

TEMA 9: LIBERACION Y DESBLOQUEO POR IMEI

LIBERACIÓN Y DESBLOQUEO POR IMEI

Primero vamos a definir algunos conceptos:

¿Qué es liberar o desbloquear el móvil por IMEI?

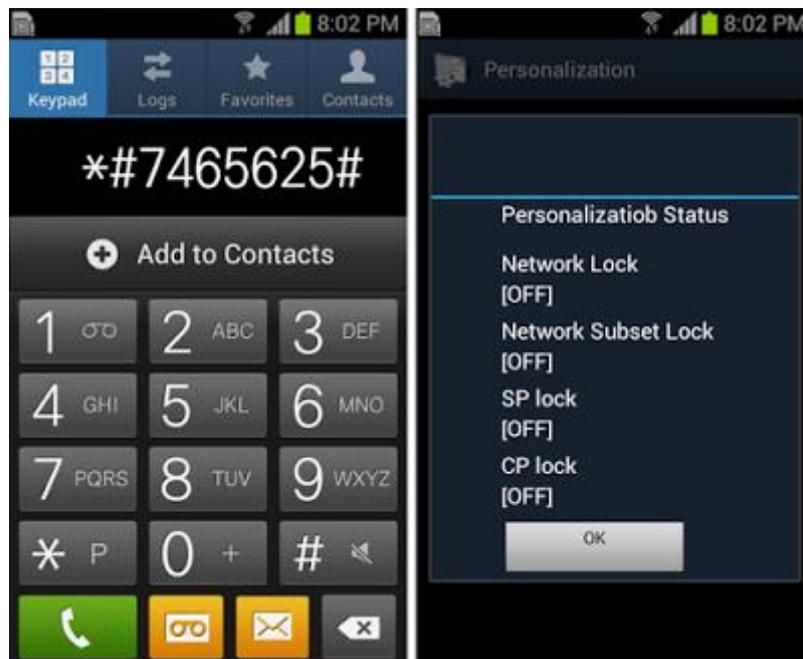
Desbloquear, liberalizar o liberar el móvil significa romper la protección que usan las compañías telefónicas, para fidelizar al cliente, suelen modificar ligeramente el software de los terminales móviles que venden para que no funcionen con tarjetas de otras compañías (**SIM Lock**). Liberar, desbloquear tu móvil significa permitir que tu terminal funcione con todas las tarjetas de todas las compañías.

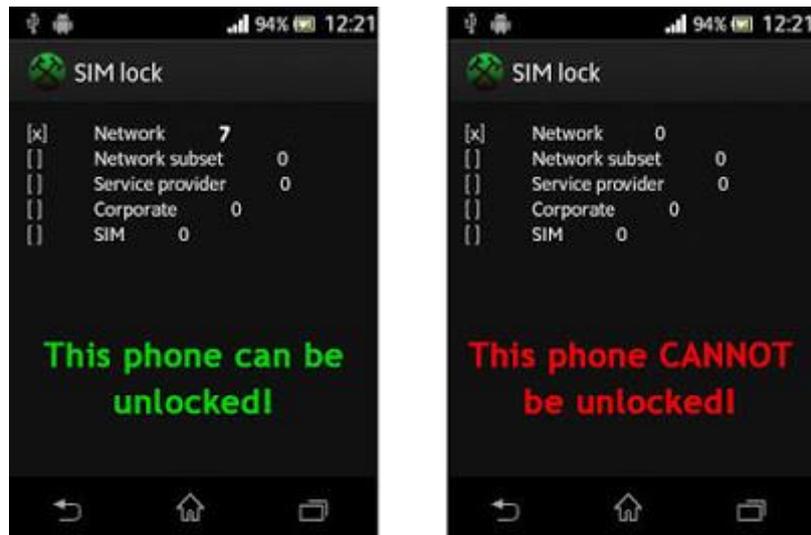
¿Cómo se rompe esta protección?

Introduciendo el código de desbloqueo de red. Cada terminal tiene un solo código de desbloqueo de red válido.

¿Qué es SIM Lock?

