

Guía de Seguridad de las TIC

CCN-STIC 1640

Procedimiento de empleo seguro

Sotera Phone H1U



Diciembre de 2024





Catálogo de Publicaciones de la Administración General del Estado

<https://cpage.mpr.gob.es>

Edita:



Pº de la Castellana 109, 28046 Madrid

© Centro Criptológico Nacional, 2022

NIPO: 083-24-316-0.

Fecha de Edición: diciembre de 2024.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

ÍNDICE.....	2
1. INTRODUCCIÓN	4
2. OBJETO Y ALCANCE	5
3. ORGANIZACIÓN DEL DOCUMENTO	6
4. FASE PREVIA A LA INSTALACIÓN.....	7
4.1 ENTREGA SEGURA DEL PRODUCTO	7
4.2 REGISTRO Y LICENCIAS	8
4.3 CONSIDERACIONES PREVIAS	8
4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN.....	8
5. FASE DE INSTALACIÓN.....	10
6. FASE DE CONFIGURACIÓN	13
6.1 MODO DE OPERACIÓN SEGURO	13
6.2 AUTENTICACIÓN.....	13
6.3 ADMINISTRACIÓN DEL PRODUCTO.....	13
6.3.1 ADMINISTRACIÓN LOCAL	13
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES	14
6.4 SINCRONIZACIÓN	14
6.5 ACTUALIZACIONES	14
6.6 AUTO-CHEQUEOS.....	15
6.7 AUDITORÍA	15
6.7.1 REGISTRO DE EVENTOS	15
6.7.2 ALMACENAMIENTO LOCAL	16
7. FASE DE OPERACIÓN	17
7.1 USO DE LA APLICACIÓN DE CONTACTOS (“CONTACTS”)	17
7.1.1 CREACIÓN DE CONTACTO	17
7.1.2 CONSULTA Y BÚSQUEDA.....	19

7.1.3 ACCIONES DE CONTACTO	19
7.2 USO DE LA APLICACIÓN DE LLAMADAS VOIP (“DIAL”)	20
7.2.1 LLAMADAS DE VOZ	21
7.2.2 HISTORIAL DE LLAMADAS.....	22
7.2.3 BUZÓN DE VOZ	23
7.3 USO DE LA APLICACIÓN DE MENSAJERÍA (“MESSAGES”)	25
7.3.1 CONVERSACIONES	25
7.3.2 ENVÍO Y RECEPCIÓN DE MENSAJES.....	26
7.3.3 BÚSQUEDA DE MENSAJES	30
7.4 USO DE LA APLICACIÓN DE AJUSTES (“SETTINGS”)	31
7.4.1 PROCEDIMIENTO DE RESETEO DE FÁBRICA	32
7.4.2 PROCEDIMIENTO DE CAMBIO DE CONTRASEÑA	33
7.4.3 PROCEDIMIENTO DE ACTUALIZACIÓN DE SOFTWARE.....	35
7.4.4 CONFIGURACIÓN DEL TIEMPO DE INACTIVIDAD	37
8. REFERENCIAS	39
9. ABREVIATURAS.....	40

1. INTRODUCCIÓN

El Sotera Phone H1U es un teléfono inteligente que se encuentra dentro de la familia de productos “Dispositivos Móviles”. El Sotera Phone H1U se caracteriza por utilizar un sistema operativo en tiempo real llamado Integrity RTOS 178B y por disponer de una serie de aplicaciones básicas preinstaladas, sin posibilidad por parte del usuario de instalar aplicaciones adicionales. El usuario puede hacer uso exclusivamente de una aplicación de agenda de contactos (“Contacts”), una de llamadas VoIP (“Dial”), una de mensajería instantánea (“Messages”) y una aplicación de ajustes (“Settings”).

Además, el producto proporciona a los usuarios la capacidad de proteger la información en reposo (data at rest), incluyendo los datos del usuario y de las aplicaciones móviles almacenados en la partición de datos del usuario. El producto utiliza una jerarquía de claves que combina una clave de cifrado con la contraseña del usuario para proporcionar protección a todas las claves criptográficas de usuario y de aplicaciones almacenadas en el producto.

El producto no dispone de una interfaz específica de administración, realizándose las labores relacionadas exclusivamente a través de la interfaz de usuario del dispositivo, una vez este ha sido desbloqueado. Es posible extraer registros de auditoría del dispositivo a través de USB, mediante herramientas proporcionadas por el fabricante.

Durante el inicio del Sotera Phone H1U, el dispositivo pasa por distintos niveles diferentes de ejecución que incluyen de manera secuencial: un cargador de arranque inmutable llamado BootROM, un cargador de arranque de la plataforma llamado Preloader, un cargador de arranque del SO llamado Bootmonitor y finalmente el sistema operativo de Integrity.

Por último, el producto solicita a los servidores del fabricante actualizaciones de firmware a través de un canal seguro. Tanto la integridad como la autenticidad de estos paquetes de actualización es verificada antes de proceder con la instalación. Los paquetes OTA son firmados con una clave privada que el producto verifica utilizando su parte pública.

2. OBJETO Y ALCANCE

Esta guía es compatible con el siguiente dispositivo y versión:

- Modelo hardware: Sotera Phone H1U
- Versión del firmware: 0.455 (Integrity RTOS 178B)

3. ORGANIZACIÓN DEL DOCUMENTO

Este documento se compone de los siguientes apartados:

- a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
- b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
- c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- d) Apartado 7. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Para verificar que el dispositivo ha sido recibido de manera segura y que su firmware no ha sido manipulado, se deberán de seguir los siguientes pasos:

1. Encender el producto y comprobar que no aparece ningún mensaje de error, garantizando de esta manera que el firmware es auténtico e íntegro.
2. Verificar que el logo del fabricante se muestra durante el inicio. Esto indica que el producto está ejecutando una versión del firmware destinada al usuario final.



3. Verificar que una vez completado el inicio del producto, se muestra una pantalla de bienvenida y no una pantalla de bloqueo. Esto garantiza que el dispositivo ha sido restaurado de fábrica y no contiene información de posibles instalaciones anteriores.

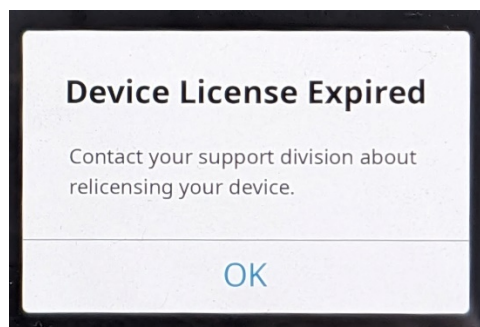


4. Una vez verificado el entorno de operación descrito en la sección **4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN**.
5. Verificar modelo y versión del producto: ir a "Settings" > "About" > "Software & Hardware Version" y comprobar que el modelo ("Model") y firmware ("Software Version") corresponden con el declarado en la sección **2 OBJETO Y ALCANCE**.

4.2 REGISTRO Y LICENCIAS

El producto requiere de una licencia activa para su uso. El usuario final no ha de seguir ningún proceso en el dispositivo para su activación, siendo el fabricante el encargado de esto. El producto realizará peticiones a un servidor de licencias del fabricante para verificar la validez de la licencia asociada al número de serie del dispositivo.

En caso de que el producto no sea activado correctamente, se mostrará un mensaje de alerta indicando el problema y sólo se le permitirá al usuario acceder a la configuración del dispositivo. No será posible acceder a la funcionalidad principal del dispositivo como mensajería, llamadas o gestión de contactos.



El administrador del dispositivo se pondrá en contacto con el fabricante o en su defecto, un representante para resolver posibles problemas con el estado de la licencia.

4.3 CONSIDERACIONES PREVIAS

Para hacer uso de toda la funcionalidad disponible en el dispositivo, es necesario disponer de una conexión a internet. Dado que el sistema operativo no permite conexiones WI-FI, se requiere introducir una tarjeta SIM con un plan de datos móviles activo. Además, para el correcto funcionamiento de esta es estrictamente necesario que se le haya deshabilitado completamente el PIN de la tarjeta con anterioridad.

Por último, cabe destacar que el Sotera Phone H1U sólo permite comunicaciones con otros dispositivos de Sotera. Es decir, no es posible enviar SMSs ni hacer llamadas de teléfono estándar a dispositivos móviles tradicionales.

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

Dada la naturaleza online del producto, se requieren una serie de servidores externos para su correcto funcionamiento. A continuación, se listan los servicios requeridos durante un uso normal del producto:

- **Servidor de licencia:** Encargado de comprobar la validez de la licencia del producto.

- **Servidor de actualizaciones:** Encargado de distribuir actualizaciones Over-The-Air (OTA).
- **Servidor de sincronización de reloj:** Encargado de mantener actualizada la fecha y hora del producto mediante el protocolo NTP.
- **Servidor de revocación de certificados:** Encargado de mantener actualizados los certificados del producto mediante Listas de Revocación de Certificados (CRL).
- **Servidor de mensajería y llamadas:** Encargado de gestionar todas las comunicaciones relacionadas con la funcionalidad de mensajería instantánea y llamadas VoIP.

5. FASE DE INSTALACIÓN

Encender el teléfono y seguir los pasos descritos en la sección **4.1 ENTREGA SEGURA DEL PRODUCTO**.

Una vez encendido, y pendiente de comprobar la versión del dispositivo, llevar a cabo los siguientes pasos para realizar la instalación:

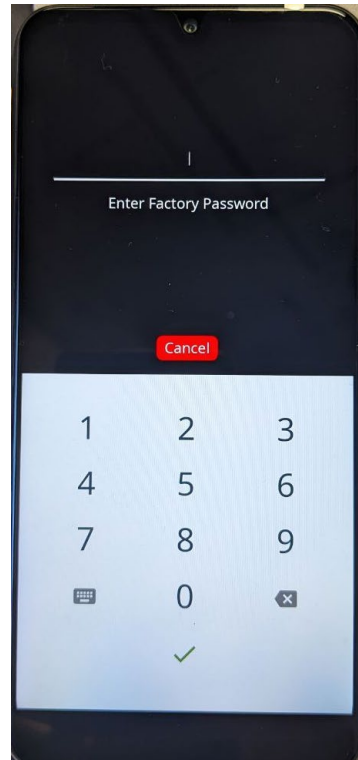
1. Enciende el dispositivo y verifica que no se muestra por pantalla ningún código de error durante el inicio.



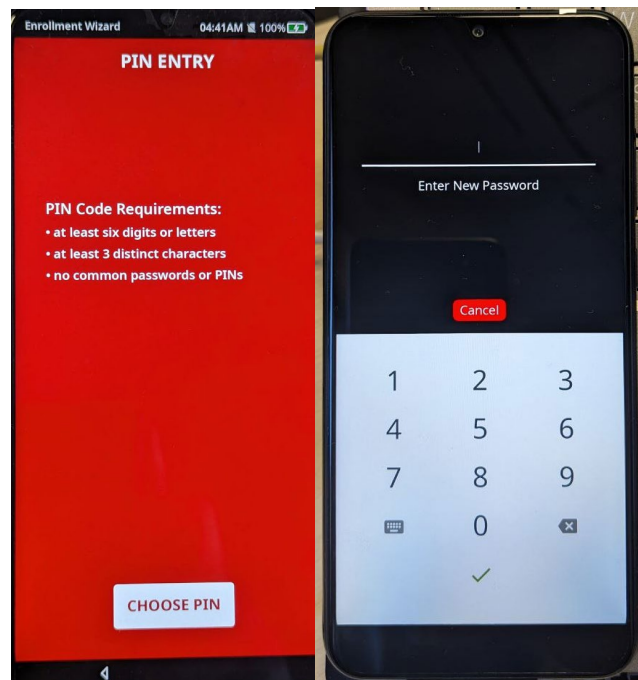
2. Una vez iniciado el sistema operativo, verifica que se muestra una pantalla de bienvenida.



