORME TÉCNICO DIGITAL

1. FASE DE RELEVAMIENTO E IDENTIFICACIÓN

1.1. Identificación del caso

Turno	26/12/22 15:00
Lugar	San Miguel de Tucumán, Tucumán, Argentina
Oficina	Departamento de Informática Forense, Equipo Científico de Investigaciones Fiscales, Ministerio Público Fiscal de Tucumán
Director	Lic. Edgar Jesús Aranda, Prosecretario.
Especialista	Alberto Daniel Pérez
Unidad fiscal	UNIDAD FISCAL DE INVESTIGACION Y ENJUICIAMIENTO ESP EN DELITOS C/LA PROPIEDAD Y C/LA INTEG FISICA
Caratula	MACIAS JOSE ALEJANDRO S/ HOMICIDIO CULPOSO AGRAVADO (Art. 84 bis 1° y 2° Párrafo C.P.) VICT GONZALEZ JOHANA ELIZABETH y CRUZ EMILSE ROMINA
Número de legajo	M-005766/2022
Número de gestión	45818104
Objeto	Adquisición forense de datos de dispositivos
Fases	1.- Relevamiento e identificación 2.- Preparación y adquisición 3.- Presentación

1.2. Identificación de documentación (legal y técnica)

Se detallará a continuación la autorización remitida a este Departamento para la realización del presente informe. En caso que la evidencia física o digital recepcionada no coincida con la obrante en dicha autorización, se suspenderá el proceso de adquisición sobre los elementos afectados.

Autorización	Resolución
Fecha	15/11/2022
Firma	Velazquez Mario Reinaldo
Carácter	Juez
Oficina	Colegio de Jueces del Centro Judicial Monteros

1.3. Identificación de los participantes

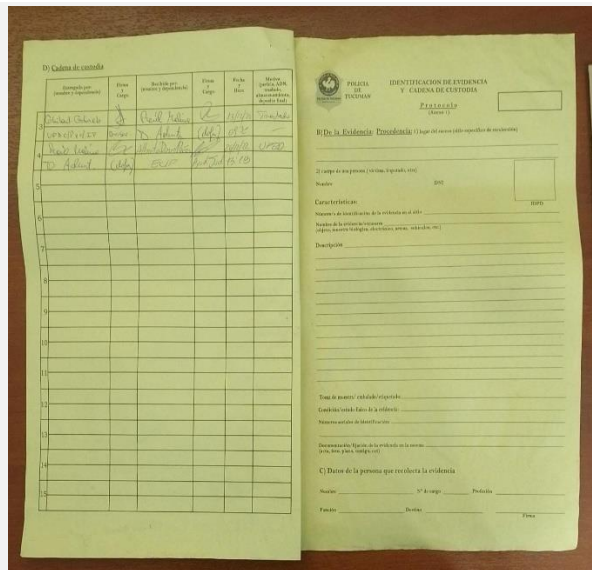
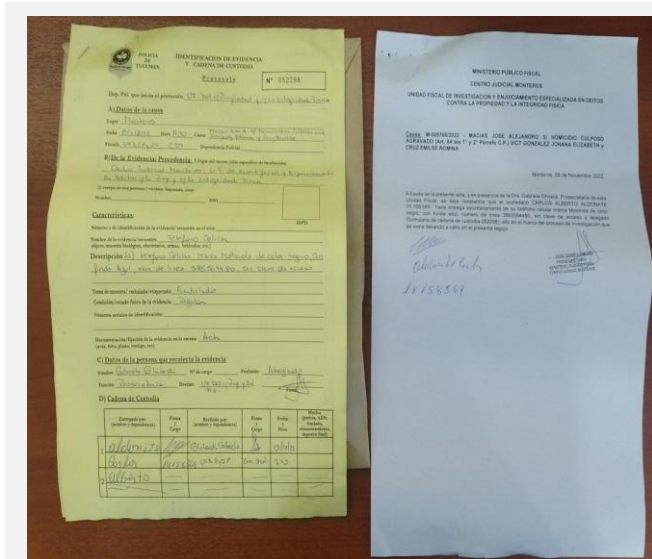
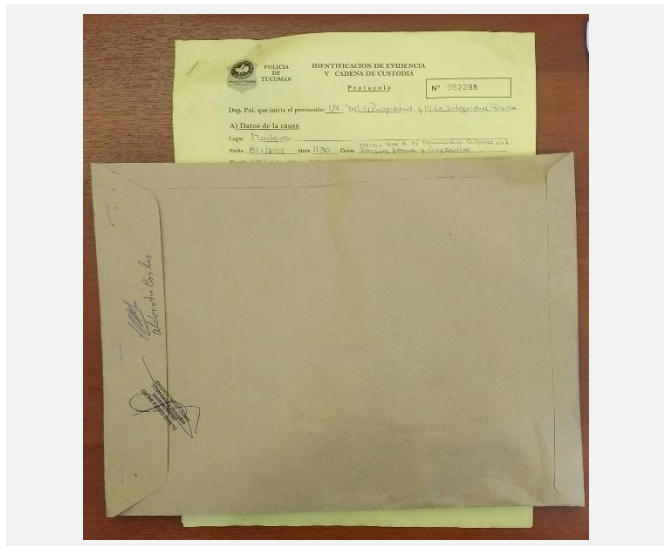
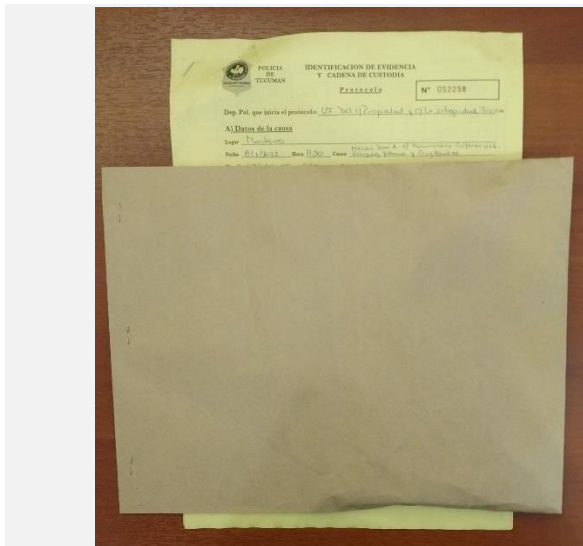
Se ha compartido a la Unidad Fiscal interviniente la información necesaria para que las partes interesadas participen de la videoconferencia por intermedio de Google Meet del proceso de relevamiento e identificación de evidencia. Este Departamento no resulta responsable de las notificaciones a dichas partes. A continuación, habiéndose esperado un tiempo prudencial, ingresan a la Sala de Google Meet, las siguientes partes interesadas, las cuales se detallan a continuación.