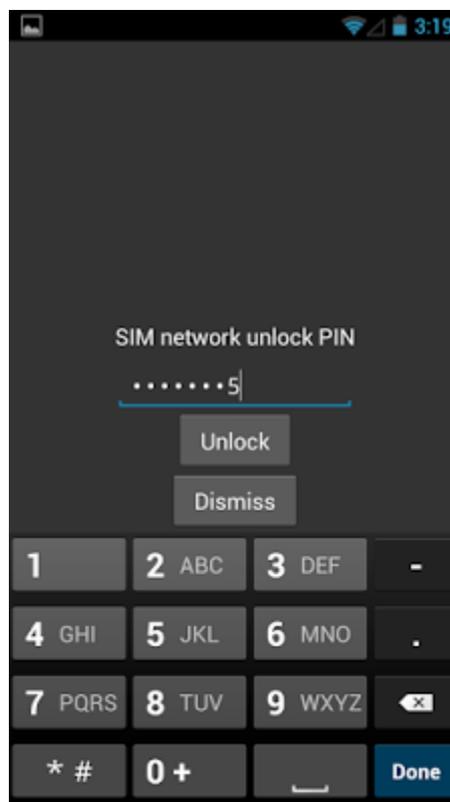
Es el bloqueo que habilitan los operadores en el terminal para que no lo puedan usar con SIM Card de otras operadoras.





¿Qué es Unlock o Desbloqueo?

Es la acción de liberar los teléfonos que cuentan con SIM Lock activo, existen varias formas de desbloqueo.



Existen distintas formas de desbloquear teléfonos Móviles, entre las que podemos mencionar: Códigos, Software y Cable, BOX Unlock y SIM Unlock. Todas estas herramientas son específicas, muchas veces dependen del modelo y marca del teléfono al que apuntamos.

Principales Bloqueos:

1-Bloqueo de SIM (Tarjeta SIM/Chip).

2-Bloqueo de Teléfono, pide algún código al encender el celular.

- 3-Liberación de Banda (de los diferente operadores)
- 4-Desbloqueo o Cambio de IMEI (cuando el equipo fue perdido o robado)

Los principales métodos de Unlock son:

- 1-Liberación por IMEI: Introduciendo un Código de desbloqueo.
- 2-Liberación por Software y Cable:
- 3-Box y Logs:
- 4-SIM de liberación:

1-Liberación Por IMEI

IMEI



International Mobile System Equipment Identity, (Sistema Internacional para la Identidad de Equipos Móviles) es un código **USSD** pre-grabado en los teléfonos móviles **GSM**. Este código identifica al aparato inequívocamente a nivel mundial, y es transmitido por el aparato a la red al conectarse a ésta.

Esto quiere decir, entre otras cosas, que la operadora que usamos no sólo conoce quién y desde dónde hace la llamada (**SIM**) sino también desde qué terminal telefónico la hizo.

La empresa operadora puede usar el **IMEI** para verificar el estado del aparato mediante una base de datos denominada **EIR** (Equipment Identity Register).

El **IMEI** permite funciones como el bloqueo de terminales móviles en caso de robo, para lo cual simplemente tendremos que notificar el **IMEI** del móvil a nuestra operadora de telefonía para que proceda su bloqueo y así pueda impedirse la comunicación hacia ese dispositivo mediante el bloqueo de llamadas. También es posible liberar un teléfono móvil bloqueado para su uso con una nueva operadora móvil a partir del código **IMEI**, independientemente de la marca o modelo.

El **IMEI** de un aparato habitualmente está impreso en la parte posterior del equipo, bajo la batería, en el caso de dispositivos que contienen batería interna este puede encontrarse al reverso en la parte inferior del equipo en números pequeños, en algunos casos también puede llegar a encontrarse en el puerto donde se ingresa la tarjeta **SIM** (Chip). Asimismo, se puede marcar el código **USSD** siguiente ***#06#** (asterisco, almohadilla, cero, seis, almohadilla) para que aparezca en la pantalla del dispositivo.