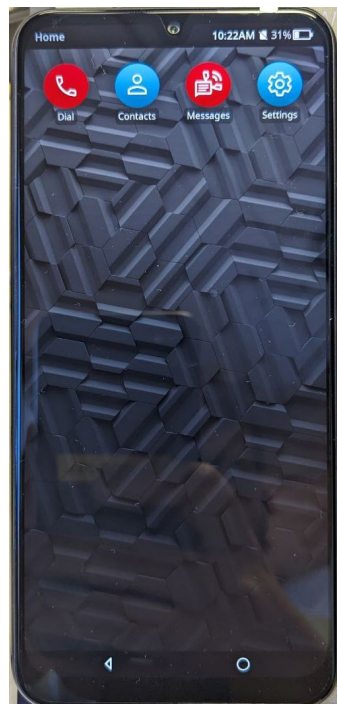
3. Pulsar en “LET’S GET STARTED” e introducir la contraseña de fábrica. Se trata de una contraseña que el fabricante vincula al hardware y que este ha de proporcionar al usuario a través de un canal seguro.



4. Pulsar en “CHOOSE PIN” para fijar una contraseña de bloqueo del dispositivo. La contraseña o PIN ha de seguir las restricciones mostradas por pantalla:
 - a. Mínimo de 6 dígitos o letras.
 - b. Mínimo de 3 caracteres distintos.
 - c. Prohibido el uso de contraseñas o pines comúnmente utilizados.



5. Introducir la contraseña o PIN una segunda vez a modo de confirmación.
6. Verificar que el dispositivo accede a la pantalla de inicio del sistema operativo.



6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Tras la fase de instalación, el dispositivo ya parte de un modo de operación seguro. Es decir, no se requiere realizar ninguna configuración adicional por parte del usuario. Es recomendable que el operador sea consciente de las actualizaciones y se mantenga la versión del producto objeto de este documento. Para comprobar la versión instalada acceder a “Settings” > “About” > “Software & Hardware Version”.

6.2 AUTENTICACIÓN

Un usuario puede autenticarse en el dispositivo haciendo uso de autenticación: PIN o contraseña.

Las restricciones aplicadas en la sección anterior aplican a ambas y se consideran equivalentes, por lo que el usuario es libre de decidir el mecanismo en función de las garantías que necesite.

En cualquier caso, los datos del usuario solo son accesibles únicamente cuando se desbloquea (autentica) por primera vez tras el encendido de la Tablet. Hasta entonces, permanecen cifrados con una clave interna que se deriva de la entrada del usuario.

Además de esto, un usuario debe autenticarse antes de ejercer la mayor parte de la funcionalidad disponible en el dispositivo. Mientras que el usuario no se autentique, la funcionalidad que puede realizarse en el teléfono es muy limitada, pudiendo únicamente:

- Reiniciar.
- Apagar.
- Ver notificaciones (Sólo si se ha producido anteriormente el primer desbloqueo tras el inicio del dispositivo).

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL

El dispositivo puede administrarse únicamente mediante dos interfaces:

- Interfaz local. El usuario se autentica en el dispositivo y puede acceder a las diferentes aplicaciones y ajustes.
- USB. El dispositivo admite una serie de comandos a través de USB para llevar a cabo tareas administrativas como extracción de logs. Para esto se requiere de software proporcionado por el fabricante.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

El producto es un sistema monousuario, en el que no se hacen distinciones de roles. Es por ello que no existe el concepto de rol o usuario administrador en el dispositivo, sino que toda la configuración será realizada por el usuario final.

Además, la política de contraseñas viene configurada por defecto y no podrá ser modificada. A continuación, se incluyen las políticas de contraseña aplicadas por el producto:

- **Política de fortaleza de contraseña:**
 - Contraseña o PIN de longitud mayor o igual a seis caracteres o dígitos.
 - Contraseña o PIN compuesto por más de dos caracteres o dígitos distintos.
 - Contraseñas o pines no usados comúnmente como “iloveyou”, “qwerty”, “abc123” o “1234”.
 - Posibilidad de usar caracteres especiales ([!, @, #, \$, %, ^, &, *, (,)]), mayúsculas y minúsculas, números y letras.
 - Uso obligatorio de un PIN o contraseña.
- **Política de intentos fallidos:**
 - El dispositivo incrementará el tiempo de bloqueo entre intentos fallidos de desbloqueo siguiendo el siguiente patrón: 0, 0, 0, 10s, 30s, 1min, 2min, 5min, 15min, 60min, 60min, 60min.
 - Tras el decimotercer intento de desbloqueo fallido, el dispositivo se bloqueará permanentemente, borrándose todos los datos de usuario en el siguiente reinicio.

Por último, respecto a la configuración de parámetros de sesión, el usuario podrá configurar el tiempo de inactividad a partir del cual el dispositivo se bloquea automáticamente. Se podrán configurar tiempos de 15s, 30s, 60s, 90s, 5min, 15min o nunca.

6.4 SINCRONIZACIÓN

El producto activa por defecto la sincronización del reloj a través de NTP. El usuario puede optar por deshabilitarlo accediendo a “Settings” > “Date & Time” > “Set Time” > “Set Time Automatically”. Esta opción se debe permanecer habilitada.

6.5 ACTUALIZACIONES

Para recibir actualizaciones, el producto se conecta a los servidores de Sotera. Esta comunicación se hace mediante el uso de mTLSv1.3. Existen dos opciones para recibir actualizaciones:

- Actualizaciones manuales. El usuario, desde la aplicación de Ajustes, puede ir a “About” > “Software Update” y pulsar en “Check for OTA Update” para comprobar si hay actualizaciones disponibles. De existir, el usuario puede decidir si actualizar o no el firmware del dispositivo.
- Actualizaciones automáticas. El usuario puede configurar que el dispositivo consulte de manera periódica si existen actualizaciones disponibles y que se instalen de manera desatendida. Para ello, desde el mismo menú descrito en el punto anterior, habilitar “Automatic Updates”. Esta opción está habilitada por defecto.

6.6 AUTO-CHEQUEOS

El producto incluye funciones para realizar auto-chequeos y comprobaciones de integridad del software/firmware, de forma que pueda detectar cuándo está fallando o puede estar corrupta. También se realizan comprobaciones durante el inicio para verificar que las implementaciones criptográficas del dispositivo no han sido manipuladas. Para esto, se compararán los resultados generados por los algoritmos contra unos valores de referencia almacenados en el firmware.

Si falla algún auto-chequeo (los cuales se ejecutan al inicio), el producto no entrará en modo operativo. También incluye mecanismos (es decir, verificación de la firma digital de cada nueva imagen) para que el propio dispositivo pueda actualizarse garantizando al mismo tiempo que las actualizaciones no introducirán cambios maliciosos o inesperados en el producto.

6.7 AUDITORÍA

6.7.1 REGISTRO DE EVENTOS

El producto usa diferentes tipos de registros de auditoría para recopilar todos los eventos necesarios:

- **Auditoría USB:** El dispositivo almacena registros de auditoría que pueden ser extraídos mediante USB haciendo uso de una herramienta específica proporcionada por el fabricante. Los registros contienen entre otros datos la fecha y hora del evento, el tipo de evento y su descripción. La consulta de esta fuente de auditoría no está destinada al usuario final sino que su uso se orienta a administradores de sistemas y uso en fábrica.
- **Histórico de llamadas:** La aplicación de teléfono (“Dial”) contiene un registro de llamadas como se muestra en la sección [7.2.2 HISTORIAL DE LLAMADAS](#). Cada entrada contiene el nombre del otro participante, su número de teléfono, fecha y hora y dirección de la llamada.

6.7.2 ALMACENAMIENTO LOCAL

Los registros de auditoría son almacenados localmente y de forma segura en el dispositivo. No es posible extraer información sensible de los registros de auditoría sin autenticación previa, es decir, sin haber desbloqueado el producto. El registro de auditoría USB tiene un tamaño máximo de 1GB y una vez alcanzado el límite, los registros de mayor antigüedad serán reemplazados por los más recientes.

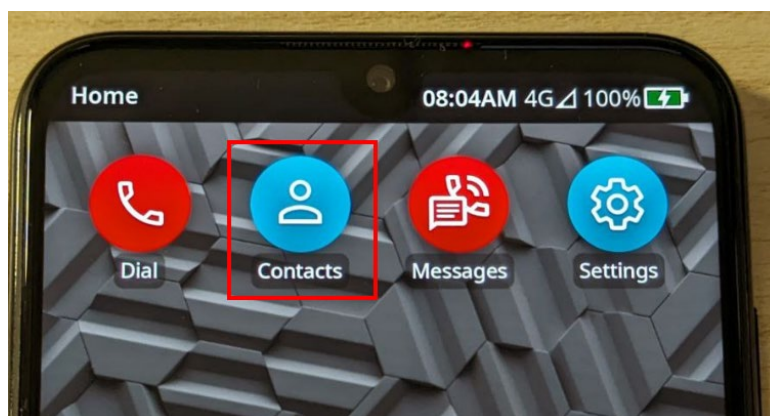
7. FASE DE OPERACIÓN

Los procedimientos operativos mínimos que deben llevarse a cabo durante la fase de operación y mantenimiento del producto son los siguientes:

- Comprobaciones periódicas del *hardware* y *software* para garantizar que no se ha introducido hardware o software no autorizado. Para ello, repetir los pasos descritos en **4.1 ENTREGA SEGURA DEL PRODUCTO**.
- Aplicación regular de las actualizaciones OTA proporcionadas por el fabricante, con objetivo de mantener una configuración segura.
- Mantenimiento de los registros de auditoría. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el usuario podrá acceder a ellos.
- La información de auditoría se consultará y guardará manualmente en las condiciones y el periodo establecido en la normativa de seguridad.
- Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

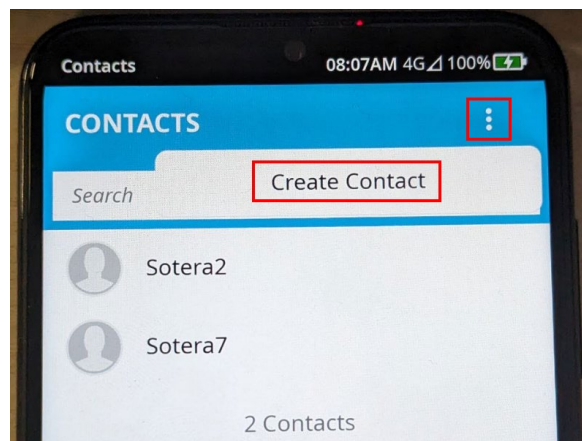
7.1 USO DE LA APLICACIÓN DE CONTACTOS (“CONTACTS”)

La aplicación de Contactos (“Contacts”) actúa como una agenda de contactos tradicional, donde el usuario puede añadir nuevos contactos y consultar los ya existentes. Una vez se accede a la aplicación, se muestra el listado de contactos del usuario junto con un cuadro superior de búsqueda.



