



El sistema israelí de ciberdefensa Grado Militar para teléfonos móviles más avanzado y seguro del mundo.

Protección TOTAL • Facilidad de uso





KAYMERA
High-End Mobile Security

Amenazas y Ciberataques Móviles



Los teléfonos que usamos para casi todos los aspectos de nuestras vidas, comunicaciones e información ¡Son extremadamente vulnerables!

Riesgo extremo para la seguridad y privacidad de los usuarios móviles.



El espionaje telefónico está proliferando alarmantemente en América Latina. Ya sea por espionaje empresarial, crimen organizado, adversarios políticos, supervisión gubernamental, intereses internacionales o geopolíticos, o inclusive por razones personales.



Ataques a usuarios móviles en América Latina.



México ocupa el 2do lugar.



Colombia ocupa el 3er lugar.

- 8 de cada 10 empresas son hackeadas.
- Un ataque cuesta en promedio US\$ 2M.
- Detectar un ataque toma en promedio 210 días.
- Los ciberataques vienen un 28% de expleados, 21% de hackers, 19% de empleados, 16% de proveedores y 16% del crimen organizado.
- Un 24% de los ataques se dirigen a directivos.



Cada vez son más frecuentes las noticias de actividades de espionaje.



Resumen de las Amenazas y Ciberataques a usuarios móviles.



VPNs y MDMs, no son suficientes para detener estas amenazas.



- Leer Emails.
- Robar passwords y tokens.
- Robar claves de VPN y Wifi.
- Acceder a apps: mensajería, redes sociales, bancarias, de negocio, etc.
- Ver fotos, videos, archivos, screen shots, Contactos, IDs.
- Interceptar cámaras, micrófono y GPS.
- Etc.



Apps legítimas que abusan de sus permisos y extraen información sensible.



Apps Falsas usan sus permisos para abrir secretamente puertas traseras para que el hacker tome control del teléfono.



Extracción física de datos usando cargadores o cables USB con circuitos espías: *USB Harpoon*.



Ingeniería Social y Phishing usan redes sociales y páginas web falsas para que los usuarios revelen información sensible.



Antenas celulares o wifi espías engañan a los teléfonos para robar su ID y contraseñas. Pueden ver y modificar la información transmitida e inyectar malware al teléfono víctima.



Malware (troyanos, gusanos, virus, spyware, etc.) que son inyectados desde SMSs, E-mails, Wifi, páginas web, apps, etc. y sin que la víctima se den cuenta.



Vulnerabilidades de las redes públicas: La señalización SS7 no tiene encriptación y son puertas abiertas para hackers.

Todas las apps piden permisos para acceder a información sensible cuando se instalan en nuestros teléfonos.



Muchas apps legítimas se exceden con los permisos que les damos, algunas con propósitos mercadológicos y otras para espiar a los usuarios para terceros.

Cámara

Tomar fotos y grabar video por sí misma en cualquier momento.



Contactos

Leer, editar o agregar contactos: nombre, teléfono, e-mail, etc.



Ubicación

Obtener en todo momento la ubicación del teléfono por el GPS, Wifi o antenas celulares.



Sensores Corporales

Leer la información de accesorios: relojes, pulseras de actividad, etc.



SMS

Enviar, recibir y leer mensajes SMS, MMS o WAP.



Identidad

Consultar identidad y estado del teléfono.



Teléfono

Hacer o recibir llamadas, ver registro de llamadas, mensajes de voz, estado de red.



Memoria

Leer o guardar archivos en memoria interna o tarjetas SD: fotos, videos, PDF, etc.



Micrófono

Escuchar el micrófono por sí misma en cualquier momento, incluyendo durante llamadas.



Calendario

Leer, editar y crear eventos; y obtener información de las personas invitadas a las reuniones.

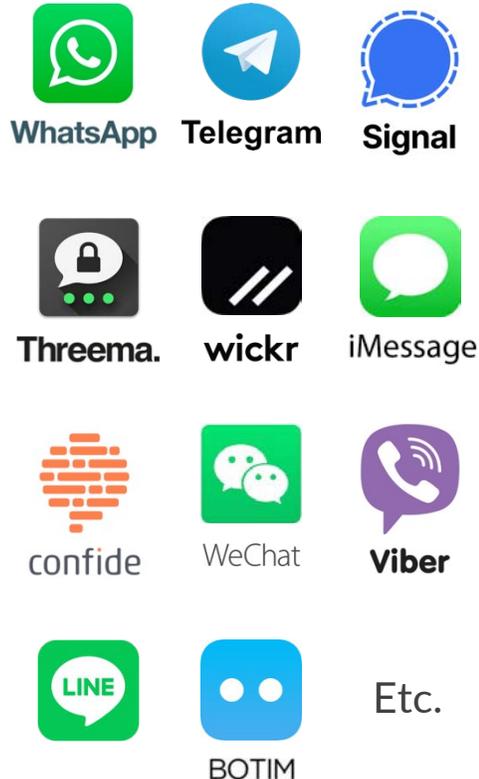


Conexión

Acceso a red y obtener información de las conexiones de wifi.

Apps populares de mensajería: ¡VULNERABILIDAD EXTREMA!

La seguridad de muchas de estas apps está clasificada como **Grado Consumidor** o en el mejor de los casos **Grado Empresarial** ya que si bien ofrecen un **cifrado** en sus comunicaciones, son vulnerables a muchos vectores de ataque. Además, **NO SON PRIVADAS**, ya que por ley tienen **puertas traseras** y comparten sus **códigos de encriptación**.



Vulnerables a infecciones

Malware existente en el teléfono puede oír el micrófono o ver por la cámara.

No encriptan Metadatos

Robo de nombre y foto de perfil, estados, última conexión, contactos, etc.

Almacenamiento en servidores y apps de escritorio

Robo de conversaciones por duplicación de escritorio y ataques a servidores.

No Son PRIVADAS

Por ley tienen que compartir llaves de cifrado, contactos, perfil de usuario a gobiernos: Ley 97 en Rusia, LAED en USA, etc.

Secuestro de cuentas

Hackers tienen formas ingeniosas para robar las cuentas de las apps.

Masivas filtraciones a Darknet

Escándalos de filtraciones de datos de millones de usuarios.

Una llave de cifrado para muchos usuarios

Robando una llave, los hackers abren las conversaciones de muchos usuarios.

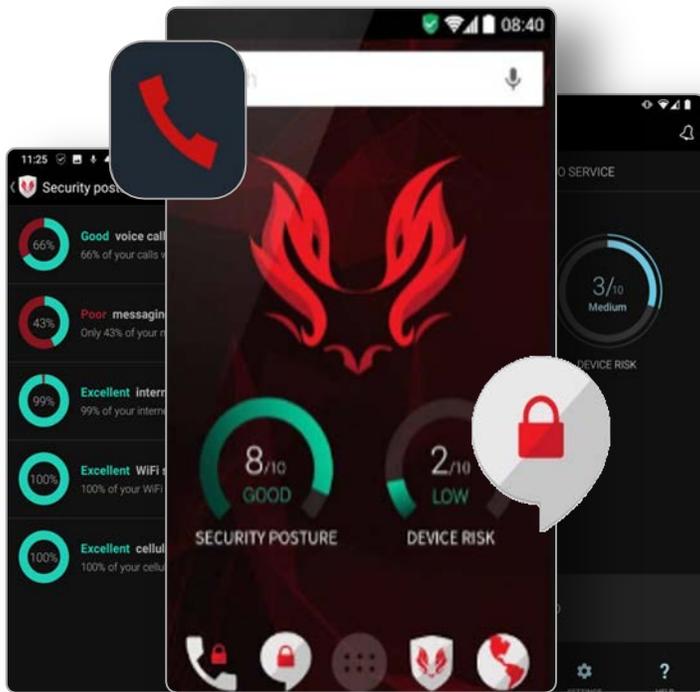
Y muchas más vulnerabilidades

Registradas en la National Vulnerability Database.