Estructura

El **IMEI** es normado por la 3GPP y el documento TS 23.003, tiene **15 cifras** (en algunos teléfonos 14, se omite el último dígito SPARE, normalmente un 0). Los **IMEI** que contengan la secuencia "17", sus 2 últimos dígitos no se emplean "00". El **IMEI** se subdivide en varios campos TAC, FAC, SNR y SPARE. El código de **IMEI** consta de cuatro partes y sigue el siguiente esquema: XXXXXX YY ZZZZZZ W.

La primera parte (XXXXXX), los 6 primeros caracteres, se denomina Type Allocation Code (TAC), en donde los primeros dos dígitos indican el país de fabricación del equipo.

La segunda parte (YY) es el Final Assembly Code (FAC) e indica el fabricante del equipo.

La tercera parte (ZZZZZZ), compuesta de seis caracteres, es el número de serie del teléfono (SNR).

El último dígito (W), es el dígito verificador o Spare, usado para verificar que el **IMEI** es correcto.

EIR

La **EIR (Equipment Identity Register)** es una base de datos en la que existe información sobre el estado de los teléfonos móviles. Dentro de esta base de datos existen tres listas de **IMEI**: la blanca, la gris y la negra.

La lista blanca: Identifica a los equipos que están autorizados para recibir y realizar llamadas. Esta lista debe siempre existir en el **EIR**, aun cuando sea la única; las otras dos son opcionales.

La lista gris: Identifica a los equipos que pueden hacer y recibir llamadas, pero que pueden ser monitoreados para descubrir la identidad del usuario utilizando la información almacenada en el chip SIM.

La lista negra: Identifica a los equipos a los que se les impide conectarse a la red. Contiene los identificativos de los equipos robados o utilizados de forma ilegal y también la de aquellos equipos que no pueden acceder al sistema porque podrían producir graves problemas técnicos; por lo tanto, no pueden realizar ni recibir llamadas.

Proceso de Liberación o desbloqueo por IMEI

1-Obtener Información:

Primero obtener el **IMEI**, que lo puedes ver debajo de la batería o marcando ***#06#** en la pantalla del móvil. Es un código de 15 dígitos el cual debes entregar SIN FALLOS, tal y como viene escrito, si no la liberación no se llevará a cabo correctamente.



-Número IMEI (15 dígitos)

- Marca y modelo del terminal
- Operador de origen del terminal.
- Email o nº de teléfono del cliente/usuario: para contacto.

Con esos datos, YA se puede realizar la liberación de un terminal.

2-Comprar Código de Liberación o Desbloqueo.

Existen diferentes Empresas dedicada a esto, para revendedores y profesionales

- Darse de alta en una empresa para profesionales.
- Comprar créditos.
- Facilitar la información obtenida del terminal que vamos a liberar.
- Introducir el código de liberación o desbloqueo.

3-Proceso de introducir el código de liberación en el terminal bloqueado.

El código de liberación se introduce siguiendo unas instrucciones, lo introducirá en el terminal y quedará libre para siempre, actualices lo que actualices y hagas lo que hagas, el teléfono quedará libre para siempre. No necesitas conocimientos informáticos ni ser un iluminado de los teléfonos para hacerlo, hasta un niño pequeño que sepa leer medianamente bien y darle a las teclas de un teléfono podría hacerlo.

¿De dónde sacan el código estas empresas?

Los códigos vienen directamente de las operadoras móviles o del fabricante, depende del tipo de servicio. **Samsung**, tiene un servicio de operador, por ejemplo, **Vodafone**, el cual es más barato que su servicio por fabricante, en nuestro país, España, por ejemplo el nombre del servicio es **Samsung Europa**. El servicio de fabricante es más caro que el del operador, pero los tiempos de entrega por norma son mucho más rápidos y no existe fallo en los códigos si los datos son correctos, cosa que si puede pasar en el servicio por operador. Además, el servicio de **Samsung Europa** ofrece más códigos, como el de resetear el contador de oportunidades de introducción del código de liberación. Y así con más marcas.

Mitos que corren por Internet o por el boca a boca

La liberación por **IMEI** es una actividad que se considera dentro del sector de la Telefonía móvil, es un servicio que se le ofrece a usuarios que no quieren esperar a terminar su contrato para que la operadora a la que pertenecen les dé un código de liberación que, aparte de que te "torean" para dártelo, a veces ni te lo dan. Y eso si es ilegal, según la legislación Española, una vez terminado el contrato la operadora está obligada a liberarte el teléfono siempre y cuando el cliente lo pida.