7.1.1 CREACIÓN DE CONTACTO

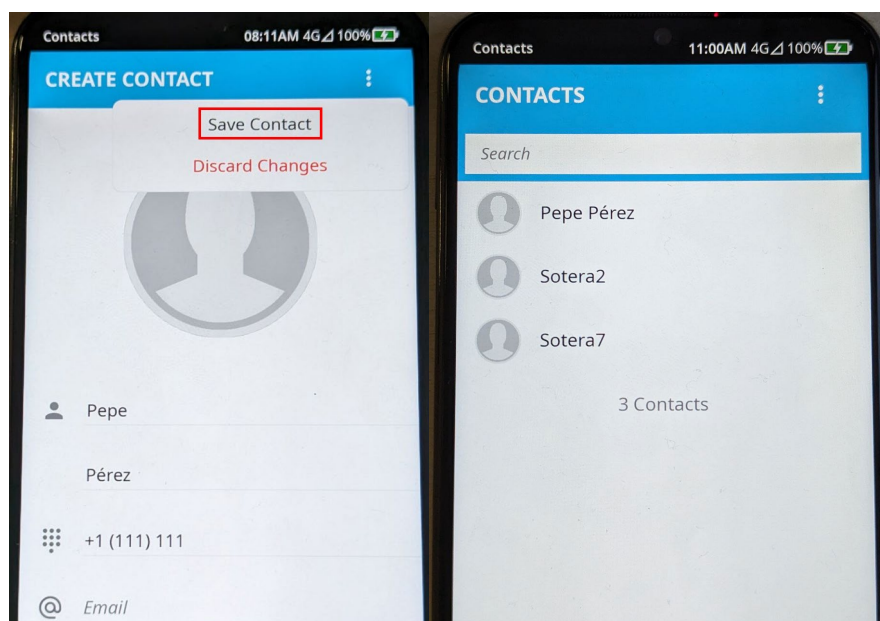
Para crear un nuevo contacto, pulsar en el botón de los tres puntos ubicado en la esquina superior derecha y luego en “Create Contact”.



En la pantalla de creación de contacto, el usuario podrá introducir los siguientes campos:

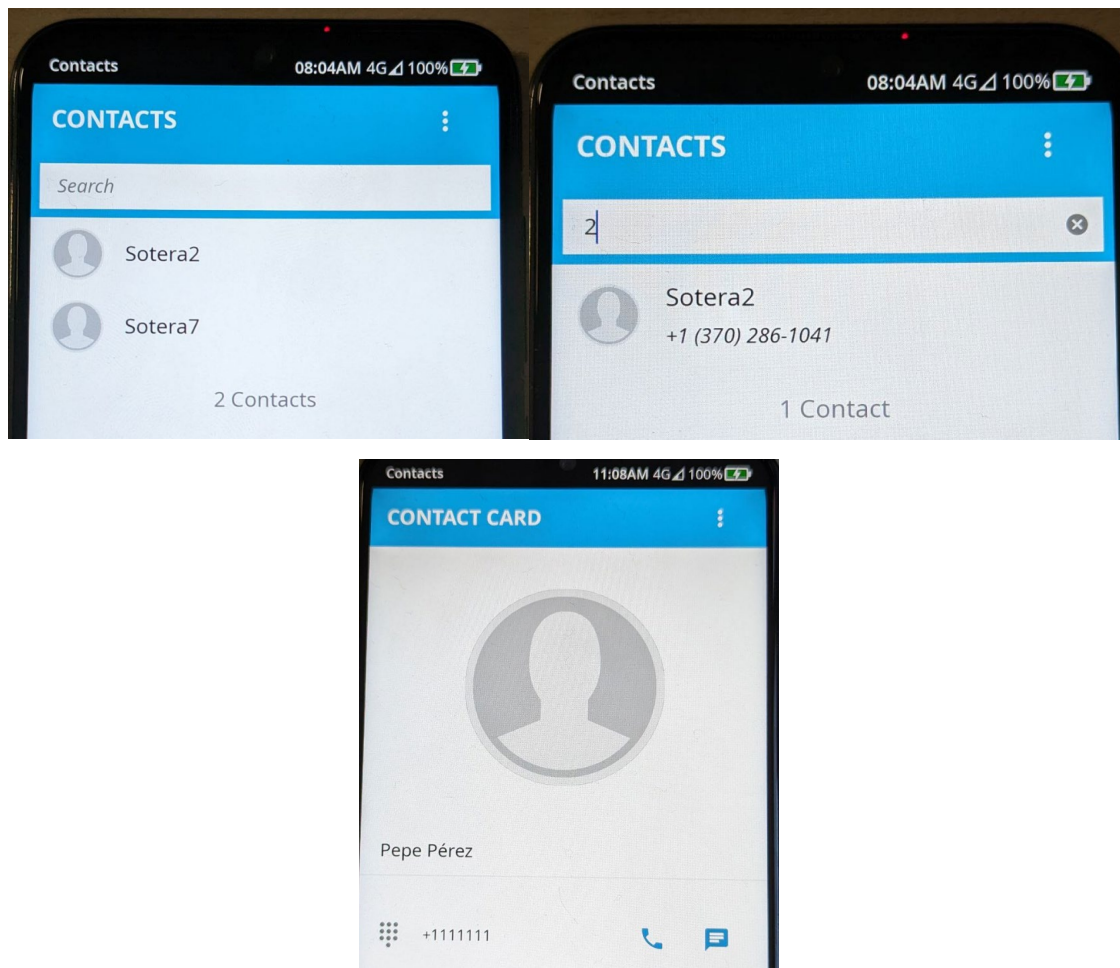
- **Nombre ("First name"):** Nombre del contacto.
- **Apellidos ("Last Name"):** Apellidos del contacto.
- **Número de teléfono ("Secure Phone"):** Número de teléfono asignado al Sotera Phone H1U.
- **Email:** Dirección de correo electrónico. Se trata de un campo opcional y meramente informativo, ya que el dispositivo carece de funcionalidad para enviar y recibir correo electrónico.

Por último, no es posible asignar una imagen de perfil para el contacto, sólo se podrá utilizar el avatar predeterminado por la aplicación. Una vez introducidos los datos del contacto, el usuario podrá guardarlo pulsando en el botón de la esquina superior derecha y luego en "Save Contact".



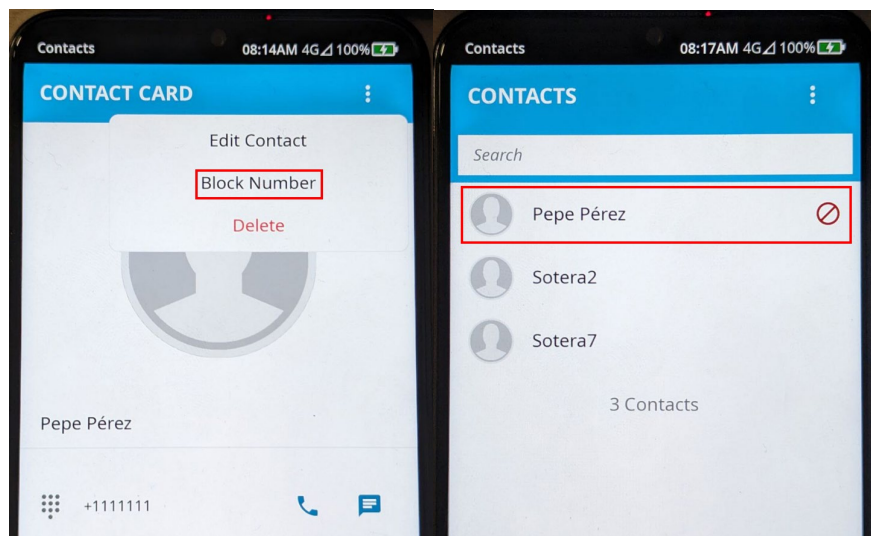
7.1.2 CONSULTA Y BÚSQUEDA

Para acceder a un contacto, pulsar en la entrada correspondiente dentro del listado principal o realizar una búsqueda con el cuadro de búsqueda ubicado en la parte superior de la aplicación.



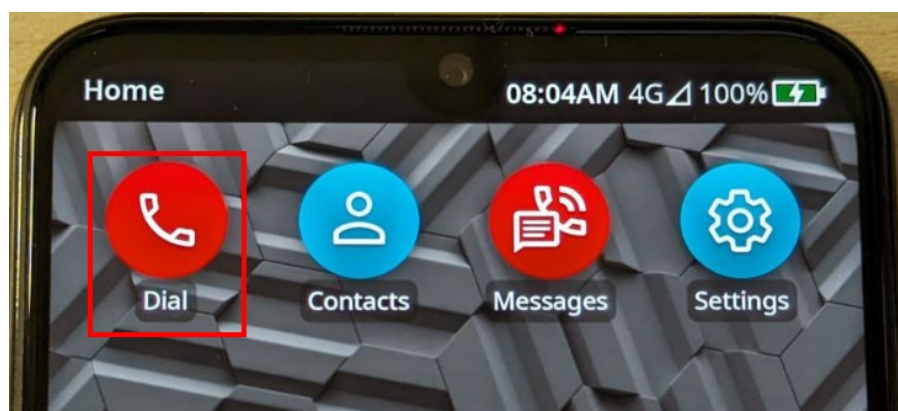
7.1.3 ACCIONES DE CONTACTO

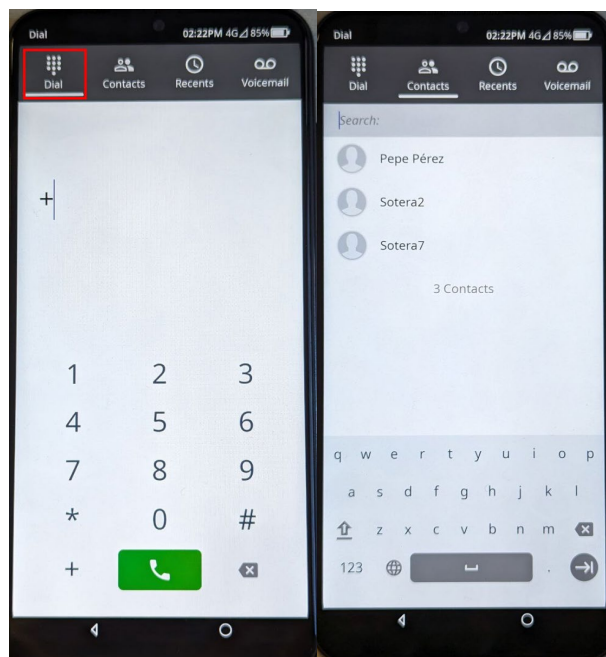
Una vez seleccionado un contacto, el usuario podrá editar su información, bloquear su número o borrar el contacto pulsando en el botón de la esquina superior derecha. Al bloquear a un contacto, el usuario dejará de recibir llamadas y mensajes de este.



