Procurador General de la Provincia

RESOLUCIÓN Nº 1616

**ANEXO I**

**MANUAL DE USO DE LA HERRAMIENTA "EVIDENTIA" PARA INSPECCIONES FORENSES EN DISPOSITIVOS ELECTRONICOS**

**1. Función**

Evidentia es una herramienta informática desarrollada para la inspección forense de dispositivos electrónicos que cuenten con tecnología Android, ya que permite registrar adecuadamente la visualización de la información contenida en ese tipo de dispositivos, sin descargar los archivos o efectuar una extracción forense.

La herramienta fue diseñada de forma tal que permita asegurar la integridad, confidencialidad, resguardo y admisibilidad probatoria de la evidencia digital recolectada. Mediante su utilización, los representantes del Ministerio Público Fiscal podrán capturar la información que surja de dispositivos móviles, cuando el procedimiento sea consentido expresamente por la víctima, por quienes voluntariamente admitan aportar información al caso o, en su defecto, cuando medie la respectiva autorización judicial.

El programa Evidentia permite que la información digital recolectada se mantenga sin alteraciones desde que se produce el registro hasta su presentación en el respectivo proceso, por medio de algoritmos criptográficos Hash, lo que permite cumplir con los requisitos de la cadena de custodia.

Por otro lado, el procedimiento que se lleva a cabo con el uso de Evidentia no resulta invasivo, en el sentido de que preserva la integridad del dispositivo y los datos allí contenidos. Opera en modo "solo lectura", sin escrituras persistentes en el dispositivo objeto de la medida.

Digitally signed by
OBEID MIRNA PAOLA
Date: 2025.05.23
13:12:49 -03:00
Reason: -
Location:

**2. Descripción de las operaciones forenses**

a) *Configuración del dispositivo sujeto a inspección*: es necesario que el dispositivo objeto de la medida sea configurado antes de ser conectado al programa Evidentia. Los pasos a seguir de acuerdo a los distintos sistemas operativos que puede tener el aparato se han detallado en el punto 9 ("Guía para depuración por puerto USB").

Este paso previo implica un simple ajuste en la configuración del dispositivo electrónico a explorar, con el objeto de que **admita la duplicación de pantalla** a través de la conexión por puerto USB que se requiere. **No es necesario realizar ningún tipo de instalación de software sobre el equipo a inspeccionar**, resguardando así el estado del mismo.

En caso de que el dispositivo cuente con un código de seguridad o patrón de desbloqueo, deberá requerirse a su titular o usuario que proceda previamente a desbloquear la pantalla para poder concretar las operaciones. Para ello no es necesario que la persona revele la clave o patrón.

b) *Registro de información relevante sobre la operación que se va a realizar*: al conectar el dispositivo objeto de la medida al cable USB, el sistema instalado en la computadora del Ministerio Público Fiscal, automáticamente procede a registrar la siguiente información del dispositivo: **marca, modelo, sistema operativo, número de IMEI** (Identidad Internacional de Equipo Móvil), **fecha y hora que reporta el equipo inspeccionado**.

Dejar constancia de la hora y fecha que registra el dispositivo sirve para diferenciarla de la fecha y hora de la PC que está realizando la inspección. Se trata del valor almacenado en el reloj interno del aparato inspeccionado, que puede o no coincidir con la hora oficial ni con la del host. Registrar el tiempo del equipo es fundamental, porque cualquier desajuste o manipulación del reloj interno podría afectar la interpretación cronológica de los eventos mostrados (mensajes, llamadas, capturas), de modo que esa referencia queda documentada para eventuales peritajes de consistencia temporal.

El programa también permite el ingreso de **datos del "Funcionario" que lleva a cabo la operación y del "Usuario" que aporta el dispositivo**. Para mayor resguardo, el sistema permite la realización de una toma fotográfica de cada uno de ellos, a través de la propia cámara del dispositivo.