La liberación por **IMEI** NO anula la garantía del terminal. Todos los móviles/Smartphone vienen preparados para que sean liberados, y tú estás en tu derecho de tener tu móvil libre. Además este sistema, a diferencia del cable o de los nuevos métodos de liberación que aparecen en Android (editando archivos internos del teléfono) NO modifica el software ni hardware del teléfono, con lo cual no pueden dejarte sin garantía por ello.

2-Liberación por Software

Este método consta de un Servidor (PC principal) donde se encuentran todos los códigos y responde a las peticiones de los clientes, en el otro extremo se encuentra la PC cliente que consta de un software que se conecta con dicho servidor a través de Internet o un acceso telefónico.

Se puede liberar bien por el operador al cual pertenece el teléfono o por el modelo del teléfono, esto depende del servicio que nos ofrece el servidor de códigos.

Es necesario tener el **Cable Unlock** correspondiente al modelo de teléfono, ya que la liberación se produce mediante el uso de un componente ActiveX (es decir el acceso a una serie de funciones de una aplicación a través de un sitio Web), entre el servidor y la PC, el servidor lee los códigos de bloqueo del teléfono, enviándole al mismo el LOG con los códigos de desbloqueo, quedando la terminal liberada en segundos.

Para todo esto es necesario realizar el previo pago del o los logs, para poder recibir por correo electrónico un usuario y contraseña para poder conectarse al servidor.

¿Cómo Funciona el Software?

Debe conectar el cable al teléfono apagado.

1-Ejecute el software.

2-Introduzca el nombre de usuario y la contraseña que le envía el proveedor

3-Haga click sobre Info. y le dirá los logs disponibles.

4-Haga click sobre el botón UNLOCK.

5-El software dará el mensaje ¡¡TURN ON THE PHONE!!

6-Encienda el teléfono. Aparecerá el mensaje LOCKS CLEARED SUCCESFULLY.

7-El teléfono estará libre.

3-Liberación por Box

¿Qué es una BOX UNLOCK?

Una BOX UNLOCK es una interface que nos permite interactuar con el terminal a través de una PC o Notebook, con el fin de realizar modificaciones del software del teléfono.

Las **BOX** o **CAJAS DE LIBERACION**, sirven para reparaciones vía Smartphone-Box-Ordenador; se emplean para liberar, flashear y en algunos casos para reparar el **IMEI** de los terminales que han sido dañados.

La mayoría de estas están separadas por Marca de fabricante, habiendo muchas cajas solo para Nokia, para Samsung, para Sony, etc. También existen cajas de tipo Multimarca que soportan a varias marcas (Su principal diferencia es que no tienen un soporte completo en estas).

La mayoría de estas cajas trabajan con la PC y el terminal a través de un software es decir que la caja está conectada a la PC y a partir de la caja esta nace el cable que va al terminal; así por medio de una serie de opciones y procesos: **Flashear, Actualizar, Desbloquear, Reparar IMEI**, etc.

Sigma Box Full Set con Cables: Especial para: Alcatel, MTK, ZTE, Motorola y Huawei



1-Lectura de códigos/liberación: Liberación directa de Alcatel, Motorola, ZTE y otras marcas MTK, y también Huawei con tipos de defensa viejos y nuevos

2-Cálculo de códigos para liberación por IMEI:

- Modelos soportados: Alcatel / Motorola / Orange / TCL / Vodafone / T-Mobile / TMN / ZTE
- No se requiere conexión a internet
- Solución totalmente autónoma, que no requiere códigos del servidor o créditos
- Posibilidad de reparar número ilimitado de terminales al día

3-Flasheo/Copia de reserva (Backup)