KAYMERA High-End Mobile Security



El sistema israelí de ciberdefensa Grado Militar para teléfonos móviles más avanzado y seguro del mundo.

- Protección Total.
- Facilidad de uso.

KAYMERA: El estándar de las comunicaciones móviles seguras.

Kaymera Technologies, Ltd. es una empresa israelí fundada en el 2013 que cuenta con la tecnología más avanzada y sofisticada del mundo para la ciberdefensa de las comunicaciones y teléfonos móviles de personas, empresas, multinacionales, fuerzas militares y gobiernos.



Forbes

Kaymera: The Anti-Spy Android OS Made By The Hottest iPhone Hackers In Surveillance

The Silicon Review Industry Platform Technology Leadership Magazine

Highest Protection and Maximum Functionality Perfectly Balanced: Kaymera

elEconomista.es

Kaymera Technologies, líder mundial en seguridad móvil avanzada, ampliará el alcance de la defensa adaptativa contra las amenazas a los dispositivos móviles

Operaciones Globales de KAYMERA:



KAYMERA:

Fundada por veteranos de ciberseguridad con profundos conocimientos y experiencia en ciberdefensa móvil, ataques cibernéticos y técnicas de recopilación de inteligencia.

Tiene inteligencia incomparable para predecir, prevenir, detectar y proteger en tiempo real contra la gama más amplia de amenazas.

KAYMERA: *Protección Total y Máxima Usabilidad en perfecto balance.*

KAYMERA logra el más alto nivel de protección por su motor contextual de análisis de riesgos con aprendizaje automático y capacidades multicapas de mitigación. El sistema puede detectar, prevenir y proteger contra cualquier amenaza móvil en tiempo real. Además, **KAYMERA** es un sistema totalmente privado ya que **NADIE** tiene acceso a los códigos de encriptación.

Máxima Seguridad

Protección **TOTAL** contra todas las amenazas y vectores de ciberataques móviles.



Privacidad y Confidencialidad

NO se almacenan llamadas, mensajes o archivos de los usuarios. La encriptación se hace en el teléfono y **NADIE** tiene acceso, ni **KAYMERA**.



KAYMERA ofrece:



Funcionalidad

Soluciones intuitivas, fáciles de usar y con mínima necesidad de soporte técnico.



Sin puertas traseras

NINGUNA agencia o gobierno en el mundo tiene acceso al cifrado o a la comunicación de los usuarios.

KAYMERA: calificado como Líder Global en Alta Seguridad Móvil.



Las soluciones de KAYMERA han sido sometidas a las pruebas más exigentes para penetrarlas. Los resultados son contundentes, KAYMERA **es el sistema más seguro existente hoy en día.**

Evaluaciones



KAYMERA es un Líder Global en Alta Seguridad Móvil.



KAYMERA es uno de los sistemas más seguros en la categoría de Alta Seguridad Grado Gobierno.



KAYMERA es el Sistema más seguro por su alto grado de protección.



Agencia holandesa de investigación de cibercrímenes, forense digital, inteligencia y ciberseguridad.

Realizó pruebas extensas de interceptación y exámenes forenses a KAYMERA:

- NO pudo interceptar las comunicaciones VoIP.
- NO pudo extraer información del teléfono.

KAYMERA es uno de los mejores sistemas de comunicaciones móviles seguras que Digitpol haya verificado.

Clientes



BGZ BNP PARIBAS



Alianzas



משרד הביטחון
MINISTRY OF DEFENCE



EUROPEAN
SECURITY AND DEFENSE
AGENCY



CODALTEC
CORPORACIÓN DE ALTA TECNOLOGÍA



Grupo Social y Empresarial
de la Defensa



La seguridad es de todos
Mindefensa

KAYMERA provee un sistema global de comunicaciones Encriptadas Grado Militar de extremo a extremo entre sus usuarios.



KAYMERA utiliza **AES-256 simétrico** con doble llave de cifrado desechable por cada mensaje o llamada del usuario; a su vez ambas llaves se encriptan con SIP/TLS con PKI. **AES-256** es el estándar usado por gobiernos, bancos y sistemas de alta seguridad en todo el mundo ya que se considera **INVULNERABLE**.



Mensajes



Grupos de Chat



Transferencias de Archivos

Fotos, videos, PDF, Word, Excel, Pdf.



Enlaces Seguros de Voz



Conferencias Seguras de Voz

Hasta 20 participantes.

KAYMERA tiene dos productos para el usuario final.

Teléfono Encriptado KAYMERA

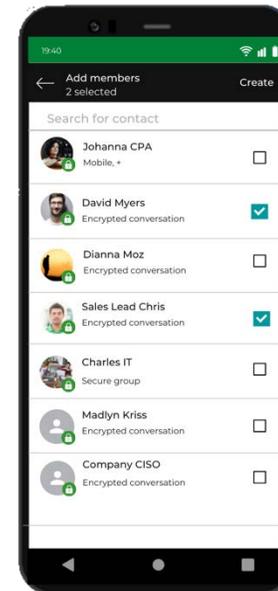
Smartphone Encriptado Grado Militar con protección **TOTAL** ante cualquier amenaza móvil e intercepciones de la comunicación: *100% seguro y muy fácil de usar.*



- Monitoreo en tiempo real de riesgos.
- Detección de ataques y lanzamiento de contramedidas para proteger el equipo.
- **INVULNERABLE** a infecciones de malware.
- Cifrado de TODA la información a nivel núcleo y protección de sensores como cámaras, micrófono y GPS.
- **INVULNERABLE** a intervenciones vía Wifi, red celular y manipulación de la señalización del operador.
- Comunicación Encriptada entre usuarios KAYMERA.
- Se pueden utilizar las apps habituales y el teléfono bloquea actividades maliciosas y espías.

App Encriptada KAYMERA

App Móvil de Comunicación Encriptada Grado Militar para enlaces de voz, mensajes y transferencias de archivos con otros usuarios KAYMERA.



- Se instala en el equipo actual de los usuarios: **iPhone** o **Android**.
- La app protege con el **Máximo Nivel de Seguridad** a todo lo que se habla, escribe o comparte a través de ella:
 - **INVULNERABLE** a intervenciones vía Wifi, red celular y manipulación de la señalización del operador.
 - **INVULNERABLE** a infecciones y software espía existentes en el teléfono del usuario.
- Encriptación de los metadatos.

KAYMERA: comparativo entre los productos para el usuario final.

Teléfono Encriptado KAYMERA



- **KAYMERA** provee tanto el teléfono (*dispositivo*) como el Sistema Operativo.
- **TODO** el equipo está protegido:
 - Información: fotos, videos, archivos.
 - Conexiones
 - Sensores: cámaras, GPS, micrófono, bluetooth, etc.
- El Teléfono es **INVULNERABLE** a infecciones de malware.
- Las conexiones de datos móviles y Wifi son **INVULNERABLES** a interceptaciones.
- Tiene comunicaciones encriptadas **Grado Militar** con otros usuarios **KAYMERA**.

App Encriptada KAYMERA



- La app se descarga en el teléfono actual del usuario.
- La app sólo protege lo que se escribe, habla o comparte a través de ella con otros usuarios **KAYMERA**.
- Las comunicaciones que se hacen a través de la app son:
 - **INVULNERABLES** a infecciones de malware.
 - **INVULNERABLES** a interceptaciones de Wifi y de red celular.
- El resto del teléfono, su información y sus sensores **NO** están protegidos por la app.

Dos opciones de implementación del sistema KAYMERA.