**c)** *Visualización remota*: la herramienta permite la **observación en tiempo real de la pantalla del dispositivo inspeccionado**, duplicándola en la computadora del usuario del Ministerio Público.

La víctima, testigo o el titular del dispositivo, pueden navegar a través de su pantalla, ingresando sólo a los aplicativos, chats, galería de imágenes, correos electrónicos, etcétera, que desee mostrar.

**d)** *Resguardo de la evidencia*: duplicada que fuera la pantalla del dispositivo inspeccionado, la evidencia se resguarda a través de capturas de pantalla y registros de video; de esa forma se registran todas las actividades relevantes observadas en el dispositivo.

Dicha actividad **no permite la descarga de los archivos contenidos en el dispositivo inspeccionado, sólo permite capturar o registrar lo reproducido a través de él**.

**e)** *Generación de Hashes*: al finalizar la sesión, Evidentia calcula -para cada una de las capturas de pantalla y para cada archivo de video que la propia herramienta genera– un valor Hash mediante el algoritmo SHA-256, produciendo un **resumen criptográfico de 256 bits que funciona como huella dactilar digital del archivo correspondiente**.

Dado que la más mínima modificación (incluso de un solo bit) arroja un hash completamente distinto, la conservación de estos valores en el informe permite que cualquier parte interesada vuelva a calcularlos y compruebe que cada imagen o video entregado es idéntico al que se obtuvo originalmente. De esta manera se garantiza la integridad de la evidencia y la cadena de custodia para su posterior admisibilidad judicial.

f) *Cifrado y embalaje de datos*: una vez generadas las capturas de pantallas y los videos, Evidentia agrupa todos los archivos generados —junto con el informe y la tabla de hashes— en un **único contenedor ZIP protegido mediante cifrado simétrico AES-256**, estándar avalado por FIPS 197 y aceptado internacionalmente para la custodia de información sensible. Para ello, el sistema genera una contraseña de longitud de veinticuatro dígitos, la cual es obtenida mediante la función PBKDF2-HMAC-SHA-256 con una "semilla" aleatoria de 128 bits; este proceso de derivación hace que la clave resultante sea computacionalmente resistente a ataques de "fuerza bruta", "diccionario" o "tablas pre calculadas".

El ZIP cifra cada byte del contenido, de modo que sólo quien posea la contraseña puede abrirlo, preservando así la confidencialidad hasta su entrega en sede judicial.

Paralelamente, Evidentia mantiene un **registro exhaustivo en el archivo *evidentia.log*, donde anota cada evento crítico** (conexión del dispositivo, inicio y fin de grabación, cálculo de hashes, creación del ZIP, etc.) utilizando marcas de tiempo en formato ISO-8601. Este formato, preciso e independiente de configuraciones regionales, facilita la correlación cronológica de hechos.

g) *Generación de informes*: el sistema, al finalizar la inspección, genera un reporte en formato PDF, a modo de informe técnico, donde se incluye la siguiente información:

- **fecha y hora del equipo oficial** desde donde se realiza el trabajo (es decir, toma el valor del reloj del computador forense y consignado en formato ISO-8601 para situar temporalmente la actuación);
- **referencias sobre el caso**: identificadores que vinculan la diligencia con las actuaciones en las que se dispuso su utilización (número de Ap-Av/causa, carátula, identificación CIF-SAL, expediente, etc.). Esta información es tomada de los datos que carga el funcionario al iniciar las operaciones;

- **datos del funcionario que participó en la inspección**: nombre, apellido, DNI y toma fotográfica. Esto permite individualizar al responsable de practicar la medida y acreditar su presencia;

- **observaciones del trabajo**: anotaciones relevantes sobre el contexto operativo, que podrían versar sobre: estado del terminal, configuración especial, incidencias o limitaciones detectadas durante la sesión, información sobre el relato de la persona que puso a disposición el dispositivo o lo que el funcionario considere pertinente consignar;

- **archivos generados en la inspección** (imágenes y/o videos): implica un listado completo de PNG, MKV, DOCX y ZIP cifrado producidos por Evidentia;

- **metadatos de los archivos generados**: el sistema registra tamaño, fecha y hora de creación y Hash SHA-256, facilitando la verificación de integridad y cronología;

- **claves resultantes de los archivos cifrados**: se documenta una contraseña de 16 dígitos y su Hash SHA-256 para corroborar autenticidad de ser necesario.