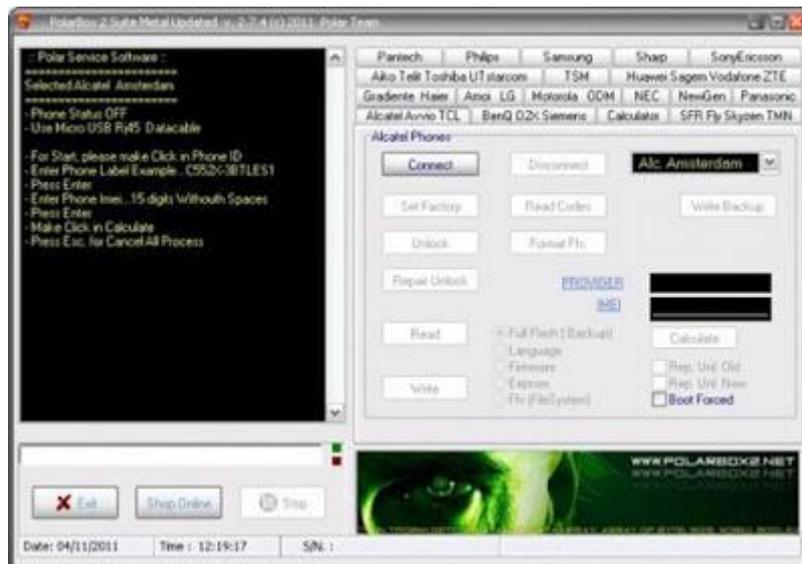
- Cálculo de códigos para liberación por IMEI
- Flasheo/Copia de reserva (Backup)
- Archivos de flasheo para Sigma se almacenan en el formato *.skf
- Lectura de versión del firmware del teléfono
- Velocidad del puerto COM – hasta 921600 bit/s
- Lectura y recuperación de copias de reserva
- Actualización del firmware (copia de reserva de un teléfono a otro)
- Actualización y degradación de versión del firmware
- Actualización correcta del firmware para celulares Alcatel (trabaja con el área CUST PARA)
- Modo de "grabación inteligente" (modo rápido)
- "Modo normal" de grabación
- Trabaja con los tipos de memoria flash NAND y NOR

TUTORIAL

EN BREVE....

Polar Box 3 Full Activación con 27 Cables: Multimarca: Samsung, LG, Alcatel, HTC, Huawei, LG, Motorola, ZTE





Polar Box Una de las Cajas Multiplataforma más Versátiles del mercado:

- Liberación directa.
- Liberación por lectura de códigos.
- Flasheo.
- Lectura y Escritura Flash.
- Reparación IMEI.
- Cambio de idiomas.
- Reparación y Flasheo para más de 50 marcas y 1200 modelos de móviles.
- Actualizada y Soportada continuamente desde 2006
- Interfaz muy sencilla de utilizar (la mayoría de los procesos con 2-3 clicks)
- Ideal para empezar a liberar
- La mejor de mundo soportando la marca Alcatel
- Sistema de Auto-Backup, evita perder o dañar el terminal.

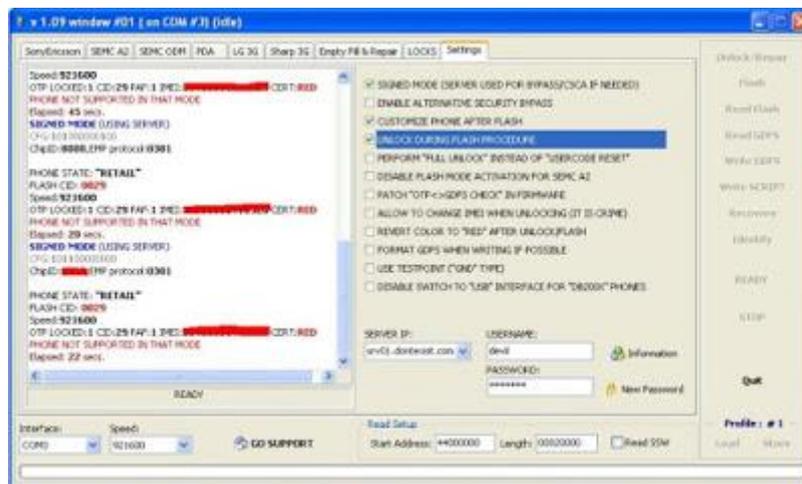
Instalación

- 1-Descargar última versión del Software instalador desde la web oficial.
- 2-Ejecutar el instalador Polar Box Update.
- 3-Conectar el Cable USB de la Polar Box a la PC.
- 4-Instalar los Drivers (Equipo/Propiedades/Adm. Disp./Otros Disp/Polar Box/Clic derecho actualizar
- 5-Registre la Polar Box.
 - 5.1-Iniciar Polar SAT.
 - 5.2-Request box certificate

