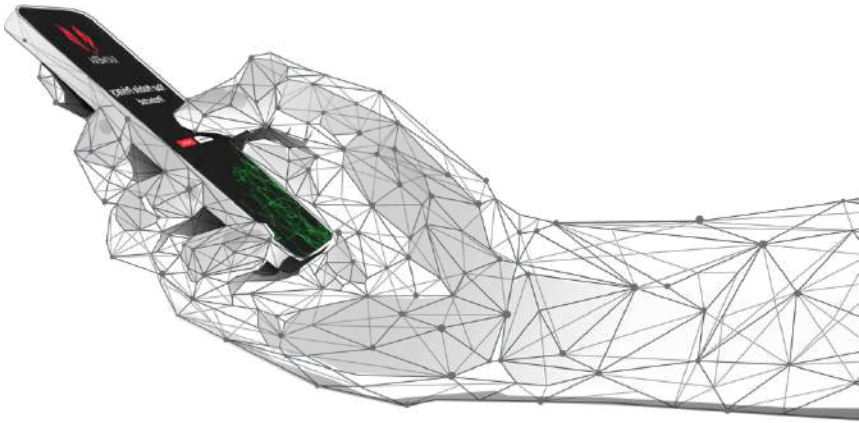
Manual de Uso de las Funciones de Comunicación

CipherFort

Enlaces de Voz & Mensajes

Versión 1.0 | 202106

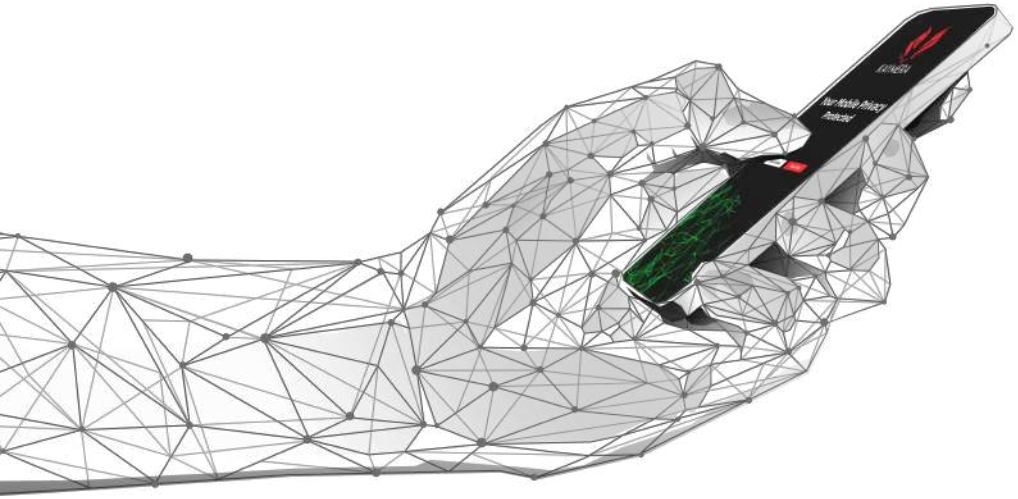
KAYMERA



invezt
Disruptive Capital

KAYMERA High-End Mobile Security | invezt Disruptive Capital

INTRODUCCIÓN



Manual de Uso de las Funciones de Comunicación CipherFort

Modelo de Comunicación y Cifrado de la **Plataforma Kaymera**

- La **Aplicación CipherBond** y los **Equipos Google Pixel con Sistema Operativo CipherFort** son los servicios para el usuario en la solución de la **Plataforma KAYMERA** para proporcionar la máxima privacidad y protección contra intercepciones de la comunicación móvil.

Comunicación ILIMITADA y ENCRIPTADA grado militar entre usuarios de la plataforma KAYMERA

- **Mensajes de Texto y Voz** con autodestrucción programada de mensajes.
- **Transferencia de Archivos**: fotos, documentos, videos, multimedia, etc.
- **Grupos de Chat.**
- **Enlaces Seguros de Voz.**

ADEMÁS:

- **Enlaces Semi-Seguros de Voz** a números fijos y móviles que **NO TENGAN** el servicio de la plataforma **KAYMERA**.
- **MODO PRIVADO** elimina el **Identificador de Llamadas** en **Enlaces Semi-Seguros de Voz**, al llamar mostrará **Número Oculto.**

BENEFICIOS:

- Los mensajes y archivos enviados y recibidos por usuarios **KAYMERA** quedan **encriptados y protegidos** en el teléfono.
- No se requiere de inversión adicional en equipos o infraestructura. No hay gastos de operación y mantenimiento.

Modelo de Comunicación y Cifrado de la **Plataforma Kaymera**

- Utilizando el **Advanced Encryption Standard (AES-256)**, el mismo usado por gobiernos, bancos y sistemas de alta seguridad en todo el mundo, **KAYMERA** proporciona comunicación de voz, comunicación escrita y mediante el intercambio de archivos electrónicos a través de **Enlaces Seguros y Enlaces Semi-seguros** hacia y desde cualquier usuario de la **Aplicación CipherBond** y de los **Equipos Google Pixel con Sistema Operativo CipherFort** .

Usuario con la **Aplicación CipherBond** en su Teléfono Inteligente o del Equipo Google Pixel con **Sistema Operativo CipherFort**.

COMUNICACIÓN SEGURA BI-DIRECCIONAL
Voz + Texto + Archivos (foto, audio, video, documento)
(todo incluído en el servicio contratado).

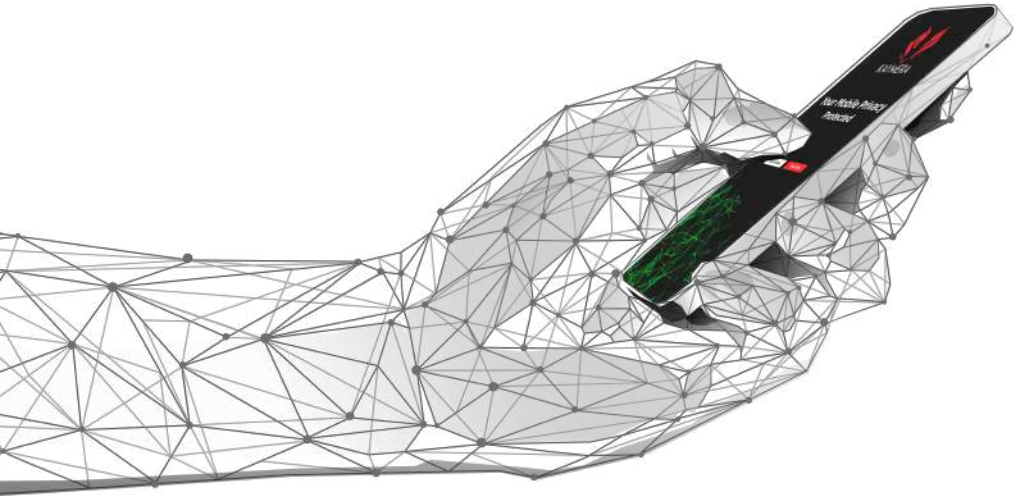
Usuario con la **Aplicación CipherBond** instalada en su Teléfono Inteligente o del **Equipo Google Pixel con Sistema Operativo CipherFort**.

COMUNICACIÓN SEMI-SEGURA UNI-DIRECCIONAL
Enlaces de Voz
(aplican cargos adicionales según Tarifas y Destinos).

Usuario **SIN servicio KAYMERA** disponible en un enlace y/o dispositivo telefónico fijo ó móvil.

KAYMERA High-End Mobile Security | invezt Disruptive Capital

Modelo de CIFRADO



Manual de Uso de las Funciones de Comunicación CipherFort

Modelo de Comunicación y Cifrado de la **Plataforma Kaymera**

- La forma como opera el **CIFRADO DE LA INFORMACIÓN & COMUNICACIÓN** se ilustra en el siguiente diagrama:

EMISOR DEL ENLACE DE VOZ
Usuario con Teléfono Inteligente con la
- **Aplicación CipherBond**

ó Equipo Google Pixel con
- **Sistema Operativo CipherFort**

En ningún momento la comunicación (mensajes, intercambio de archivos y enlaces de voz) entre **usuarios de la Plataforma KAYMERA** se encuentra disponible para su almacenamiento, consulta o acceso por parte de **KAYMERA** y/o de alguna entidad que solicite hacerlo.

RECEPTOR DE LA COMUNICACIÓN:
Usuario con Teléfono Inteligente con la
- **Aplicación CipherBond**

ó Equipo Google Pixel con
- **Sistema Operativo CipherFort**

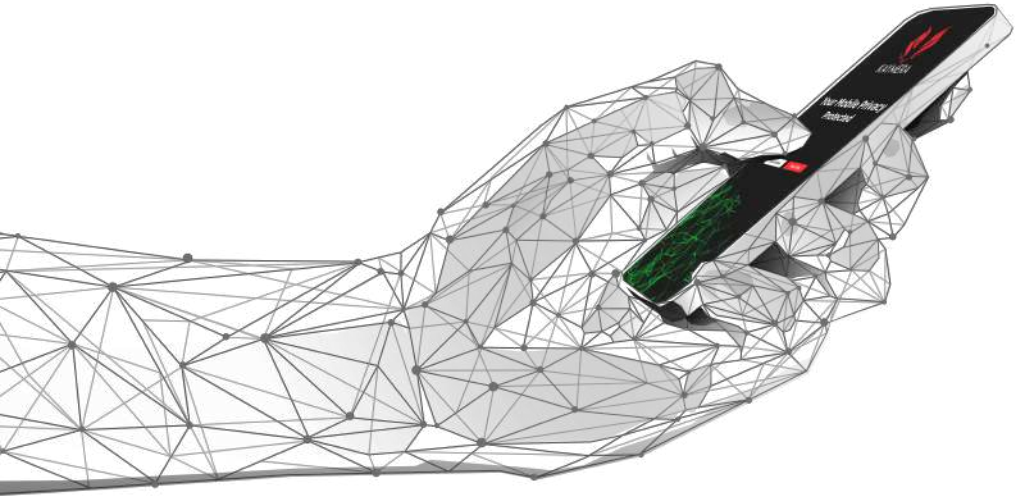
android

KAYMERA High-End Mobile Security | invezt Disruptive Capital

Modelo de Comunicación

ENLACES SEGUROS

Voz & Mensajes



Manual de Uso de las Funciones de Comunicación CipherFort

Modelo de Comunicación y Cifrado de la **Plataforma Kaymera**

- La forma como **operan** los **ENLACES SEGUROS DE VOZ** se ilustra en el siguiente diagrama:

Modelo de Comunicación y Cifrado de la **Plataforma Kaymera**

- Existen diferentes **condiciones necesarias** para que los **ENLACES SEGUROS DE VOZ** puedan ser realizados:

ENTORNO PROTEGIDO CON ENCRIPCIÓN AES-256 Bits

ESTABILIDAD EN LA CONEXIÓN A INTERNET
Cuando el dispositivo, de manera automática, alterna su señal de internet entre una conexión a datos móviles y una conexión a la red WiFi, se puede generar inestabilidad en la conexión del dispositivo con la plataforma.

SEÑAL SUPERIOR A 2G
Los Enlaces de Voz requieren que la conexión del dispositivo a la red de telefónia celular y datos móviles sea con antenas de red 3G o superiores.
** Los mensajes si pueden realizarse con red 2G.*

CALIDAD/SEGURIDAD EN LA CONEXIÓN A INTERNET
La Plataforma requiere que el enlace con el dispositivo (Emisor o Receptor) se realice dentro de una conexión a internet con las condiciones de calidad y seguridad adecuadas para permitir la creación de un canal encriptado, ya sea del Emisor a los Servidores, o de los Servidores al Receptor.

ESTABILIDAD EN LA CONEXIÓN A INTERNET
Cuando el dispositivo, de manera automática, alterna su señal de internet entre una conexión a datos móviles y una conexión a la red WiFi, se puede generar inestabilidad en la conexión del dispositivo con la plataforma.

SEÑAL SUPERIOR A 2G
Los Enlaces de Voz requieren que la conexión del dispositivo a la red de telefónia celular y datos móviles sea con antenas 3G o superiores.
** Los mensajes si pueden realizarse con red 2G.*

EMISOR DEL ENLACE DE VOZ
Usuario con Teléfono Inteligente con la
- **Aplicación CipherBond**

ó Equipo Google Pixel con
- **Sistema Operativo CipherFort**

Si la Aplicación **CipherBond**, el Sistema Operativo **CipherFort** o los servidores de la Plataforma **KAYMERA** detectan que no existen las condiciones adecuadas (red suficiente, estable y segura) para realizar el enlace entre Emisor y Receptor, el Enlace NO PODRÁ ser realizado para mantener la integridad del entorno seguro.

RECEPTOR DEL ENLACE DE VOZ
Usuario con Teléfono Inteligente con la
- **Aplicación CipherBond**

ó Equipo Google Pixel con
- **Sistema Operativo CipherFort**

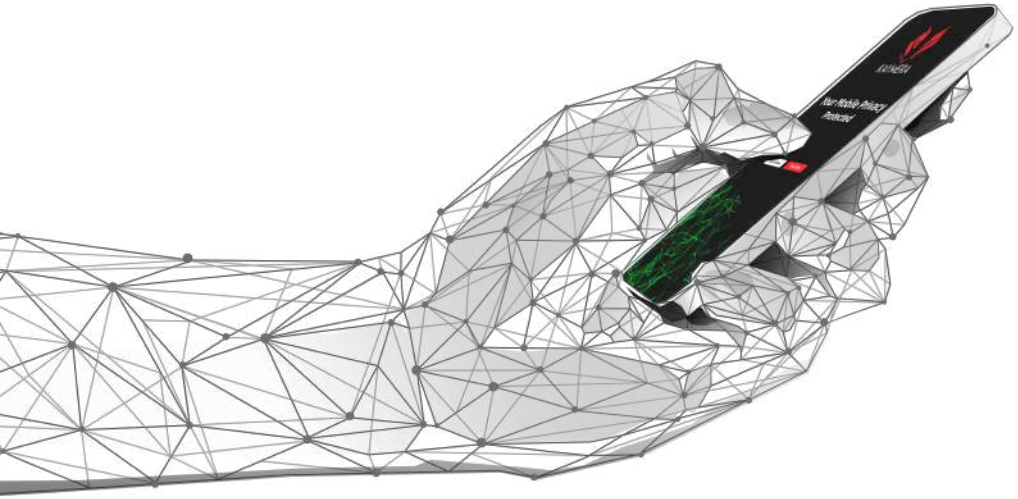
Modelo de Comunicación y Cifrado de la **Plataforma Kaymera**

- La **protección y vulnerabilidad** en los **ENLACES SEGUROS DE VOZ** se ilustra en el siguiente diagrama:

KAYMERA High-End Mobile Security | invezt Disruptive Capital

Modelo de Comunicación

ENLACES DE VOZ SEMI-SEGUROS



Manual de Uso de las Funciones de Comunicación CipherFort

Modelo de Comunicación y Cifrado de la **Plataforma Kaymera**

- La forma como **operan** los **ENLACES SEMI-SEGUROS DE VOZ** se ilustra en el siguiente diagrama:

Modelo de Comunicación y Cifrado de la **Plataforma Kaymera**

- Existen diferentes **condiciones necesarias** para que los **ENLACES SEMI-SEGUROS DE VOZ** puedan ser realizados:

ENTORNO PROTEGIDO CON ENCRIPCIÓN GRADO MILITAR

ESTABILIDAD EN LA CONEXIÓN A INTERNET
Cuando el dispositivo, de manera automática, alterna su señal de internet entre una conexión a datos móviles y una conexión a la red WiFi, se puede generar inestabilidad en la conexión del dispositivo con la plataforma.

SEÑAL SUPERIOR A 2G
Los Enlaces de Voz requieren que la conexión del dispositivo a la red de telefónia celular y datos móviles sea con antenas de red 3G o superiores.
** Los mensajes si pueden realizarse con red 2G.*

CALIDAD/SEGURIDAD EN LA CONEXIÓN A INTERNET
La Plataforma requiere que el enlace con el dispositivo (Emisor o Receptor) se realice dentro de una conexión a internet con las condiciones de calidad y seguridad adecuadas para permitir la creación de un canal encriptado, ya sea del Emisor a los Servidores, o de los Servidores al Receptor.

EMISOR DEL ENLACE DE VOZ
Usuario con Teléfono Inteligente con la
- **Aplicación CipherBond**
  Servicio de Enlaces Semi-seguros habilitados

ó Equipos Google Pixel con
- **Sistema Operativo CipherFort**
  Servicio de Enlaces Semi-seguros habilitados

Si la Aplicación CipherBond, el Sistema Operativo CipherFort o los servidores de la Plataforma KAYMERA detectan que no existen las condiciones adecuadas (red suficiente, estable y segura) para realizar el enlace entre Emisor y Receptor, el Enlace NO PODRÁ ser realizado para mantener la integridad del entorno seguro.

ACEPTACIÓN DEL CARRIER A VoIP
La conexión con una plataforma de llamadas telefónicas VoIP (voz sobre Internet) debe ser aceptada por la empresa proveedora del servicio de telefonía al número del Destinatario.

NÚMERO REGISTRADO
El número telefónico del Destinatario debe haber sido registrado previamente para recibir llamadas desde números internacionales (aunque sea el número del Emisor el que conectará el servicio)

RECEPTOR DEL ENLACE DE VOZ
Usuario de cualquier tipo de servicio de telefonía fija o móvil en el mundo
Según destinos disponibles y habilitados

android

Modelo de Comunicación y Cifrado de la **Plataforma Kaymera**

- La **protección y vulnerabilidad** en los **ENLACES SEMI-SEGUROS DE VOZ** se ilustra en el siguiente diagrama:

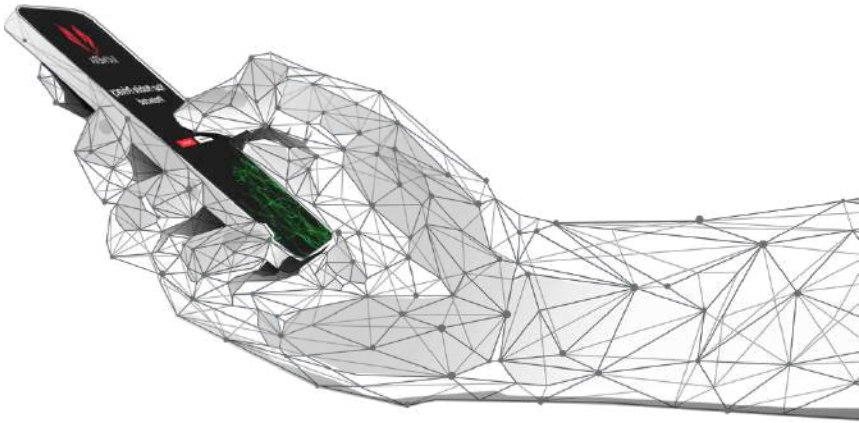
Manual de Uso de las Funciones de Comunicación

CipherFort

Enlaces de Voz & Mensajes

Versión 1.0 | 202106

KAYMERA

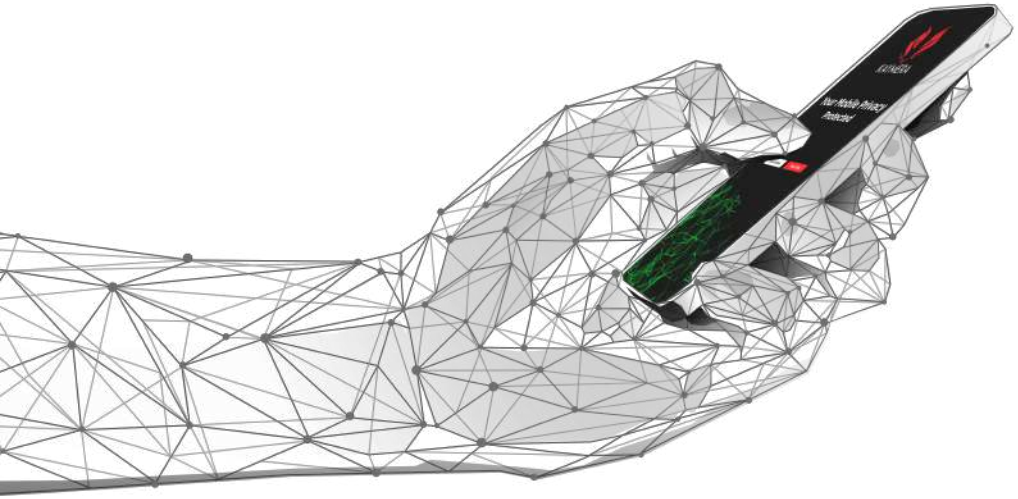


invezt
Disruptive Capital

KAYMERA High-End Mobile Security | invezt Disruptive Capital

USO DE LA FUNCIONALIDAD

ENLACES DE VOZ **SECURE PHONE**



Manual de Uso de las Funciones de Comunicación CipherFort

3: Uso de la Funcionalidad Secure Calls

- El **CipherFort** / equipo Google Pixel con Sistema Operativo **Kaymera** dispone de **dos íconos para servicios de comunicación segura**:

SECURE PHONE
Es el acceso directo a la función de Enlaces de Voz

CIPHERBOND
Es el acceso directo a la función de Mensajes y envío de Archivos, así como a la Configuración de la Aplicación.

3: Uso de la Funcionalidad Secure Phone

ÍCONO SECURE PHONE

Se utiliza para realizar **Enlaces de Voz** con el equipo **CipherFort**, con el cual se pueden realizar tres tipos de Enlace de Voz:

1. **Enlace Seguros de Voz.**
2. **Enlaces Semi-seguros de Voz.**
3. **Enlaces No seguros de Voz**
   (Llamadas telefónicas no protegidas).

