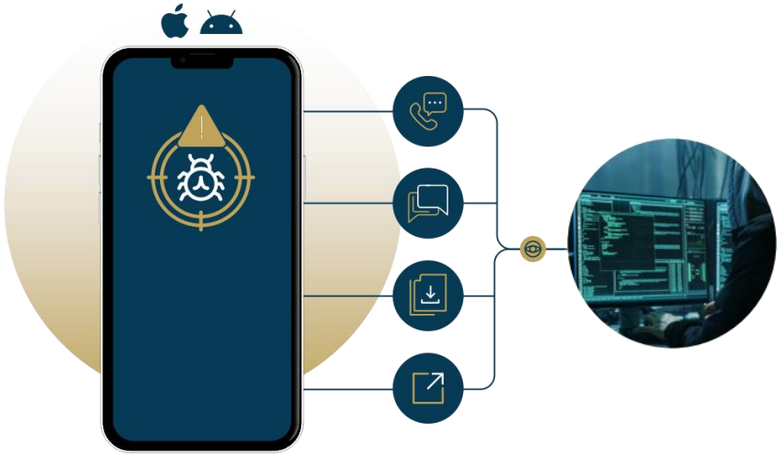
EL MUNDO HA
CAMBIADO

La necesidad de privacidad y seguridad móvil nunca ha sido mayor. Los sistemas operativos de teléfonos móviles como iOS y Android no son capaces de proteger contra software espía como Pegasus.



Los hackers explotan las vulnerabilidades en los sistemas operativos comerciales, especialmente en Android o iOS, y en aplicaciones de mensajería como Signal o WhatsApp.

Para que un teléfono móvil sea completamente seguro, debe proteger las aplicaciones, el sistema operativo y el hardware. Solo un enfoque integral que aborde todos los aspectos de las comunicaciones móviles puede garantizar una protección absoluta.

PRESENTAMOS EL
SOTERA SECUREPHONE

Confiado a nivel mundial por gobiernos, empresas e individuos como su lugar seguro para comunicaciones de voz y texto.

El Sotera SecurePhone utiliza el mismo sistema operativo (Integrity 178B) que asegura el arsenal nuclear de los Estados Unidos, múltiples sistemas de armas y los sistemas espaciales de NASA/DOD.




Solo una solución que proteja las diferentes capas del teléfon o puede proteger exitosamente tus datos.

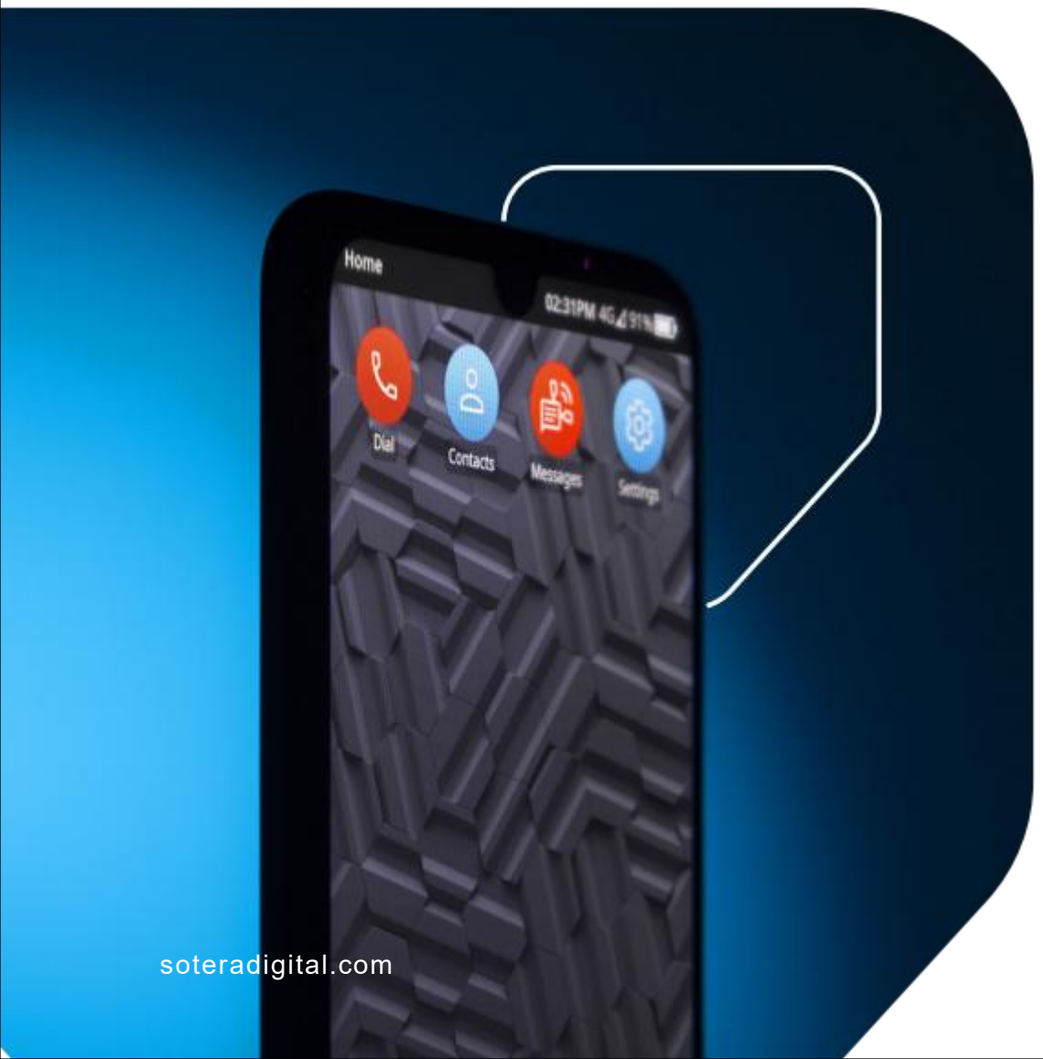
Capa 1: Las Aplicaciones.
Las aplicaciones VoIP encriptadas como WhatsApp, Signal y Telegram no protegen sus comunicaciones de extremo a extremo.