Liberación Directa

- 1-Iniciar Programa.
 - 1.1-Habilitar Depuración USB.
- 2-Seleccionar marca del terminal.
 - 2.1-Seleccionar Modelo del terminal.
 - 2.2-Seguir instrucciones.
 - 2.3-Seleccionar Función conectar.
- 3-Seleccionar Función Unlock.

SETOOL BOX 3; SELG FUSION BOX: SONY/LG



SETOOL BOX 3

- Liberación de todos los CID soportados (16/29/36/49).
- Reparación de todos los CID soportados (16/29/36/49).
- Escritura de idiomas de todos los CID soportados (16/29/36/49).
- Flasheo de todos los CID soportados (16/29/36/49).
- Actualización de firmware de todos los CID soportados (16/29/36/49).
- Lectura/escritura de la zona GDFS y todos sus parámetros (e.g. security, battery, calibration, etc) -
- Lectura de datos de todos los CID soportados (16/29/36/49).
- Escritura y sustitución de archivos personalizados (mp3, fotos, tonos, cambio de SMS tones, etc.).
- Despersonalización de todos los CID soportados (16/29/36/49).
- Lectura del código de seguridad de todos los CID soportados (16/29/36/49).
- Eliminación del sonido de la cámara de fotos de todos los CID soportados (16/29/36/49).
- Reseteo total del tiempo de llamada de todos los CID soportados (16/29/36/49).
- Repara el área GDFS dañada de todos los CID soportados (16/29/36/49).
- Cambia el número CDA y la revisión de todos los CID soportados (16/29/36/49).

- Cambia las cerraduras de las bandas de todos los CID soportados (16/29/36/49).
- Reparación de IMEI de todos los CID soportados (16/29/36/49).
- Flasheo ultrarápido vía USB para cualquier CID (16/29/36).
- Hasta 16 terminales soportados al mismo tiempo.
- Liberación de todas las versiones.
- Reparación de todas las versiones.
- Flasheo y cambio de idiomas.
- Flasheo de todas las versiones de los terminales soportados.
- Flasheo "forzado".
- Lectura y copia de seguridad de la zona GDFS y de todos sus parámetros.

Instalación

- 1- Descargue Setool Card Version.
- 2- Extraer el archivo zip.
- 3- Conecte su Setool USB.
- 4- Aparecerá el asistente para instalar nuevo hardware.
- 5- Elija "Instalar desde un lugar específico"
- 6- Seleccione los drivers/ en la carpeta card drivers folder, por ejemplo:
desktop/setool_card/drivers/card_drivers
- 7- Clic en OK y Windows encontrará el egate card reader y lo instalará
- 8- Reinicie su PC

Registro y Acceso

- 1- Visite <http://www.setool.net/support/> Los usuarios pueden encontrar el mejor soporte y las más rápidas actualizaciones aquí!
- 2- Complete todos los campos con la información CORRECTA.

Nombre: Elija un login para el área de soporte Setool

Password: Elija una clave de su elección.

Reingrese el Password: Ingrese nuevamente su clave.

E-mail: Proporcione una cuenta de e-mail válida.

ICQ: (Para facilitar el contacto on-line con el soporte)

Reseller: El revendedor con el cual obtuvo su Setool

Date of Purchase: Fecha de compra

Reseller price: Cuanto pago por el producto (varía entre proveedores).

Old or New customer: Usted ya tiene Setool2 UFS? O es un nuevo cliente de Setool3?

Location: Por favor, proporcione datos reales de su localización.

Dongle ID: El numero serial de su Box S/N (0000XXXX) - El texto íntegro en negro (número).

