

# HS - 9398 IPHONE-SHIELD



## Hable con SEGURIDAD desde su IPHONE

IPHONE hace que sus llamadas sean privadas y seguras, para que siempre pueda hablar con confianza.

### Principales Características

#### Seguridad

- Sólida encriptación de punta a punta
- Certificado por el Ministerio de Defensa de los Estados Unidos de Norteamérica bajo la norma FIPS 140-2 del NIST (Cert# 1310)

#### Sencillez

- Funciona en teléfonos inteligentes de uso común como Nokia y IPHONE
- Sin equipos especializados
- Experiencia intuitiva para el usuario, funciona en un segundo plano y se integra con el directorio telefónico del aparato

#### Desempeño

- Alta calidad de llamadas con baja latencia
- Opera en todas las redes inalámbricas con capacidad de transmisión de datos



## Protección de Información Valiosa

Tanto Empresas como Organismos de Gobierno realizan esfuerzos significativos a fin de proteger sus datos valiosos contra pérdida o interceptación -particularmente cuando se conectan desde fuera de la oficina y cuando viajan.

En el 2010 el costo de interceptación móvil se redujo considerablemente, ya que el libro de códigos para descifrar llamadas GSM -utilizado en 80% de los teléfonos celulares a nivel mundial- fue computado y publicado en Internet por un grupo de hackers, quienes además hicieron demostraciones públicas de equipos de interceptación que actualmente se encuentran ampliamente disponibles por poco dinero.

Con **IPHONE-SHIELD**, las llamadas pueden ser fácilmente protegidas en teléfonos celulares de uso generalizado -y conectadas de forma segura a sistemas telefónicos de oficina - de modo que usted tenga la certeza de que dichas conversaciones permanecen confidenciales donde se realicen.





## Hable con Confianza

**IPHONE-SHIELD** es un software de última generación, fácil de usar y que funciona en teléfonos móviles estándar utilizando el canal de datos para proveer una calidad de voz única, períodos muy cortos de demora en la voz (latencia), cobertura global y capacidad intercontinental de llamadas -todo de manera segura. Utilizar **IPHONE-SHIELD** es tan fácil como hacer una llamada normal, con el agregado de tener la confianza de que las llamadas telefónicas que realiza ya sea en ambiente móvil o de oficina, en su país o en el exterior, entre departamentos o dentro de los mismos, o bien con proveedores y socios de negocio, están protegidas de punta a punta. La seguridad está garantizada. Para proteger estas comunicaciones de voz, **IPHONE-SHIELD** utiliza las mismas tecnologías de encriptación que se usan en la protección de laptops, datos corporativos y transacciones de servicios financieros.

## Tecnología IPHONE-SHIELD

La solución avanzada de **IPHONE-SHIELD** encabeza la industria en tanto que proporciona seguridad en multi-niveles a fin de establecer una llamada encriptada de óptima calidad entre dispositivos móviles confiables. **IPHONE-SHIELD** utiliza EMCP (Encrypted Mobile Content Protocol - Protocolo de Encriptación de Contenido Móvil), un conjunto de protocolos basados en estándares tecnológicos, con el fin de optimizar el intercambio de contenido entre teléfonos celulares en tiempo real y a través de redes inalámbricas con bajo ancho de banda.

*Certificado por el Ministerio de Defensa de los Estados Unidos de Norteamérica bajo la norma FIPS 140-2 del NIST (Cert# 1310)*

## Criptografía y Generación de Números Aleatorios

**Criptografía de Clave Pública (RSA de 2048 bits y ECDSA utilizando curvas con módulos primos de 384 bits)** El RSA y ECDSA son utilizados para la autenticación. Los pares de la clave se generan en el teléfono durante la instalación y son únicos para cada aparato telefónico. Una clave privada jamás se comparte. Los algoritmos de Curva Elíptica Diffie-Hellman (ECDH) y los algoritmos RSA se utilizan para el intercambio de claves. La clave de sesión es válida para una sola llamada y se destruye de forma segura al finalizar su uso.

**Criptografía Simétrica (AES y RC4 ambas de 256 bits)**

Ambos algoritmos de encriptación se utilizan al mismo tiempo. El paquete de datos se encripta primeramente con RC4 y el texto cifrado resultante se encripta nuevamente con AES en modo de operación "Contador" (CTR). Ambos algoritmos se inicializan con el intercambio de clave de sesión.

**Algoritmos Base "Hash" (SHA512, MD5)**

Dos algoritmos base "Hash", estándares en la industria, son utilizados para obtener una mayor garantía en la integridad de la encriptación.

**Generación de Números Aleatorios**

Durante el proceso de instalación se genera una base inicial de valores numéricos de 2048 bits que se actualiza periódicamente. El valor inicial se obtiene del input del micrófono.



## Acerca de IPHONE-SHIELD

**IPHONE-SHIELD** es el sistema líder en encriptación de comunicaciones de voz (llamadas) en teléfonos celulares. Con **IPHONE-SHIELD** se desarrolló el Protocolo de Encriptación de Contenido Móvil (Encrypted Mobile Content Protocol - EMCP) para solucionar los retos existentes en la industria en términos de desempeño. EMCP es una tecnología basada en estándares que utiliza IP (Protocolo de Internet) para proveer una óptima entrega de datos encriptados.

Hoy en día, las soluciones **IPHONE-SHIELD** son utilizadas mayormente por gobiernos, empresas y ejecutivos de alto nivel alrededor del mundo.



### Plataformas Compatibles

- IPHONE 3GS
  - IPHONE 4
  - IPAD
- Sistema operativo iOS4.

IPHONE-SHIELD es 100% compatible y seguro con la línea BLACKBERRY-SHIELD