7.2 USO DE LA APLICACIÓN DE LLAMADAS VOIP (“DIAL”)

La aplicación de llamadas (“Dial”) permite al usuario realizar llamadas VoIP a otros dispositivos Sotera, ya sea a través de la agenda de contactos o introduciendo el número de teléfono del destinatario. Además, de realizar llamadas, se incluyen pestañas adicionales donde el usuario puede acceder a su listado de contactos, su histórico de llamadas y su buzón de voz.

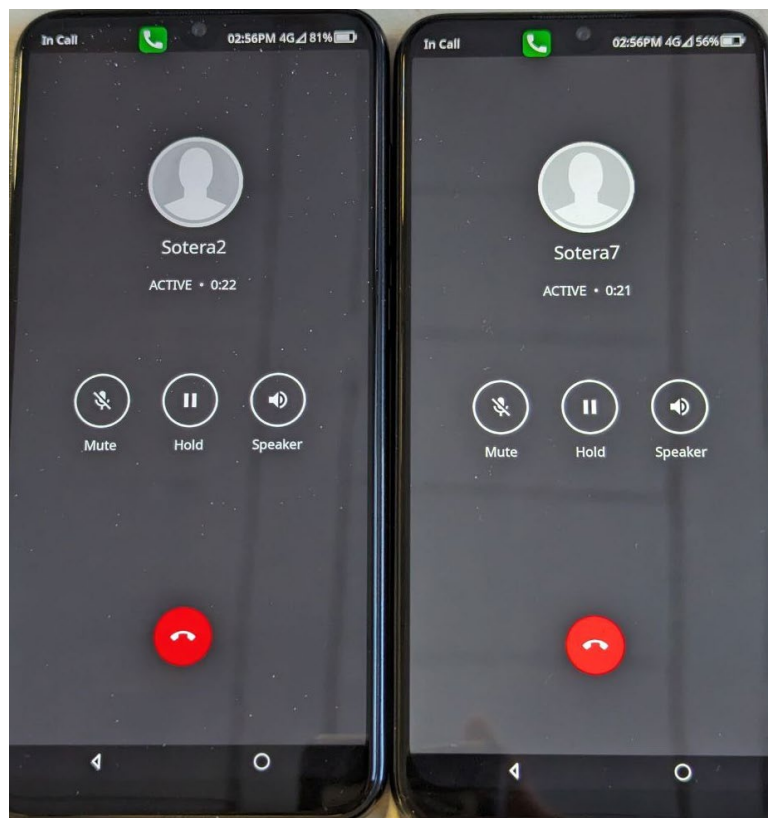




7.2.1 LLAMADAS DE VOZ

Al introducir un número de teléfono en el marcador y pulsar el botón verde de llamada o seleccionar un contacto desde la pestaña de contactos, se iniciará una llamada con el usuario en cuestión. No hay posibilidad de realizar llamadas de voz grupales ni llamadas de vídeo.

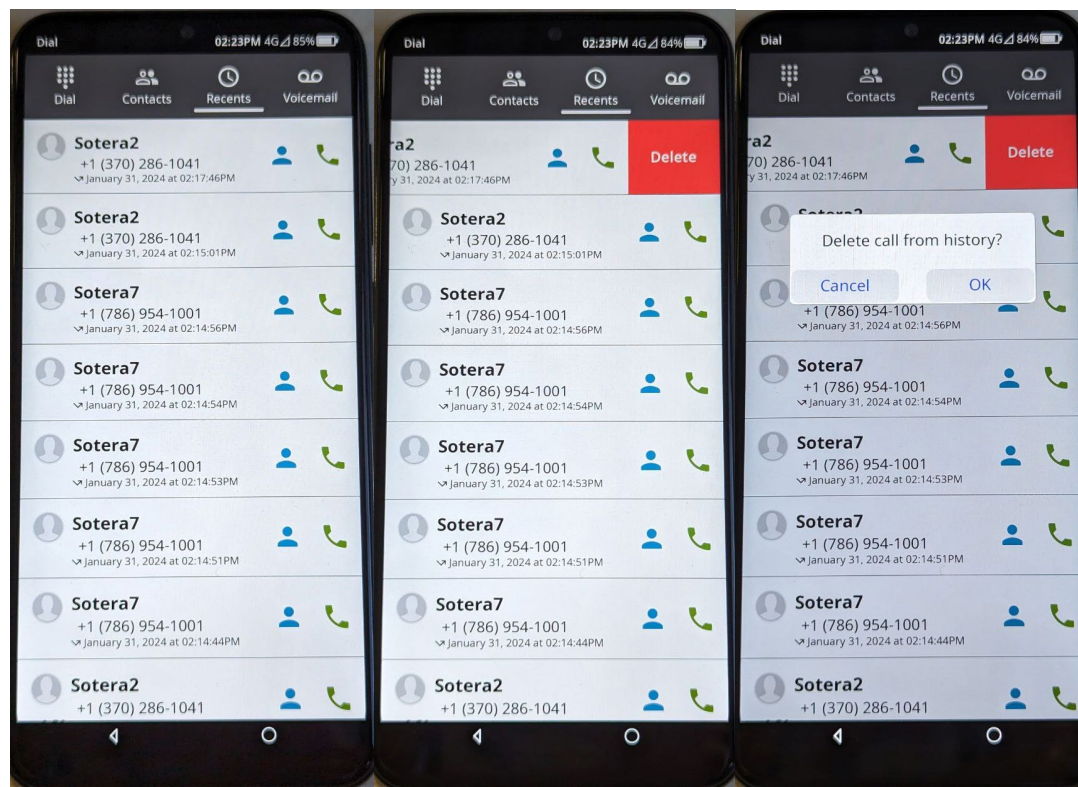




Los participantes de la llamada pueden silenciar su micrófono (botón “Mute”), poner la llamada en espera (botón “Hold”), poner la llamada en altavoz (botón “Speaker”) o colgar la llamada pulsando en el botón rojo ubicado en la parte inferior de la pantalla.

7.2.2 HISTORIAL DE LLAMADAS

El histórico de llamadas se encuentra en la pestaña de Recientes “Recents”. Aquí el usuario puede consultar, acceder al contacto relacionado y realizar llamadas, además de poder eliminar entradas del histórico deslizando el elemento hacia la izquierda, pulsando en “Delete” y en “OK”.

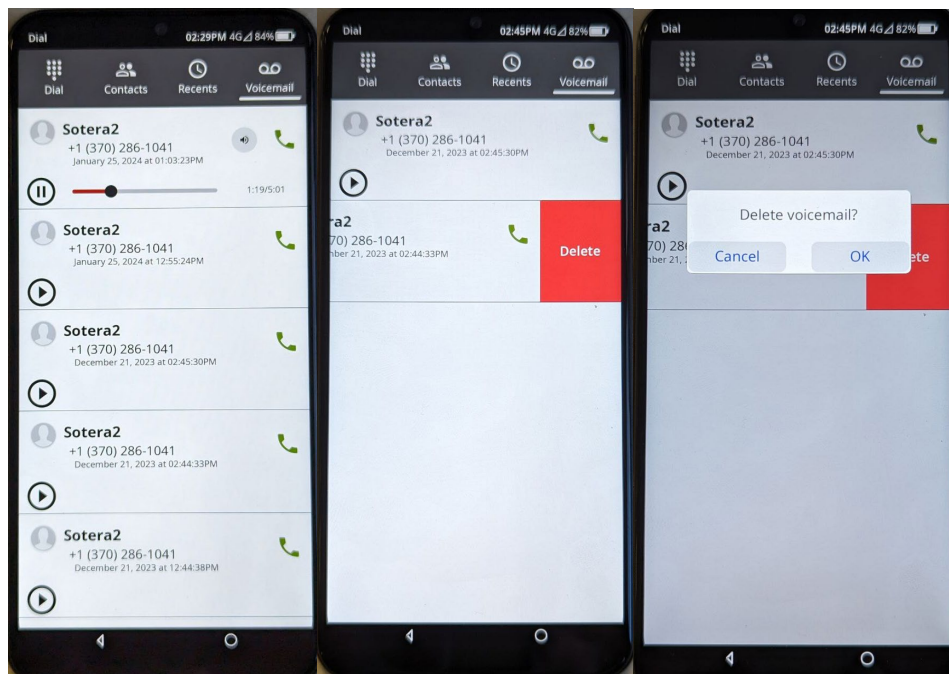


7.2.3 BUZÓN DE VOZ

Si el destinatario de una llamada no responde en aproximadamente 30 segundos, se le ofrecerá al usuario dejar un mensaje en el buzón de voz de un máximo de 5 minutos. Pulsar en “SEND” para enviar el mensaje de voz o en “CANCEL” para cancelar la grabación.

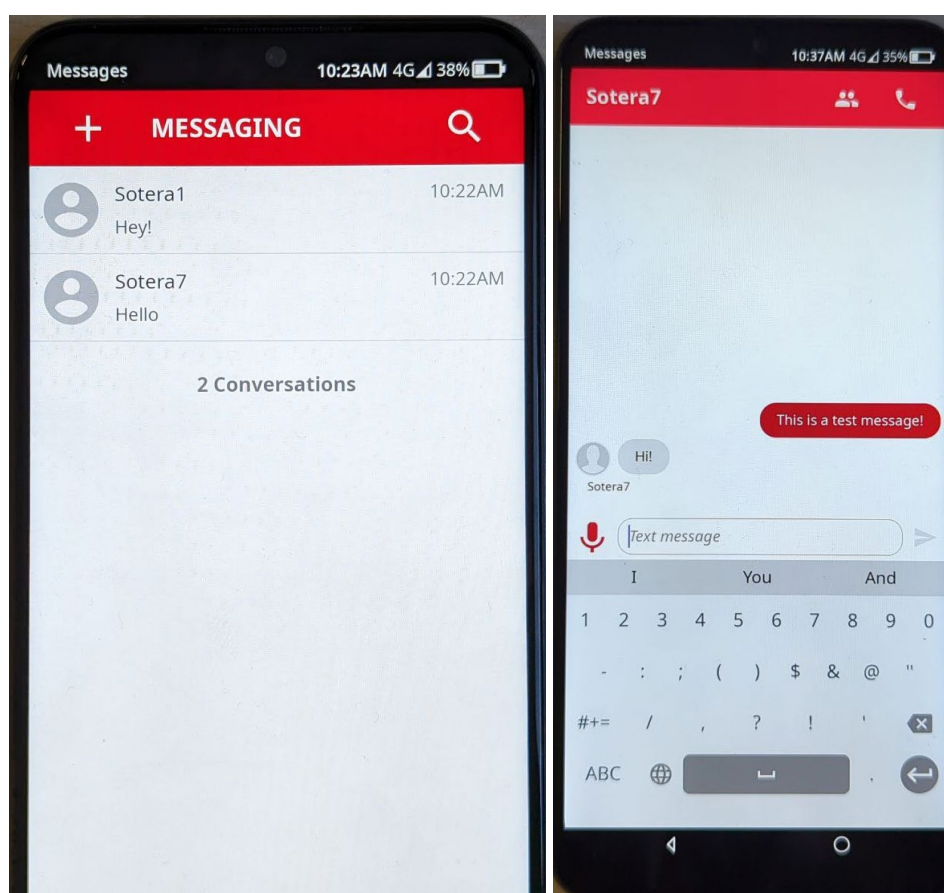
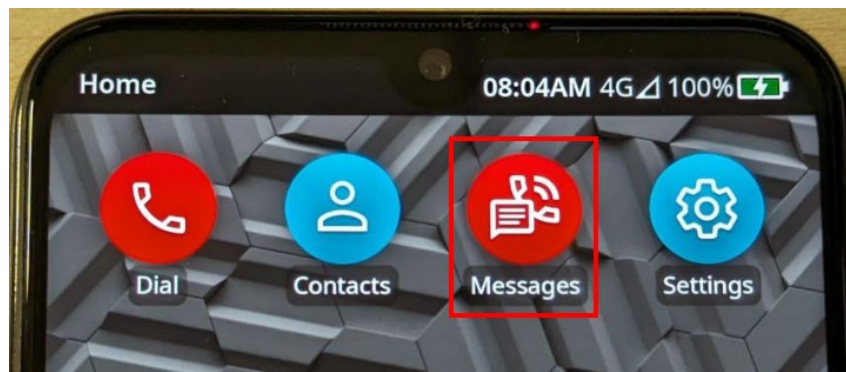


El buzón de voz se ubica en la pestaña de “Voicemail” y permite al usuario escuchar los mensajes que otros usuarios le hayan dejado en el contestador. De la misma forma que en la pestaña de “Recents”, el usuario puede eliminar mensajes de voz.