Nube KAYMERA (SaaS)



El servicio se ofrece desde la **Nube KAYMERA** con una **Arquitectura de Nube Global Múltiple** para ofrecer los más altos estándares de:

- Seguridad.
- Privacidad de la información.
- Calidad y disponibilidad de servicio.
- Recuperación a desastres (DRP).
- Respuesta inmediata a picos de demanda de servicios.

Beneficios:

- Servicio listo para usarse.
- Sólo se pagan las licencias (*Software as a Service*) de la App y del Sistema Operativo **KAYMERA**.
- NO se requiere inversión adicional en infraestructura.
- NO hay gastos adicionales de operación o mantenimiento.
- NO se requiere personal dedicado al soporte.

Sistema Privado (On-Premise)



El servicio se ofrece desde un **Sistema Privado de Seguridad Móvil**, el cual se implementa “*On-Premise*” por **KAYMERA** en la infraestructura de hardware y software provista, operada y mantenida por el **CLIENTE**.

La operación del sistema depende totalmente de la infraestructura propiedad del cliente.

Beneficios:

- El cliente tiene control total sobre el servicio.
- El sistema está dentro del data center del cliente y es operado conforme a sus políticas.
- Se puede integrar con otros sistemas de comunicación y ciberseguridad del cliente.
- Se pueden hacer desarrollos de funcionalidades sobre el sistema.

Nube KAYMERA con Arquitectura de Nube Global Múltiple.



El servicio se ofrece desde la **Nube KAYMERA** con una **Arquitectura de Nube Global Múltiple**.



Para ofrecer los más altos estándares de:

- Seguridad.
- Privacidad de la información.
- Calidad y disponibilidad de servicio.
- Recuperación a desastres (DRP).
- Respuesta a picos de demanda de servicios.

La Nube **KAYMERA** utiliza la infraestructura de los proveedores líderes a nivel mundial del servicio de Nube Pública Global.



Para ofrecer una red de puntos de acceso del servicio distribuida por todas las regiones y otorgar el nivel más avanzado de seguridad y disponibilidad.



Características y Beneficios de la Nube KAYMERA.

- Adicional a la seguridad del sistema **KAYMERA** se tiene la seguridad de los proveedores de nube.
- Dependiendo de su ubicación, el usuario recibe el servicio desde el punto de acceso más cercano.
- En caso de haber un incidente o ataque en una localidad, el punto de acceso se mueve rápida y virtualmente a otro.
- La **Nube KAYMERA** no es un blanco estático, sino que se mueve periódicamente por todo el mundo y entre los proveedores de nube.
- La privacidad de las comunicaciones es **TOTAL, NADIE** tiene acceso, ni **KAYMERA**.
- Clientes de Gobierno y Multinacionales han hecho inspecciones al sistema con resultados satisfactorios.

KAYMERA: Ofrece un Sistema customizable y modular que se ajusta a la estructura organizacional de los clientes.



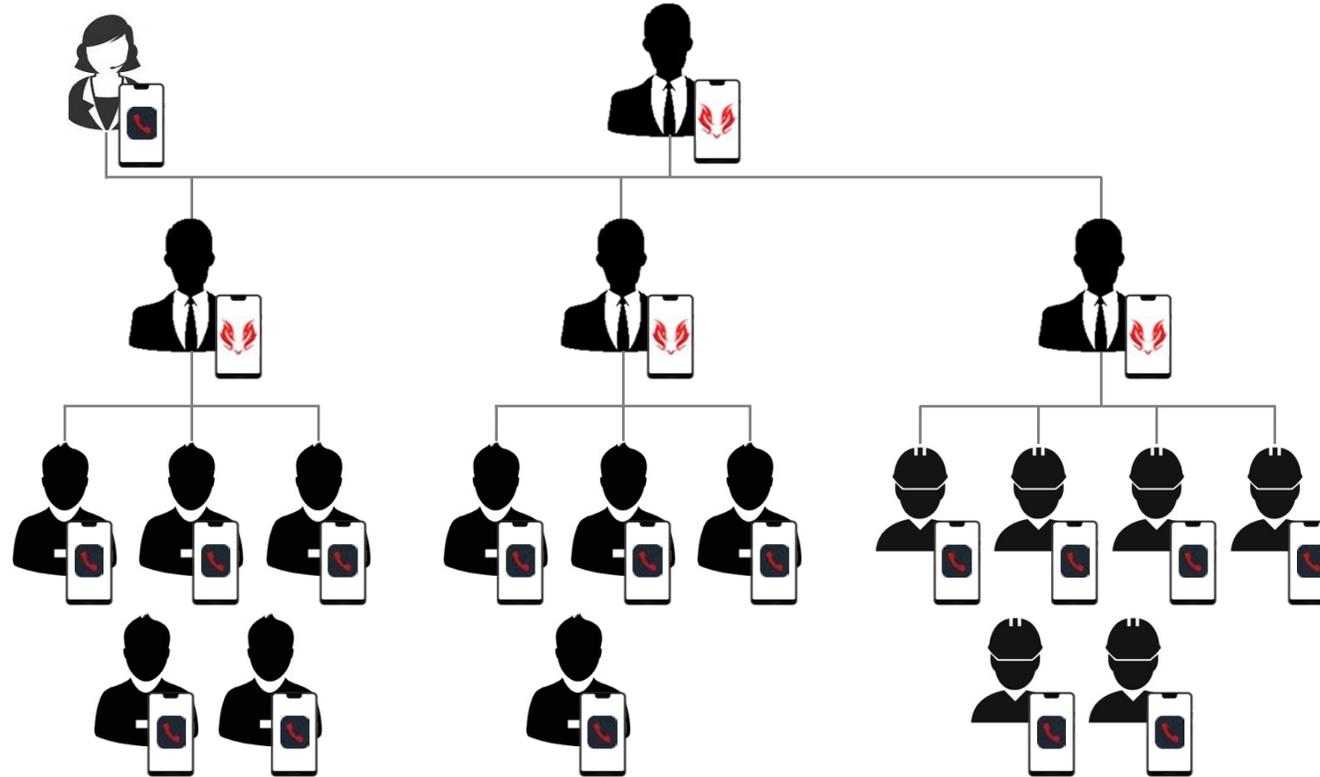
**Teléfono
Encriptado
KAYMERA**

Protección
TOTAL de los
teléfonos,
información y
comunicación
de los líderes



**App
Encriptada
KAYMERA**

Comunicación
segura para
los equipos de
trabajo



Opciones de
Implementación



**Nube
KAYMERA
SaaS**



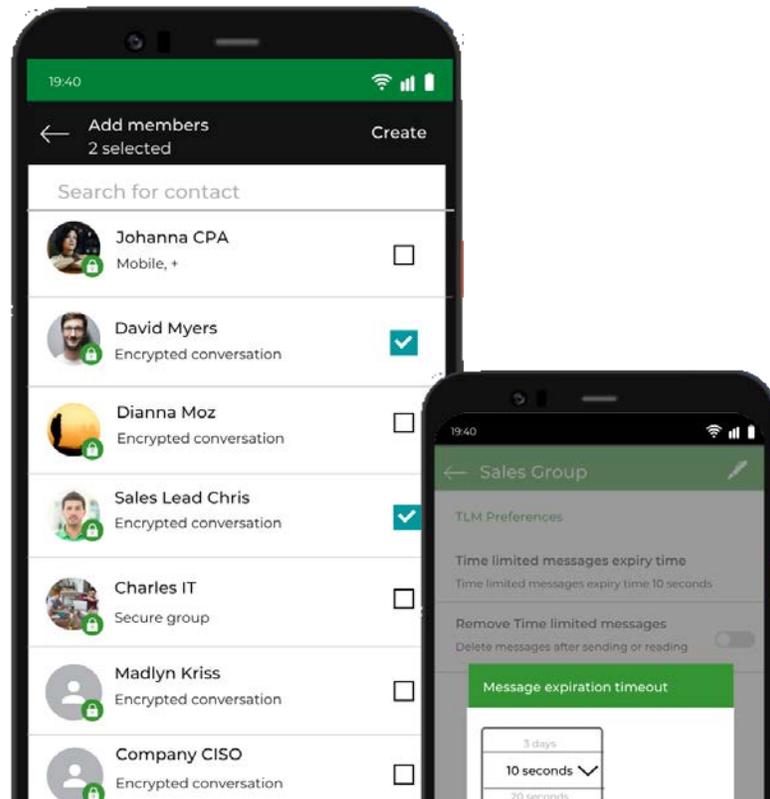
**Sistema
Privado
On-Premise**



Command Center



App Encriptada KAYMERA



Comunicaciones con Máxima Seguridad

App Móvil de Comunicación Encriptada Grado Militar para enlaces de voz, mensajes y transferencias de archivos entre usuarios KAYMERA.