**3. Encuadre jurídico**

El uso de la herramienta Evidentia debe llevarse a cabo en el marco de la investigación de un hecho con apariencia delictiva, ya sea en sus inicios o luego de formulado el acto por el que se formaliza la investigación penal preparatoria, con el objeto de obtener información sobre el hecho que se está investigando.

La operación producida a través del programa Evidentia forma parte de los medios probatorios previstos como facultad del Ministerio Público Fiscal en el art. 293 del Código Procesal Penal, como consecuencia de la carga probatoria que le compete (art. 282, CPP), ya que constituye una "inspección de cosas".

**4. Formalidades mínimas de la actividad**

La actividad de inspección que se realiza a través de Evidentia se podrá llevar a cabo en un dispositivo electrónico de uso privado, lo que implicará -como regla- la intromisión en la esfera de privacidad de su titular y/o usuario, para lo que se requerirá el consentimiento expreso de esa persona.

Cuando el titular del derecho de exclusión sea la víctima o un testigo, bastará que conste en el acta respectiva el consentimiento informado de esa persona, acompañado de su firma.

Cuando el dispositivo pertenezca o sea de uso frecuente por parte de una persona imputada, en sede de la Fiscalía se podrá llevar a cabo el registro pero, para ello, no sólo se deberá recabar su consentimiento con la debida información sobre los alcances e implicancias de la medida, sino que en el mismo acto deberá estar presente también la defensa técnica.

Ante el supuesto de ausencia de consentimiento por parte del titular del derecho de exclusión, se deberá proceder conforme lo previsto en el segundo párrafo del art. 293 del CPP (cfr. Ley 7690 o la que la reemplace), es decir, solicitando fundadamente al Juez de Garantías que autorice la medida y, en caso positivo, se deberá fijar fecha y horario del acto, con notificación de ello a la defensa técnica, a los fines de darle la oportunidad de que participe de la inspección.

**5. Sugerencias prácticas para la inspección**

A los fines de que la inspección practicada en el dispositivo electrónico sea lo más eficiente posible, en el sentido de que permita contar con la mayor cantidad de información precisa sobre lo observado, se recomienda lo siguiente:

a) al *inspeccionar imágenes o fotografías* puede hacerse una captura de pantalla de la imagen completa y otra en la que se muestren los metadatos del archivo, por ejemplo a través del acceso a "propiedades", "información", "detalles" u otras formas de acceder al campo que permite hacer constar

la fecha y horario que allí figura, el nombre del archivo, su ubicación dentro del dispositivo, su tamaño, etcétera;

b) al *inspeccionar videos* debe grabarse la pantalla en formato de video y luego de finalizada su reproducción hacer una captura de los metadatos del archivo, como se señala en el punto anterior;

c) al *inspeccionar un registro de audio* se deberá grabar en formato de video mientras el archivo es reproducido y luego, en caso que sea posible, hacer captura de pantalla de los metadatos del archivo;

d) al *inspeccionar el contenido y/o actividad en una red social*, se puede registrar un video que muestre la navegación que se hizo, pero resulta importante que se tome captura de pantalla de los siguientes campos:

- datos del perfil de la persona titular de la cuenta desde la cual se lleva a cabo la inspección, en caso de que sean visibles, tales como: URL -Uniform Resource Locator- o dirección web, fecha de creación de la cuenta, correo electrónico asociado, o cualquier dato que la plataforma o aplicación ponga a disposición para identificar al usuario;
- datos del perfil de terceras personas con las que se establece la comunicación que se pretende registrar o de las personas que llevaron a cabo una publicación que se pretende registrar, en caso de que sean visibles;
- conversaciones por mensajes de texto, abarcando la secuencia completa de la conversación que se quiere aportar;
- registro de llamadas entrantes y salientes, con la correspondiente información que se registre sobre el número o contacto que habría efectuado o intentado la comunicación;

e) la *inspección sobre el registro de geo-referenciamiento o de ubicaciones y recorridos*, en el caso de que la persona lo tenga activado, se puede hacer con captura de pantalla, procurando registrar toda la información que el dispositivo muestre sobre esa actividad;

f) la *inspección de comunicaciones por correo electrónico*, debe hacerse captura de pantalla del mensaje completo, de los

datos que figuren de los contactos entre los que se entabló la comunicación (tanto remitentes como destinatarios) y de los archivos adjuntos que hubiera;

g) la *inspección sobre documentos o archivos contenidos en el dispositivo*, debe hacerse con captura de pantallas sobre el contenido del documento y sobre sus metadatos, a través del acceso a "propiedades", "información" o "detalles" del mismo, a los fines de registrar ubicación dentro del dispositivo, tipo y tamaño, fecha de creación y de modificación, así como cualquier otro dato que permita visualizar el aparato.

Es importante destacar que en algunos casos, la inspección sobre los datos de perfil de un contacto en una red social o las actividades llevadas a cabo en ciertas aplicaciones (como billeteras virtuales, por ejemplo), por las propias políticas de seguridad o privacidad de sus desarrolladores, no permite capturar la información privada allí contenida, ello repercutirá en la captura del registro llevado a cabo de forma tal que la imagen o video permanecerá en negro mientras se inspeccione ese elemento. Para esos supuestos, a los fines de darle utilidad a la inspección, resulta conveniente que de alguna otra forma se genere una constancia del elemento inspeccionado que la aplicación o red social bloquea, por lo que se sugiere tomar una fotografía de ese campo a través de otro dispositivo y acompañarla con el informe que genera Evidentia, o dejar constancia de la información allí contenida transcribiendo los datos en el acta que se confeccionó. Tanto el operador que llevó a cabo el registro como la persona cuyo dispositivo fue inspeccionado, al firmar el acta, darán cuenta de la vinculación entre esa información bloqueada y la constancia que se acompaña.

**6. Recomendaciones para el uso de la información en la audiencia de debate**

La operación que se lleve a cabo a través de la herramienta Evidentia constituye, técnicamente, una actividad investigativa documentada. Es decir que se trata de una constatación efectuada por un actuario del Ministerio Público Fiscal sobre un

dispositivo electrónico, con la particularidad que es registrada debidamente en imágenes y/o videos.

Para la introducción de la información recogida en una audiencia de debate, se recomienda el momento de la declaración de la víctima o del testigo usuario y/o titular del dispositivo inspeccionado. También puede complementarse con el testimonio del operador que ha practicado la medida, de forma tal que pueda explicar cómo se utilizó la herramienta.

En los supuestos que la inspección haya sido sobre el dispositivo electrónico del imputado, se recomienda su introducción mediante el testimonio del operador que ha practicado la medida, sin perjuicio de que pueda ser utilizada también al momento de la declaración del propio imputado.

**7. Recomendaciones para el usuario y/o titular del dispositivo**

Toda vez que se lleve a cabo una inspección a través de la herramienta Evidentia, se deberá hacer constar en el acta que se labre a tales efectos, que se recomienda al titular y/o usuario del dispositivo electrónico objeto de la medida, que no altere ni elimine la información que formó parte de la operación, por cuanto podría ser susceptible de una pericia informática, para lo cual se podrá requerir oportunamente la entrega voluntaria del dispositivo o, en su defecto, el secuestro por orden judicial.