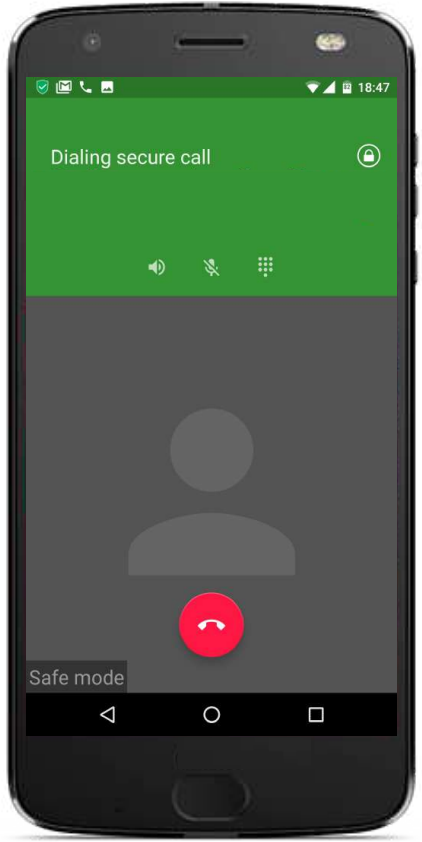
3: Uso de la Funcionalidad Secure Phone

ENLACE SEGUROS DE VOZ

Los enlaces seguros “de punta a punta” para voz y mensajes, sólo pueden ser realizados entre dos o más dispositivos que utilicen servicios de **KAYMERA** (**CipherBond** / **CipherFort**), los cuales operan bajo el mismo entorno de encripción de grado militar.

Ambas “puntas” (extremos) requieren de una conexión a Internet durante el enlace entre ambas (WiFi y/o datos 3G/4G).

La notificación de encontrarse bajo un enlace seguro se realiza a través de un ícono que aparece en la parte superior derecha con la imagen de un **Candado color “VERDE”** en la pantalla de discado/marcado del Teléfono Inteligente.



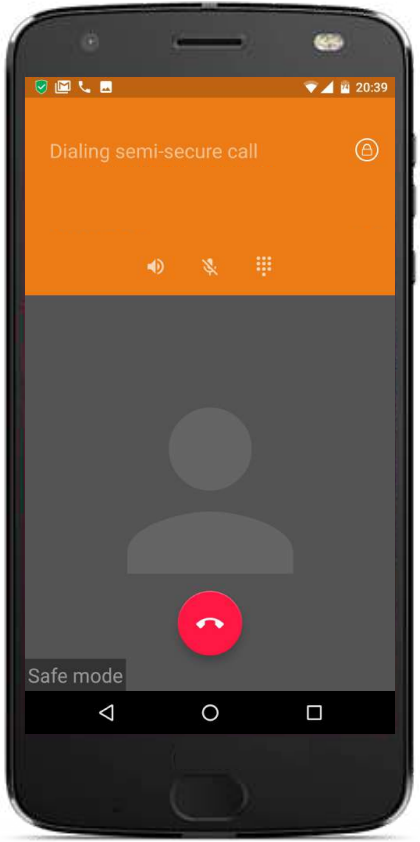
3: Uso de la Funcionalidad Secure Phone

ENLACE SEMI-SEGUROS DE VOZ

Los enlaces semi-seguros sólo aplican para voz y suceden cuando son realizados entre un dispositivo que utilice los servicios de **KAYMERA** (**CipherBond** / **CipherFort**) y uno que no cuenta con ellos.

Si esta opción ha sido habilitada para la cuenta del usuario, los enlace de voz desde el dispositivo móvil - teléfono inteligente serán encriptados únicamente para ese lado del enlace.

La notificación de encontrarse bajo un enlace semi-seguro se realiza a través de un ícono que aparece en la parte superior derecha con la imagen de un **Candado color "NARANJA"** en la pantalla de discado/marcado del Teléfono Inteligente.

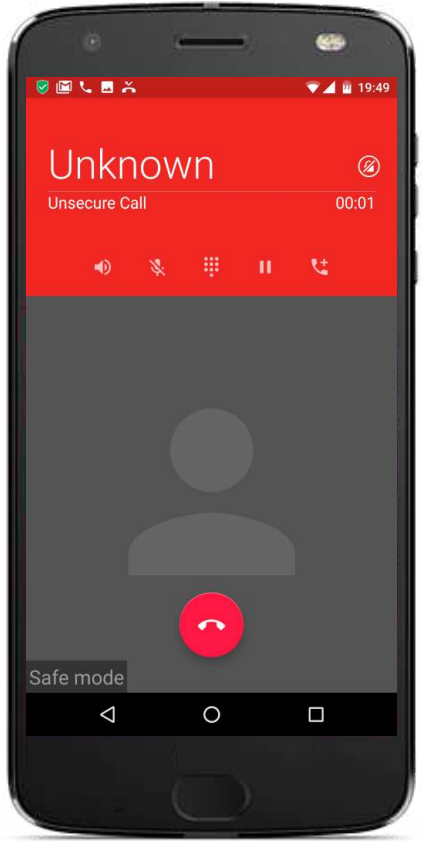


3: Uso de la Funcionalidad Secure Phone

ENLACE NO SEGUROS DE VOZ

El Equipo **CipherFort** puede ser utilizado para recibir enlaces de voz no-seguros a través de llamadas telefónicas de cualquier contacto; en este caso la comunicación será abierta (no encriptada).

La notificación de encontrarse bajo un enlace no seguro se realiza a través de un ícono que aparece en la parte superior derecha con la imagen de un **Candado color "ROJO"** en la pantalla de discado/marcado del Teléfono Inteligente.

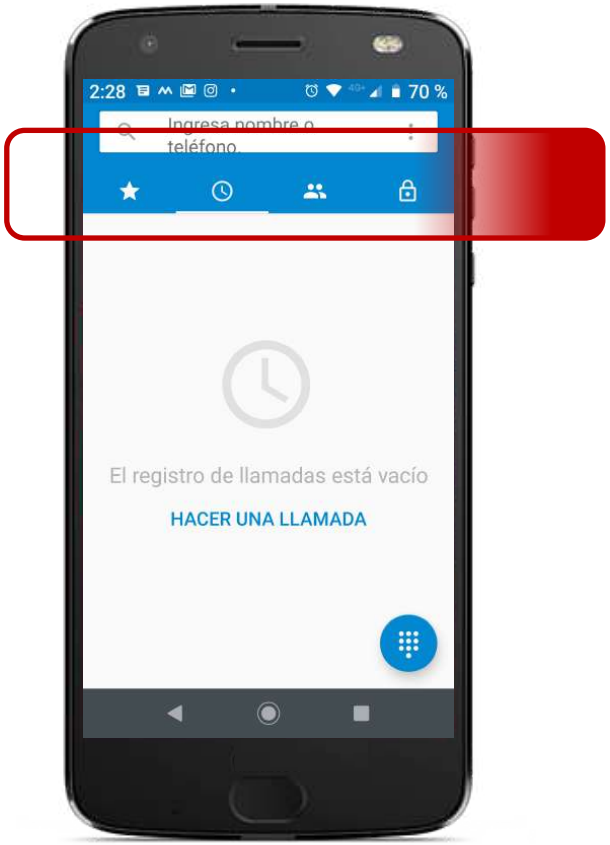


3: Uso de la Funcionalidad Secure Phone

Al abrir la sección del Teléfono Inteligente se presentarán **4 opciones de vista – secciones** para realizar los **Enlaces de Voz**:

- **Favoritos.**
- **Histórico.**
- **Contactos.**
- **Contactos Seguros.**

Para iniciar un Enlace Seguro y Semi-Seguro de voz o una llamada telefónica, simplemente deberá pulsar / hacer “click” en el Contacto en cualquiera de las secciones.



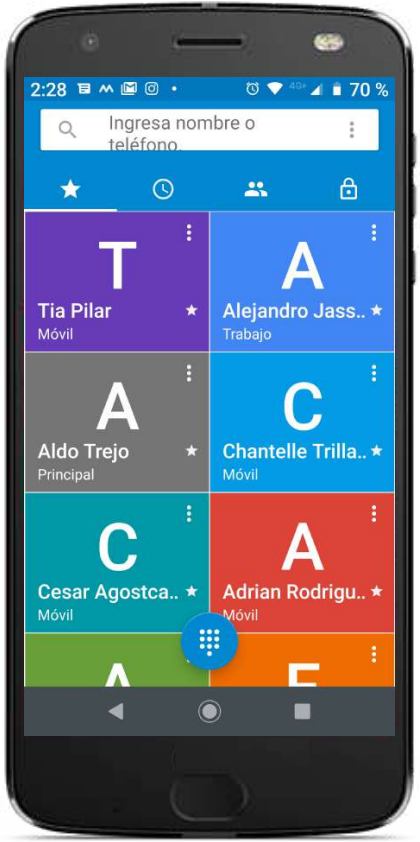
3: Uso de la Funcionalidad Secure Phone

FAVORITOS

Marcados con un icono con imagen de “**estrella**” - esta “sección” se utiliza para enlaces de voz de manera rápida a los números favoritos y más recientes, pulsando el “contacto” provocará el inicio de un Enlace de Seguro y Semi-Seguro de Voz, o una llamada telefónica.

Los Contactos con **Enlace Seguro de Voz** aparecerán marcado con un icono con imagen de “**candado color verde**” en su esquina inferior derecho.

Nota: Esta lista contiene contactos tanto para enlace de voz Seguro y Semi-seguro como para llamadas telefónicas



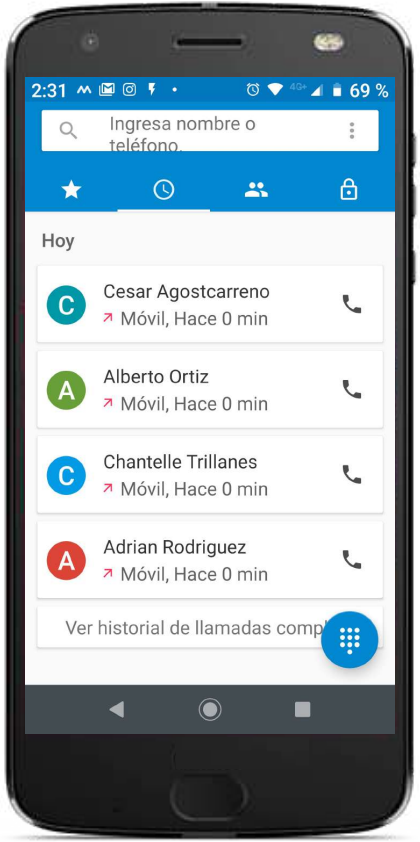
3: Uso de la Funcionalidad Secure Phone

HISTÓRICO

Marcados con un icono con imagen de "**reloj**" - esta "sección" se utiliza para mostrar el registro histórico tanto para enlace de voz Seguro y Semi-seguro como para llamadas telefónicas.

Los íconos de "flecha hacia arriba" indicarán que el enlace o llamada se originó en el Teléfono Inteligente, y los íconos de "flecha hacia abajo" indicarán que el enlace o llamada se recibió en el Teléfono Inteligente.

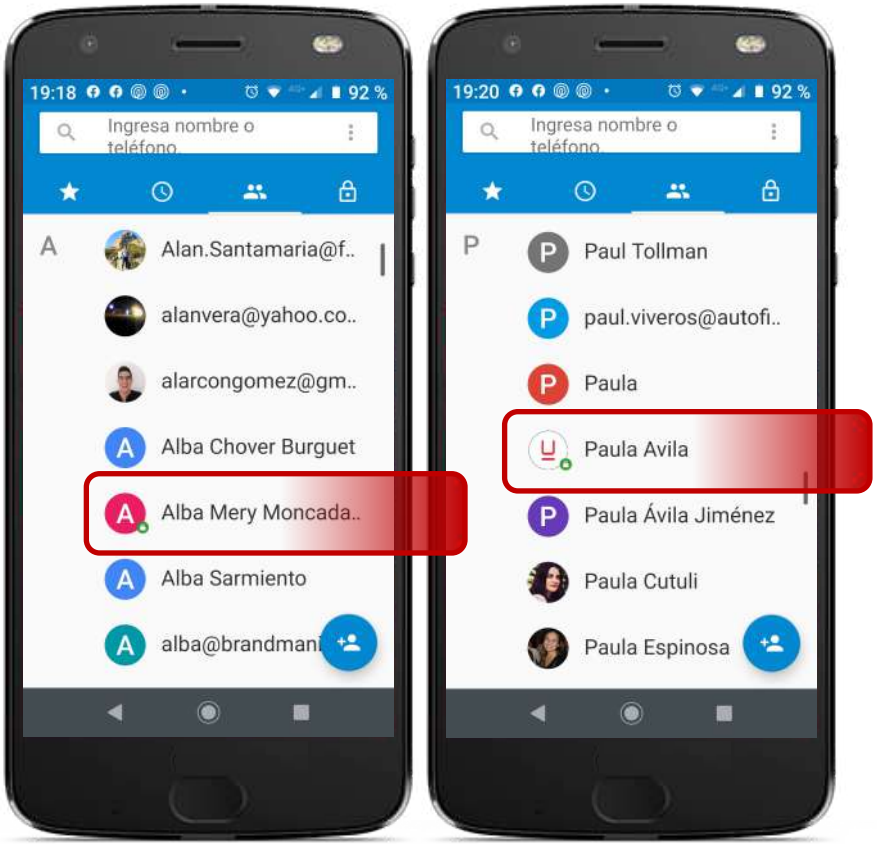
En estos casos, el ícono de "flecha" en color "verde" indica que el enlace fue realizado o la llamada fue atendida y de color "rojo" cuando no lo fue.



3: Uso de la Funcionalidad Secure Phone

TODOS LOS CONTACTOS
Marcados con un icono con imagen de "**dos personas**" - esta "sección" se utiliza para mostrar todos los contactos registrados en el directorio del Teléfono Inteligente (con Enlace Seguro y Semi-seguro de Voz y no seguros – llamadas telefónicas).

Los Contactos con **Enlace Seguro de Voz** aparecerán marcado con un icono con imagen de "**candado color verde**" en su esquina inferior derecho.

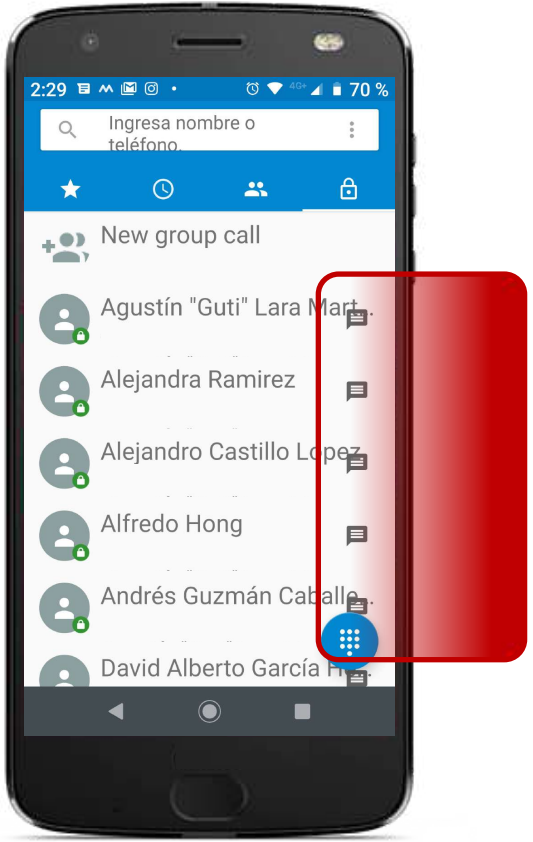


3: Uso de la Funcionalidad Secure Phone

CONTACTOS “SEGUROS”

Marcados con un icono con imagen de “un **candado cerrado**” - esta “sección” se utiliza para mostrar exclusivamente los contactos con Enlace Seguro de Voz a partir de todos Contactos registrados en el Teléfono Inteligente.

Esta misma pantalla puede ser utilizada para el envío de Mensajes Seguros a los contactos, para ello se debe hacer “click” / pulsar el ícono situado del lado derecho del nombre del Contacto Seguro con forma de ”diálogo”.



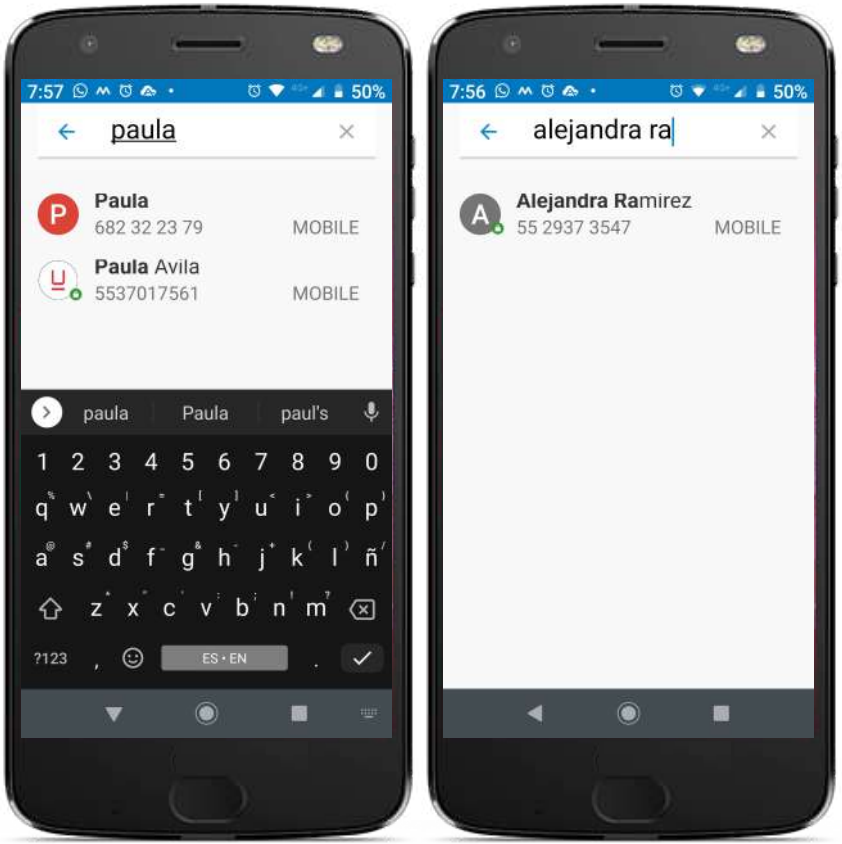
3: Uso de la Funcionalidad Secure Phone

SINCRONIZACIÓN DE CONTACTOS

Para que un contacto, ya sea para realizar Enlaces Seguros o Semi-seguros de Voz, aparezca disponibles dentro de la sección **Secure Phone** de **CipherFort**, estos deberán estar previamente disponibles en la aplicación Google Contacts o en el Directorio interno del Teléfono Inteligente.

Los Contactos con **Enlace Seguro de Voz** aparecerán marcado con un icono con imagen de "**candado color verde**" en su esquina inferior derecho.

La función "**buscar**" de la parte superior puede ser utilizada con una fracción del nombre del contacto o de su número.



3: Uso de la Funcionalidad Secure Phone

MARCADOR / DISCADO TELEFÓNICO

Utilice la funcionalidad de discado de su Teléfono Inteligente tal y como lo realizaría de manera normal, utilizando el ícono con imagen de “10 puntos” para ello.

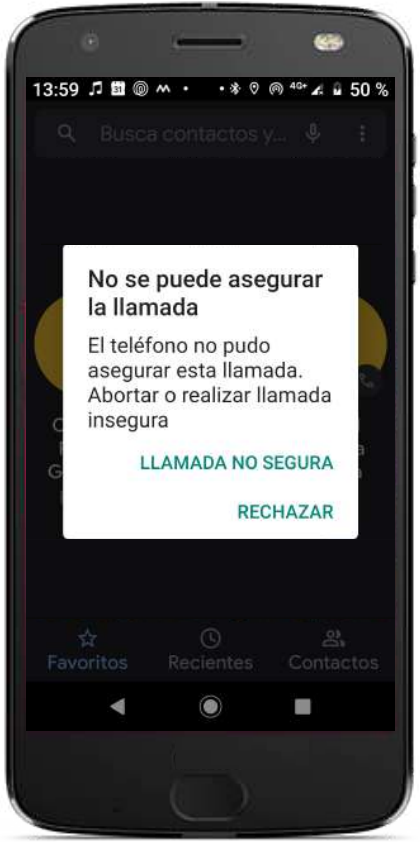
El Equipo **CipherFort** identificará automáticamente si usted está realizando un enlace con un Contactos Seguros.

3: Uso de la Funcionalidad Secure Phone

ASEGURAMIENTO DE ENLACES DE VOZ

El Equipo **CipherFort** opera utilizando cualquier conexión de internet en el Teléfono Móvil, ya sea **Red Móvil (mínimo 3G) o Wi-Fi** en cualquier parte del mundo. Por lo anterior:

- Para realizar un Enlace de Voz se require de **acceso rápido y abierto (no bloqueado) a internet**.
- Cuando el Teléfono Inteligente no logre la conexión con el servidor KAYMERA, la conexión a internet sea inestable o existan fugas o bloqueos, **el Enlace de Voz no podrá ser realizado.**

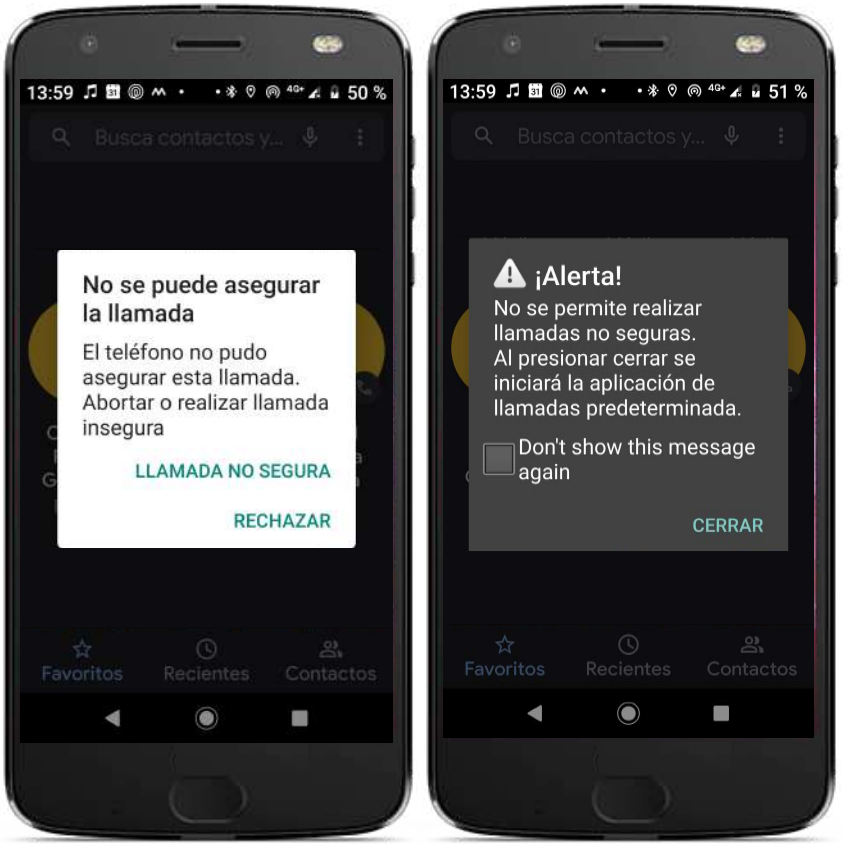


3: Uso de la Funcionalidad Secure Phone

ASEGURAMIENTO DE ENLACES DE VOZ
La aplicación mostrará una notificación de ello para prevenir al usuario.