7.3 USO DE LA APLICACIÓN DE MENSAJERÍA (“MESSAGES”)

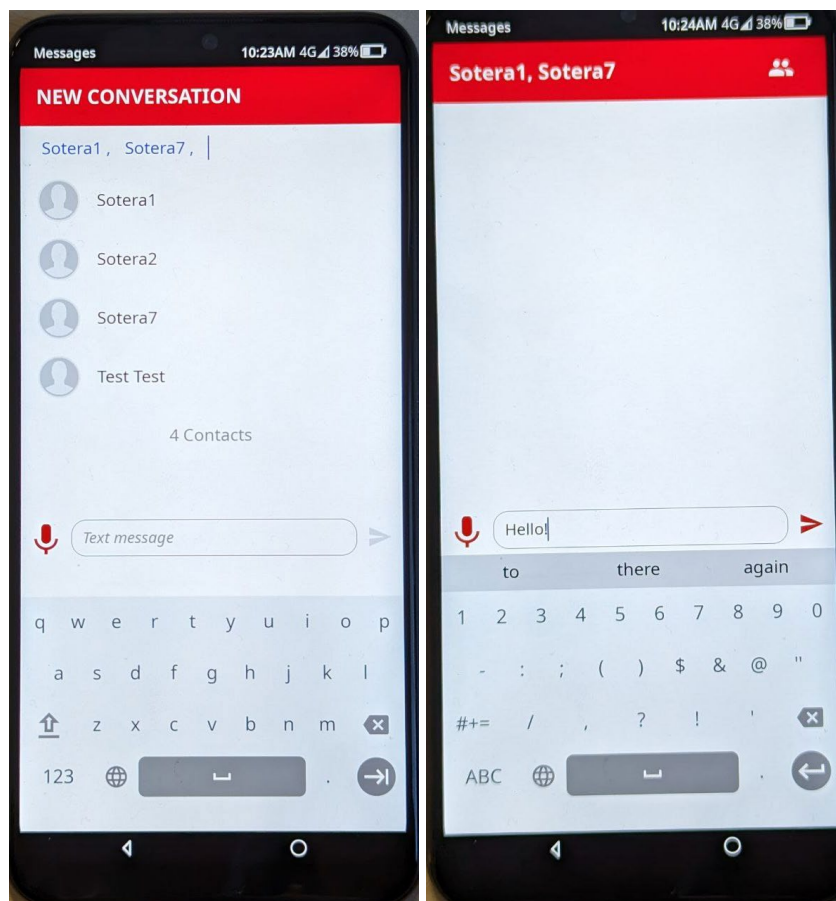
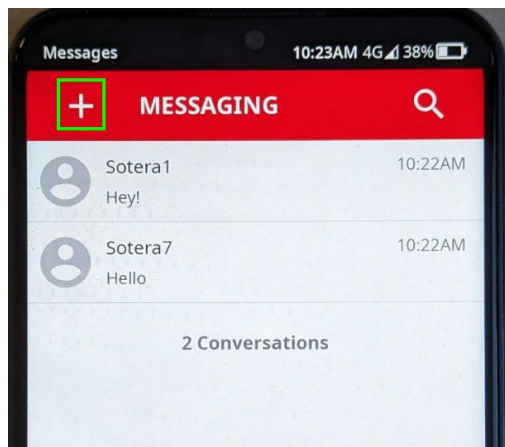
La aplicación de mensajes (“Messages”) permite al usuario enviar y recibir mensajes de texto y notas de voz. Las conversaciones pueden ser tanto individuales como grupales.



7.3.1 CONVERSACIONES

La pantalla principal muestra un listado con las conversaciones del usuario junto con su último mensaje. El usuario puede acceder a ellas pulsando en la entrada correspondiente.

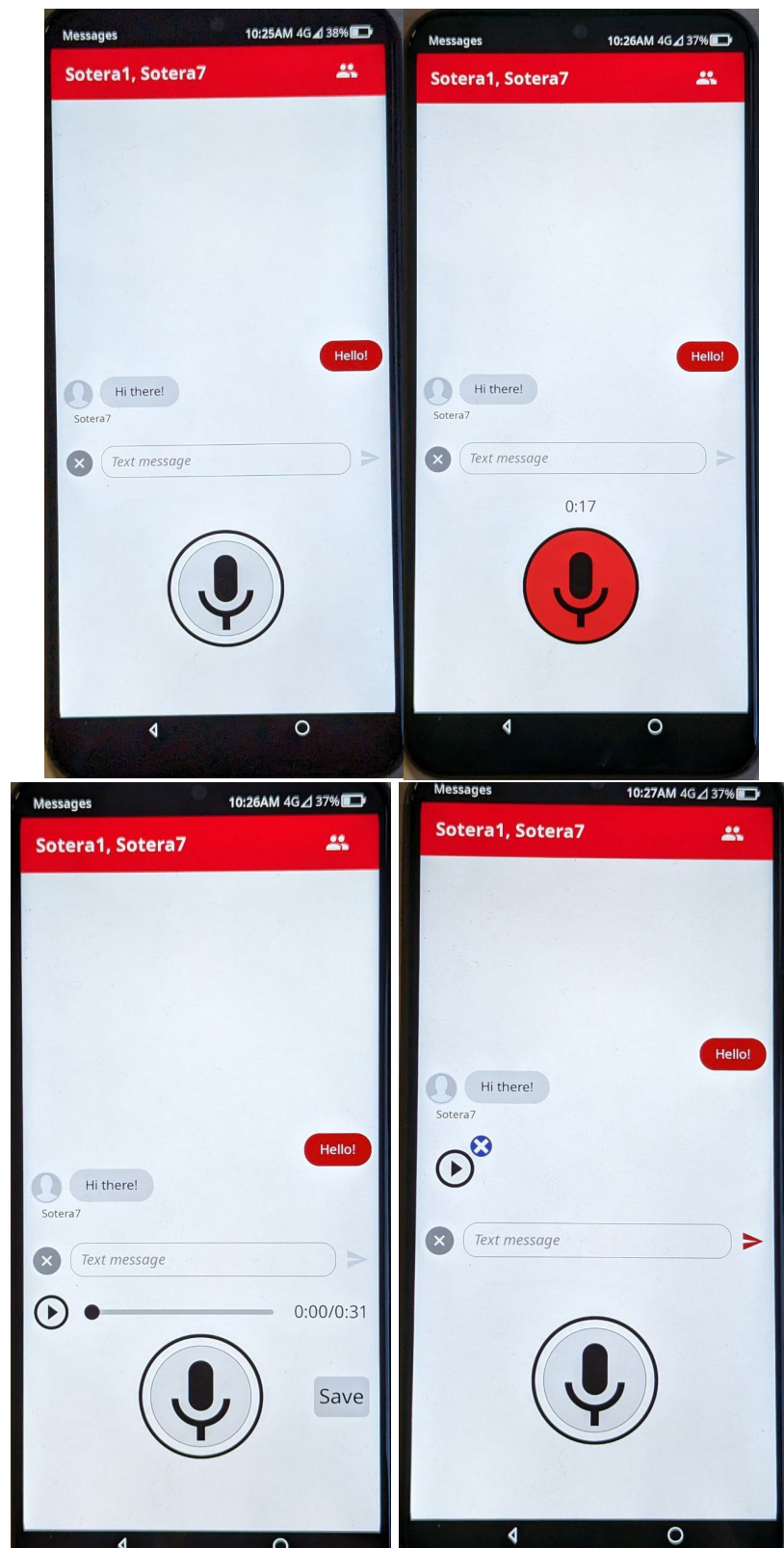
Para iniciar una nueva conversación, pulsar en el botón de “+” ubicado en la esquina superior izquierda. A continuación, se seleccionarán los contactos con los que se desee comunicarse. En este punto, es posible enviar un mensaje inicial o iniciar la conversación vacía pulsando en el botón de enviar sin haber introducido contenido.



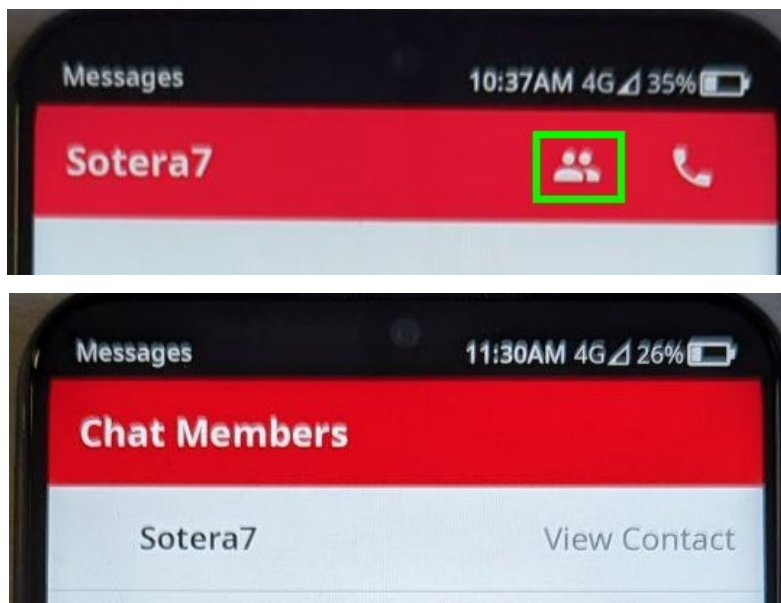
7.3.2 ENVÍO Y RECEPCIÓN DE MENSAJES

Para enviar mensajes dentro de una conversación, utilizar el teclado ubicado en la parte inferior y pulsar el botón de enviar. Para enviar notas de voz será necesario pulsar el

botón del micrófono y pulsar el nuevo micrófono que aparece en pantalla para iniciar la grabación. Una vez se desee detener la grabación, pulsar de nuevo el botón del micrófono. El usuario podrá revisar su grabación pulsando el botón de reproducción y guardar el audio como adjunto pulsando el botón de “Save”. Tras añadir el adjunto, el usuario puede añadir texto al mensaje o enviar exclusivamente el audio.