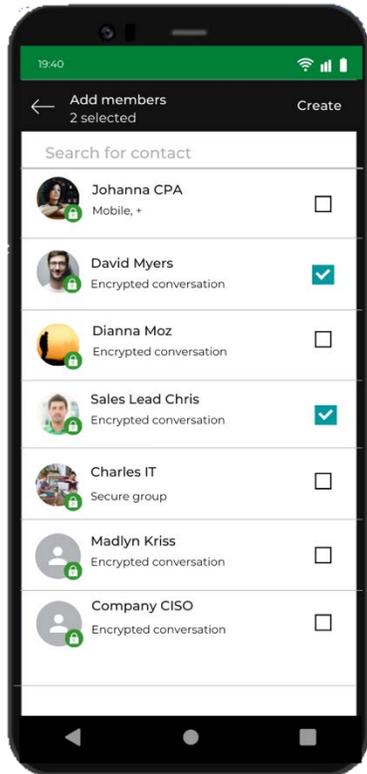
- Disponible para iPhone y Android.



App Móvil de Comunicación Encriptada Grado Militar



La App Encriptada KAYMERA ofrece comunicaciones **ILIMITADAS** y **ENCRYPTADAS** Grado Militar entre la red mundial de usuarios KAYMERA. Con cifrado **AES-256** simétrico para la máxima seguridad y privacidad contra todo tipo de interceptaciones.



-  **Mensajes**
-  **Grupos de Chat**
-  **Transferencias de Archivos**
Fotos, videos, PDF, Word, Excel, Pdf.
-  **Enlaces Seguros de Voz**
-  **Conferencias Seguras de Voz**
Hasta 20 participantes.

ADEMÁS



Enlaces Semi-Seguros de Voz
Para llamar por el sistema KAYMERA a cualquier teléfono. Encripta el tramo de la llamada del usuario a la Nube KAYMERA.



Modo Privado
Elimina el identificador de las llamadas de Enlaces Semi-Seguros de Voz: el receptor ve Número Oculto.

App Encriptada KAYMERA: *Funcionalidad y facilidad de uso.*



Contactos

La app detecta los contactos que tienen KAYMERA y crea la carpeta de contactos SEGUROS.



Mensajes

Pueden enviarse texto, notas de voz, fotos, videos y archivos.



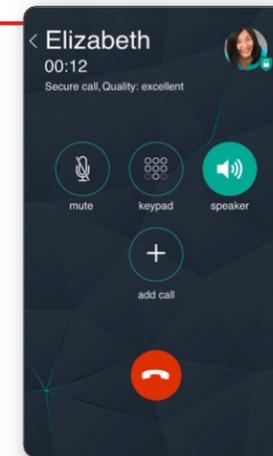
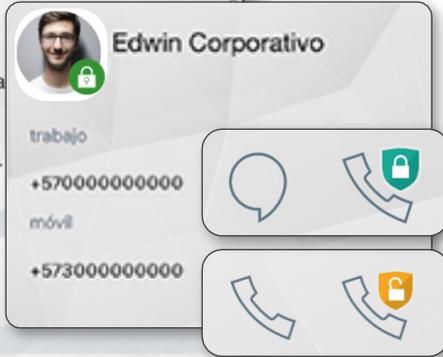
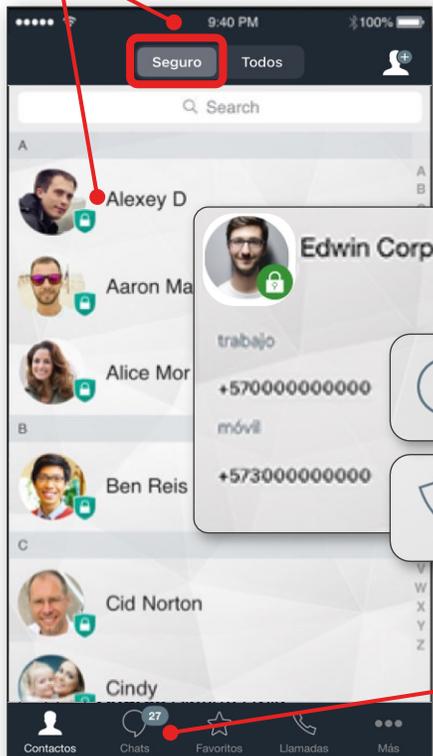
Enlace Seguro de Voz

Enlace VoIP encriptado de extremo a extremo, con alta nitidez de voz.

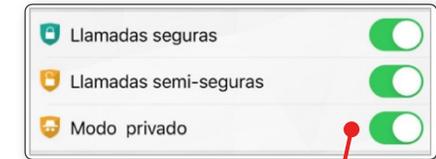


Enlace Semi-Seguro de Voz

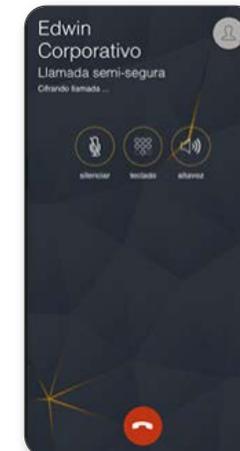
Para llamar a teléfonos que no tienen KAYMERA. Se encripta sólo el tramo de la llamada del usuario a la Nube KAYMERA.



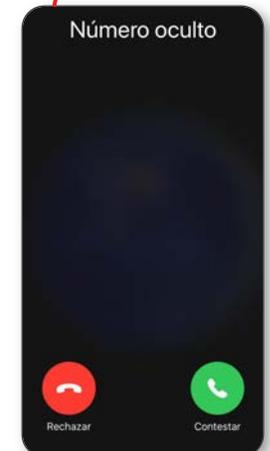
Panel de control de la app.



Abrir teclado



Receptor



Autodestrucción programada de Mensajes

App Encriptada KAYMERA: Comunicaciones con Máxima Seguridad.

La App Encriptada KAYMERA es **INVULNERABLE** a todo tipo de interceptaciones, manipulaciones o infecciones en teléfono del usuario y en su conexión celular o de wifi. La app cuenta con características y funciones que le dan el **Máximo Nivel de Seguridad** a todo lo que se habla, escribe o comparte a través de ella.

1. Detecta Amenazas

Antes de conectar llamadas o enviar mensajes, la app detecta la existencia de infecciones e interceptaciones.



2. Bloquea Amenazas

Para evitar el robo de información directamente del micrófono, teclado, procesador, etc.



3. Encripta con AES-256

AES 256 Simétrico de extremo a extremo con doble llave de cifrado que se renuevan por cada mensaje o llamada.



360°



4. También cifra los Metadatos

Esta es información sensible que acompaña a la comunicación.