Capa 2: El Sistema Operativo
Los sistemas operativos de Apple y Android no son seguros y tienen miles de vulnerabilidades conocidas.

Capa 3: El Hardware.
Los teléfonos inteligentes estándar no protegen contra las amenazas de malware en ninguno de los dispositivos finales.

SOTERA

ENCRYPTION



Cifrado de disco:

XTS-AES256

Intercambio y cifrado seguro de texto y mensajes:

Utilizamos el protocolo Double Ratchet par a intercambiar mensajes cifrados. X3DH se utiliza para acuerdos de claves entre las partes.

Los algoritmos utilizados por estos proto colos son:
EdSA con Ed25519
ECHD con Curve25519 (X25519)
Esquema de cifrado **AEAD** utilizando HK DF con AES256-CBC / HMAC-SHA256

Intercambio y cifrado de voz:

El secreto compartido se intercambia a través del canal de mensajería segura entre dispositivos:
La voz se cifra utilizando AEAD AES25 6-GCM después de derivar un AES256 -CM_PRF mediante HKDF a partir del secreto compartido.

Además, para el tráfico de red, aplicamos:

TLS 1.3 utilizando ED25519/X25 519 y autenticación mutua

XEdDSA y VXEdDSA: Se utilizan para crear y verificar firmas compatibles con EdDSA utilizando formatos de clave pública y privada inicialmente definidos para las funciones X25519 y Diffie-Hellman de curva elíptica.
Además, se utiliza VXEdDSA, que extiende XEdDSA para convertirlo en una función aleatoria verificable o VRF.

X3DH: El protocolo Extended Triple Diffie-Hellman es un protocolo de acuerdo de claves. X3DH establece una clave secreta compartida entre dos partes que se autentican mutuamente en función de las claves públicas. X3DH proporciona secreto hacia adelante y negación criptográfica.

Double Ratchet: El algoritmo Double Ratchet, que se utiliza para que dos partes intercambien mensajes cifrados basados en una clave secreta compartida. Las partes derivan nuevas claves para cada mensaje Double Ratchet para que las claves anteriores no puedan calcularse a partir de las posteriores.
Las partes también envían valores públicos Diffie-Hellman adjuntos a sus mensajes. El resultado de los cálculos Diffie-Hellman se mezcla en la clave derivada para que las claves posteriores no puedan calcularse a partir de las anteriores. Estas propiedades brindan cierta protección a los mensajes cifrados anteriores o posteriores en caso de compromiso de las claves de una de las partes.

Sesame: El algoritmo Sesame se utiliza para gestionar sesiones de cifrado de mensajes en un entorno asincrónico y multi-dispositivo.