**8. Especificaciones técnicas del Programa Evidentia**

**a)** Evidentia es una herramienta informática que combina tres *componentes esenciales*:

- Python: lenguaje de programación de alto nivel que orquesta todo el flujo —desde la conexión y el registro de eventos hasta el cálculo de hashes y la generación automática del informe—;
- ADB (Android Debug Bridge): herramienta oficial del SDK Android y protocolo cliente-servidor que habilita la comunicación fiable por USB/TCP entre el ordenador forense y el dispositivo, permitiendo enviar comandos de sistema y

capturar pantallas sin requerir permisos de super-usuario (usuario con acceso completo y sin restricciones);

- Scrcpy: programa de código abierto que envía al teléfono un pequeño servidor Java temporal (el cual se borra inmediatamente tras cargarse) para convertir la pantalla en un flujo de vídeo H.264 que se recibe en el host y puede grabarse o capturarse puntualmente. Al actuar en modo "solo lectura" y borrar su binario al vuelo, scrcpy garantiza que ningún archivo quede instalado, de modo que Evidentia documenta fielmente lo que se visualiza en el dispositivo (mensajes, imágenes, aplicaciones) sin descargar contenido ni realizar una extracción lógica o física, preservando la integridad del equipo.

**b)** El programa Evidentia cuenta con las siguientes *especificaciones técnicas*:

| Id | Documento / fuente |
|---|---|
| ISO/IEC 27037:2012 | Identificación, colección y preservación de evidencia digital |
| NIST SP 800-86 | Buenas prácticas de hashing y cadena de custodia |
| Blog "Introducingscrcpy" | No intrusividad y limpieza automática del dispositivo blog.rom1v.com |
| scrcpy develop.md (GitHub) | Push a /data/local/tmp, privilegios shell, sockets separados GitHub |
| Android ADB docs | Acceso shell de sólo lectura |

**c)** *Flujo de trabajo*: los componentes principales del flujo de trabajo son:

- Estación de trabajo (Host - PC del analista Forense) donde se encuentra instalado el sistema EVIDENTIA y posibilita:
  - Utilizar ADB (Android Debug Bridge): Herramienta que permite la comunicación de un dispositivo Android desde el Host. Version 34.0.5
  - Scrcpy (cliente): Aplicación en el PC forense que recibe la transmisión de la pantalla del dispositivo Android

- GUI (Interfaz Gráfica de Usuario): ventana en el host que muestra la pantalla duplicada del dispositivo Android, proporcionada por scrcpy_client.

- Dispositivo Android: El dispositivo móvil que se encuentra bajo análisis.
  - Scrcpy Server (scrcpy-server.jar): servidor que se ejecuta temporalmente en el dispositivo Android para capturar la pantalla.

Descripción del Flowchart (Diagrama de flujo) con el sistema Evidentia:

- *Conexión inicial*: se establece una conexión física (USB) entre el Dispositivo Android y el Host. Para esto es necesario que se encuentre habilitada la depuración USB y autorizada la conexión.
- *ADB*: se utiliza para iniciar la comunicación con el dispositivo Android a través de la conexión USB.
- *Despliegue del Servidor Scrcpy*: el scrcpy_client en el PC forense utiliza la conexión ADB para transferir (push) el archivo scrcpy-server.jar al sistema de archivos temporal del Dispositivo Android.
- *Inicio del Servidor Scrcpy*: una vez transferido, el scrcpy_client (a través de ADB) ejecuta el scrcpy-server.jar en el Dispositivo Android.
- *Transmisión de pantalla*: El scrcpy-server en el dispositivo Android captura la pantalla del dispositivo, codifica el video de la pantalla utilizando el códec H.264 y envía el flujo de video H.264 al scrcpy_client en el Host a través de la conexión establecida.
- *Visualizacion*: El scrcpy_client recibe el flujo H.264 y decodifica el video, lo muestra en una ventana GUI, duplicando la pantalla del dispositivo Android en tiempo real.
- *Documentación*: se registran por medio de videos y capturas de pantallala inspección observada desde la interfaz del dispositivo. Para ello se utiliza el siguiente flujo:
  - Para video: scrcpy --recordvideo.mkv --cleanup:
    - --recordvideo.mkv: graba la sesión del duplicado de pantalla directamente en un archivo video.mkv en el

Host. Con esto captura toda la interacción visual como evidencia en el video.