7. Guarda todo en una Bóveda Segura

Los mensajes y archivos recibidos quedan cifrados y protegidos en la bóveda de la app, dentro del teléfono del usuario.



6. También encripta las Llaves de cifrado

Ambas llaves de cifrado se transmiten por un canal encriptado SIP/TLS con PKI.



5. Asegura privacidad

El cifrado se hace en el teléfono del usuario. **NADIE** tiene acceso a las llaves de cifrado, ni KAMERA.

App Encriptada KAYMERA: *Requerimientos técnicos.*

El usuario debe contar con:



Un equipo:

- iPhone con **iOS 9.3** o posterior.
- **Android 6.0** o posterior, excepto Android 10 Go versión.
- VPNs y MDMs afectan el funcionamiento de la **App Encriptada KAYMERA**.



Un Plan o paquete de datos móviles:

- **0.5 GB** para un consumo mensual de **2000 minutos** de Enlaces Seguros de Voz.



Una **línea celular** activa:

- Con un **número telefónico válido**.
- Con red móvil **3G** (HSPA+), **4G** (LTE) o **WiFi**.
- Con red **2G** sólo pueden mandarse mensajes.



Funciona sobre **líneas** de:

- **Pospago** (plan de renta) y **prepagadas**.
- Todos los **operadores** y **MVNO's**.



La **App Encriptada KAYMERA** se maneja por separado de su cuenta celular por lo que **NO AFECTA** su línea de crédito.



- La **App Encriptada KAYMERA** funciona sobre **datos móviles**.
- Se requiere buena **cobertura** y **estabilidad** de red **3G** o **4G** en las áreas donde el usuario transita.
- En el extranjero se requiere **roaming internacional de datos** o acceso a **wifi** en los destinos que se visite.

App Encriptada KAYMERA: Se instala y se activa muy rápido y fácil.



La App Encriptada KAYMERA se descarga directamente de **Apple Store** o de **Google Play Store**, pero para poder activarla y usar el servicio es necesario adquirir una **Licencia de Servicio** para tener usuario en el sistema y recibir el **Código de Activación** de la app.

El usuario puede descargar la **App Encriptada KAYMERA** sin costo desde las **tiendas de apps** para instalarla en su equipo **iPhone** o **Android**.



Código de Activación enviado directamente por **KAYMERA** al **e-mail** registrado como usuario en el sistema.





Teléfono Encriptado KAYMERA



El teléfono inteligente más seguro del mundo.

Smartphone Encriptado Grado Militar con protección total contra todas las amenazas móviles y vectores de ataque existentes.

- Máxima seguridad.
- Facilidad de uso.

Teléfono Encriptado KAYMERA: *El smartphone más seguro del mundo.*



El Teléfono Encriptado KAYMERA de Grado Militar está basado en un smartphone de gama alta (*Google Pixel*) y el Sistema Operativo Altamente Seguro (SO) KAYMERA que lo hacen 100% seguro y fácil de usar.

Seguridad de Apps

Pueden descargarse apps desde **Google Play Store**. El teléfono bloquea actividades maliciosas y espías de las apps.



Funcionalidad y facilidad de uso
Experiencia nativa **Android**.



Conexiones y Comunicaciones Seguras
Detecta y protege contra amenazas en conexiones a la red móvil y wifi.



Comunicaciones Encriptadas Grado Militar
entre usuarios **KAYMERA**.



Seguridad Personal
Modo Camaleón y Modo Pánico.







Sistema Operativo Altamente Seguro

Monitoreo en tiempo real del nivel de riesgo. Si detecta amenazas o ataques lanza de inmediato contramedidas.



Encriptación a nivel núcleo

de **TODA** la información dentro del teléfono: *archivos, fotos, videos, etc.*



Protección de Sensores

Protección contra extracción física de datos e interceptación de cámaras, micrófono y **GPS**.



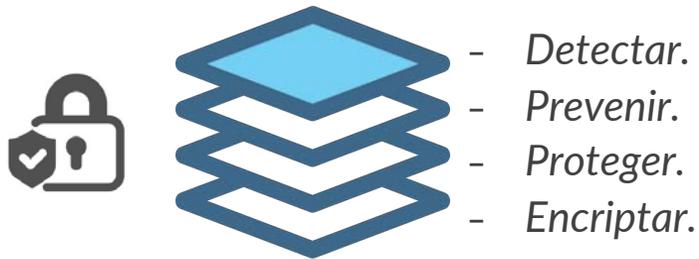
INVULNERABLE a infecciones de todo tipo de malware: *troyanos, virus, spyware etc.*

Sistema Operativo Altamente Seguro (SO) KAYMERA

La mayor protección y la máxima funcionalidad en perfecto balance.

El Teléfono Encriptado KAYMERA se basa en el Sistema Operativo Altamente Seguro (SO) KAYMERA, el cuál está construido para maximizar la protección del dispositivo a la vez que logra los más altos estándares de usabilidad.

KAYMERA tiene un sistema de ciberdefensa de 4 capas:



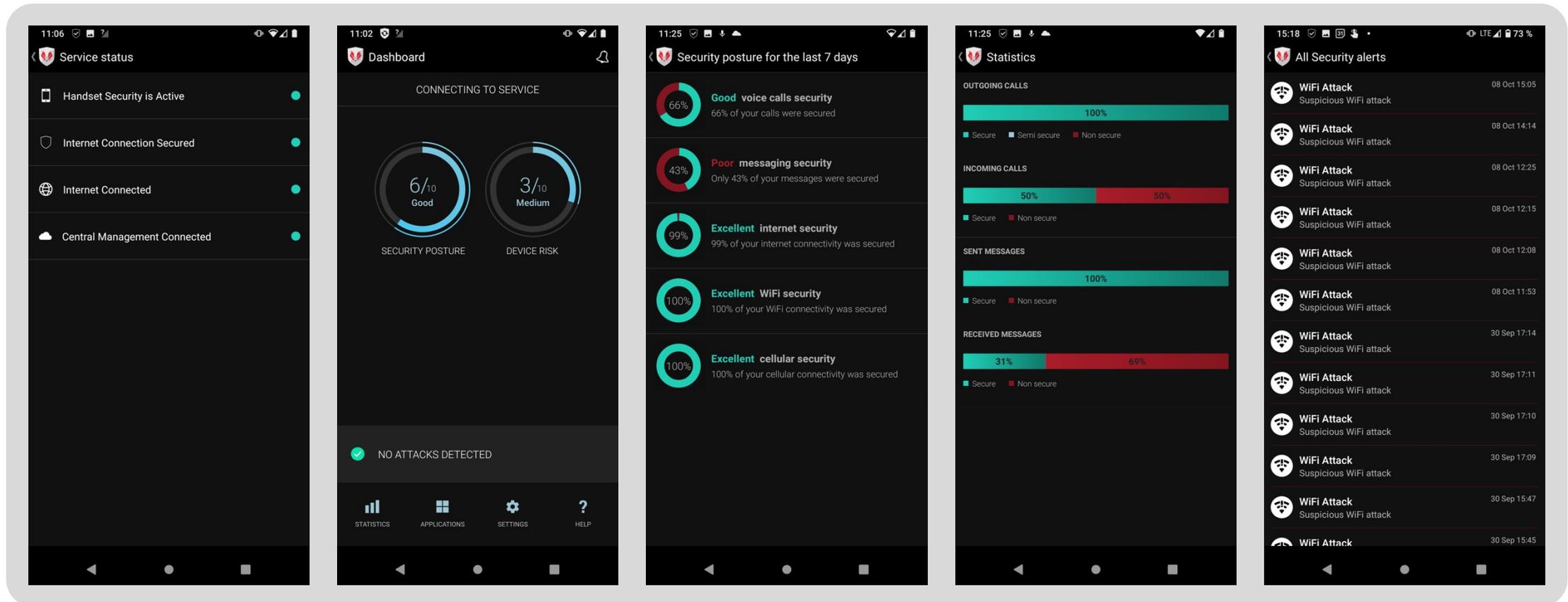
La usabilidad se logra con una experiencia de uso basada en las últimas versiones de **Android**, pero sin las molestas e inútiles apps preinstaladas.