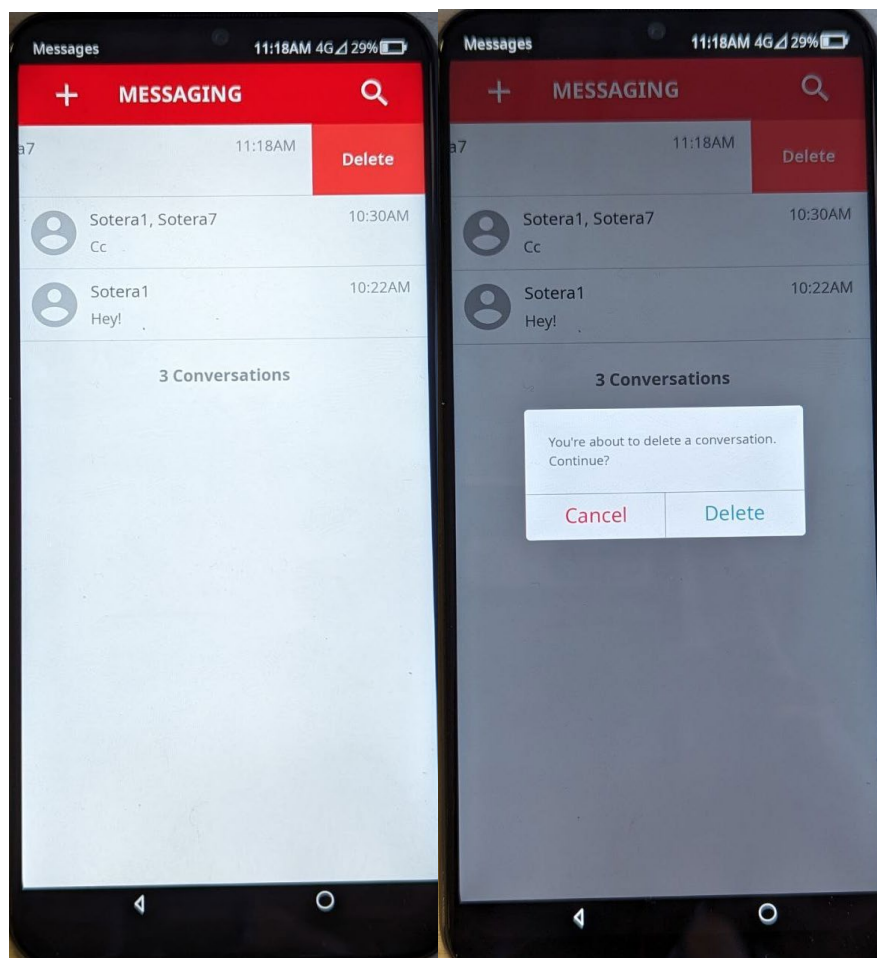


En la esquina superior derecha se muestran los iconos de participantes y el de teléfono (sólo en conversaciones individuales). El primero te permite listar los participantes de la conversación actual y opcionalmente, consultar su información de contacto.

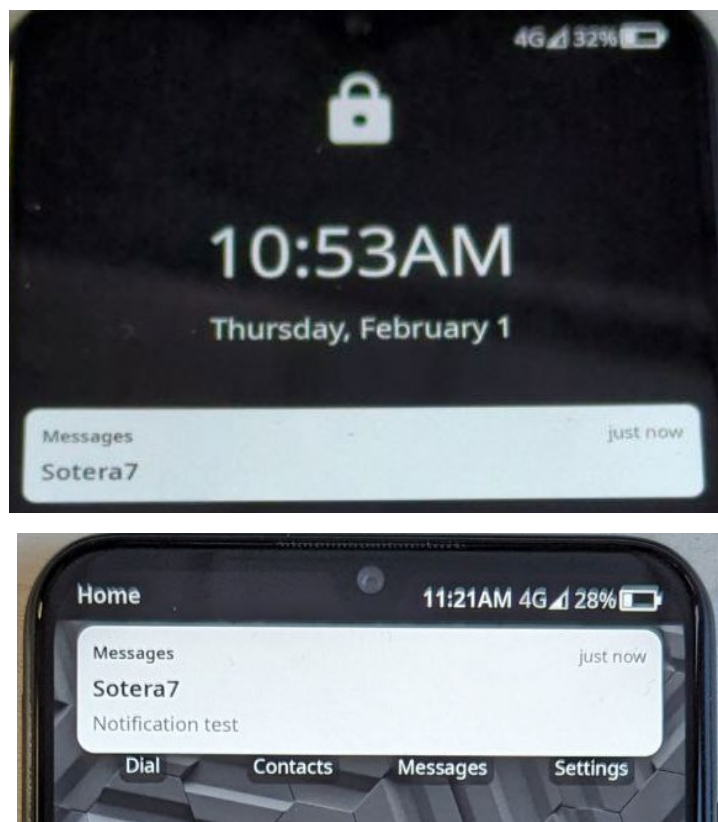


El botón de teléfono iniciará una llamada con el usuario en cuestión.

No es posible eliminar mensajes individuales, solo conversaciones en su totalidad. Para ello, desde el menú principal deslizar hacia la izquierda la conversación deseada, pulsar en "Delete" y confirmar la acción.

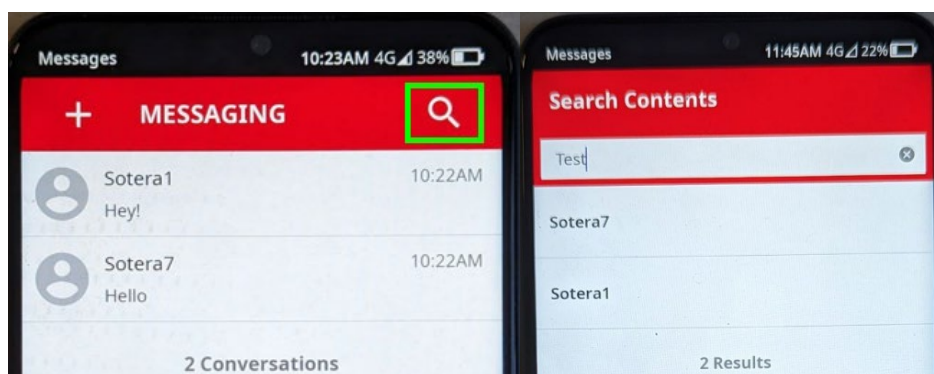


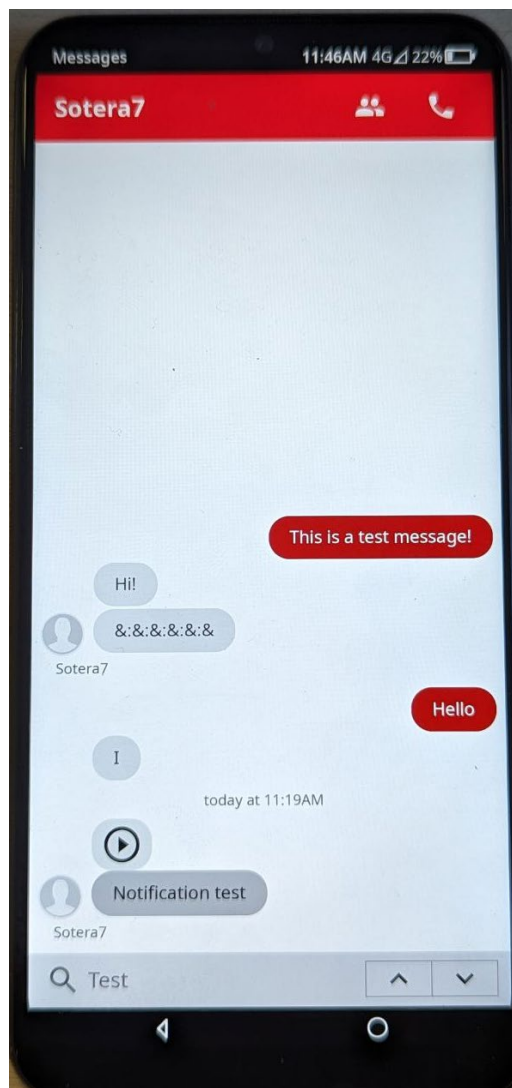
Los mensajes recibidos se mostrarán también a modo de notificación si el dispositivo está desbloqueado. En caso contrario, su contenido no podrá ser leído desde la pantalla de bloqueo hasta que el usuario desbloquee el dispositivo.



7.3.3 BÚSQUEDA DE MENSAJES

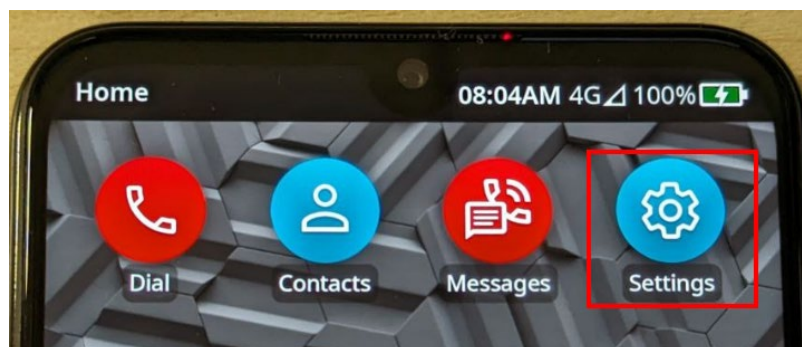
Para realizar una búsqueda de conversaciones por contenido, pulsar en el icono de la lupa ubicado en la esquina superior derecha de la pantalla principal. Una vez en el menú de búsqueda, introducir la cadena de texto a buscar y pulsar sobre la conversación deseada para acceder al mensaje encontrado.

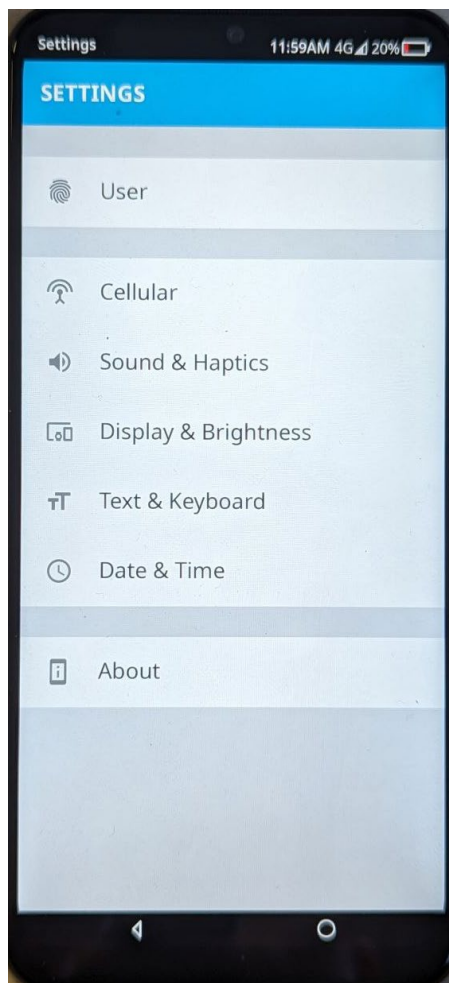




7.4 USO DE LA APLICACIÓN DE AJUSTES (“SETTINGS”)

La aplicación de ajustes (“Settings”) permite al usuario configurar aspectos concretos del dispositivo. En esta sección se documentarán los pasos necesarios para realizar un reseteo de fábrica del dispositivo, para cambiar la contraseña y para actualizar el firmware del teléfono mediante OTA.