- Si la opción seleccionada es “**Llamada no segura**”, el Equipo **CipherFort** ejecutará de manera normal (sin utilizar la aplicación) una llamada telefónica mediante la función de discado.

- Si la opción seleccionada es “**Rechazar**”, el Equipo **CipherFort** simplemente cancelará la operación para realizer un Enlace de Voz, ya sea Seguro o Semi-Seguro.

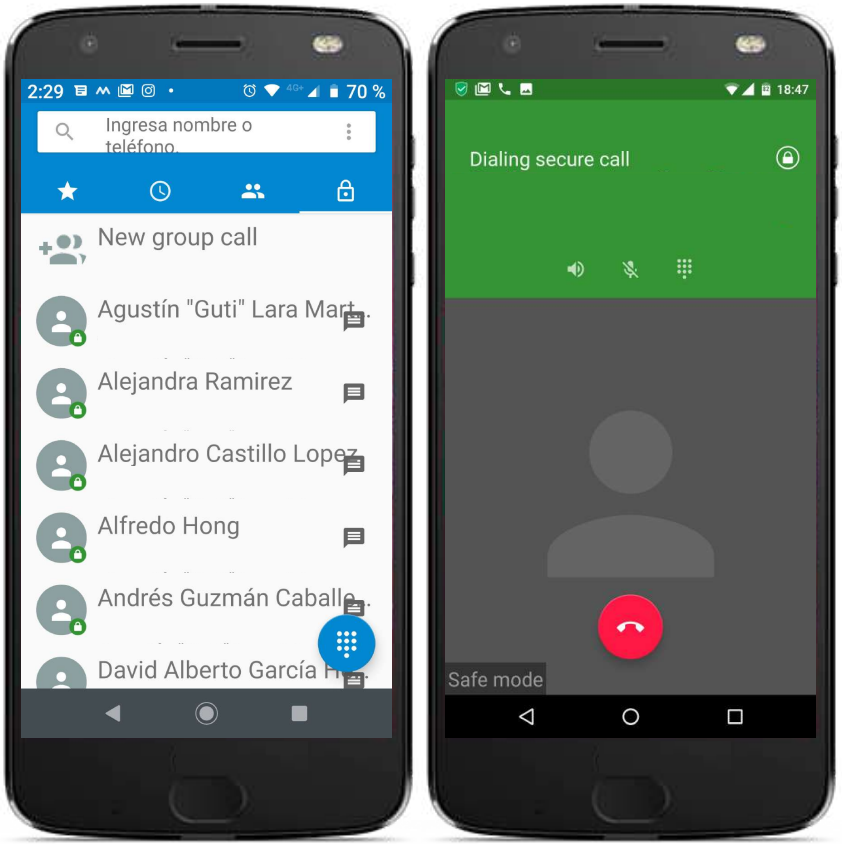


3: Uso de la Funcionalidad Secure Phone

TIPOS DE ENLACE DE VOZ

Recuerde que el comportamiento de cada tipo de Enlace de Voz depende del tipo de Contacto con el que lo establezca:

- **Enlaces Seguros de Voz**:
  1. Se logran únicamente cuando el contacto - **destinatario** cuenta con un servicio **KAYMERA** activa en su Teléfono Inteligente (**CipherBond** o **CipherFort**).
  2. Son **ilimitados en cantidad y tiempo.**
  3. Se identifican a través del ícono en la esquina inferior derecha del contacto con la imagen de un "**candado color verde**"



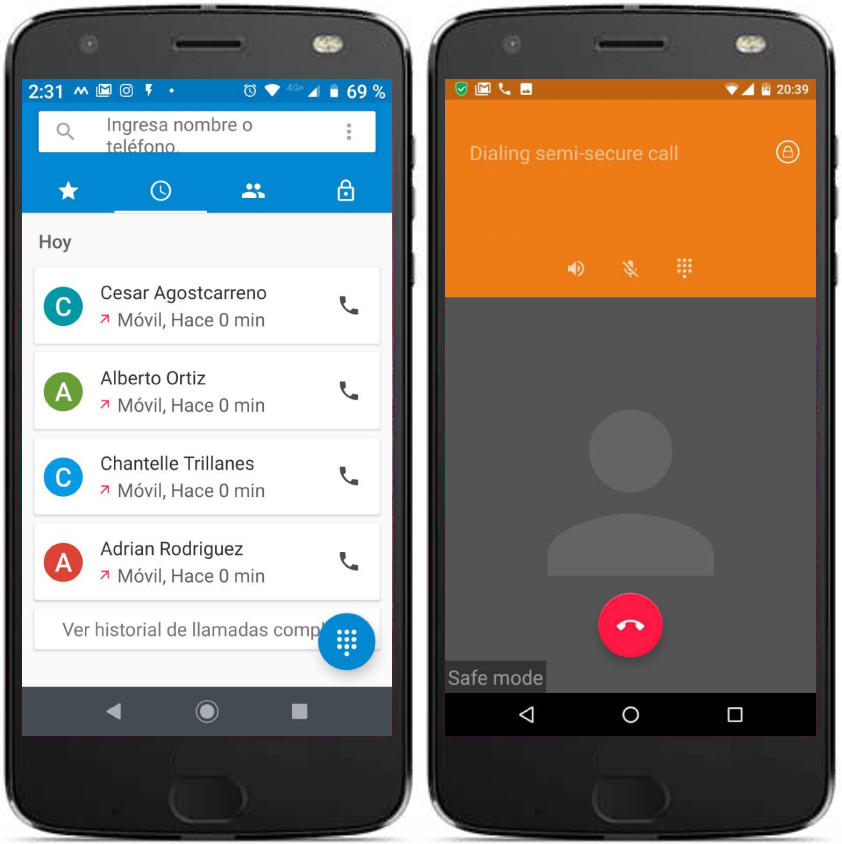
3: Uso de la Funcionalidad Secure Phone

TIPOS DE ENLACE DE VOZ

Recuerde que el comportamiento de cada tipo de Enlace de Voz depende del tipo de Contacto con el que lo establezca:

- **Enlaces Semi-seguros de Voz**:
  1. Se pueden realizar a cualquier número telefónico (fijos o móviles) que no cuente con el servicio **KAYMERA**.
  2. Es necesario haber contratado/contratar esta funcionalidad para poder utilizarla.
  3. La parte protegida (encriptada) es del lado del Emisor (con **CipherFort**) mientras la contraparte – Receptor) no lo está.
  4. Aplican tarifas adicionales por minuto de enlace según destino.

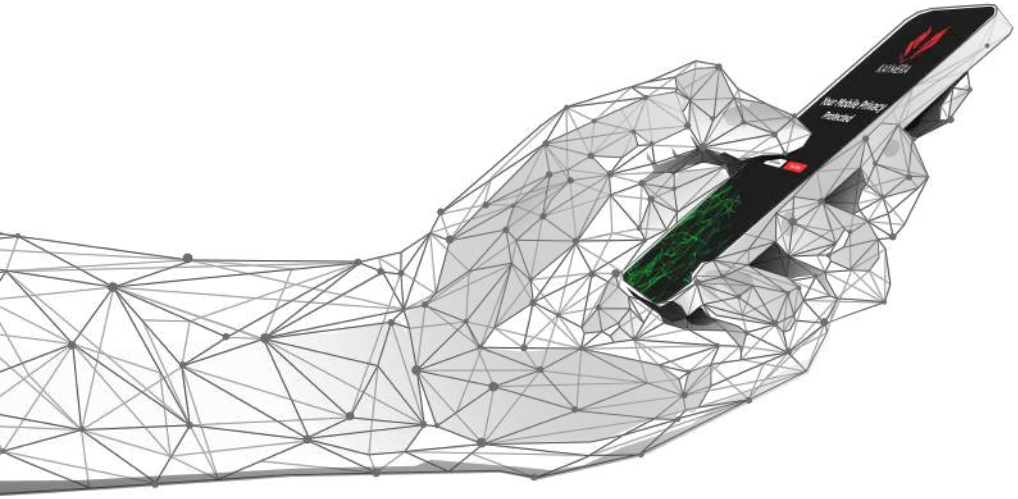
https://invezt.co/kaymera/es/tarifas/enlaces-semi-seguros-de-voz/



KAYMERA High-End Mobile Security | invezt Disruptive Capital

USO DE LA FUNCIONALIDAD

ENLACES SEGUROS DE VOZ **GRUPALES**



Manual de Uso de las Funciones de Comunicación CipherFort

4: Uso de la Funcionalidad Group Calls

El Equipo **CipherFort** puede realizar **Enlaces Seguros de Voz** con múltiples Contactos Seguros de manera simultánea a modo de una **Audio Conferencia**, identificadas como **“Group Calls”**.

Para lo anterior, se utilizarán los **dos íconos** que presenta para funciones de comunicación:

CIPHERBOND
Configuración de su perfil de identificación en los Enlaces Seguros de Voz en Grupo..

SECURE PHONE
Creación de Grupos y Ejecución de los Enlaces Seguros de Voz en Grupo.

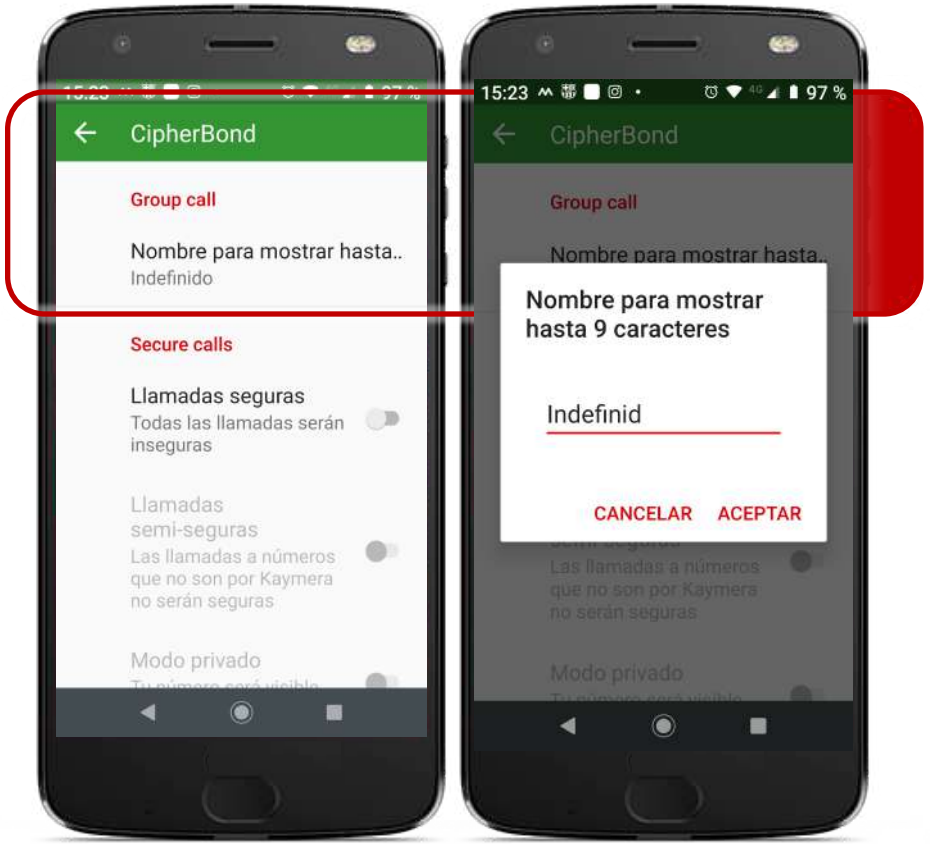
4: Uso de la Funcionalidad Group Calls

IDENTIFICADOR EN GRUPOS

A modo de que cada participante del Enlace Seguro de Voz en Grupo se identifique antes los demás, se requiere establecer una etiqueta de identificación de manera previa al uso de estas.

Utilizando el ícono de **CIPHERBOND** y el **Menú de Configuración** (descrito en una siguiente sección de este Manual) podrá identificar la opción **Group call**.

Al pulsar / hacer "click" sobre esta opción, se presentará el espacio para definir el **Nombre para mostrar**, pudiendo hacerlo con una longitud máxima de 9 caracteres (se pueden utilizar letras, números, caracteres especiales e incluso "emoticones").



4: Uso de la Funcionalidad Group Calls

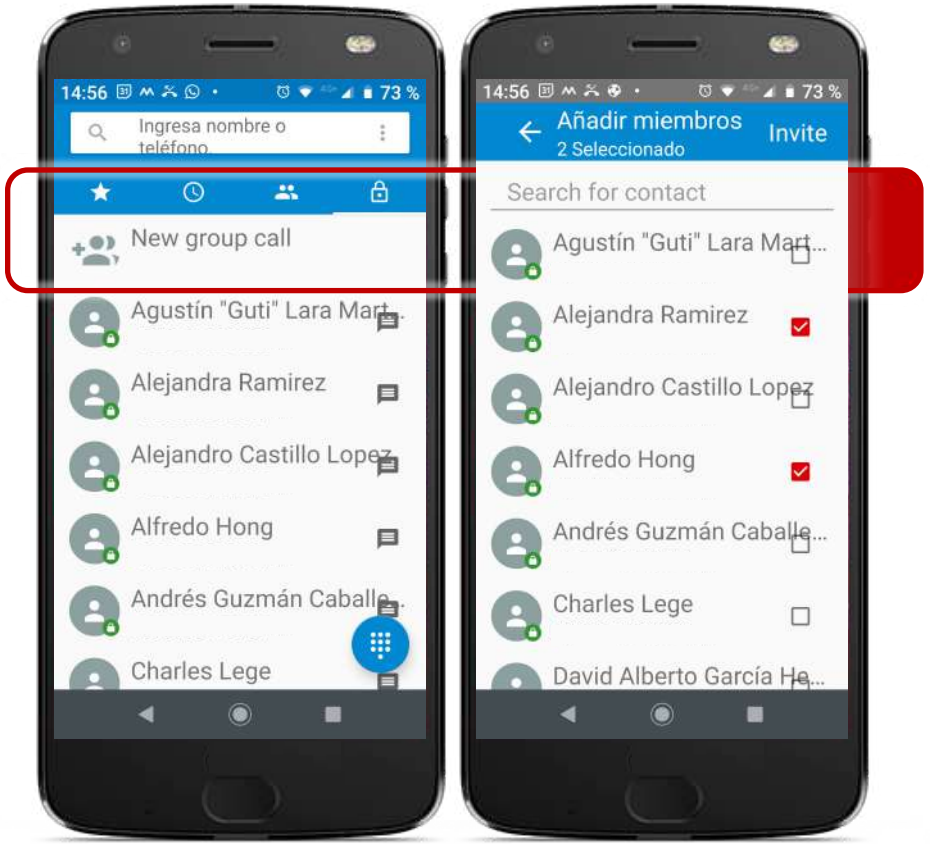
CREACIÓN DE GRUPOS

Utilizando el ícono de **SECURE PHONE**, se debe acceder a la sección donde se encuentran los **CONTACTOS SEGUROS**, identificada por el ícono con imagen de un "**candado cerrado**".

Al pulsar / hacer "click" sobre esta opción, se habilitará una "**casilla de selección**" al lado derecho de cada uno de los contacto seguros.

Se podrán seleccionar hasta un máximo de **20 contactos** seguros para realizar un **Enlace de Voz en Grupo**.

Se puede utilizar la opción "buscar" en la parte superior de la pantalla si así se requiere

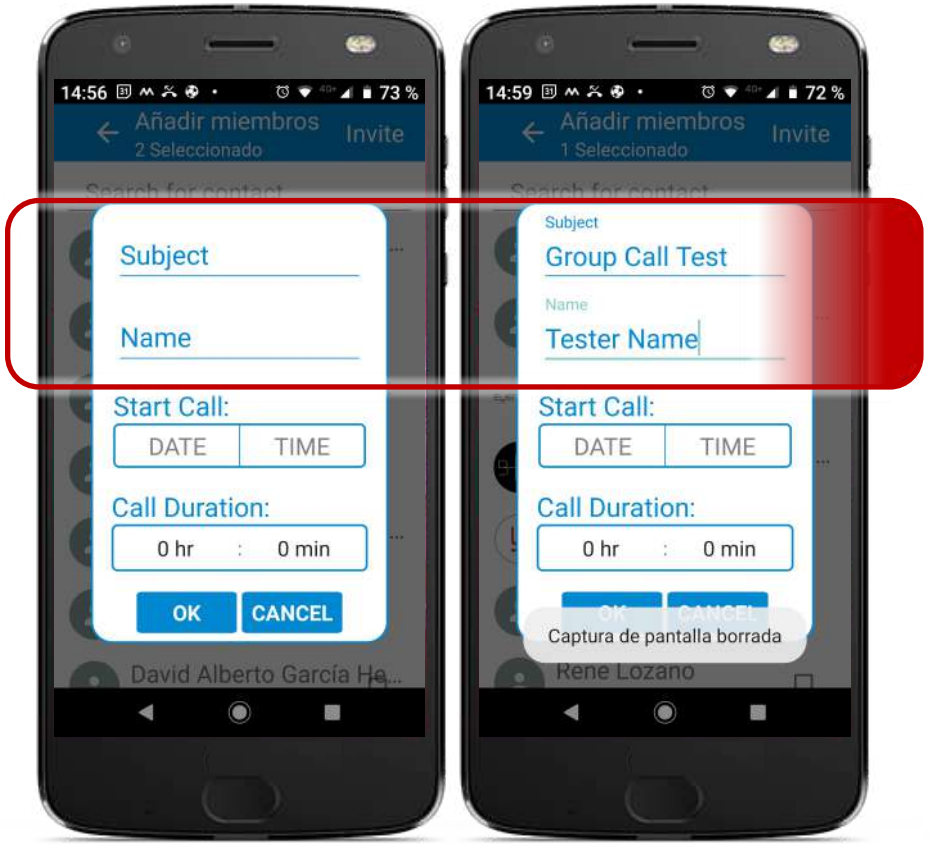


4: Uso de la Funcionalidad Group Calls

PROGRAMACIÓN DE UN ENLACE DE GRUPO
El equipo **CipherFort** dará acceso al **menú de programación del Enlace Seguro de Voz en Grupo**, que incluye:

- **Subject [Asunto]**: Se utiliza para dar un título o identificar la temática de la Audio Conferencia en Grupo.
- **Name [Nombre]**: Se utiliza para registrar el nombre del Organizador o Anfitrión de la Audio Conferencia en Grupo

Ambos datos se incluirán en la Invitación o Notificación que recibirán los Invitados o Convocados al Enlace Seguro de Voz en Grupo.

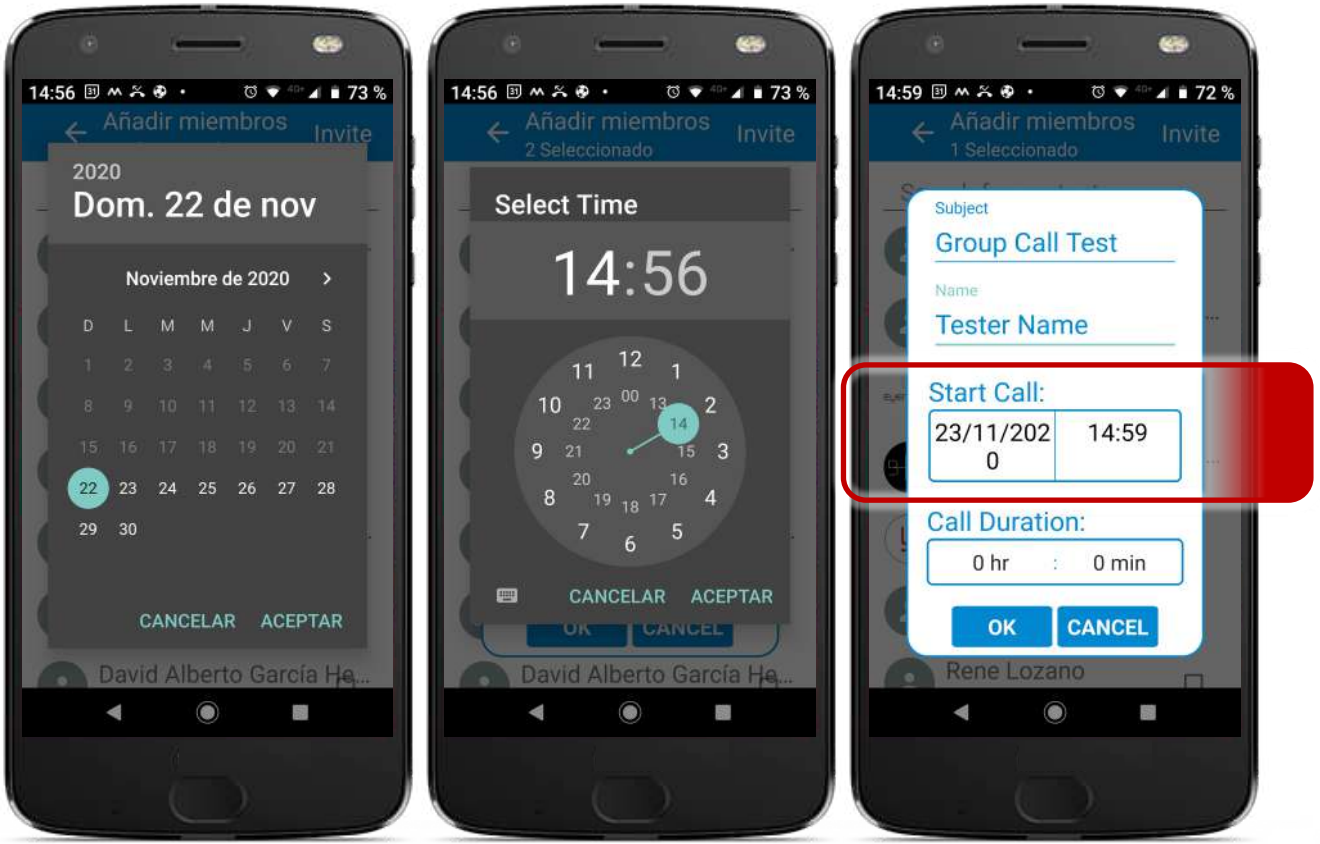


4: Uso de la Funcionalidad Group Calls

PROGRAMACIÓN DE ENLACE DE GRUPO

A continuación se registrará la **fecha de realización y la hora de inicio** del Enlace Seguro de Voz en Grupo.