Centro de Comando y Control KAYMERA Integrado en el Teléfono.



El Centro de Comando y Control integrado en el teléfono monitorea y gestiona toda la actividad dentro y fuera del dispositivo. KAYMERA envía **Actualizaciones Automáticas Remotas (OTA)** del Sistema Operativo (SO) al teléfono, para mantener la ciberdefensa siempre varios pasos adelante de las amenazas.



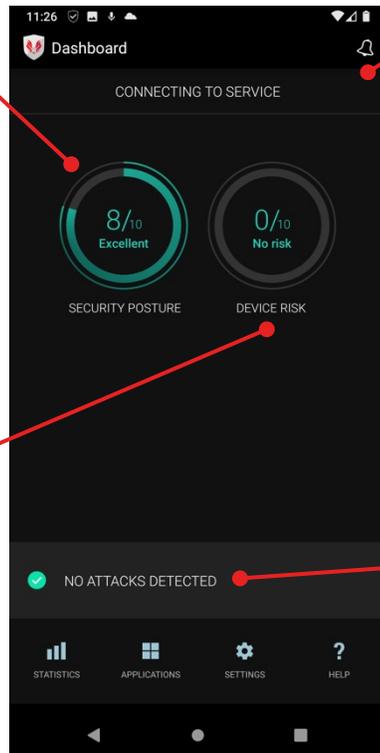
Teléfono Encriptado KAYMERA: *Detección y prevención de riesgos.*



El Centro de Comando y Control integrado en el (SO) KAYMERA monitorea en tiempo real el nivel de riesgos dentro y fuera del teléfono. Si se detecta una amenaza o un ataque, realiza una resolución avanzada de la situación y lanza contramedidas desde el mismo teléfono.

Postura de Seguridad

Mide la fortaleza de la defensa del equipo.



Nivel de Riesgo

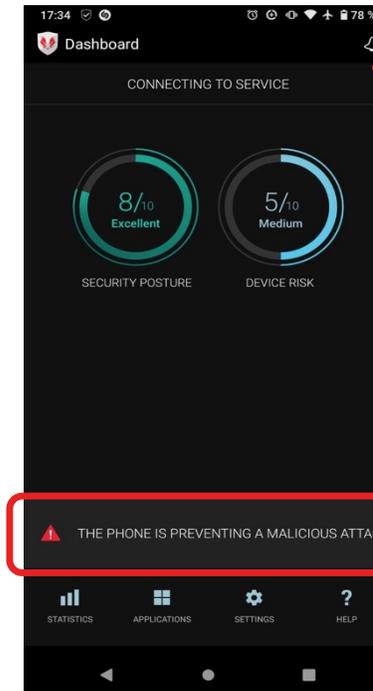
Riesgo Ambiental: en la red celular o Wifi
Riesgo Interno: apps maliciosas, expulsión de código, extracción física de datos, etc.

Alertas de seguridad

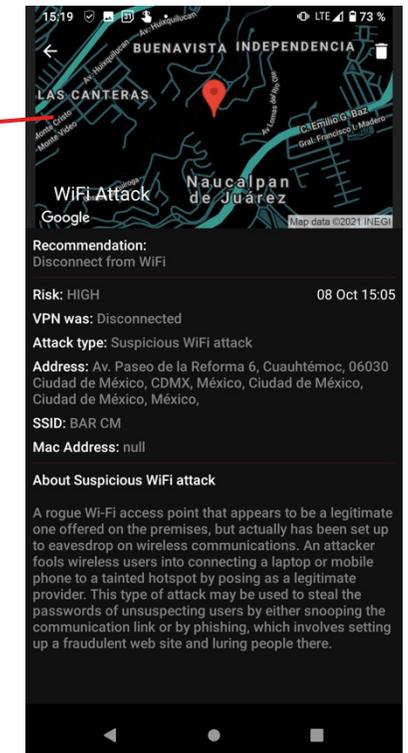
Historial y reporte de los ataques recibidos.

Alertas en tiempo real

Notifican al usuario que el teléfono enfrenta una amenaza y sugieren contramedidas.



Reporte de ataques



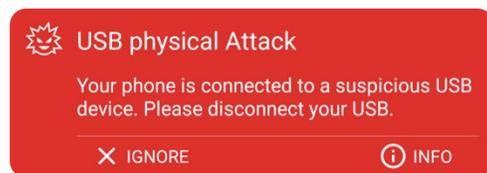
El Teléfono Encriptado KAYMERA tiene protección de 360°.



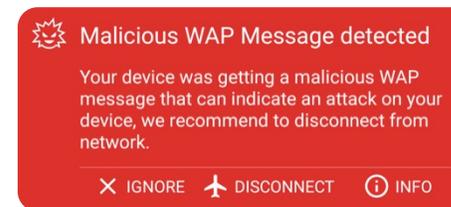
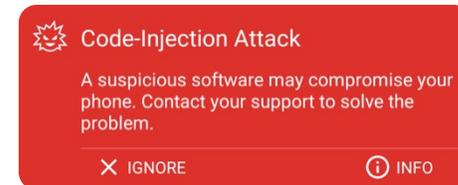
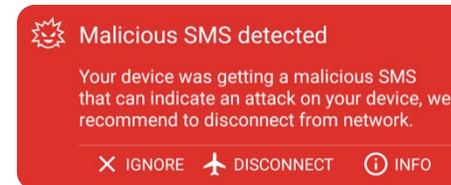
El Teléfono Encriptado KAYMERA es **INVULNERABLE** a infecciones, inyecciones de código, apps maliciosas y malware. Así como también a accesos maliciosos o inconveniente de las aplicaciones a la información y sensores del teléfono para robar información o utilizar el teléfono como un dispositivo remoto de escucha, rastreo y monitoreo.



Evita que las apps o software instalados en el teléfono tengan accesos maliciosos a sensores como **cámaras, micrófonos y GPS**; o se realice una extracción física de datos.