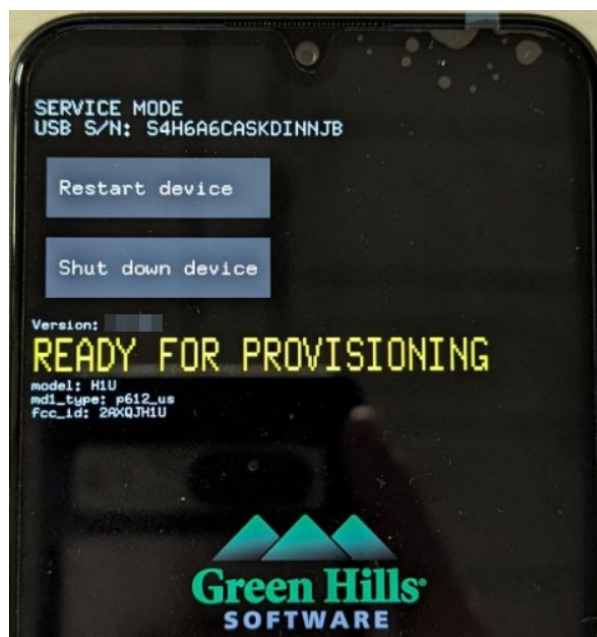
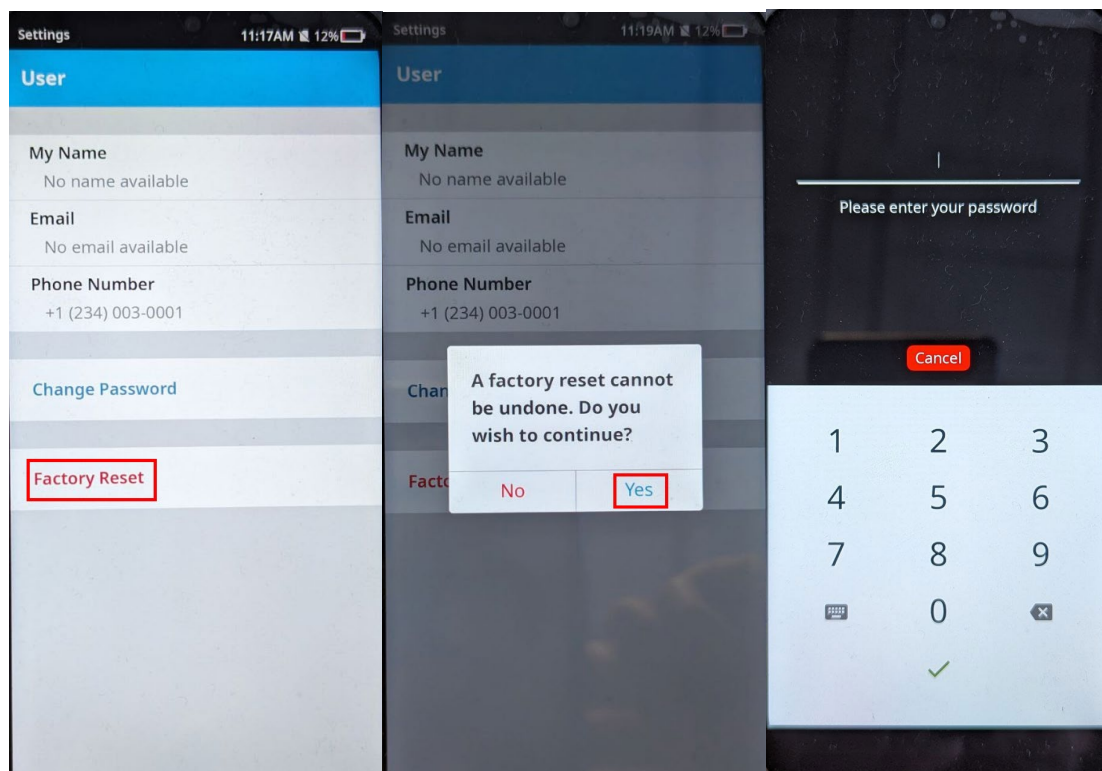




7.4.1 PROCEDIMIENTO DE RESETEO DE FÁBRICA

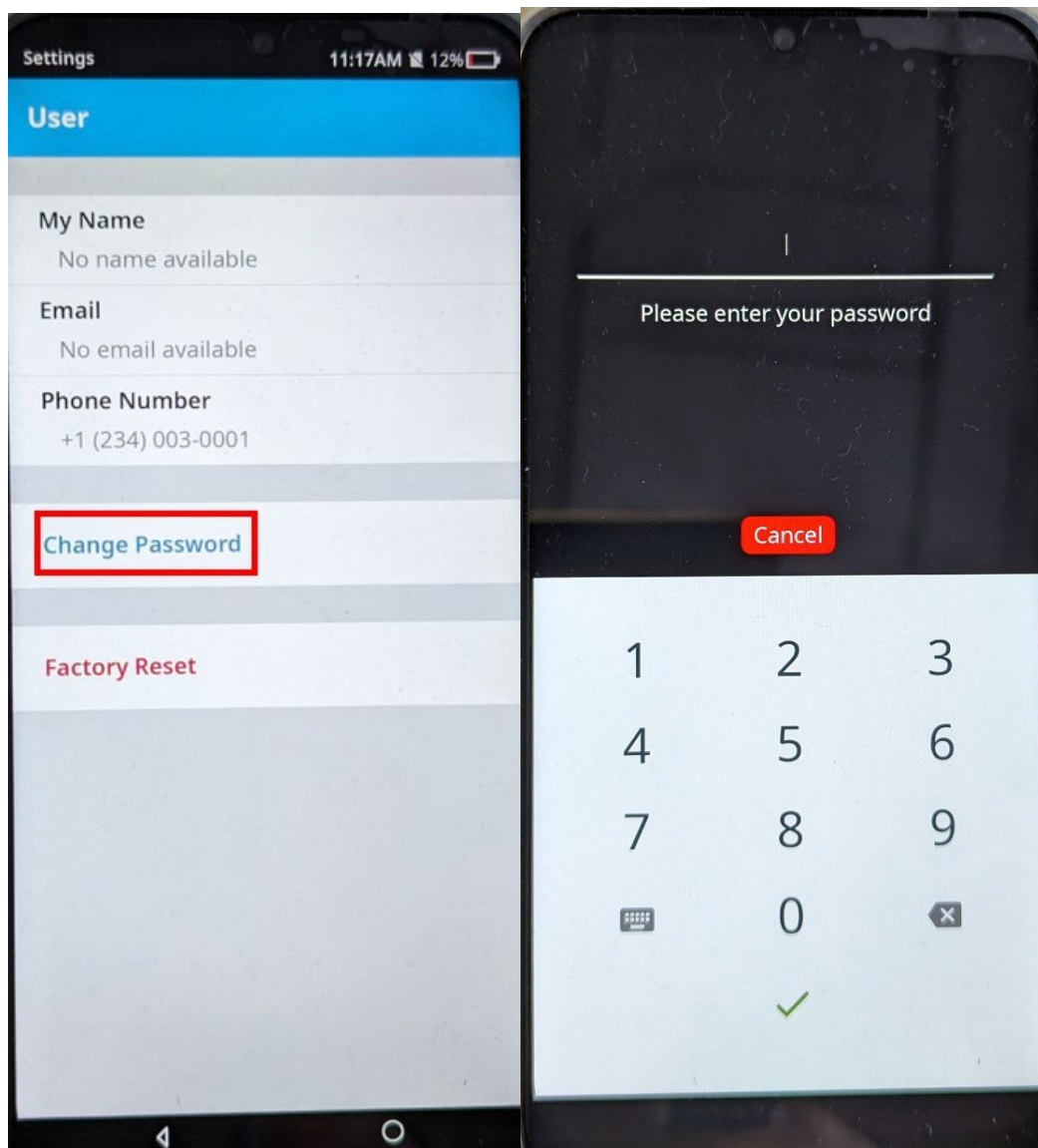
El reseteo de fábrica del Sotera Phone H1U no se comporta de la misma manera que el resto de dispositivos móviles tradicionales. En este caso, al realizar el borrado **se eliminarán también las claves y certificados del usuario**, siendo necesario **devolver el dispositivo a fábrica** para que vuelva a ser provisionado. Una vez termine el proceso, el dispositivo se reiniciará en modo Servicio y no podrá ser utilizado hasta que un técnico autorizado lo restaure.