Nombre y apellido	Carácter/Observaciones
Alberto Daniel Pérez	Especialista. Departamento de Informática Forense
Dr. Angel Genaro Gramajo	MP 1149, colegio de abogados del Sur- apoderado de la querella
Sr Juan Romano	DNI 29879138 por la querella.

1.4. Relevamiento de la evidencia

La UNIDAD FISCAL DE INVESTIGACION Y ENJUICIAMIENTO ESP EN DELITOS C/LA PROPIEDAD Y C/LA INTEGRACIÓN FÍSICA ha ofrecido los siguientes elementos para su adquisición, siendo presentados conforme las imágenes que se muestran a continuación.

Protocolo de identificación y cadena de custodia
052298

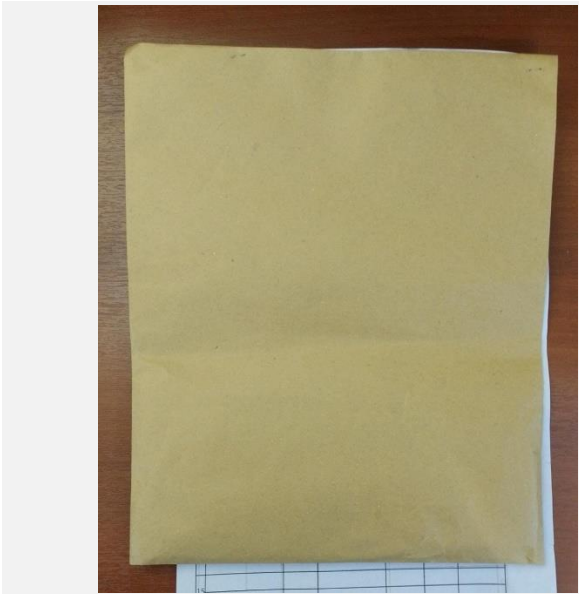


Detalle del contenido conforme se encuentra detallado en el protocolo de identificación y de cadena de custodia

Item n° 1.