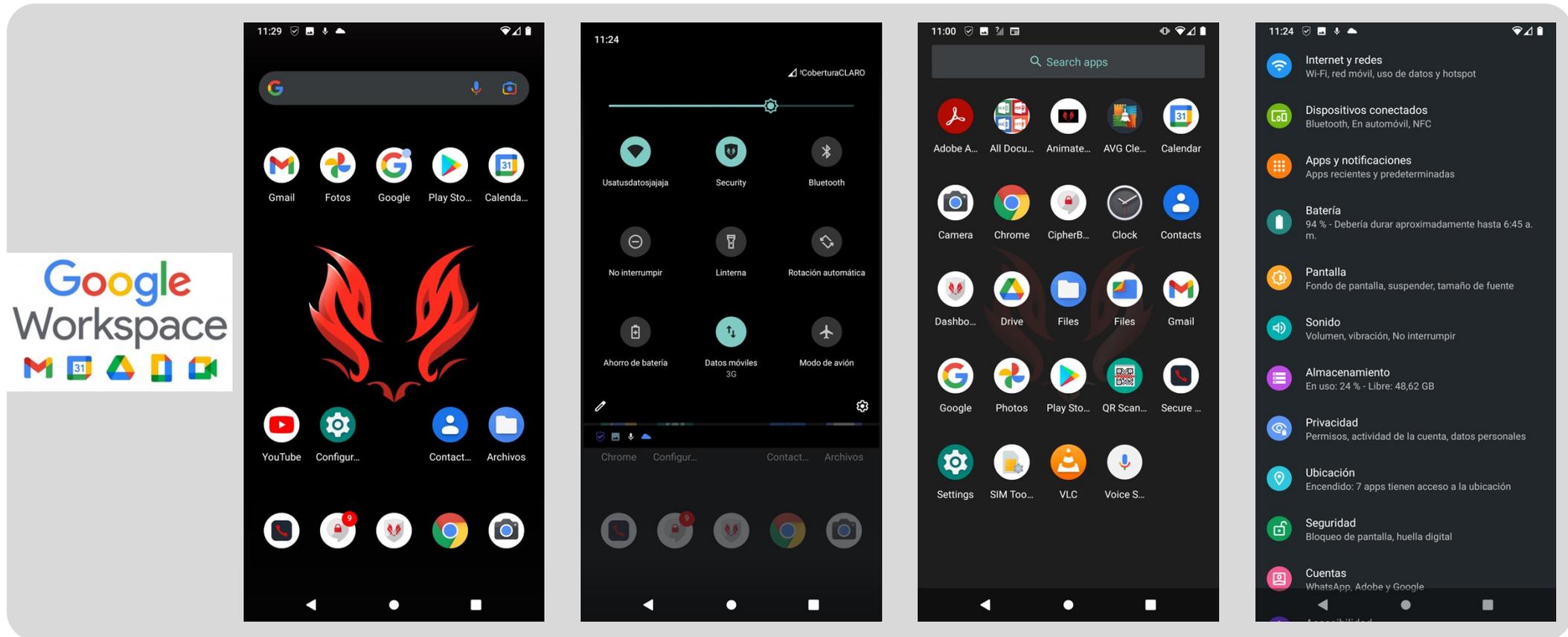
Bloquea los intentos de infección e inyección de código o malware (*troyanos, gusanos, virus, etc.*) mediante SMS, WAP, mail, páginas web, apps, etc.



Facilidad de Uso con experiencia nativa Android.



El Teléfono Encriptado KAYMERA ofrece una experiencia de usuario nativa de Android, la cual incluye las herramientas y apps de Google Workspace.



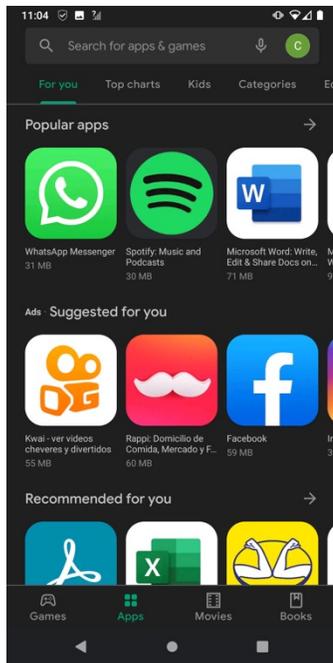
Puedes usar tus apps habituales con TOTAL protección y seguridad.



El usuario puede descargar sus apps desde **Google Play Store** disponible en el equipo y el **Teléfono Encriptado KAYMERA** se encarga de bloquear todas las actividades maliciosas y espías de las apps.

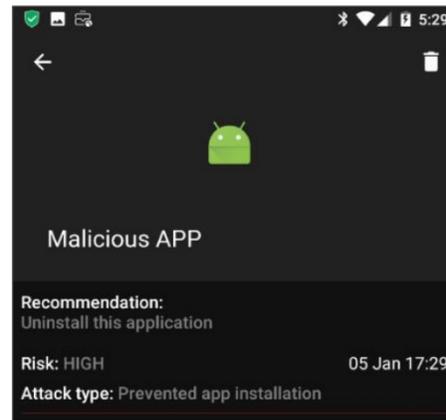
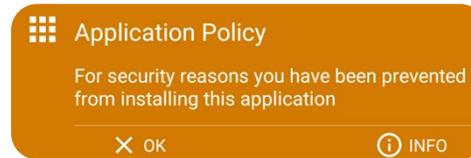
Google Play Store

Se pueden descargar apps como en cualquier Smartphone Android.



Lista Negra

KAYMERA tiene identificadas app maliciosas o espías.



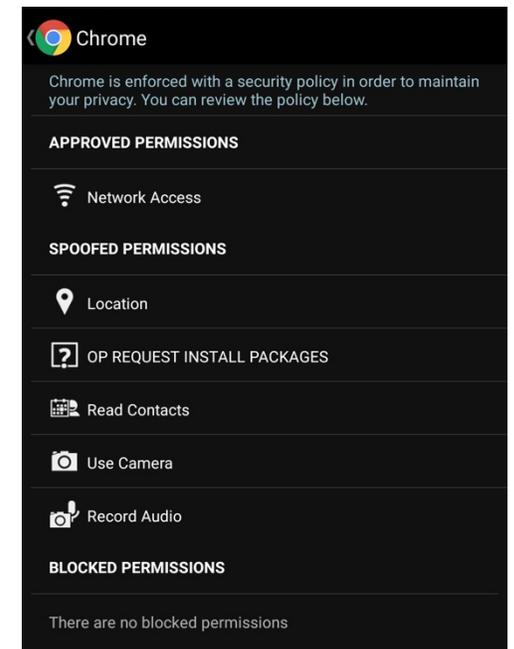
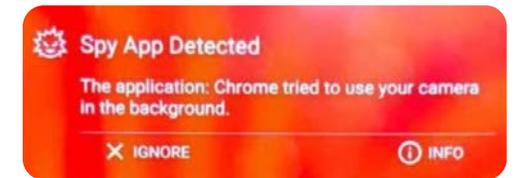
Control de Permisos

KAYMERA asigna 3 tipos de permisos a las apps.

Aprobados: dan permisos reales a las apps para acceder a elementos e información del teléfono.

Spoofed: el sistema engaña a las apps y les proporciona información falsa.

Bloqueados: niega a las apps el acceso a los elementos e información del teléfono.



Conexiones y Comunicaciones Protegidas.



El Teléfono Encriptado KAYMERA detecta, previene y protege contra vulnerabilidades, manipulaciones, infecciones e intervenciones de las redes móviles y conexiones Wifi.

Detecta y Protege contra:

- Intercepciones, manipulación de datos e infección vía **Wifi**.
 - **ARP Spoofing**: el atacante puede interceptar los datos, detenerlos o modificarlos.
 - **SLL Split**: el atacante puede robar passwords y espiar las comunicaciones o realizar phishing con sitios fraudulentos.
- Vulnerabilidades, amenazas y ataques desde la red celular: Stingrays, “Man in the Middle” o IMSI Catchers.
- Manipulaciones de señalización SS7 del operador celular.

 **Unsecure network connection**

You device is connected to 2g network. Secure communication is not available, your calls and messages can be easily snooped.

✕ IGNORE ⏸ DISMISS ✓ TRUST ALL

 **Warning: Suspicious Wi-Fi connection detected**

The characteristics of <unknown ssid> seems different than your last interaction with this network. It is recommended to terminate this connection. Alternatively choose TRUST to add <unknown ssid> to your trusted network list.

✓ TRUST ✕ DISCONNECT ⓘ INFO

 **Alert: Non-encrypted Wi-Fi connection detected**

ssid was identified as a non-encrypted Wi-Fi network and your connection could not be secured. It is recommended to terminate this connection. Ignoring this Alert will maintain this connection and may put your device at risk.

✕ IGNORE ✕ DISCONNECT ⓘ INFO

 **Alert: Wi-Fi Attack Detected**

Wi-Fi attack detected. It is recommended to disconnect from Wi-Fi

✕ IGNORE ✕ DISCONNECT ⓘ INFO



Comunicaciones Encriptadas Grado Militar entre usuarios KAYMERA.