Se debe considerar que el Enlace Seguro de Voz en Grupo sólo estará habilitado en esa fecha y partir de la hora establecida.

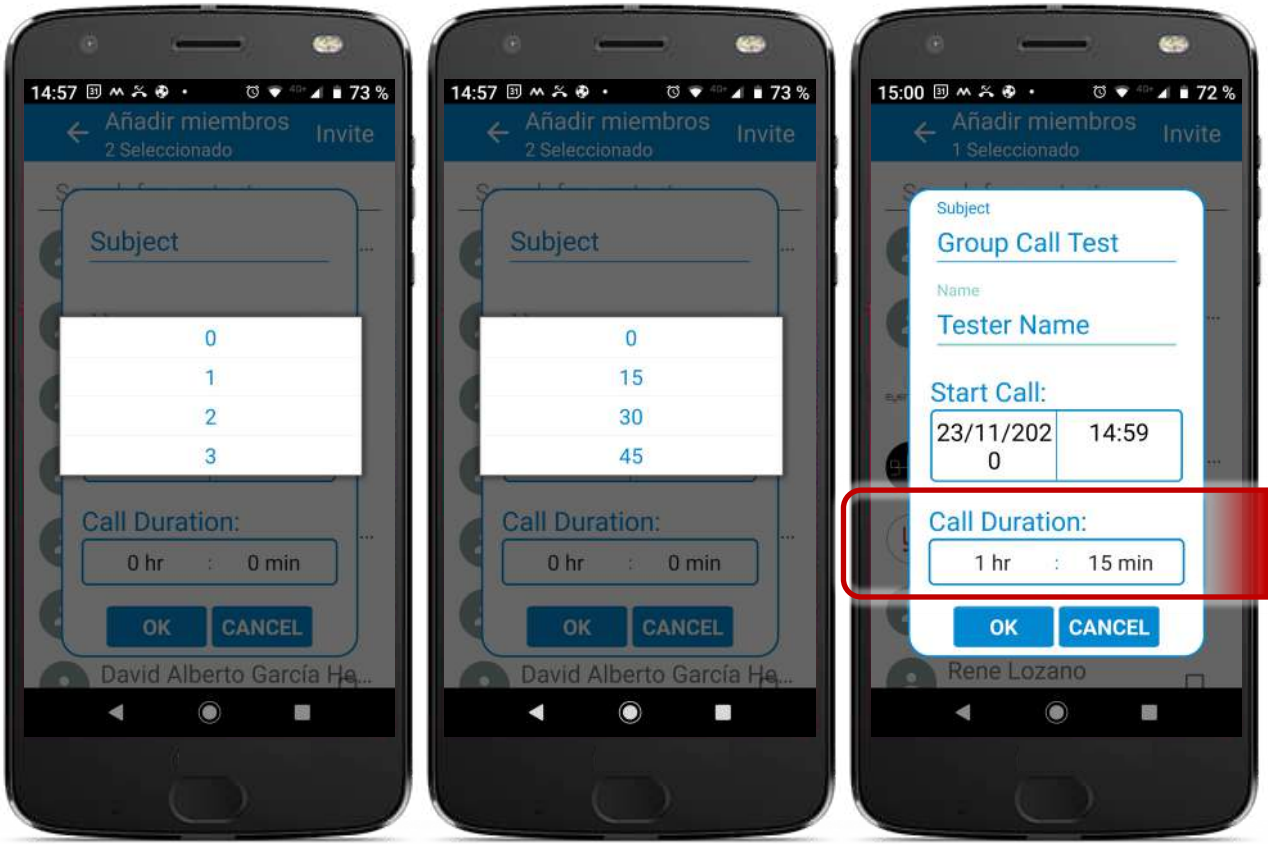


4: Uso de la Funcionalidad Group Calls

PROGRAMACIÓN DE ENLACE DE GRUPO

A continuación se registrará una **duración informativa** para el Enlace Seguro de Voz en Grupo en múltiplos de una hora y fracciones de 15 minutos.

El Enlace Seguro de Voz en Grupo se mantendrá abierto aunque el tiempo registrado concluya.



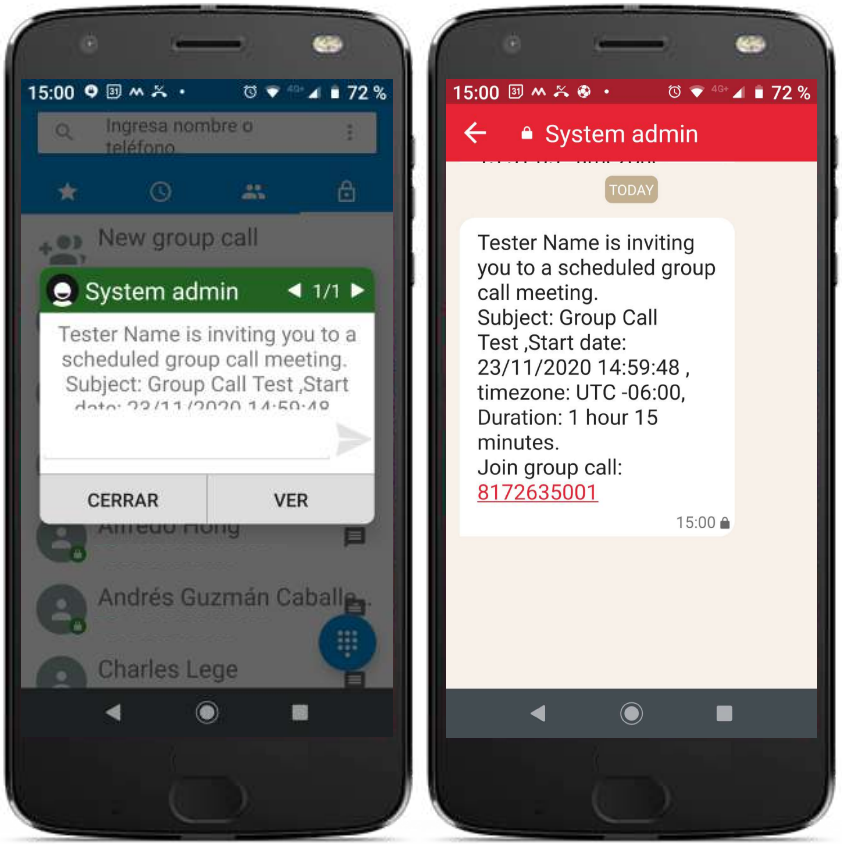
4: Uso de la Funcionalidad Group Calls

NOTIFICACIÓN DE ENLACE DE GRUPO
Cada uno de los participantes al **Enlace Seguro de Voz en Grupo**, recibirán una notificación, tanto los Invitados como el Anfitrión a esta.

En esta notificación/invitación se incluye

- **Descripción e Información**: incluyendo el título de la Audio Conferencia, el Organizados o Anfitrión, así como la fecha de realización y la hora de inicio (**no se podrá accesar al enlace si no hasta cumplida la hora de inicio**).

- **Liga de acceso**: a modo de un número telefónico que se utilizará como Enlace Seguro de Voz.

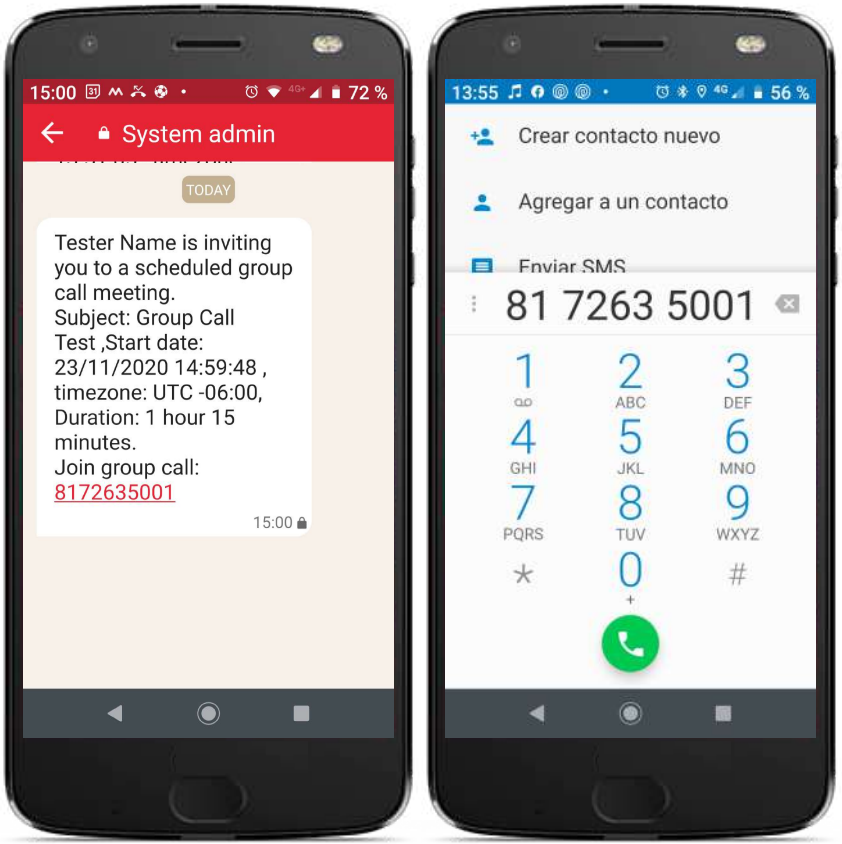


4: Uso de la Funcionalidad Group Calls

PARTICIPACIÓN EN UN ENLACE DE GRUPO

Al recibir una invitación/notificación (del System admin) para participar en un Enlace Seguro de Voz en Grupo, el mensaje contendrá una **liga de acceso** a modo de número de 10 dígitos debajo de la leyenda "**Join group call**".

Al pulsar / hacer "click" sobre esta liga, se invocarán a la función para la generación de llamadas telefónicas instaladas y habilitadas en el **CipherFort.**



4: Uso de la Funcionalidad Group Calls

PARTICIPACIÓN EN UN ENLACE DE GRUPO
Una vez que el Equipo **CipherFort** realice la conexión al **Enlace Seguro de Voz en Grupo**, aparecerá la pantalla del Espacio (Room) asignado al mismo

En este se podrán visualizar las personas – contactos que ya se encuentren participando o paulatinamente las que se vayan conectando al **Enlace Seguro de Voz en Grupo.**

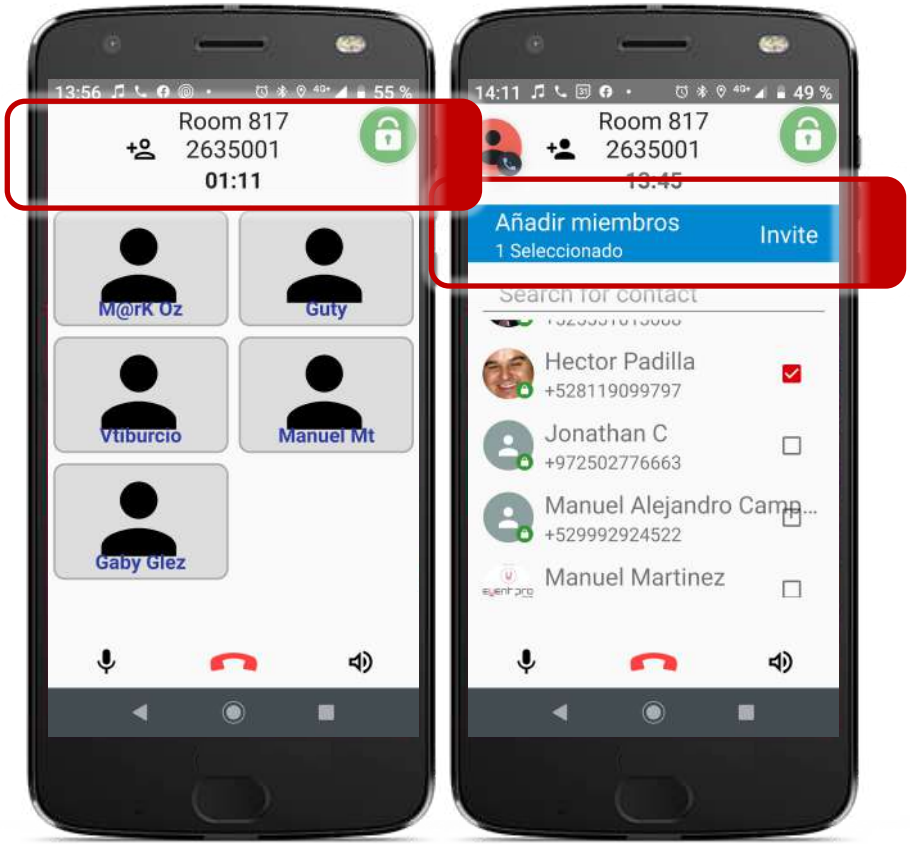
Cada íconos con imagen de "persona" representa a cada uno de los contactos participantes, pudiéndose identificar a través del Nombre que aparece debajo de los íconos y que es el registrado como Identificador por cada uno de ellos.

4: Uso de la Funcionalidad Group Calls

AGREGAR PARTICIPANTES AL GRUPO
Cualquier de los participantes en el **Enlace Seguro de Voz en Grupo** podrá **agregar mas participantes** a mismo en el momento que se desee.

Para ello se debe pulsar / hacer “click” sobre el ícono con imagen de “**personas con un símbolo de suma del lado izquierdo**”.

Esta función presentará el directorio de Contactos Seguros, donde se deberá señalar la “**casilla de selección**” al lado derecho de cada uno de los Contactos Seguros que se pretenda agregar al Enlace Seguro de Voz en Grupo y pulsar / hacer “click” sobre la palabra “Invite” (invitar) en la parte superior de la pantalla.

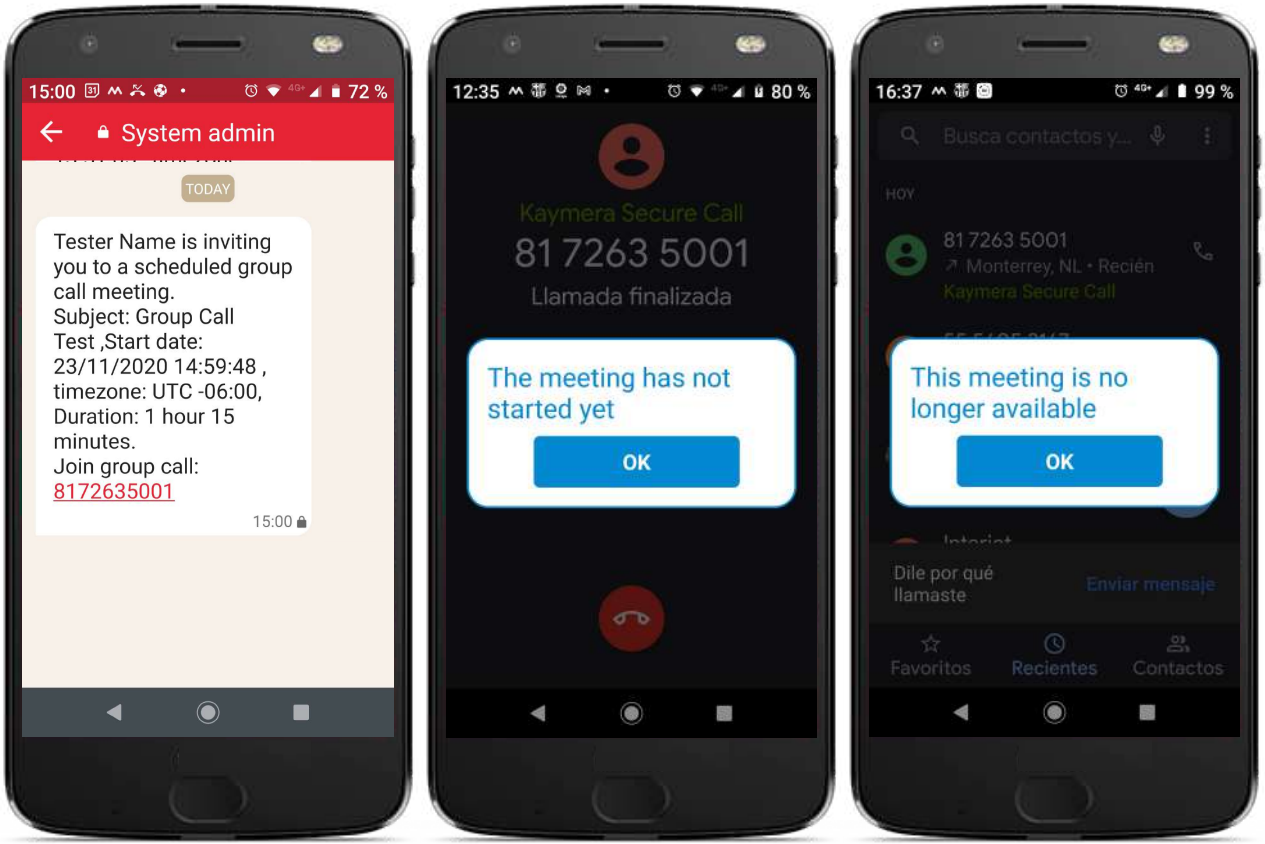


4: Uso de la Funcionalidad Group Calls

HORARIO DE PARTICIPACIÓN

La adhesión a un Enlace Seguro de Voz en Grupo debe realizarse **dentro del horario establecido** en la programación de este, incluso siendo el Anfritrión del mismo.

Los detalles del horario se pueden encontrar disponibles en la **invitación** generada para dicho Enlace.



4: Uso de la Funcionalidad Group Calls

TERMINACIÓN EN UN ENLACE DE GRUPO
Para abandonar el **Enlace Seguro de Voz en Grupo**, simplemente se debe pulsar / hacer "click" sobre el ícono con imagen de "**teléfono**" de color rojo ubicado en la parte central inferior de la pantalla.

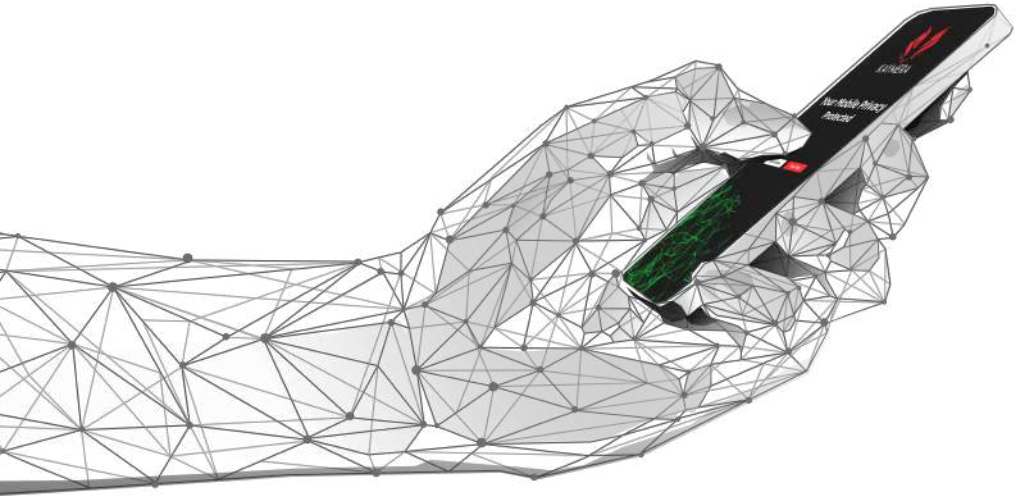
- Si posteriormente de abandonar el **Enlace Seguro de Voz en Grupo** se desea regresar a él, sólo se debe acceder mediante la notificación/invitación del mismo y repetir el proceso realizado para conectarse a este.

- Si el **Anfitrión/ Organizador** el Enlace Seguro de Voz en Grupo **abandona o desea abandonarlo**, este permitirá que el resto de los participantes se mantengan enlazados sin interrumpir el mismo.

KAYMERA High-End Mobile Security | invezt Disruptive Capital

USO DE LA FUNCIONALIDAD

MENSAJES SEGUROS **CIPHERBOND**



Manual de Uso de las Funciones de Comunicación CipherFort

3: Uso de la Funcionalidad Secure Calls

- El **CipherFort** / equipo Google Pixel con Sistema Operativo **Kaymera** dispone de **dos íconos para servicios de comunicación segura**:

SECURE PHONE
Es el acceso directo a la función de Enlaces de Voz.

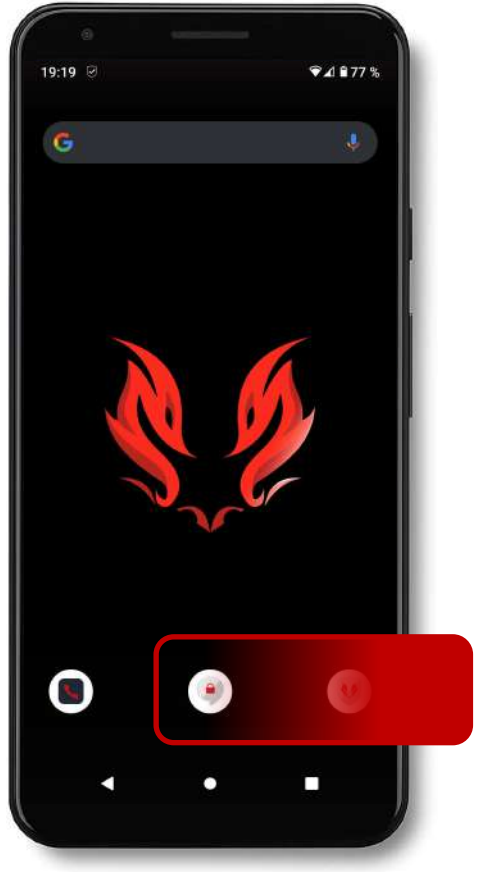
CIPHERBOND
Es el acceso directo a la función de Mensajes y envío de Archivos, así como a la Configuración de la Aplicación.