Un teléfono celular marca Motorola, modelo no visible, de color negro, con funda de color azul, número de línea 3865564480.

Protocolo de identificación y cadena de custodia
076410



POLICIA DE TUCUMAN IDENTIFICACION DE EVIDENCIA Y CADENA DE CUSTODIA
Protocolo N° 076410

Dep. Pol. que inicia el protocolo: Dep. de Investigaciones Científicas y Forenses

A) Datos de la causa
Lugar: San Juan
Fecha: 21/11/2024 Hora: 11:00 Causa: Proceso penal de homicidio agravado
Fiscalía: Nº 1000 contra la Delincuencia Dependencia Pública

B) De la Evidencia, Procedencia: (Fuente del suceso (sólo especificar de recordación))
de la víctima

Se excepta de una persona (víctima, lesionado, otro):
Nombre: _____ DNI: _____

Características
Número de identificación de la evidencia (escrito en el objeto):
Número de la evidencia (sucesos, víctimas, etc.):
Descripción: Un teléfono celular de color rojo, marca Xiaomi Redmi M1903C3EG, con el n° 3863455623 de la empresa claro, en funcionamiento, de color oscuro en la parte superior con degradado de color rojo en la parte baja.
Tema de suceso: robado
Cualquier otro dato de la evidencia: ninguno
Número serial de identificación: _____

Documentación (Especie de la evidencia en la sucesión (foto, foto plana, video, etc.))
foto y video

C) Datos de la persona que recolecta la evidencia
Nombre: Alberto Daniel Pérez N° de cargo: Agente Prolado: Alberto Daniel Pérez
Firma: Alberto Daniel Pérez Domicilio: San Juan de los Rios

D) Cadena de Custodia

Entregado por (nombre y dependencia)	Fecha y Cargo	Recibido por (nombre y dependencia)	Fecha y Cargo	Observaciones (daños, roturas, deterioros, etc.)
1. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>
2. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>

D) Cadena de custodia

Entregado por (nombre y dependencia)	Fecha y Cargo	Recibido por (nombre y dependencia)	Fecha y Cargo	Observaciones (daños, roturas, deterioros, etc.)
3. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>
4. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>
5. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>
6. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>
7. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>
8. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>
9. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>
10. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>
11. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>
12. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>
13. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>
14. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>
15. <u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>Alberto Daniel Pérez</u>	<u>21/11/2024</u>	<u>ninguna</u>

Detalle del contenido conforme se encuentra detallado en el protocolo de identificación y de cadena de custodia

Item n° 2.

Un teléfono celular marca Xiaomi redmi modelo M1903C3EG, con el n° 3863455623 de la empresa claro, en funcionamiento, de color oscuro en la parte superior con degrade de color rojo en la parte baja.

FIN DE LA FASE DE RELEVAMIENTO E IDENTIFICACION

2. FASE DE PREPARACIÓN Y ADQUISICIÓN

En esta fase, se realizará la extracción de la evidencia digital obtenida previamente en los dispositivos objeto de este informe. Se registrará los detalles específicos de la misma, con su número de hash y programas utilizados a tales efectos

2.1 Preparación del lugar de trabajo

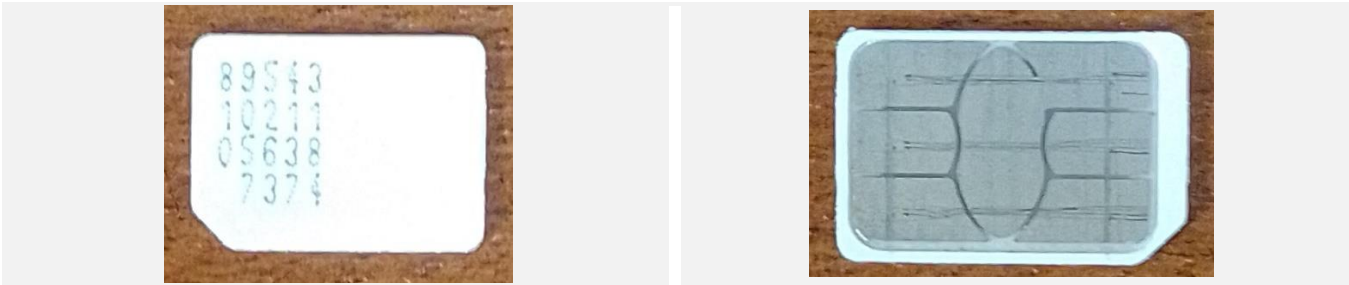
Se ha preparado previamente el lugar de trabajo, estableciéndose zonas libres de exposición a descargas eléctricas o magnéticas.