El Teléfono Encriptado KAYMERA ofrece comunicaciones **ILIMITADAS** y **ENCRYPTADAS** Grado Militar entre la red mundial de usuarios KAYMERA. Con cifrado **AES-256 simétrico** para la máxima seguridad y privacidad contra todo tipo de interceptaciones.



Mensajes



Grupos de Chat



Transferencias de Archivos

Fotos, videos, PDF, Word, Excel, Pdf.



Enlaces Seguros de Voz



Conferencias Seguras de Voz

Hasta 20 participantes.

ADEMÁS



Enlaces Semi-Seguros de Voz
Para llamar por el sistema KAYMERA a cualquier teléfono. Encripta el tramo de la llamada del usuario a la Nube KAYMERA.



Modo Privado
Elimina el identificador de las llamadas de Enlaces Semi-Seguros de Voz: el receptor ve Número Oculto.

Enlace Semi Seguro de Voz

Llamada Celular Convencional



Enlace Seguro de Voz

Modo Camaleón: protección de la identidad y la información del usuario.



El **Modo Camaleón** ofrece una **Doble Identidad Digital** (o *doble perfil*) dentro del mismo teléfono para ocultar información y limitar en general el acceso a su **Teléfono Encriptado KAYMERA** en caso de que el usuario tenga que desbloquearlo en contra de su voluntad durante un robo con violencia o en una inspección.



Con su **PIN Habitual** el usuario tiene acceso completo a su teléfono: información, apps, registro, etc.

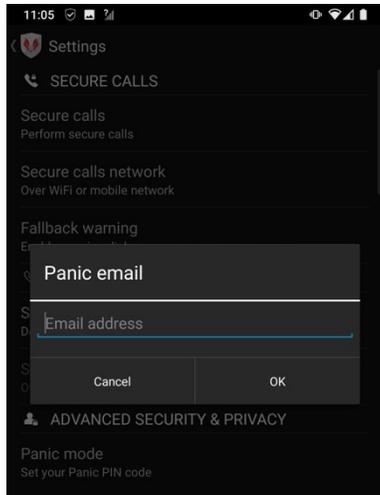
Con el **PIN Alternativo** el teléfono oculta sus archivos, fotos, videos, apps, mensajes, registros de llamadas, etc.



Modo Pánico: envía una alerta cuando el usuario está en peligro.



Cuando el usuario desbloquea el Teléfono Encriptado KAYMERA con su PIN Alternativo además de activarse el Modo Camaleón, se activa el **Modo Pánico**: el teléfono envía correos con alertas de pánico al **Panic email** definido por el usuario.



Al activarse el **Modo Pánico**, se envían 2 correos con alertas de pánico incluyendo la siguiente información:



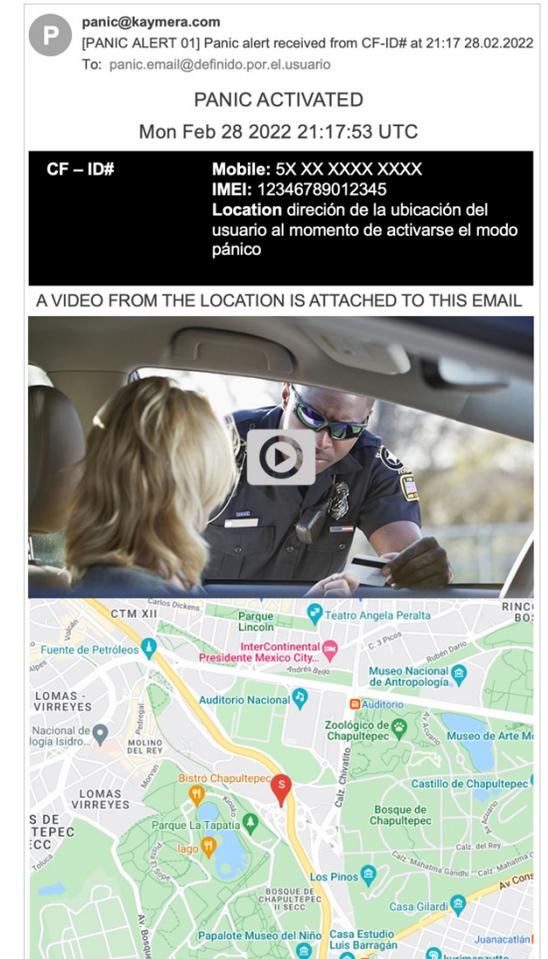
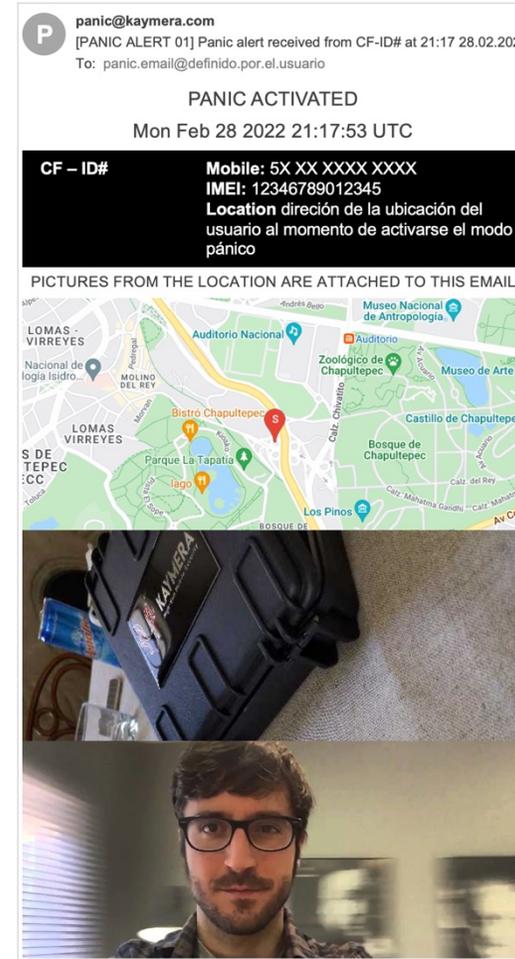
La ubicación donde se activó el Modo Pánico.



Foto de la cámara frontal y trasera.



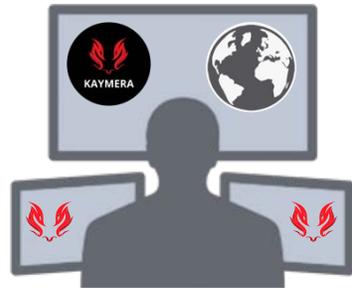
Un video de 4 segundos de la cámara frontal.



Borrado remoto de emergencia del Teléfono Encriptado KAYMERA.



En caso de que el equipo se pierda, sea robado o se encuentre bajo un ataque extremo; desde el **Comando Central de Seguridad KAYMERA** podemos borrar o inutilizar totalmente el equipo de **forma remota** a solicitud del **CLIENTE** para proteger su información.



Acción	Resultado	Caso de Uso
Borrar Información del Dispositivo	Restablecimiento remoto de datos de fábrica	En caso de que el dispositivo se pierda o esté en medio de un ataque intenso, se puede borrar la información del usuario para que el teléfono sea restablecido a los valores de fábrica
Inutilizar el Dispositivo	El dispositivo deja de funcionar	En caso de que el dispositivo sea robado, se puede borrar el sistema operativo junto con todos los datos del dispositivo



*Estamos aquí para asegurarnos
que su comunicación e información
no caiga en malas manos.*



www.invict.com.co/kaymera



Contacto

INVICT | KAYMERA
Equipo Comercial
kaymera@invict.com.co