5: Uso de la Funcionalidad Mensajes Seguros

ÍCONO CIPHERBOND

Se utiliza para realizar el **ENVÍO DE MENSAJES Y COMPARTIR ARCHIVOS DE FORMA SEGURA** a través de la Aplicación **CipherBond**, con la cual se pueden realizar tres acciones diferentes:

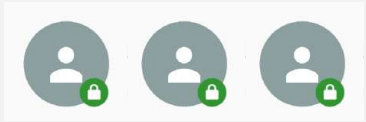
1. **Enviar Mensajes y Compartir Archivos de manera individual.**
2. **Enviar Mensajes y Compartir Archivos de manera grupal.**
3. De igual forma se utilizará para personalizar o modificar funciones dentro de la Aplicación.

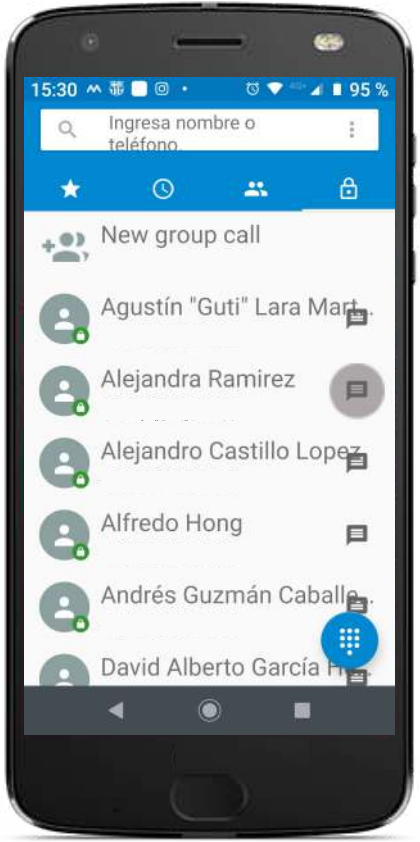


5: Uso de la Funcionalidad Mensajes Seguros

Recuerde que esta función se puede realizar únicamente con contactos (destinatarios) que cuenten con el servicio KAYMERA activo en su Teléfono Inteligente (CipherBond o CipherFort) y con datos de contacto registrados en el Directorio Telefónico del mismo:

1. Son **ilimitados en cantidad y frecuencia.**
2. Los Contactos se identifican a través del ícono en la esquina inferior derecha del contacto con la imagen de un "**candado color verde**"





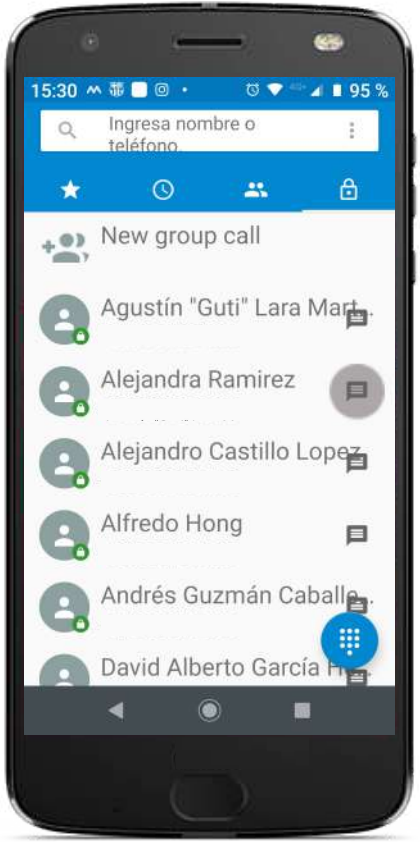
5: Uso de la Funcionalidad Mensajes Seguros

ENVÍO DE MENSAJES Y ARCHIVOS DE FORMA SEGURA

Para iniciar la creación y envío de un **Mensaje Seguro** en el Equipo **CipherFort**, existen dos formas para poder hacerlo:

La primera es desde la opción de **Contactos Seguros** (mediante el ícono de **Secure Calls**).

Utilice los íconos con la imagen de un **"Globo de Conversación"** que aparecen en la parte lateral derecha de cada uno de los contactos. Pulse / haga "Click" sobre el ícono que corresponda al contacto al que desea realizar el envío de un mensaje o archivo de forma segura.

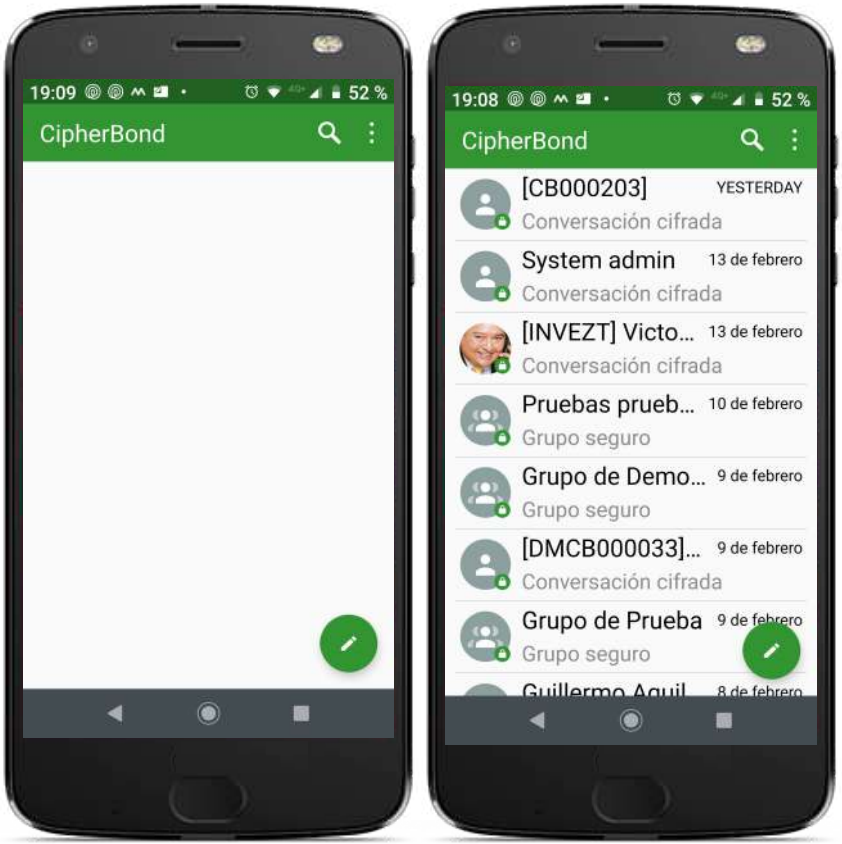


5: Uso de la Funcionalidad Mensajes Seguros

ENVÍO DE MENSAJES
Y ARCHIVOS DE FORMA SEGURA

La segunda forma de enviar mensajes y archivos de forma segura es utilizando la aplicación con el **ícono de CipherBond** que forma parte del Sistema Operativo **CipherFort**.

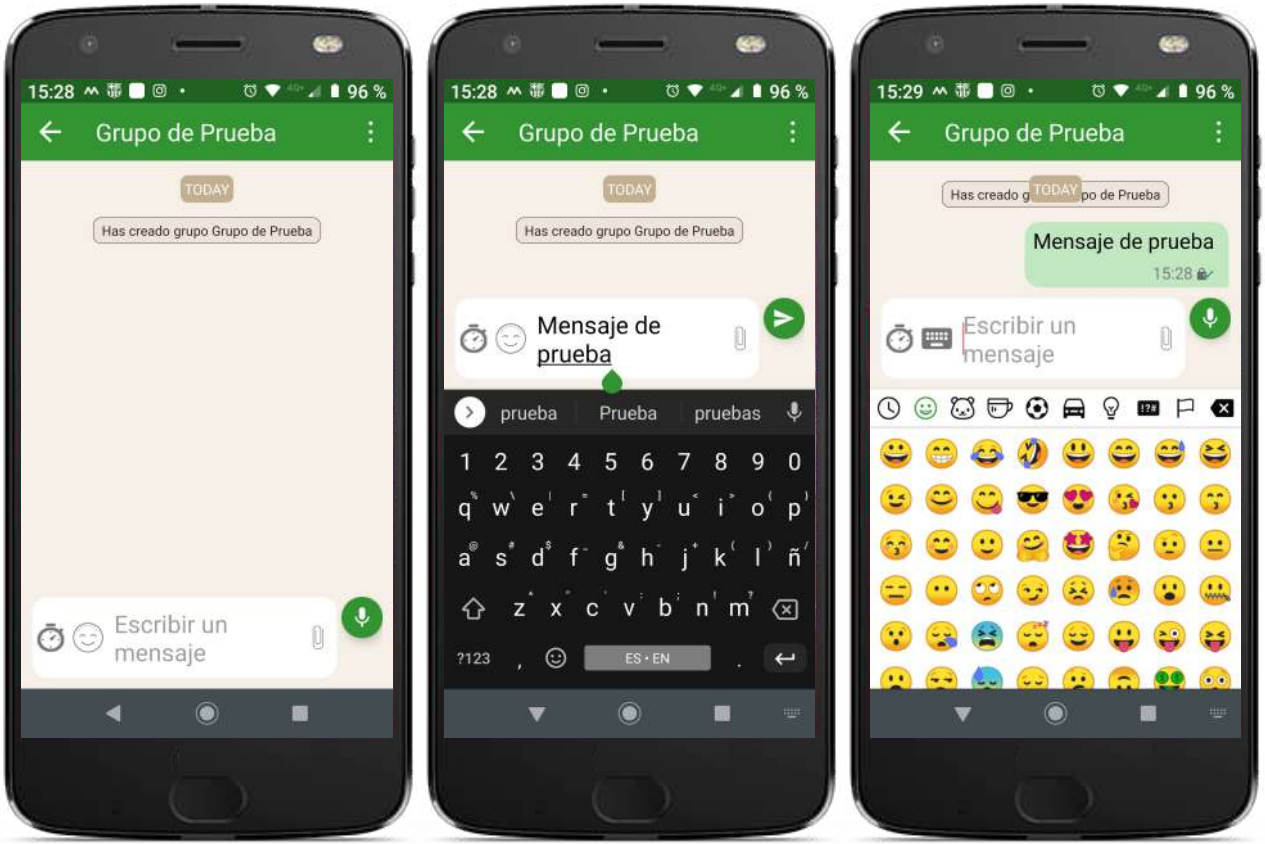
En la pantalla principal se utiliza el ícono con la imagen de un "**Lapiz"** que aparecen en la parte inferior derecha de la misma pantalla, pulse / haga "Click" sobre este ícono, e identifique al Contacto al que desea contactar con Mensaje Seguro. Para facilitar su búsqueda, utilice la opción de la parte superior en el ícono con la imagen de un "**Lupa".**



5: Uso de la Funcionalidad Mensajes Seguros

ENVÍO DE MENSAJES SEGUROS

Una vez que haya seleccionado el **Contacto** al que enviará un mensaje o archivo de forma segura, escriba el mensaje como lo haría en cualquier otra aplicación de mensajería en su Teléfono Inteligente, utilizando letras, números e incluso "emoticones".



5: Uso de la Funcionalidad Mensajes Seguros

RECEPCIÓN DE MENSAJES SEGUROS

Cuando se recibe un mensaje enviado por un usuario **KAYMERA**, este aparecerá en la pantalla de el Equipo **CipherFort**, **ícono CipherBond** y dentro del espacio de mensajes que corresponden al Usuario del que se recibe.

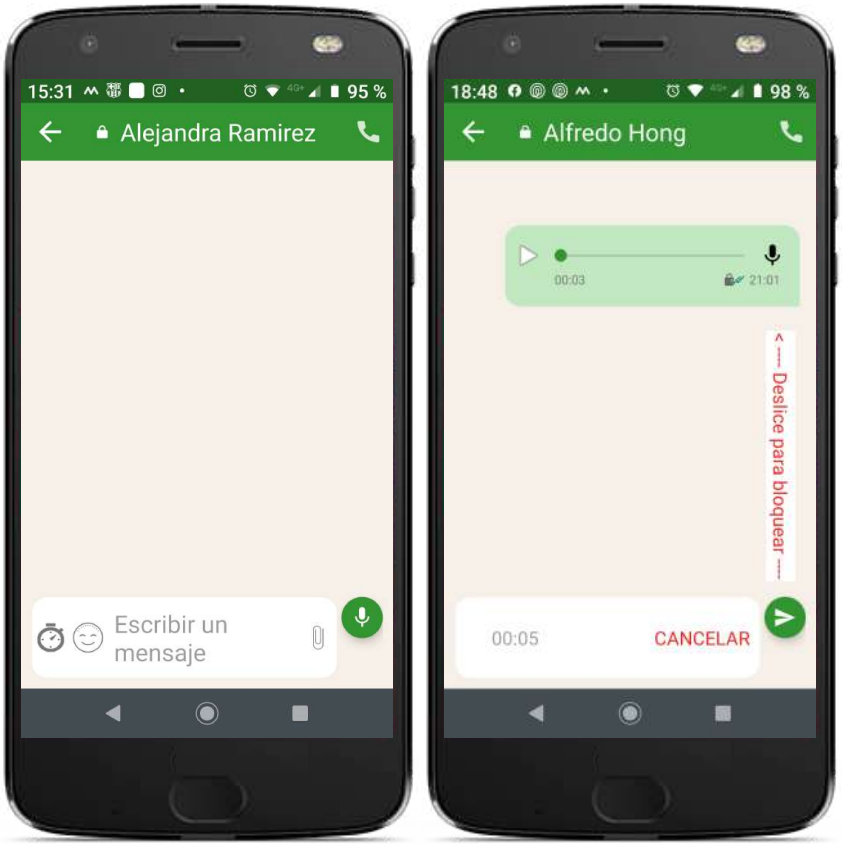
- Si la opción de "**Notificaciones**" ha sido activada, en la pantalla principal del Teléfono Inteligente aparecerá el mensaje recibido (sin necesidad de accesar a la aplicación CipherBond), donde se tendrán las opciones de "**Cerrar**" para consultarlo posteriormente o la opción de "**Ver**", la cual abrirá la Aplicación CipherBond para poder visualizarlo y en caso de requerirlo, contester al misma través de la función de **Envío Seguro de Mensajes**.

5: Uso de la Funcionalidad Mensajes Seguros

ENVÍO SEGURO DE NOTAS DE AUDIO/VOZ

Podrá enviar **Grabaciones de mensajes hablados o grabaciones de sonido** como Mensaje Seguro en el Equipo **CipherFort** utilizando el ícono con la imagen de un "**Micrófono"** que aparecen en la parte inferior derecha de la misma pantalla, pulsando / haciendo "click" sobre este

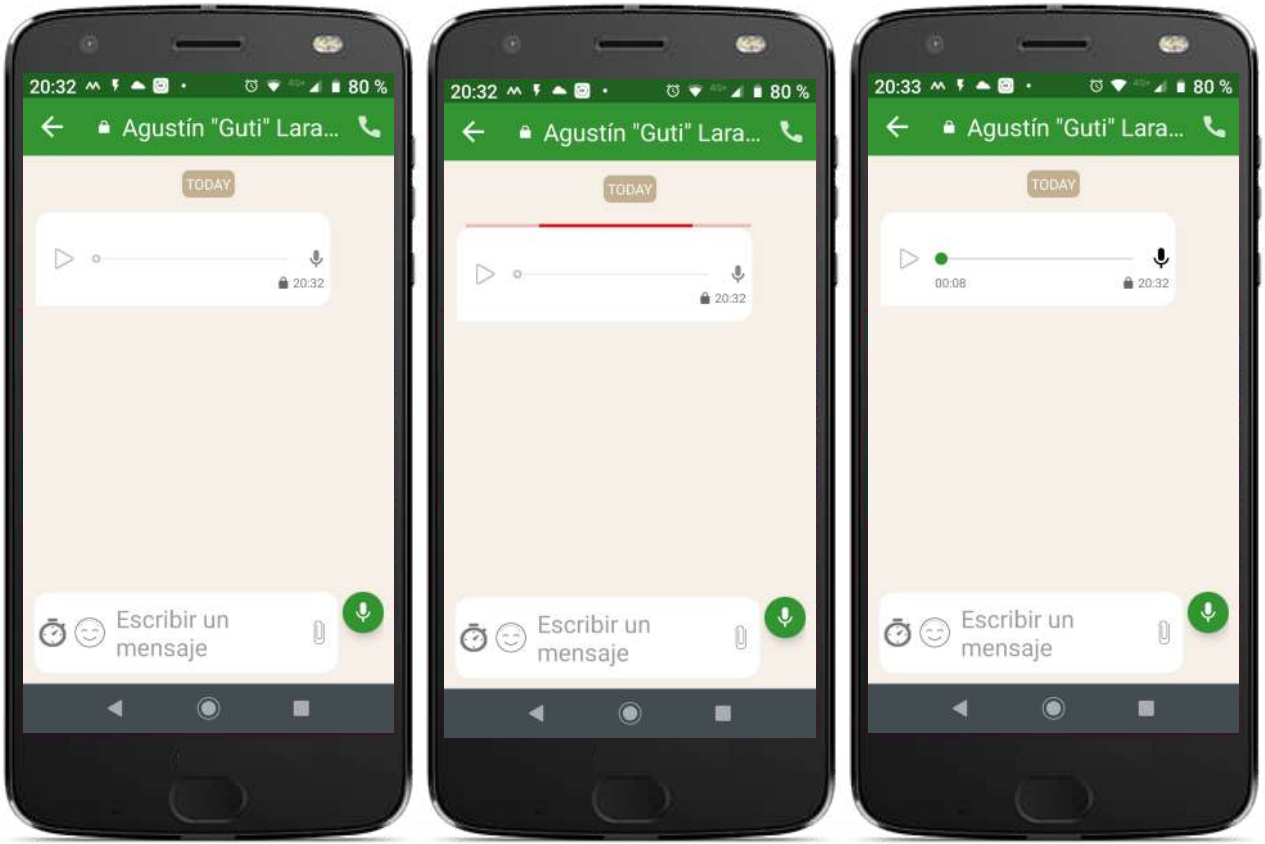
- Mantenga pulsado el ícono para realizar la grabación de su mensaje, hablando al micrófono de su Teléfono Inteligente.
- Si desea cancelar la grabación, deslice su dedo hacia el lado izquierdo sin dejar de presionar el ícono.
- Para su comodidad, deslice su dedo hacia arriba y suéltelo, esto bloquerá la función y podrá seguir grabando su mensaje el tiempo que desee, alterminar pulse / haga "click" en el ícono con imagen de "**fle**



5: Uso de la Funcionalidad Mensajes Seguros

RECEPCIÓN DE NOTAS DE VOZ/AUDIO

Cuando reciba una **Grabación de Audio** entre sus Mensajes Seguros de el Equipo **CipherFort**, esta deberá ser descargada en su Teléfono Inteligente para ser escuchada dentro de la Aplicación CipherBond, pulse / haga “click” sobre el mensaje, mismo que podrás escucharse cuando el ícono del lado izquierdp con imagen de “círculo” pase de color “blanco” a color “verde”.

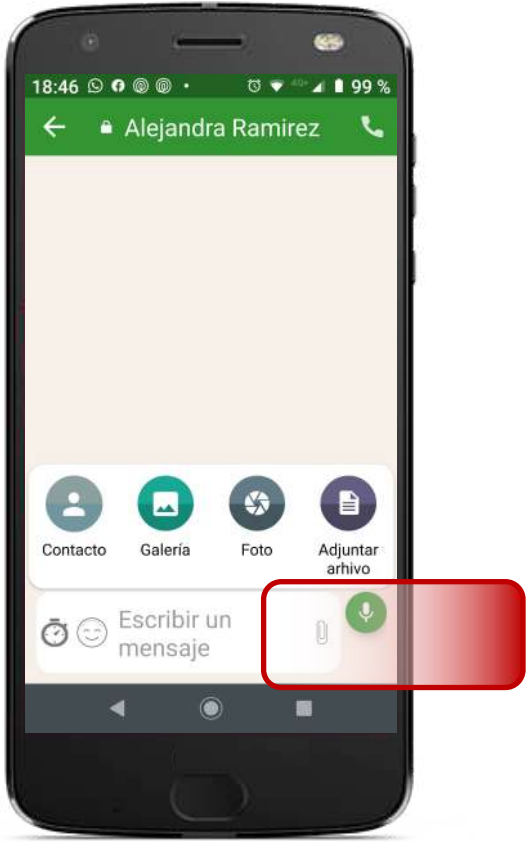


5: Uso de la Funcionalidad Mensajes Seguros

ENVÍO SEGURO DE ARCHIVOS ELECTRÓNICOS
Se realiza pulsando / haciendo "click" sobre el ícono con la imagen de un **"Clip"** ubicado del lado derecho de la zona de escritura de mensajes.