Se han preparado y dispuesto las herramientas, accesorios, y programas que puedan llegar a ser utilizados durante la realización del proceso de adquisición. Los mismos, serán detallados en cada dispositivo según corresponda. El sistema operativo utilizado durante la confección de este informe es Windows, edición Windows 10 Pro, versión 21H2, tipo de sistema 64 bits.

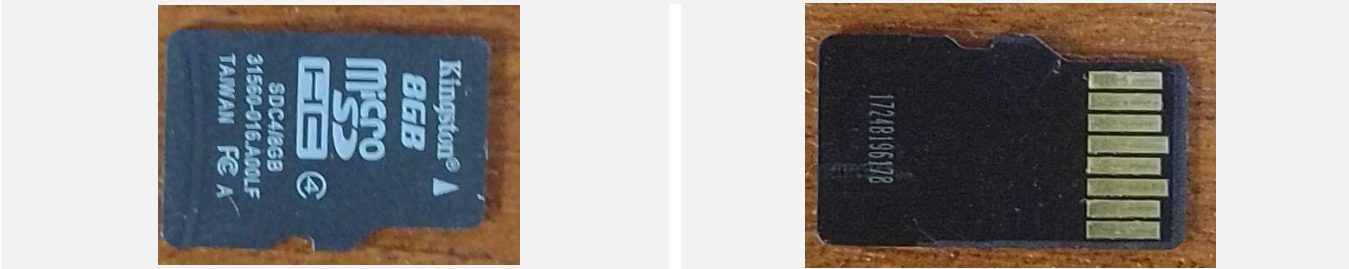
Se ha retirado al personal ajeno a este departamento, asegurándose la privacidad en el manejo de los datos sensibles.

2.2 Adquisición forense de datos

Protocolo de identificación y cadena de custodia 052298		Número de evidencia 01			
					
<i>Categoría</i>				<i>Detalle</i>	
Dispositivo				Teléfono celular marca Motorola, modelo XT2159-1 Moto E40, en mal estado de conservación, IMEI físico n° 354434980920782, IMEI electrónico n° 354434980920782.	
Marco temporal de inicio				26 de diciembre de 2022 a horas 16:07.	
Resultados obtenidos				Positivos.	
Programas utilizados				Cellebrite UFED 4PC versión 7.60.0.222.	
Tipo de adquisición realizada				Sistema de archivos (Live), Lógica avanzada	
Procesamiento de datos				Cellebrite Physical Analyzer.	
Observaciones				Al iniciar el proceso de adquisición, el dispositivo se encontraba desbloqueado. .	



Categoría	Detalle
Dispositivo	Tarjeta SIM , empresa Claro Argentina, en regular estado de conservación, ICCID físico n° 8954310211056387374, ICCID electrónico n° 8954310211056387374.
Marco temporal de inicio	26 de diciembre de 2022 a horas 17:26.
Resultados obtenidos	Positivos.
Programas utilizados	Cellebrite UFED 4PC versión 7.60.0.222.
Tipo de adquisición realizada	Lógica.-
Procesamiento de datos	Cellebrite Physical Analyzer.
Observaciones	.

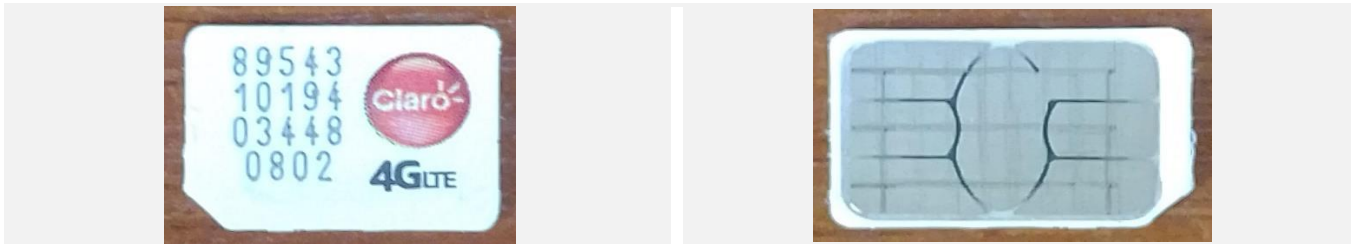


Categoría	Detalle
Dispositivo	Tarjeta de memoria , marca Kingston, clase 4 (C4), capacidad 8gb, en regular estado de conservación
Marco temporal de inicio	26 de diciembre de 2022 a horas 17:15.
Resultados obtenidos	Positivos.
Programas utilizados	Cellebrite UFED 4PC versión 7.60.0.222.
Tipo de adquisición realizada	Física.-
Procesamiento de datos	Cellebrite Physical Analyzer.
Observaciones	.