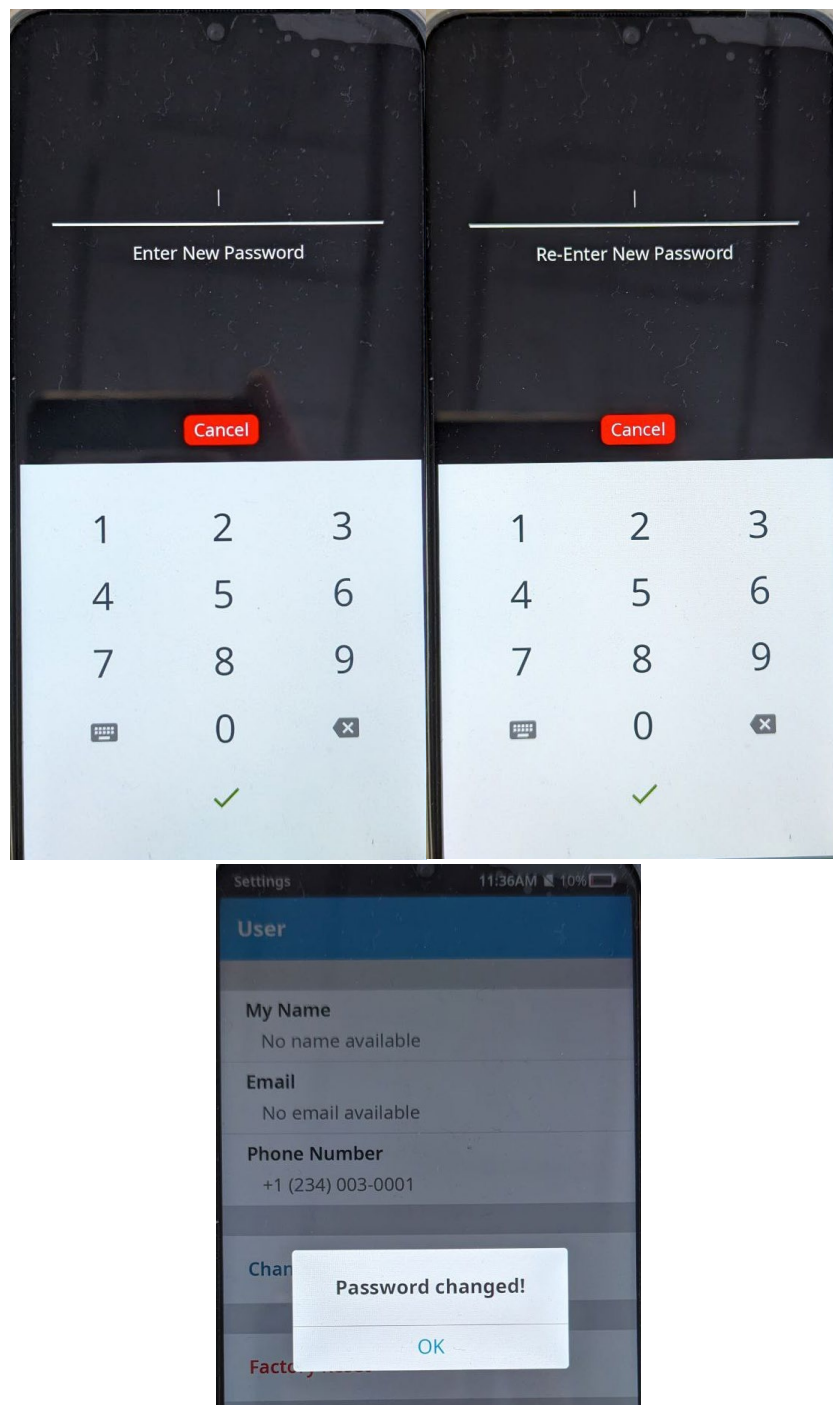
Para iniciar el reseteo de fábrica, navegar a “User” > “Factory Reset” y confirmar la acción pulsando en “Yes”. Será necesario introducir la contraseña actual del usuario para aprobar la operación.



7.4.2 PROCEDIMIENTO DE CAMBIO DE CONTRASEÑA

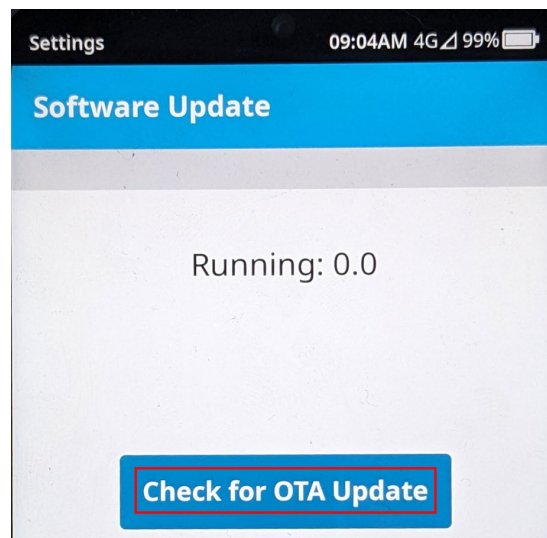
Es posible cambiar la contraseña actual del usuario navegando a “User” > “Change Password”. Será necesario introducir la contraseña actual antes de proceder con el cambio de contraseña. Si la nueva contraseña cumple con las políticas descritas en la sección **5 FASE DE INSTALACIÓN**, se mostrará un mensaje de éxito indicando “Password changed!”.



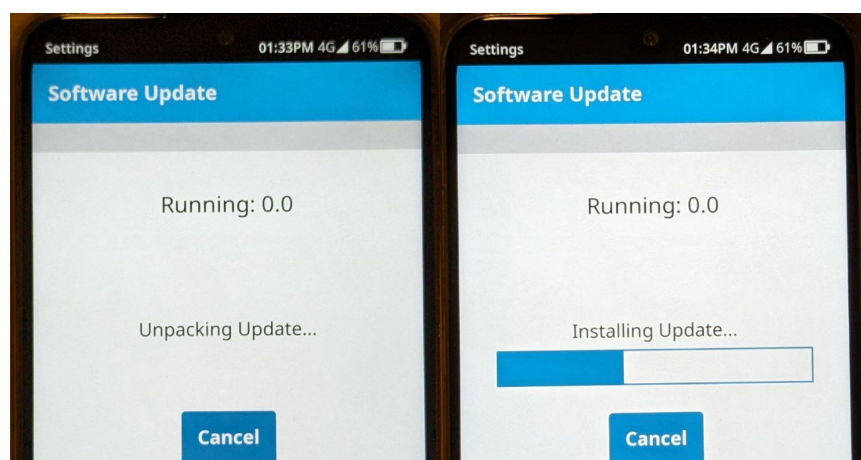
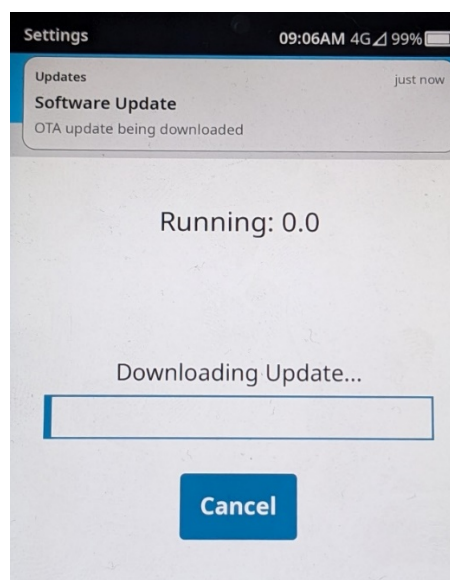


7.4.3 PROCEDIMIENTO DE ACTUALIZACIÓN DE SOFTWARE

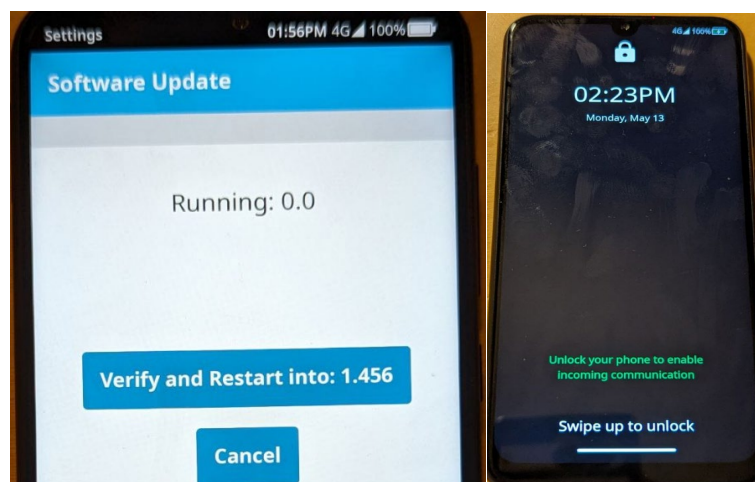
Para iniciar manualmente el proceso de actualización de firmware vía OTA, será necesario acceder a “Settings” > “About” > “Software Update” y pulsar el botón “Check for OTA Update”.



En caso de haber una actualización disponible, comenzará su descarga y se notificará al usuario de ello.



Cuando la descarga es finalizada, el paquete de actualización es instalado en disco. Para aplicar la actualización en el dispositivo es necesario reiniciarlo.



Una vez reiniciado el dispositivo, verificar que el nuevo paquete de actualización ha sido aplicado, para ello acceder a “Settings” > “About” > “Software & Hardware Version”.

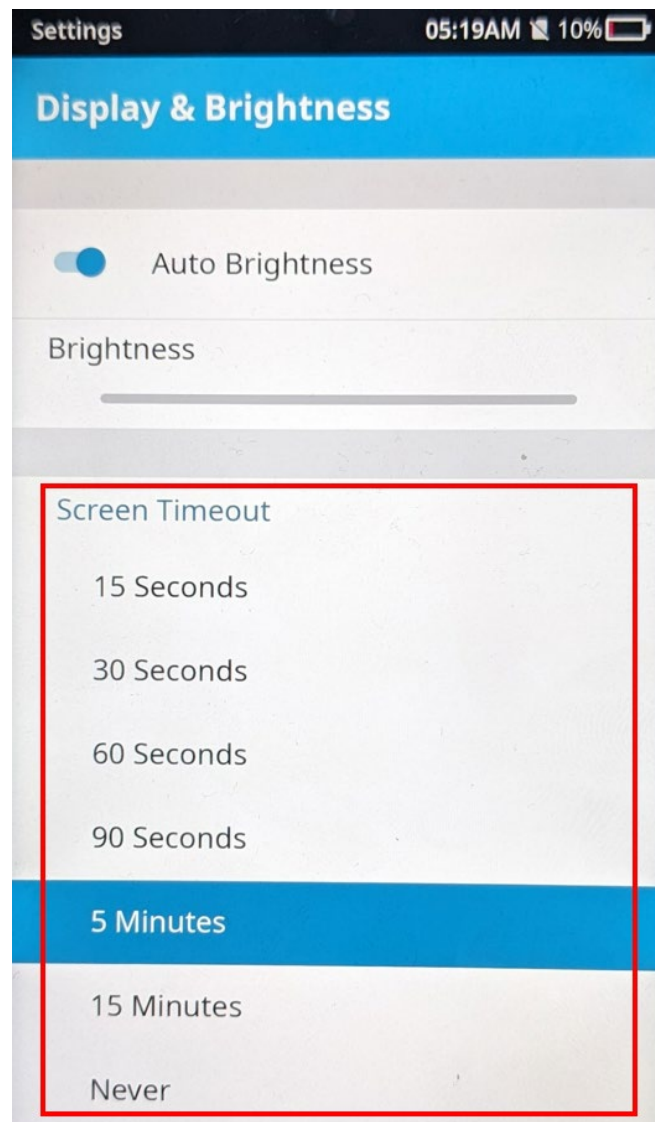


Si el usuario ha habilitado la opción de actualizaciones automáticas, el producto iniciará la descarga, verificación e instalación del paquete de actualización sin interacción por parte del usuario.

7.4.4 CONFIGURACIÓN DEL TIEMPO DE INACTIVIDAD

Es posible configurar un tiempo de inactividad durante el cual, si el usuario no interactúa con el dispositivo, este se bloqueará automáticamente, teniendo que volver a introducir la contraseña o PIN del usuario para desbloquearlo.

Para configurar el tiempo de inactividad, será necesario acceder a “Settings” > “Display & Brightness” y fijar el valor para el tiempo de inactividad deseado en la sección de “Screen Timeout”.



8. REFERENCIAS

CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad, Mayo 2022.

9. ABREVIATURAS

API	Application Programming Interface
CA	Certificate authority
CPSTIC	Catálogo de Productos STIC.
EAP	Extensible Authentication Protocol
ENS	Esquema Nacional de Seguridad.
IPSEC	IP Security
MDM	Mobile Device Management
PIN	Personal Identification Number
QR	Quick Response code
RSA	Rivest-Shamir-Adleman algorithm
SDK	Software Development Kit
TEE	Trusted Execution Environment
TLS	Transport Layer Security
VoIP	Voice over IP
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