Los tipos de archivo que pueden ser enviados son:

1. **Contactos de su Directorio Telefónico.**
2. **Imágenes desde su Galería.**
3. **Imágenes utilizando la cámara fotográfica**
4. **Cuaquier otro tipo de Archivo ubicado en la memoria interna o externa de su Teléfono.**

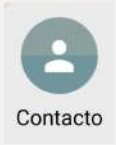


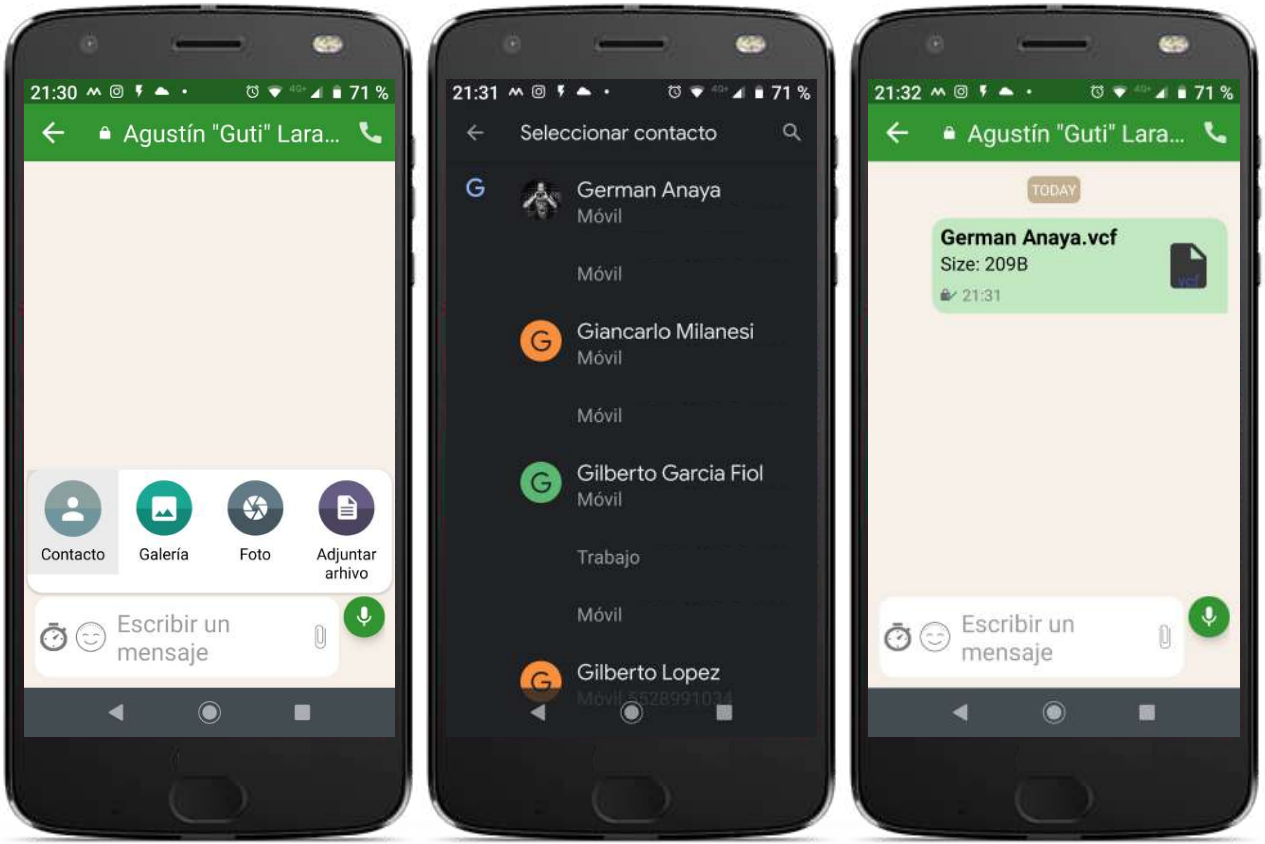
5: Uso de la Funcionalidad Mensajes Seguros

ENVÍO DE CONTACTOS

Pulse / haga "click" sobre el ícono con la imagen de "**Una Persona**",

Seleccione o busque la Tarjeta del Contacto que desea enviar en el mensaje y pulse / haga "click" sobre este.





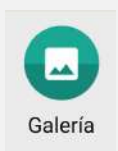
5: Uso de la Funcionalidad Mensajes Seguros

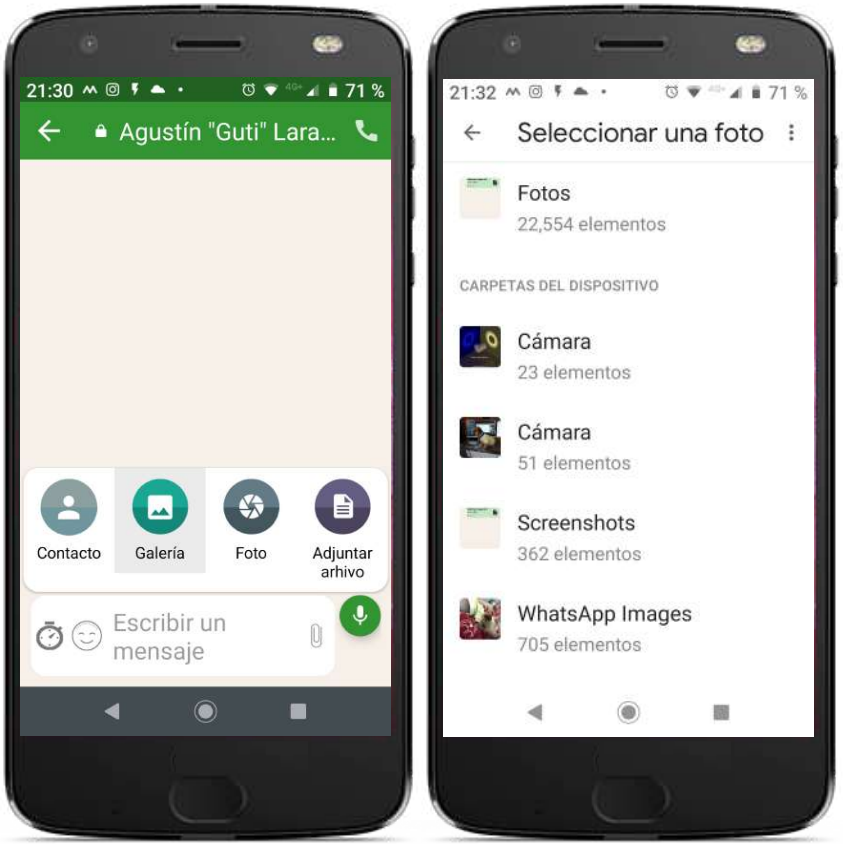
ENVÍO DE IMÁGENES
Pulse / haga “click” sobre el ícono con la imagen de “**Una Fotografía”.**

Seleccione o busque la imagen que desea enviar por Mensaje Seguro.

Deberá ubicarla a través de las diferentes carpetas de la **memoria interna** de su Teléfono Inteligente (no aplica para las **memorias externas “en la nube”** a las que se tenga acceso).

Una vez identificada y ubicada, pulse / haga “click” sobre ella para seleccionarla.





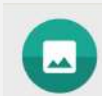
5: Uso de la Funcionalidad Mensajes Seguros

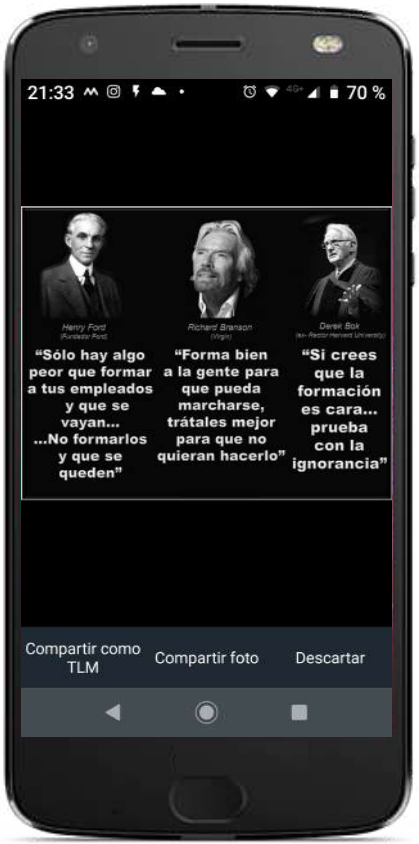
ENVÍO DE IMÁGENES

Una vez que la imagen seleccionada aparezca en la pantalla de su Teléfono Inteligente, en la parte baja aparecerán **diferentes opciones para su envío como Mensaje Seguro:**

1. **Compartir como TLM** provocará que la imagen sea enviada con la función de "bloqueo/borrado de tiempo" .

2. **Compartir foto** enviará la imagen sin limite de tiempo y veces para su visualización en el Destinatario **KAYMERA**.





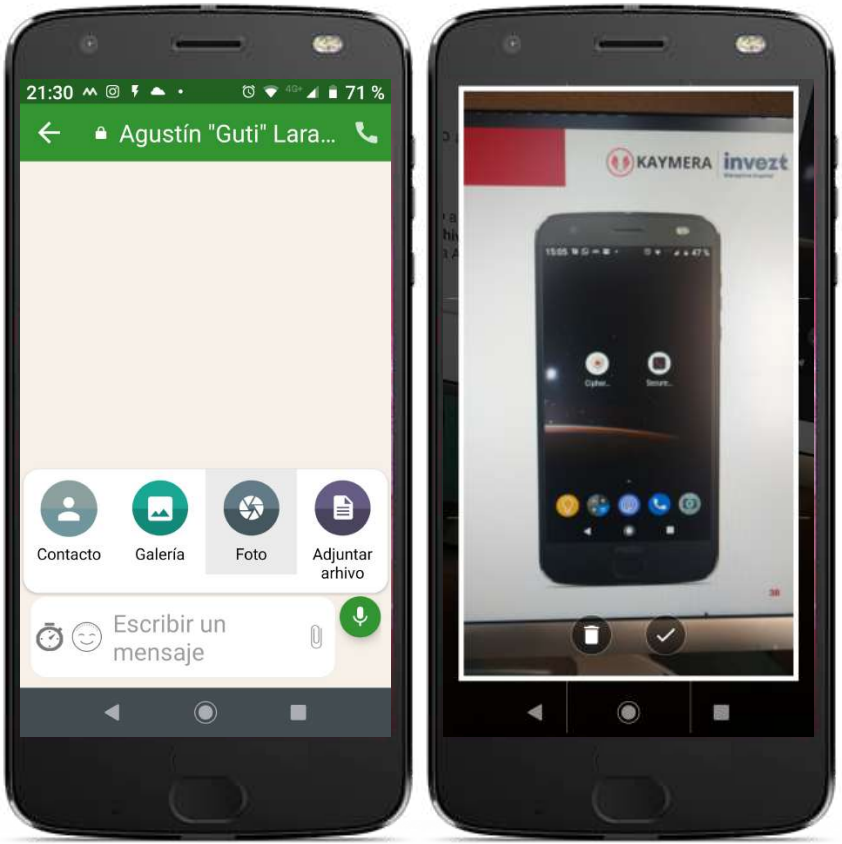
5: Uso de la Funcionalidad Mensajes Seguros

ENVÍO DE FOTOGRAFÍAS
Pulse / haga “click” sobre el ícono con la imagen de “**Una Diafragma de Cámara Fotográfica”.**

El equipo **CipherFort** activará la función de **Cámara Fotográfica instalada en el Teléfono Inteligente**.

Realice la toma fotográfica como realizaría cualquier otra, incluso utilizando las funciones disponibles para ello (flash, iluminación, enfoque, efector, etc) en dicha aplicación.

Una vez conforme, pulse / haga “click” para seleccionarla.



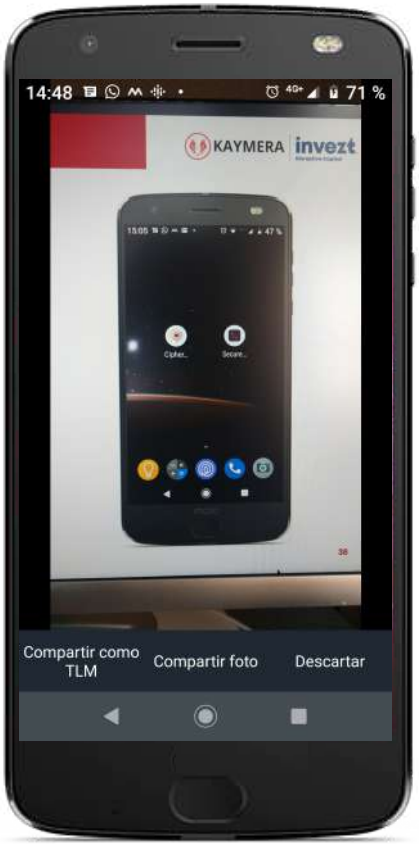
5: Uso de la Funcionalidad Mensajes Seguros

ENVÍO DE FOTOGRAFÍAS

Una vez que la fotografía realizada aparezca en la pantalla de su Teléfono Inteligente, en la parte baja aparecerán **diferentes opciones para su envío como Mensaje Seguro:**

1. **Compartir como TLM** provocará que la fotografía sea enviada con la función de "bloqueo/borrado de tiempo" .

2. **Compartir foto** enviará la fotografía sin limite de tiempo y veces para su visualización en el Destinatario **KAYMERA**.



5: Uso de la Funcionalidad Mensajes Seguros

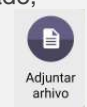
ENVÍO DE ARCHIVOS ELECTRÓNICOS

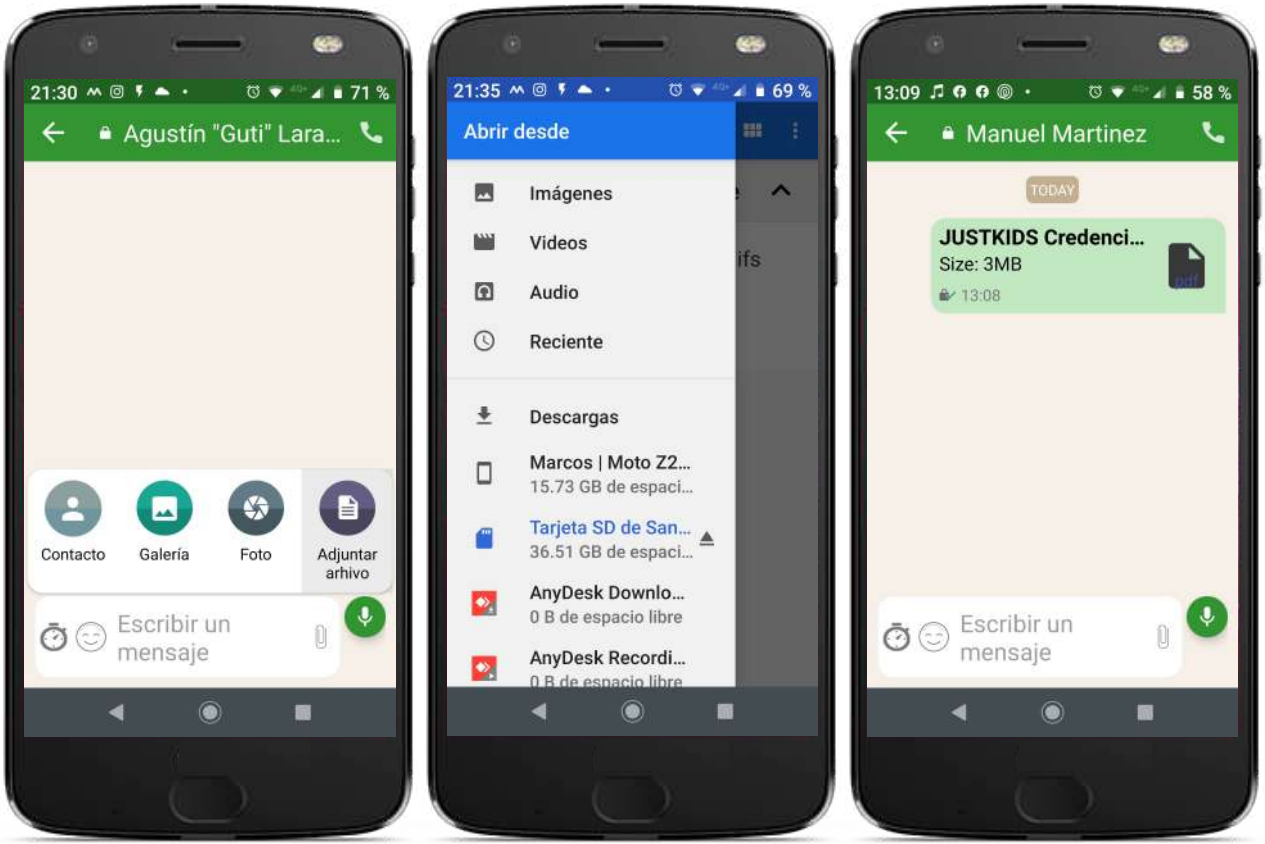
Pulse / haga “click” sobre el ícono con la imagen de “**Un Documento”.**

Seleccione o busque el archivo que desea enviar.

Deberá ubicarlo a través de las diferentes carpetas de la **memoria interna**, de las **memoria externa** e incluso de repositorios **“en la nube”** a los que tenga acceso desde su Teléfono Inteligente

Una vez identificado y ubicado, pulse / haga “click” sobre él para seleccionarlo.





5: Uso de la Funcionalidad Mensajes Seguros

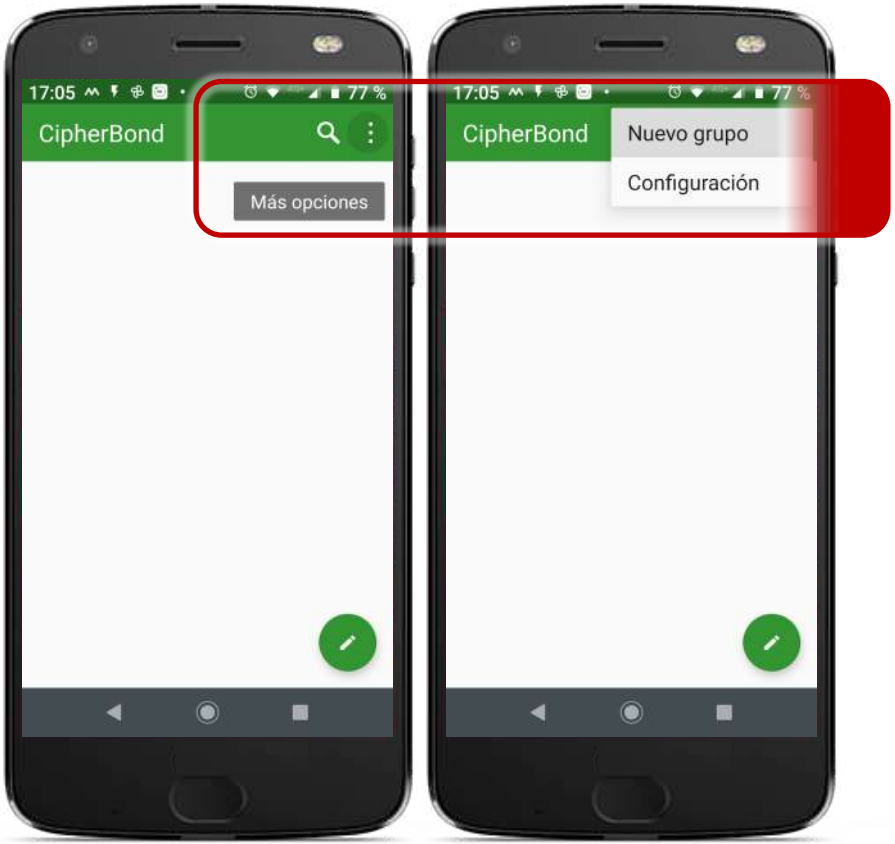
CREACIÓN DE GRUPOS PARA ENVÍO DE MENSAJES SEGUROS

El Equipo **CipherFort** permite enviar mensajes y compartir archivos de manera grupal para la **comunicación simultánea** con varios Contactos a la vez, mediante la creación y uso de **Grupos**.

Deberá utilizar la aplicación con el **ícono de CipherBond.**

En la pantalla principal se utiliza el ícono con la imagen de un "**tres puntos"** que aparecen en la parte superior derecha de la misma pantalla, pulse / haga "Click" sobre este ícono, lo que desplegará el menú de opciones.

Pulse / haga "click" en la opción "**Nuevo grupo**".



5: Uso de la Funcionalidad Mensajes Seguros

CREACIÓN DE GRUPOS
PARA ENVÍO DE MENSAJES SEGUROS

En la parte superior de la pantalla aparecerá un espacio dispuesto para dar **nombre al grupo**, el cual podrá tener una extension de hasta 20 caracteres, incluyendo:

- **Letras**
- **Números**
- **Espacios**
- **Caracteres**
- **Emoticones.**

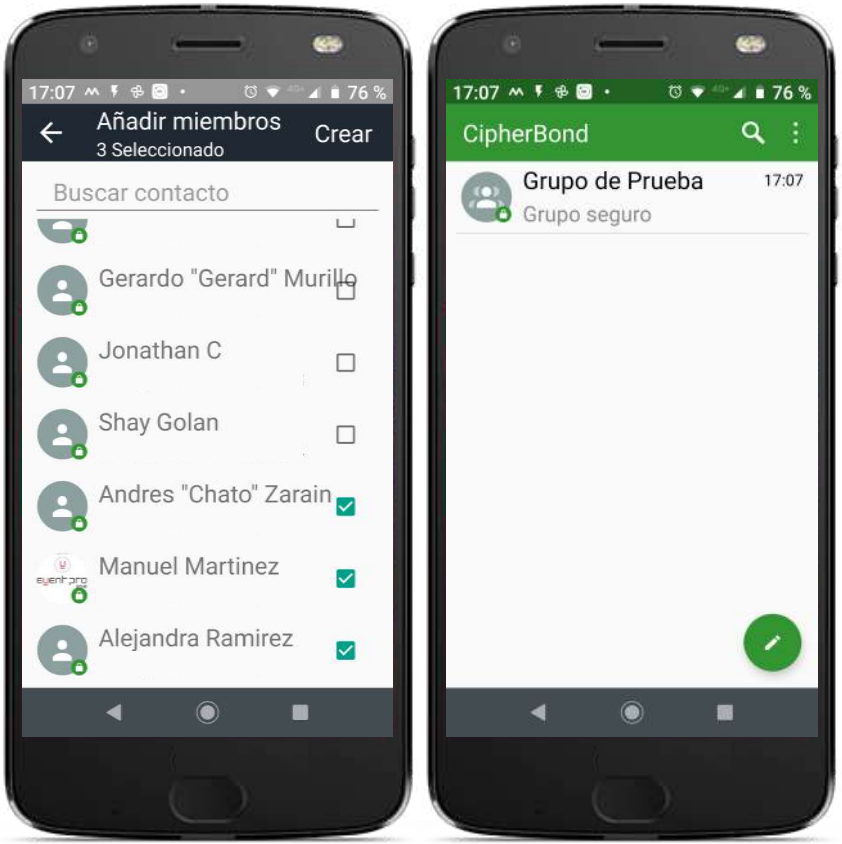
Cuando termine de escribir el nombre del Grupo, pulse / haga “click” sobre la palabra “**Siguiente**” que aparece en la parte superior de la pantalla.

5: Uso de la Funcionalidad Mensajes Seguros

CREACIÓN DE GRUPOS
PARA ENVÍO DE MENSAJES SEGUROS

Una vez creado y nombrado el Grupo, se podrán **agregar Contactos Seguros** a este, para ello deberá (posteriormente se podrán adicionar más):

1. **Buscar y seleccionar** a cada Contacto que requiera agregar al Grupo.
2. Seleccionarlo hacienda “click / pulsando la casilla del lado derecho de cada uno de ellos para que apareza un **ícono** con imagen y color “**verde**”.
3. Al terminar de seleccionarlos, pulse / haga “click” en la palabra “**Crear**” que se encuentra en la parte superior de la pantalla.