- --cleanup: asegura que Scrcpy elimine automáticamente el scrcpy-server.jar del directorio /data/local/tmp del dispositivo Android una vez que la conexión se cierra. También restaura cualquier "flag" o configuración temporal que pudiera haber modificado.

- Para Capturas: adbexec-outscreencap -p (flujo por pipe)
  - exec-out: ejecuta el comando screencap -p en el dispositivo.
  - screencap -p: comando nativo de Android para capturar la pantalla y enviar la imagen en formato PNG a la salida estándar.
  - flujo por pipe: La salida (imagen PNG) se envía directamente a través de la conexión ADB al Host, sin necesidad de guardarla primero como un archivo en el almacenamiento del dispositivo Android.
    Se utiliza el proceso de streaming H.264 diseñado para minimizar la escritura en el almacenamiento interno del dispositivo Android, operando principalmente en RAM (memoria utilizada para almacenar temporalmente). Esto ayuda a preservar el estado original del dispositivo.

- *Reportes*: se genera un reporte forense en formato PDF con el detalle de lo ingresado en el sistema EVIDENTIA, se calculan los Hash (SHA-256) de las capturas y videos para asegurar integridad.
- *Empaquetado*: se genera un único archivos ZIP que se cifra con el algoritmo AES-256 asegurando la confidencialidad y seguridad.
- *Finalización*: scrcpy elimina JAR y revierte flags.

**d)** *Procedimiento detallado de adquisición*:

| Fase | Comando | Impacto en dispositivo |
|---|---|---|
| Activar USB Debug | Ajustes > Opciones desarrollador | Cambia solo bandera de sistema |
| Conexión ADB | adbdevices | Daemonshell (lectura) |

| | | |
|---|---|---|
| Capturas fotos | am start … + exec-outscreencap p | PNG generado en host |
| Grabación vídeo | scrcpy --record … --no-control | Streaming; sin archivos locales |
| Cierre | CTRL-C o API | scrcpy borra JAR y revierte flags |
| Hashing | hashlib.sha256() | Solo en host |
| Informe | python-docx | N/A |
| Embalar | pyzipper AES-256 | N/A |

**e)** *Mecanismos de garantía de integridad*:

| Mecanismo | Implementación | Valor probatorio |
|---|---|---|
| Hash individual | SHA-256 (FIPS 180-4) | Verificación unitaria |
| Hash maestro | SHA-256 del ZIP | Detección de alteraciones |
| Log operativo | evidentia.log ISO-8601 | Trazabilidad |
| Versionado | Se documentan versiones de scrcpy, ADB y Evidentia | Repetibilidad |
| Cifrado | AES-256, PBKDF2-HMAC-SHA-256 | Confidencialidad e integridad |

**f)** *Análisis de no-intrusividad*:

- Sin root: scrcpy se ejecuta como shell.
- Binario efímero: unlink inmediato del JAR blog.rom1v.com.
- Operaciones de sólo lectura: screencap, am start.
- Restauración automática: --cleanup revierte flags.
- Control opcional: --no-control evita inputs accidentales.

**g)** *Evaluación de riesgos y controles*:

| Riesgo | Prob. | Sev. | Control |
|---|---|---|---|
| JAR persiste tras desconexión | Muy baja | Baja | --cleanup + unlink |
| Inputs involuntarios | Media | Media | --no-control |
| Desbordes de búfer vídeo | Baja | Baja | Scrcpy descarta frames retardados |

| | | | |
|---|---|---|---|
| Filtración de contraseña | Baja | Alta | Entrega por canal seguro; no se registra |

**h)** *Conformidad con buenas prácticas*:

- ISO/IEC 27037 §7.3: Dispositivos operados en modo non-invasive.
- NIST SP 800-86 §4.2: Algoritmos hash aprobados.
- Principio ACPO (UK): Ninguna acción debe cambiar datos confiables en corte.