OCTOPLUS BOX: Samsung, LG





OCTOPLUS BOX

- Liberación directa
- Desbloqueo de todo tipo de bloqueos
- Grabación de firmware, FullFlash, datos de calibración
- Lectura de FullFlash, datos de calibración
- Lectura de versión de firmware
- Restablecimiento de ajustes de fábrica
- Soporte para teléfonos LG 3G-Cyon-Show-FOMA
- Soporte para teléfonos Anycall
- Reparación de IMEI
- Lectura de cargador (boot)/ flash
- Grabación de cargador (boot)/ flash
- Borrado de cargador (boot)/ flash
- Reparación de cargador (boot)/ flash
- Interface multilingüe: inglés, español, portugués, rumano, ruso, ucraniano, árabe, húngaro.

CHIMERA TOOL (Samsung, BlackBerry y Nokia)





Samsung

Direct unlock ([Supported Models](#))

Read unlock codes (NCK, etc)

IMEI repair ([Supported Models](#))

Most Qualcomm models can be unlocked without rooting (KNOX will not void)

Reading out all available software informations like software version, unique serial, [simlockstate](#), etc.

Read / Write certificate

Software update to any version with one click. (Firmware will be downloaded and flashed automatically - first in the world)

Manual root is not required, ChimeraTool will do it for you

Root / Unroot function

Repair damaged calibration data (mostly it is called NV_ITEM)

Backup / restore security fields, EFS

Backup calibration data

'Public beta' model statuses for testing purposes (you can read more about this [here](#))

Remove Factory Reset Protection (FRP) lock

Remove Google Accounts

Reset reactivation lock



Blackberry OS10 functions:

Direct unlock - first in the world

Remove BB Protect also known as "Anti-Theft Protection" if you do not know the original email/pass - first in the world

Flashing support to any OS 10 version, of course also to the recent one

Read detailed phone information, such like PIN number, etc..

Wipe unknown phone password, user data

Blackberry OS 5, 6, 7 functions:

Direct unlock (MEP0 reset is supported on all models)

Backup BlackBerry security fields

Restore BlackBerry security fields

Refurbish on all OS7 models (repairs 100% of software problems)

Change Vendor ID (Logo remove / Change to any logo)

Change Keyboard layout (QWERTZ, QWERTY, AZERTY)

Enabling Camera auto-detect

Enabling LCD auto-detect (you can place any type of LCD)

IMEI repair ([Supported Models](#))

Auto turn on (phone will turn on automatically after inserting the battery)

Turn Java on (for only a white screen at start and can not continue problem)

Fixing APP errors ([BlackBerry App error codes](#))

Ability to flash own module list in 2 method full and minimum (like official updater)

After connecting your BlackBerry to the computer it takes just 2 clicks to install the latest firmware/languages

You can add / remove any of the available languages to your phone

Reading out all informations from your BlackBerry like IMEI, Carrier lock ([sim-lock](#)), software version, etc.

You can also unlock your phone by calculating the correct code (MEP based calculation, except OS10)

Nuke function for deep formating internal memory and resetting user code if it is not known



LG functions:

Network unlock without root, just 5 seconds

IMEI repair without root, just 45 seconds

Safe unlock, IMEI will remain original

Dual SIM phones are supported without further network or IMEI problems

Read phone informations

WiFi & MAC address repair function



Lumia Windows 7 functions:

Read the factory NCK from phone: Forget modem patch based unlocks, this one is the best permanent solution

Factory modem reset: If you damaged somehow both modem filesystem copies, this will most likely fix the problem. NCK counter can be reset by this way too

Flash Qualcomm bootloader: You can upload custom windows images later / root the phone

Flash DLOAD bootloader to a Qualcomm bootloader phone, so you can update it with official Nokia Tools. We also fix the problem where DLOAD doesn't work, because the keystore has been damaged in qualcomm mode. No need to worry about that anymore, we guarantee that DLOAD and software update will work properly.

IMEI repair function can be used if your phone doesn't have the original serial number or if it has been damaged while any procedure you did before

Firmware upgrade to the most recent version

Lumia Windows 8, 10 functions:

Read detailed phone informations

Firmware upgrade

Repair dead, bricked phones with a single USB cable

[TUTORIALES EN BREVE....](#)

4-Liberacion con SIM UNLOCK

EN BREVE