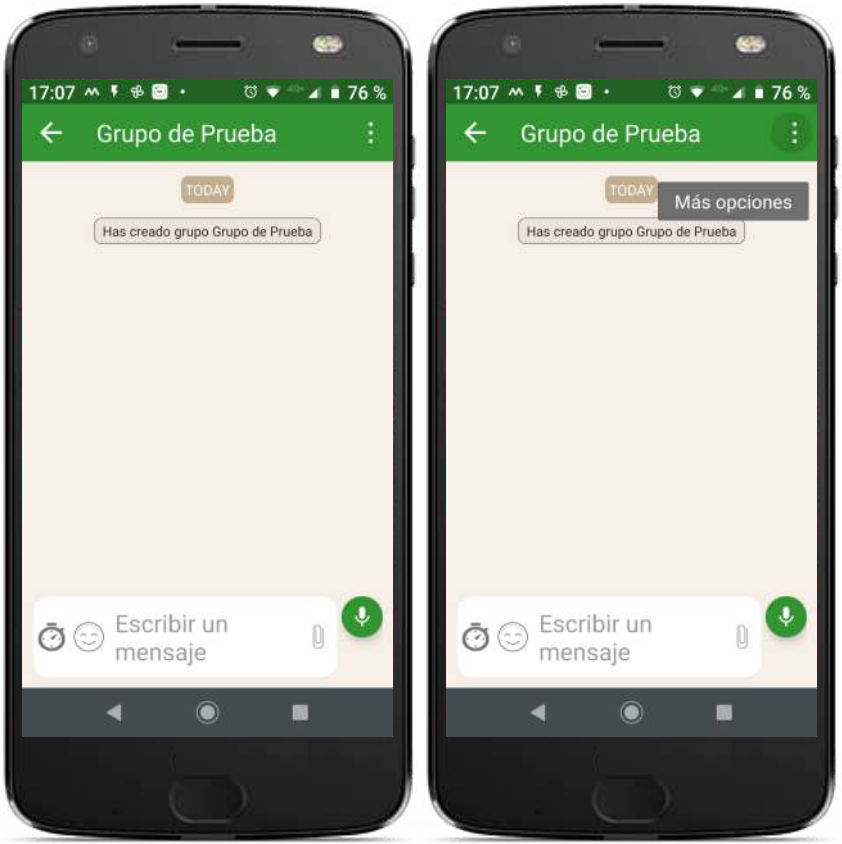


5: Uso de la Funcionalidad Mensajes Seguros

CREACIÓN DE GRUPOS
PARA ENVÍO DE MENSAJES SEGUROS

Una vez creado el Grupo, se podrá realizar el **envío de cualquier tipo de mensaje** (escritos o grabaciones de audio) y archivo electrónico a todos los **integrantes del Grupo** de manera simultánea y con la misma configuración que se haya establecido (con/sin auto-bloqueo/borrado por tiempo).

Utilizando el ícono con la imagen de un **"tres puntos"** que se encuentra en la parte superior derecha de la misma pantalla, pulse / haga "Click" sobre este ícono para desplegar el menú de opciones del Grupo.



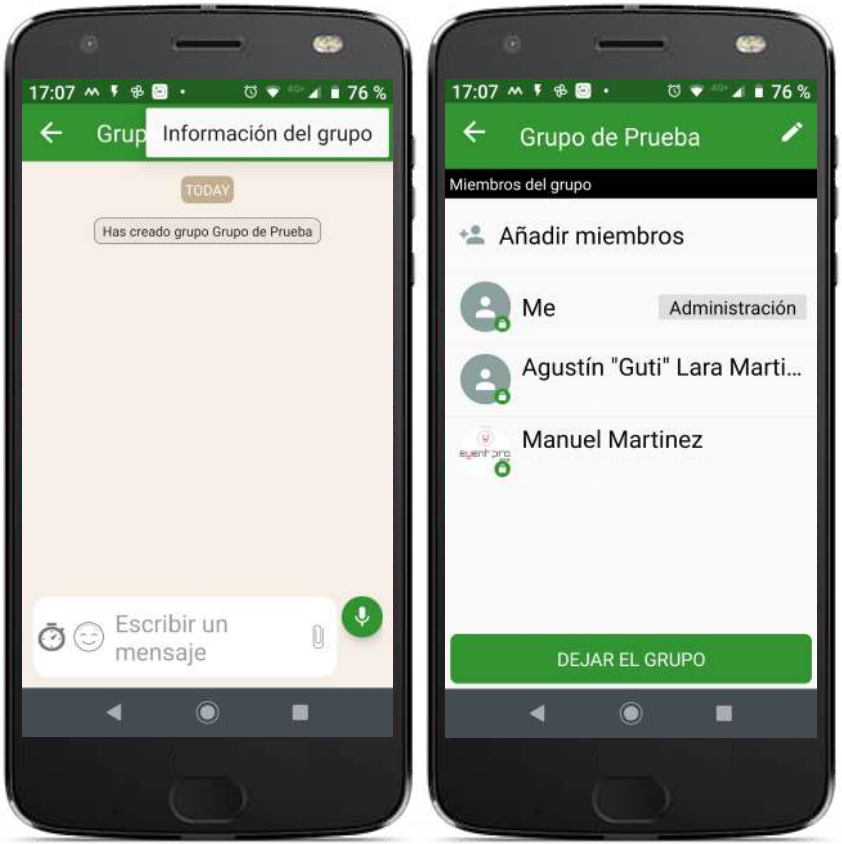
5: Uso de la Funcionalidad Mensajes Seguros

CREACIÓN DE GRUPOS
PARA ENVÍO DE MENSAJES SEGUROS

Pulse / haga “click” en la opción ”**Información del grupo**” para que aparezca el listado de Contactos Seguros que pertenecen al Grupo

Si desea **cambiar o modificar el nombre del Grupo**, pulse/haga “click” en el ícono con imagen de “**lápiz**” ubicado en la esquina superior derecha de la pantalla

Si desea **abandonar** el Grupo que ha creado o al cual pertenece, pulse / haga “click” en el cuadro inferior de la pantalla con la leyenda “**Dejar el Grupo**”

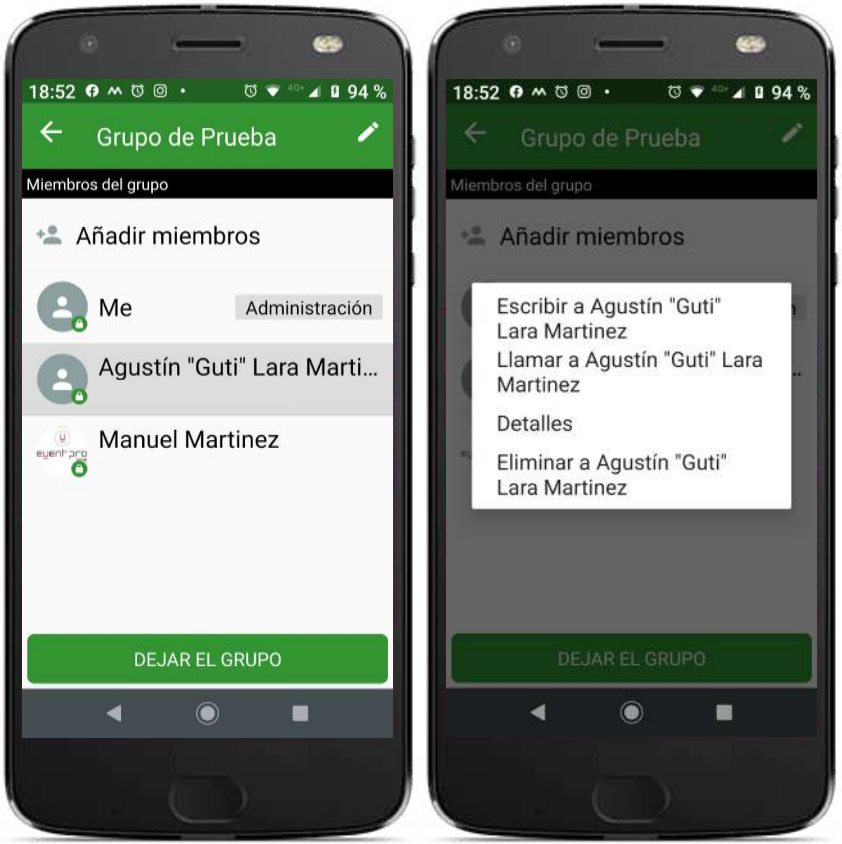


5: Uso de la Funcionalidad Mensajes Seguros

CREACIÓN DE GRUPOS
PARA ENVÍO DE MENSAJES SEGUROS

Si usted pulsa / hace "click" sobre alguno de los contactos, el Equipo **CipherFort** dará acceso al **menú de opciones sobre ese Contacto**, que incluye:

1. Crear un **mensaje individual** exclusivo para el Contacto seleccionado, por separado del Grupo.
2. Establecer un **Enlace Seguro de Voz** con el Contacto seleccionado.
3. Visualizar la **información del Contacto** a través de la aplicación de Directorio Telefónico instalada en el Teléfono Inteligente.
4. **Eliminar del Grupo** al Contacto seleccionado.



5: Uso de la Funcionalidad Mensajes Seguros

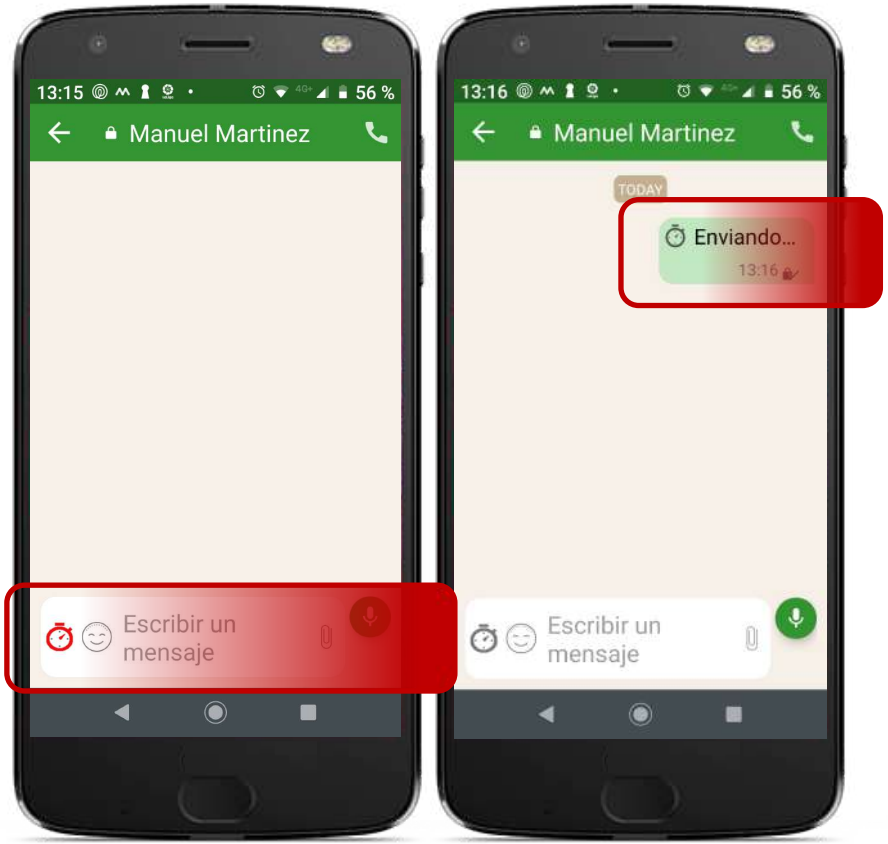
ENVÍO DE MENSAJES CON AUTO-BLOQUEO POR TIEMPO

Para cada uno de sus mensajes, se puede configurar para que tras su lectura, el mensaje quede **bloqueado sin poder leerlo de nuevo**.

Para ello se utiliza el ícono con imagen de "**reloj**" ubicado del lado izquierdo de la zona de escritura, únicamente tendrá que pulsar / hacer "click" hasta que cambie de color "gris" a "**rojo**"

Esta función opera para mensajes "**escritos**", mensajes con uso de "**emoticones**" y mensajes con "**grabación de audio**".

El mensaje enviado presentará el mismo ícono de "reloj" en el lado izquierdo del mismo.

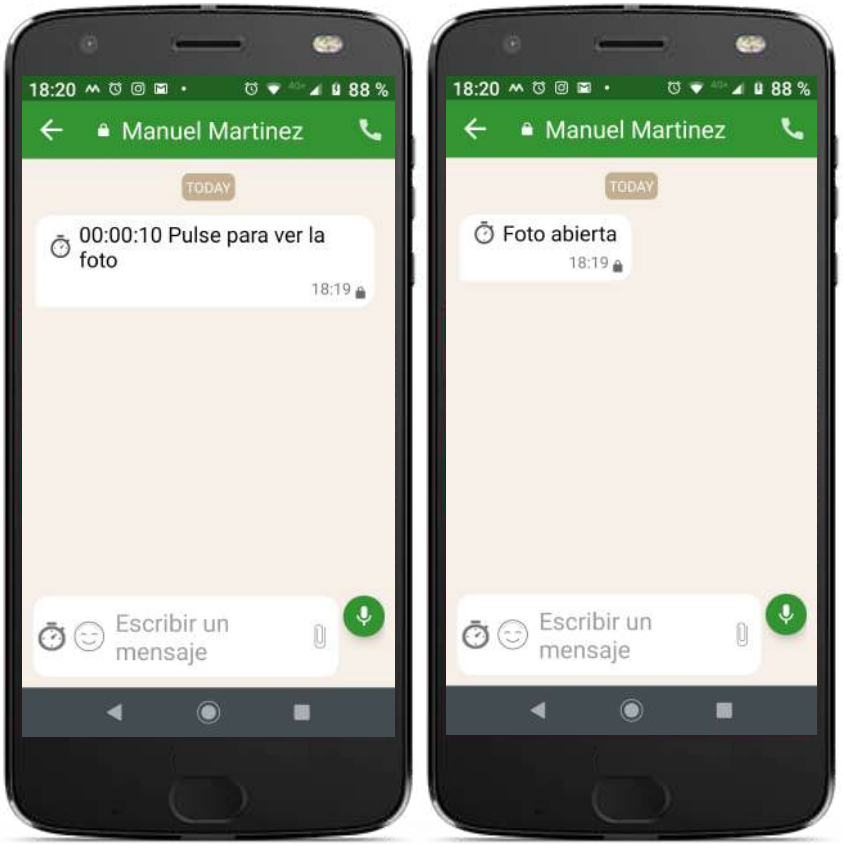


5: Uso de la Funcionalidad Mensajes Seguros

RECEPCIÓN Y LECTURA DE MENSAJES CON AUTO-BLOQUEO POR TIEMPO

Cuando se recibe un mensaje con este tipo de configuración, este aparece como cualquier otro en la pantalla del Contacto o Grupo de Contactos, pero mostrará tres características distintivas:

- Un **ícono** con imagen de "**reloj**" en la parte izquierda del mensaje
- La **nota del tiempo** que el mensaje estará disponible para visualizarse antes de bloquearse.
- **No se mostrará su contenido** si no hasta pulsarlo / hacerle "click" para que sea descargado en el Equipo **CipherFort**.
- Una vez que sea visualizado este **no podrá ser accesado de nuevo**.



5: Uso de la Funcionalidad Mensajes Seguros

CONFIGURACIÓN PARA EL ENVÍO DE MENSAJES CON AUTO-BLOQUEO POR TIEMPO

Esta función puede ser aplicada o configurada de diferentes formas según sea requerido:

- **POR MENSAJE**
  Se aplica **únicamente al mensaje** que se aplique configura para ello (explicado anteriormente).

- **EN GENERAL – TODOS LOS MENSAJES**
  Se aplica a **todos los mensajes enviados** por el usuario sin diferencia de Destinatarios.

- **POR CONTACTO**
  Se aplica a **todos los mensajes enviados al usuario "Destinatario"** sobre el que se configure y tiene prioridad sobre la Configuración General.

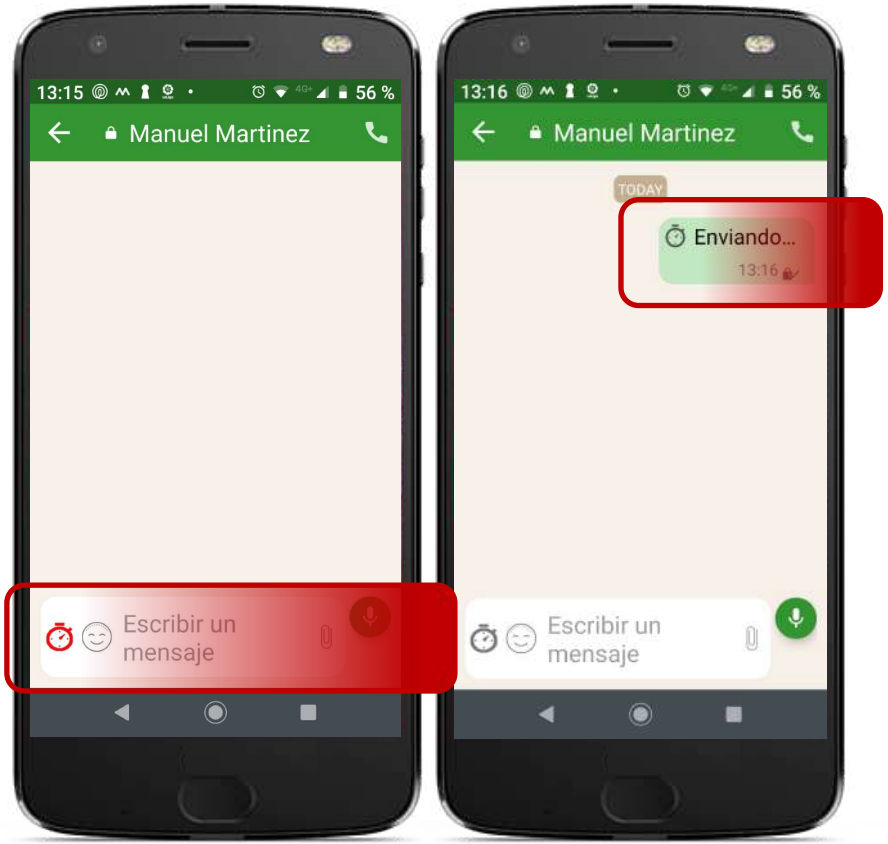
5: Uso de la Funcionalidad Mensajes Seguros

CONFIGURACIÓN POR MENSAJE
PARA EL ENVÍO DE MENSAJES CON AUTO-BLOQUEO POR TIEMPO

Para cada uno de sus mensajes y de manera individual e independiente al resto de los mensajes al mismo contacto “destinatario”, se utiliza el ícono con imagen de “**reloj**” ubicado del lado izquierdo de la zona de escritura, únicamente tendrá que pulsar / hacer “click” hasta que cambie de color “gris” a “**rojo**”

Esta función opera para mensajes “**escritos**”, mensajes con uso de “**emoticones**” y mensajes con “**grabación de audio**”.

El mensaje enviado presentará el mismo ícono de “reloj” en el lado izquierdo del mismo.

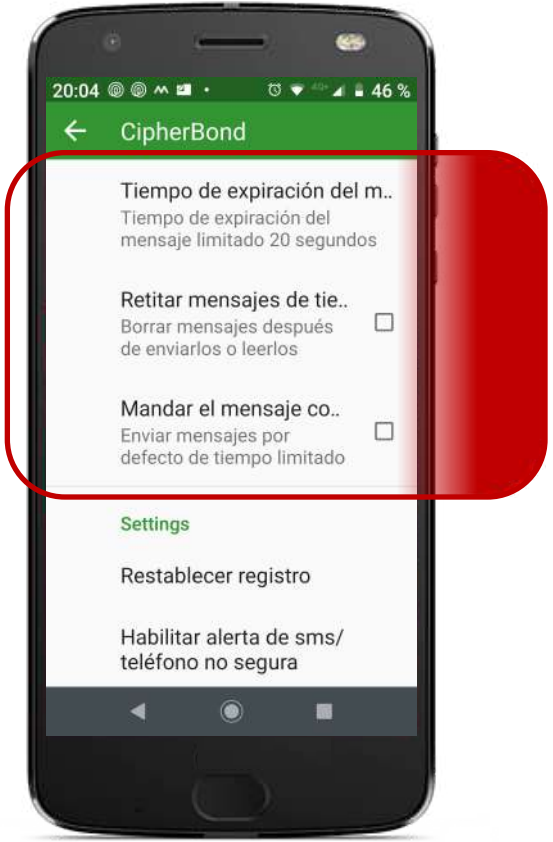


5: Uso de la Funcionalidad Mensajes Seguros

CONFIGURACIÓN GENERAL – TODOS LOS MENSAJES
PARA EL ENVÍO DE MENSAJES CON AUTO-BLOQUEO POR TIEMPO

Las diferentes opciones de configuración del auto-bloqueo de tiempo que se aplican para todos los mensajes en general se ubican en la sección de Configuración de la Función **CipherBond**.

Cada una de estas se explican mas adelante en la **Sección Configuración & Personalización**.



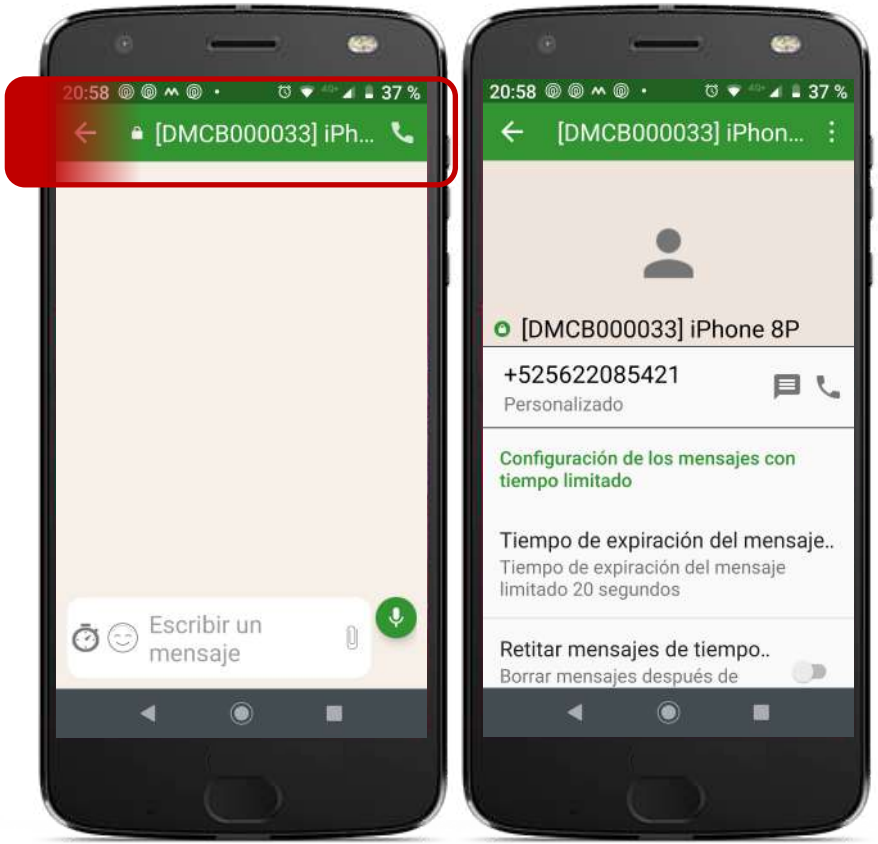
5: Uso de la Funcionalidad Mensajes Seguros

CONFIGURACIÓN POR CONTACTO PARA EL ENVÍO DE MENSAJES CON AUTO-BLOQUEO POR TIEMPO & AUTODESTRUCCIÓN

Para cada configurar que **todos los mensajes enviados a un Contacto en particular** queden bloqueado, sin poder leerlo de nuevo tras su lectura o se autodestruyan; se debe acceder al menu de estas funciones para el Contacto correspodiente.