**9. Guía para depuración por puerto USB según la marca del dispositivo**

**a.** *Dispositivo electrónico marca Motorola*:

1°) Seleccione en el menú principal la opción "AJUSTES";
2°) una vez dentro buscar la opción "ACERCA DEL TELÉFONO" (generalmente se encuentra al final del menú);
3°) Una vez dentro buscar la opción "NUMERO DE COMPILACIÓN" y presionar 7 (siete) veces (ingresar patrón o contraseña);
4°) Volver al menú AJUSTES e ingresar en la opción "SISTEMA";
5°) Una vez dentro buscar "OPCIONES DE DESARROLLADORES" o "PROGRAMADOR";
6°) Una vez dentro buscar la opción "DEPURACIÓN POR USB" y activar.
7°) Salir del menú AJUSTES.

**b.** *Dispositivo electrónico marca Samsung*:

1°) Seleccione en el menú principal la opción "AJUSTES";
2°) Una vez dentro buscar la opción "ACERCA DEL DISPOSITIVO" (generalmente se encuentra al final del menú);
3°) Una vez dentro buscar la opción "NUMERO DE COMPILACIÓN" y presionarla 7 (siete) veces. (ingresar patrón o contraseña);
4°) Volver al menú AJUSTES e ingresar en la opción "OPCIONES DE DESARROLLADOR";

5°) Una vez dentro buscar la opción "DEPURACIÓN POR USB" y tildar/activar;

6°) Salir del menú AJUSTES.

**c.** *Dispositivo electrónico marca Xiaomi*:

1°) Seleccione en el menú principal la opción "CONFIGURACIÓN";

2°) Una vez dentro buscar la opción "ACERCA DEL TELÉFONO" (generalmente se encuentra al principio del menú);

3°) Una vez dentro buscar la opción "VERSIÓN MIUI" y presionar 7 (siete) veces. (ingresar patrón o contraseña);

4°) Volver al menú CONFIGURACIÓN e ingresar en la opción "AJUSTES ADICIONALES";

5°) Una vez dentro buscar "OPCIONES DE DESARROLLADORES";

6°) Una vez dentro buscar la opción "DEPURACIÓN USB" y activar;

7°) Salir del menú AJUSTES.

**d.** *Dispositivo electrónico marca Huawei*:

1°) Seleccione en el menú principal la opción "AJUSTES";

2°) Una vez dentro buscar la opción "SISTEMA" (generalmente se encuentra al final del menú);

3°) Una vez dentro buscar la opción "ACERCA DEL TELÉFONO";

4°) Una vez dentro buscar la opción "NUMERO DE COMPILACIÓN" y presionar 7 (siete) veces. (ingresar patrón o contraseña);

5°) Volver al menú SISTEMA e ingresar en la opción "OPCIONES DE DESARROLLADOR";

6°) Una vez dentro buscar la opción "DEPURACIÓN USB" y activar;

7°) Salir del menú AJUSTES.

**e.** *Dispositivo electrónico marca LG*:

1°) Seleccione en el menú principal la opción "AJUSTES";

2°) Una vez dentro buscar la pestaña "GENERAL";

3°) Buscar la opción "OPCIONES AVANZADAS";

4°) Una vez dentro de OPCIONES AVANZADAS en el apartado "DEPURACIÓN" buscar la opción "DEPURACIÓN USB" y activar;

5°) Salir del menú AJUSTES.

PROCURACIÓN GENERAL - PROVINCIA DE SALTA

Dr. PEDRO OSCAR GARCIA CASTIELLA
PROCURADOR GENERAL DE LA PROVINCIA
MINISTERIO PUBLICO DE SALTA

Ante mí

Dra. MARIA BELEN RUBIO
SECRETARIA DE SUPERINTENDENCIA
PROCURACION GENERAL DE LA PROVINCIA
MINISTERIO PUBLICO DE SALTA