Protocolo de identificación y cadena de custodia 076410	Número de evidencia 02
--	---------------------------



Categoría	Detalle
Dispositivo	Teléfono celular marca Xiaomi, modelo M1903C3EG (Redmi 7A) , en mal estado de conservación, IMEI físico n° no visible, IMEI electrónico 1 n° 866679049934924, IMEI electrónico 2 n° 866679049934932,.
Marco temporal de inicio	26 de diciembre de 2022 a horas 16:29.
Resultados obtenidos	Positivos.
Programas utilizados	Cellebrite UFED 4PC versión 7.60.0.222.
Tipo de adquisición realizada	Sistema de archivos (Live), Lógica avanzada.
Procesamiento de datos	Cellebrite Physical Analyzer.
Observaciones	Al iniciar el proceso de adquisición, el dispositivo se encontraba bloqueado con código numérico . Se implementó el método de fuerza bruta, el código correspondió al número 1967.



Categoría	Detalle
Dispositivo	Tarjeta SIM , empresa Claro Argentina, en regular estado de conservación, ICCID físico n° 8954310194034480802, ICCID electrónico n° 8954310194034480802.
Marco temporal de inicio	26 de diciembre de 2022 a horas 17:50.
Resultados obtenidos	Positivos.
Programas utilizados	Cellebrite UFED 4PC versión 7.60.0.222.
Tipo de adquisición realizada	Lógica.-
Procesamiento de datos	Cellebrite Physical Analyzer.
Observaciones	.

FIN DE LA FASE DE PREPARACIÓN Y ADQUISICIÓN

3 FASE DE PRESENTACION

3.1. Responsabilidad y opinión del Director

3.1.1. Responsabilidad del Director

El **Director** es responsable de la preparación y correcta presentación del informe en conformidad con las políticas y controles internos del Departamento, realizando las correcciones necesarias para procurar evitar las declaraciones erróneas.

3.1.2. Opinión del Director

En opinión de la Dirección, el presente informe cumple con los principios básicos de relevancia, suficiencia, validez legal y confiabilidad. El examinador ha respetado los parámetros y modelo establecido para la confección del informe.

3.2 Resguardo de la evidencia digital

Habiendo finalizado las diferentes fases del presente informe el **27 de diciembre de 2022 - 18:42**, se procede a resguardar las imágenes forense obtenidas de los dispositivos afectados, las que serán conservados por un plazo mínimo de 90 días y un plazo máximo de 6 meses. Es posible solicitar una extensión de dicho período de tiempo, mediante una nueva solicitud.

A continuación, se detallará la evidencia adjunta y en que formato es remitida.

Soporte óptico	Marca	Cantidad	Observaciones
DVD-R	TDK	20	.

3.3 Conclusiones y recomendaciones

El examinador, en caso de considerarlo necesario, podrá realizar recomendaciones no vinculantes a la Unidad Fiscal para poder profundizar sobre la adquisición de ciertos dispositivos.

Se considera que no hay recomendaciones para realizar en esta etapa.

3.4 Firma electrónica

Las firmas electrónicas que a continuación son plasmadas se encuentran controladas en forma interna por este Departamento de Informática Forense. Poseen un cifrado con algoritmo clave RSA 1024-bits, la cual cumple con los requisitos de validez del artículo 1 y 9 de la Ley Nacional n° 25.506.-

MPF

Alberto Daniel Perez
Examinador
San Miguel de Tucumán
2022-12-27 18:43-03:00

Firma del examinador (Control 1 de 2)

MPF

Edgar Jesus Aranda
Dirección
San Miguel de Tucumán
2022-12-27 18:43-03:00

Firma del director (Control 2 de 2)

FIN DE LA FASE DE PRESENTACIÓN

FIN DEL INFORME TÉCNICO