Este proceso de acceso se realiza pulsando 7 haciendo “click” sobre el nombre del contando y que aparece en la parte superior de la pantalla.

Con ello se desplegará el menú de **TLM – Time Limited Messages.**



5: Uso de la Funcionalidad Mensajes Seguros

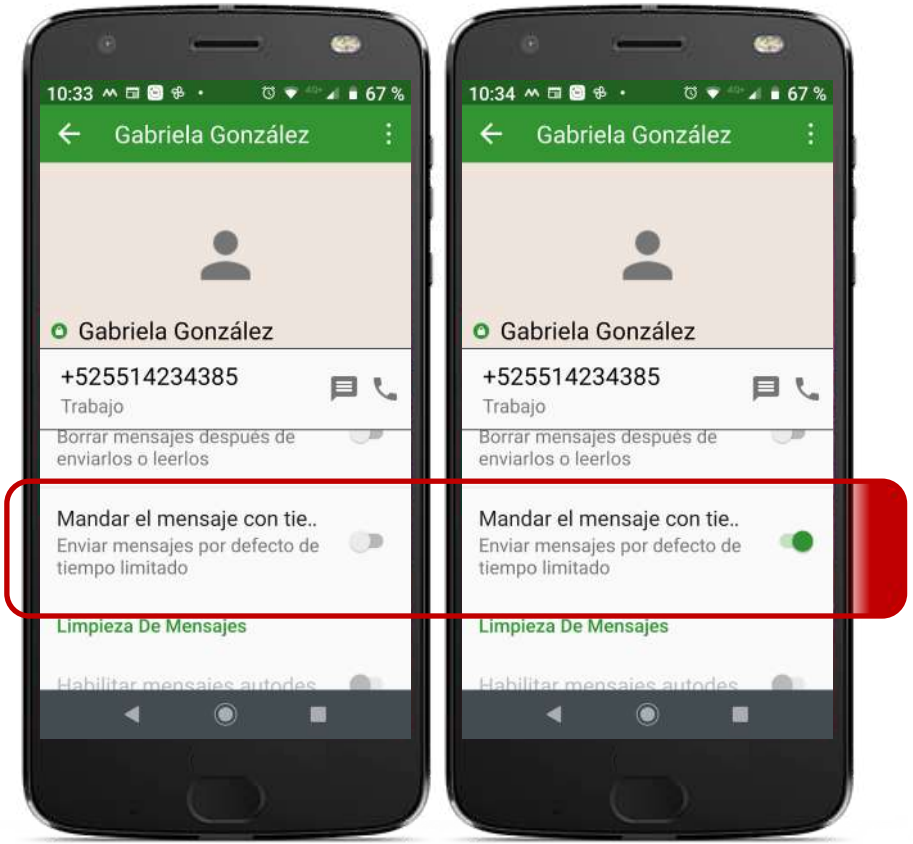
CONFIGURACIÓN POR CONTACTO

ACTIVACIÓN DEL ENVÍO DE MENSAJES CON AUTO-BLOQUEO POR TIEMPO

Esta función se utiliza para que **todos los mensajes enviados** por usuario del equipo **CipherFort al Destinatario** que corresponde el menu de configuración, sean realizados con auto-bloqueo de tiempo.

Para **activar** la función se deberá pulsar / hacer "click" sobre la imagen de "**botón**" colocada en la parte derecha del texto hasta que este aparezca en color "**verde**".

Para desactivarla se deberá hacer el mismo procedimiento hasta que la imagen de botón aparezca en color "gris claro".



5: Uso de la Funcionalidad Mensajes Seguros

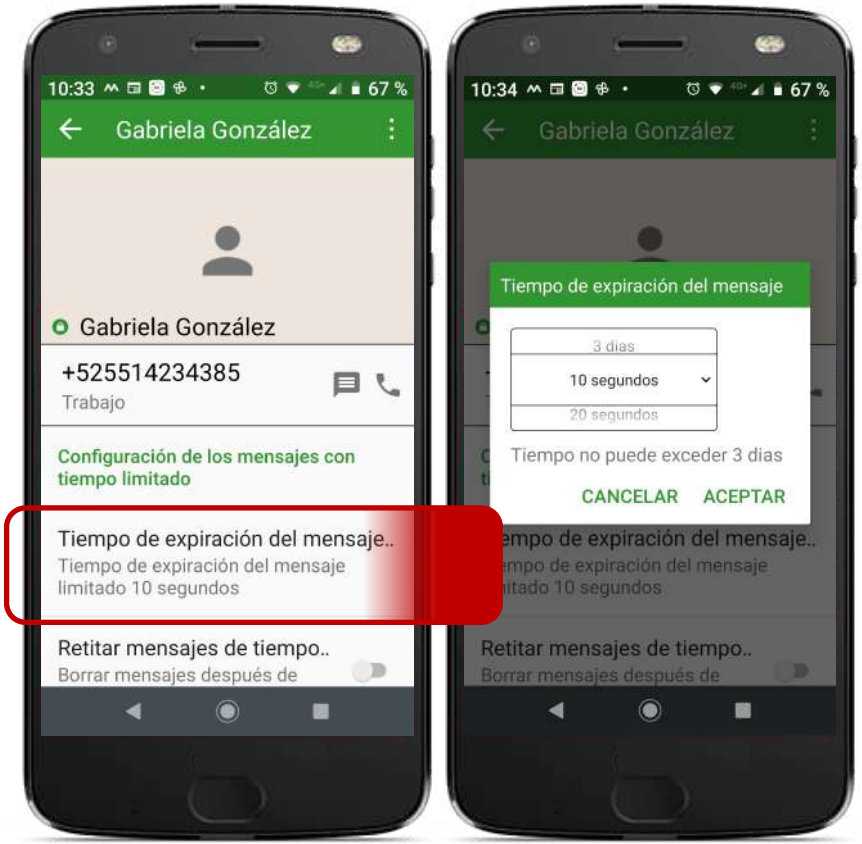
CONFIGURACIÓN POR CONTACTO

TIEMPO DE EXPIRACIÓN DEL MENSAJE CON AUTO-BLOQUEO POR TIEMPO

Esta función se utiliza para definir la cantidad de tiempo que se asignará a cada mensaje enviado a este Destinatario, para poder ser leído y auto-bloquearse a su terminación.

Pulsar / hacer “click” sobre el texto de la función, lo que accionará un acceso tipo “notificación”.

En el Submenú que se muestra, se elige la cantidad de tiempo que se asignará para el auto-bloquedo de todos los mensajes enviados a ese Destinatario, en fracciones de tiempo desde los 10 segundos hasta los 3 días.



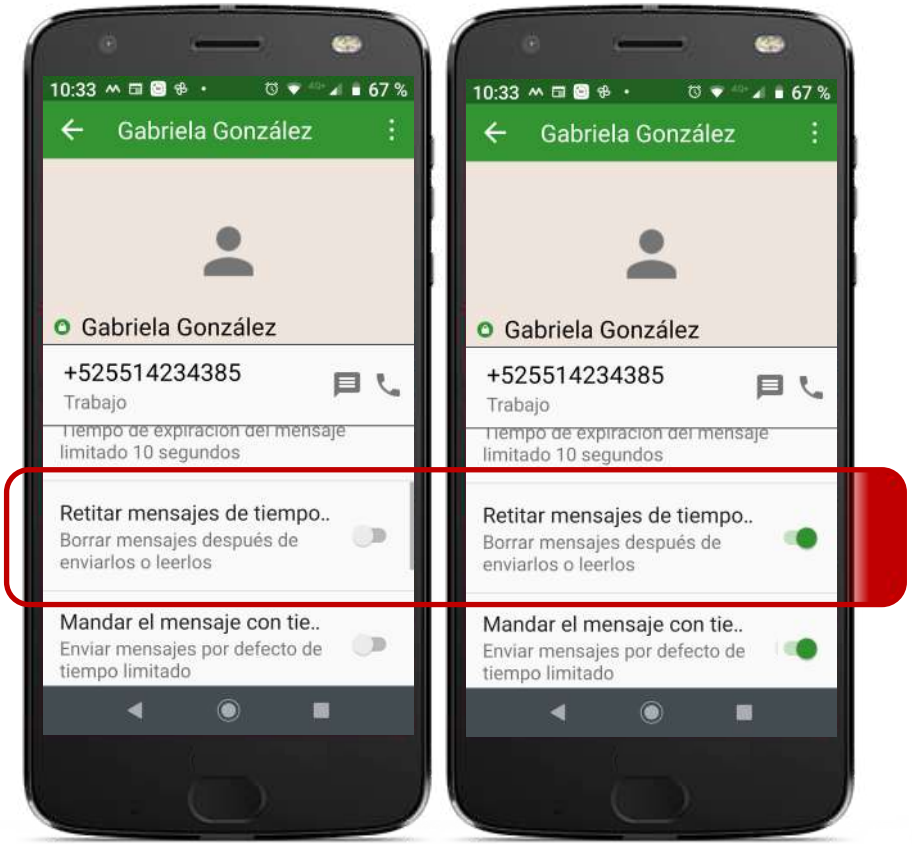
5: Uso de la Funcionalidad Mensajes Seguros

CONFIGURACIÓN POR CONTACTO
AUTO-BORRADO DE MENSAJES ENVIADOS

Esta función se utiliza para que todos los mensajes enviados con auto-bloqueo de tiempo sean, **inmediatamente tras ser enviados, borrados de la pantalla** del usuario del equipo **CipherFort** que los envía (no son borrados de la aplicación del contacto "Destino" al que se configura esta función).

Esta función sólo opera si la función de "Envío de Mensajes con Auto-Bloqueo de tiempo" se encuentra activada en el mismo menu.

Para **activar** la función se deberá pulsar / hacer "click" sobre la imagen de "**botón**" colocada en la parte derecha del texto hasta que este aparezca en color "**verde**".



5: Uso de la Funcionalidad Mensajes Seguros

CONFIGURACIÓN POR CONTACTO
PARA EL ENVÍO DE MENSAJES CON AUTO-BLOQUEO POR TIEMPO

La configuración y ajustes a los mensajes al destinatario en particular mostrarán notificaciones tanto al usuario que emite los mensajes como al que los recibirá.

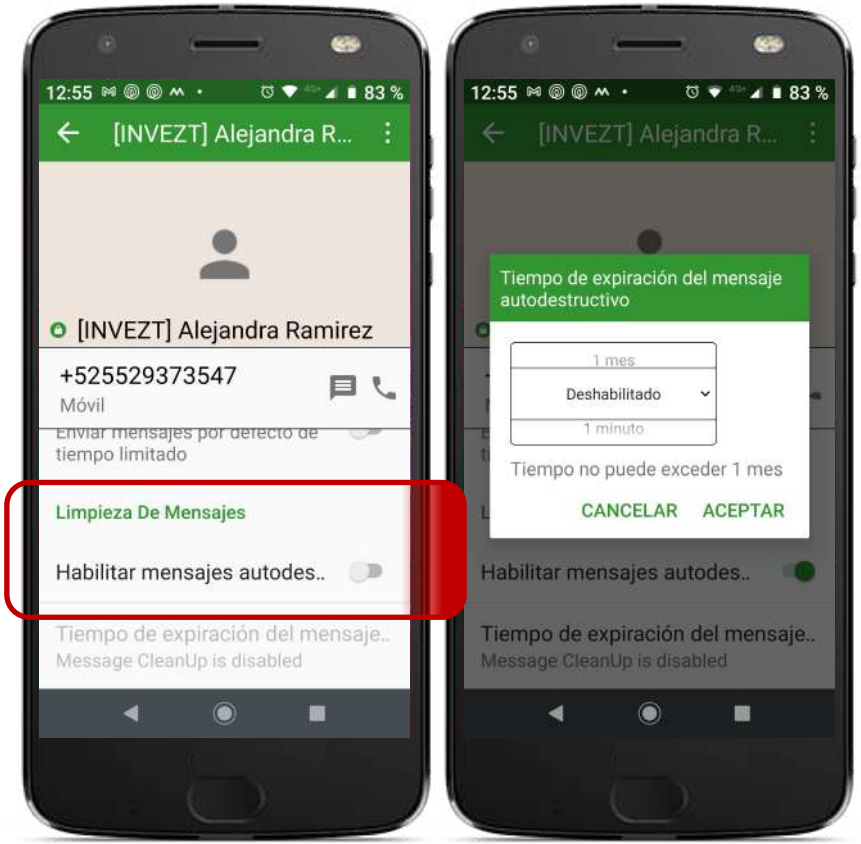
5: Uso de la Funcionalidad Mensajes Seguros

AUTODESTRUCCIÓN DE MENSAJES

El **Equipo CipherFort** cuenta con la función para que todos los mensajes seguros se autodestruyan - sean borrados de manera automática - tras un período de tiempo de vida, **tanto para el usuario que lo envía como para el usuario que lo recibe**.

Para **activar** la función se deberá pulsar / hacer "click" sobre la imagen de "**botón**" colocada en la parte derecha del texto hasta que este aparezca en color "**verde**".

Inmediatamente despúes, aparece el menu para seleccionar el período de tiempo que el mensa existirá y que al concluir, borrará el mensaje.



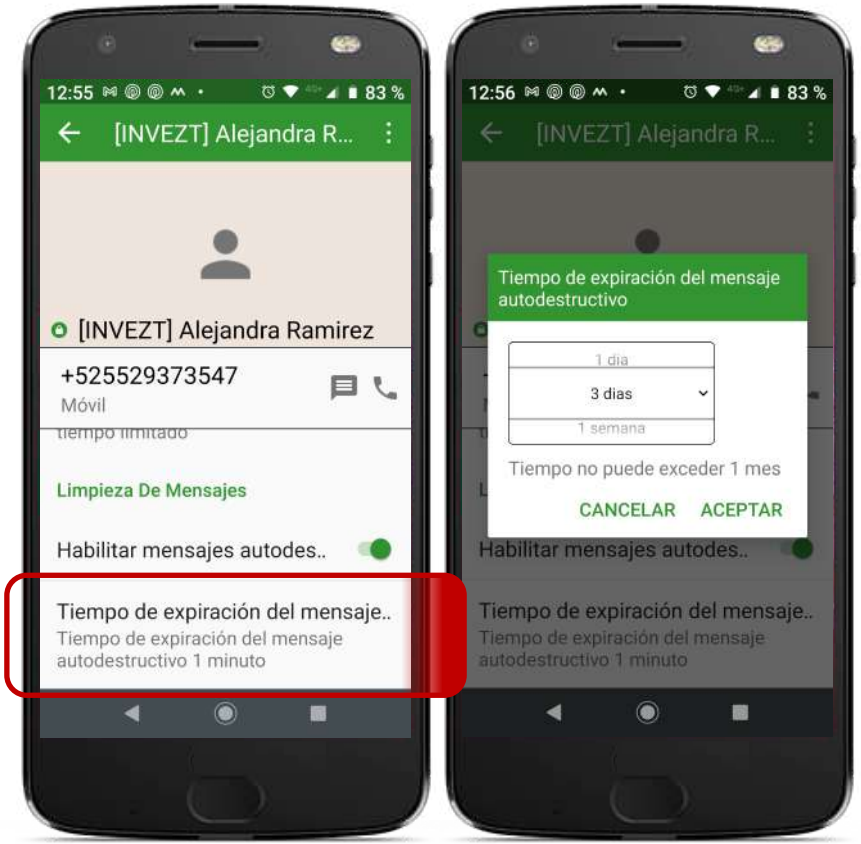
5: Uso de la Funcionalidad Mensajes Seguros

AUTODESTRUCCIÓN DE MENSAJES

Si se desea cambiar el tiempo de vida de los mensajes antes de su borrado automático tanto en el usuario que los envía como en el que los recibe, utilice la opción "**Tiempo de expiración del mensaje autodestructivo**", pulsando / hacienda "click" sobre el texto que describe la función.

Con ello aparece el menú para seleccionar una opción diferente de tiempo, que es **desde un minute hasta un mes.**

Esta función aplica para mensajes con y sin auto-bloqueo de tiempo.



5: Uso de la Funcionalidad Mensajes Seguros

AUTODESTRUCCIÓN DE MENSAJES

Tras la configuración de los mensajes autodestructivos, en la barra superior sobre el nombre del contacto, aparece un ícono con la imagen de un "**bote de basura**" que en su parte inferior indica el **tiempo de vida** del mensaje antes de su borrado automático.

La configuración y ajustes a los mensajes al destinatario en particular mostrarán notificaciones tanto al usuario que emite los mensajes como al que los recibirá.

5: Uso de la Funcionalidad Mensajes Seguros

MENSAJES GRUPALES
AUTO-BLOQUEO POR TIEMPO & AUTODESTRUCCIÓN DE MENSAJES

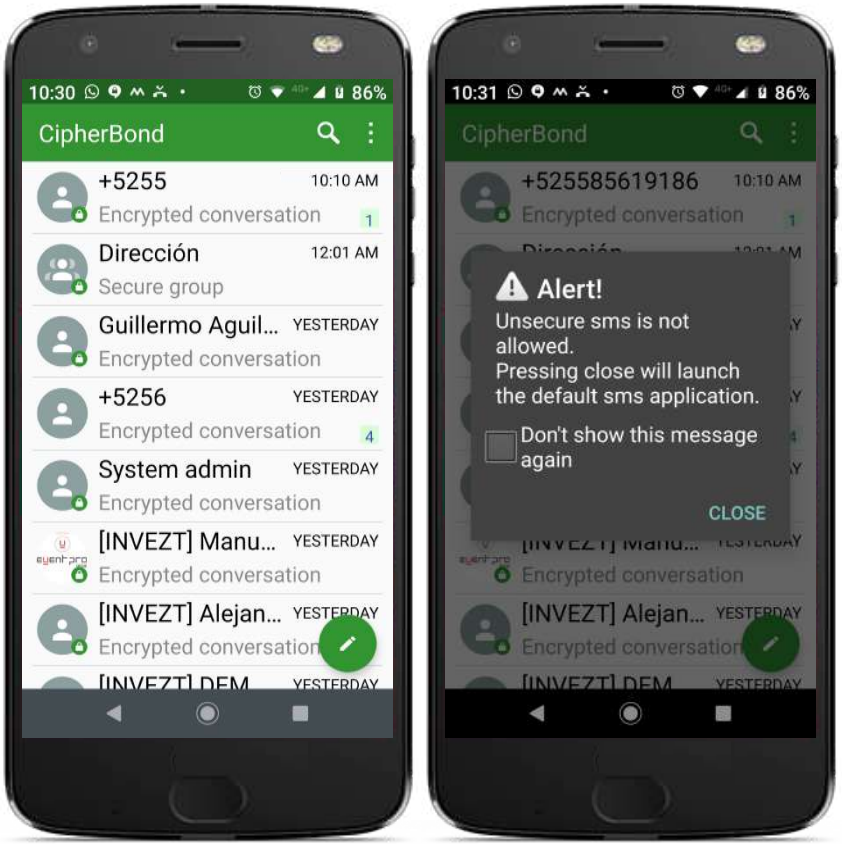
Todas las funciones y configuraciones de bloqueo automático y borrado automático que pueden ser aplicadas a mensajes seguros a contactos específicos, **pueden ser igualmente aplicadas a mensajes de seguros grupales**.

5: Uso de la Funcionalidad Mensajes Seguros

NOTIFICACIONES DE ERROR

Si alguno de los **Contactos Seguros** registrados y visibles en el **Equipo CipherFort** llega a estar deshabilitado del servicio en el momento en que se le intenta enviar un **Mensaje Seguro**, la Aplicación generará una **Notificación** alertando sobre ello y no será posible realizar el envío.

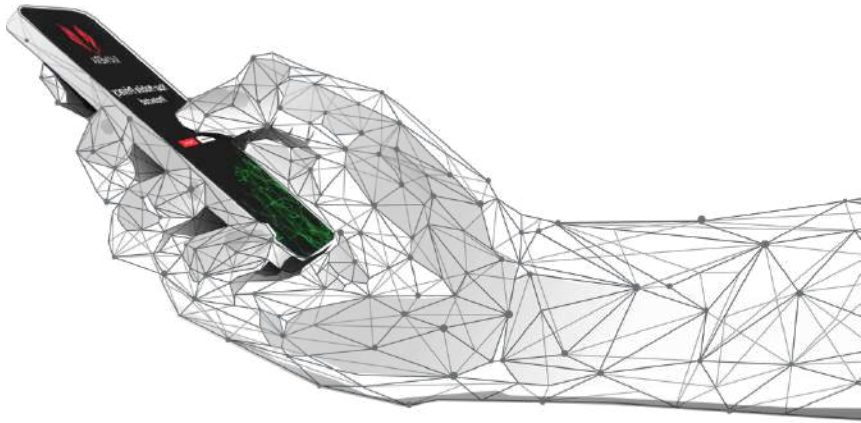
De manera automática se vinculará con la **aplicación pre-determinada** en el Teléfono Inteligente para realizar el envoi del mensaje a dicho contacto de una forma normal – como **mensaje no seguro – sin encripción**.



Manual de Uso de las Funciones de Comunicación CipherFort

KAYMERA

Soporte a Usuarios:
atencion.kaymera@invezt.co
+(52) 55 6792 4305



invezt
Disruptive Capital