

# Bittium

Bittium Secure Suite™  
Conjunto de servicios  
completo para  
comunicaciones  
seguras

## Servicios de Seguridad

VPN Móvil

Administración  
de Dispositivos Móviles

Administración  
de Aplicaciones Móviles

Atestación Remota

Actualización Aérea (OTA)  
de Firmware

Servidor de Bitácora y  
Analíticos

Mensajes Push Seguros



**Bittium Secure Suite** proporciona un conjunto de servicios completo para las comunicaciones seguras, la transferencia de información y la administración de dispositivos cuando se utiliza la familia de productos de teléfonos inteligentes ultra seguros Bittium Tough Mobile. Con Bittium Secure Suite, usted no dependerá de la conectividad a internet público, terceros o servicios de nube. Opere y controle todos los servicios de Bittium Secure Suite en instalaciones seguras propias, o utilice el operador confiable para alojar los servicios. El aprovisionamiento de un sólo paso con códigos QR permite el despliegue fácil y sin costuras de Bittium Secure Suite para toda su flota de dispositivos. En conjunto, Secure Suite y la familia de productos de teléfonos inteligentes Tough Mobile, forman la solución de comunicaciones seguras más segura del mundo que haya sido aprobada hasta un nivel Confidencial (NCSA-FI).

PARA MÁS INFORMACIÓN, POR FAVOR CONTACTE A:

info@gigsrl.com • [www.gigsrl.com](http://www.gigsrl.com)

## Beneficios



### Tráfico de Red Seguro

Con la VPN móvil Bittium SafeMove®



### Control eficiente sobre la flota de dispositivos

Con la función de Administración de Dispositivos Móviles



### Sólo aplicaciones aprobadas

Las aplicaciones se ponen a disposición con el Administrador de Aplicaciones Móviles.



### Sin Filtraciones de Datos

Acceso a servicios otorgado sólo a los dispositivos cuya integridad ha sido autenticada de manera remota



### Sin Violaciones a la Información

Actualizaciones de firmware entregadas por aire a los Bittium Tough Mobile



### Rastro auditable innegable de los dispositivos

Rastro auditable de los dispositivos y de los componentes del servidor con el Servidor de Bitácoras



### Entrega Segura de Información para Aplicaciones

Mensajería push segura a dispositivos sin los riesgos de los servicios de nube públicos

# Bittium Secure Suite™

## Especificaciones técnicas

### Características de la VPN móvil

- › IPsec, IKEv2 MOBIKE
- › Firewall integrado y política IPsec
- › Siempre encendida, no puede ser omitida por aplicaciones ni por usuarios
- › Requiere atestación remota exitosa para acceso a la VPN
- › VPN por aplicación
- › Código base probado extensivamente y auditado externamente

### Cifrado de la VPN móvil

- › Compatible con suite B CNSA/NSA
- › SHA2-512
- › AES-256, SERPENT
- › Cifrado de curva elíptica:
- › Grupos ECDH 19,20, 21 (NIST) y 27,28,29 y 30 para IKEv2 (Brainpool)
- › Certificados ECDSA
- › Llaves RSA de hasta 16k

### Administración de Dispositivos Móviles

Administración remota y centralizada del Tough Mobile y las funciones de seguridad Android, desde el servidor.

- › Actualización remota de políticas (push)
- › Administración de las políticas de la VPN SafeMove
- › Borrado remoto
- › Bloqueo remoto
- › Recuperación de bitácora auditoría del dispositivo
- › Administración de certificados confiables CA
- › Administración de Wi-Fi:
- › Configuración SSID
- › Política de Seguridad
- › Credenciales

### Política de Dispositivos

- › Política de contraseña de bloqueo de dispositivo:
  - › Numérica, alfanumérica, compleja
  - › Longitud de contraseña
  - › En conjunto, es posible controlar un total de 100+ parámetros
- › Borrado de dispositivo tras ingresos

- › fallidos de contraseña
- › Límite de tiempo para bloqueo de dispositivo
- › Caducidad de duración de la contraseña
- › Habilitar/deshabilitar:
  - › Software de fuentes no confiables
  - › Android Debugging Bridge (ADB)
  - › Configuraciones del desarrollador
  - › Bluetooth
  - › Cámara
  - › Envío y recepción de MMS
  - › Servicios de ubicación
  - › iZat (Qualcomm AGPS)
  - › Revisión de conectividad Android
  - › Ajuste de volumen
  - › Control de configuraciones de aplicación
  - › Transmisión celular
  - › Configuración de las credenciales del dispositivo
  - › Configuración de redes móviles
  - › Anclaje para datos (tethering)
  - › Configuración de la VPN
  - › Configuración de WiFi
  - › Restablecimiento de valores de fábrica iniciado por el usuario
  - › Instalación y desinstalación de aplicaciones
  - › Modificación de cuentas
  - › Montaje de medios físicos externos
  - › (USB, tarjeta SD)
  - › Restablecimiento de configuraciones de red iniciadas por el usuario
  - › Haz NFC saliente
  - › Llamadas salientes
  - › SMS
  - › Ajuste del volumen del micrófono
  - › Transferencia de archivos vía USB

### Administración Móvil de Aplicaciones

- › Biblioteca de aplicaciones administrada de manera privada para proporcionar aplicaciones a los dispositivos.
- › Base de instalación de aplicaciones se mantiene actualizada con las versiones y ajustes de seguridad más recientes.

### Atestación remota

El elemento criptográfico del hardware de los Tough Mobile proporciona evidencia que el dispositivo remoto está exactamente igual que como salió de la fábrica y que lleva el firmware oficial sin

modificaciones. El servicio de atestación remota permite revisar la integridad que es usada por el MDM, el Gateway de la VPN y los servicios de terceros.

- › Integridad de componentes clave de hardware y software revisada vía remota a través del Elemento Seguro.
- › Integración a la VPN, control de acceso
- › API para integrar servicios de terceros

### Actualización aérea (OTA) del firmware

Control completo sobre cuáles dispositivos son actualizados, cuando y con qué firmware.

- › Búsqueda automática de actualizaciones
- › Posibilidad de asignar actualizaciones por dispositivo o grupo
- › Opcionalmente protegido por la VPN

### Servidor de Bitácora y Visualización

- › Analíticos de registro visuales para una respuesta a incidentes eficiente e incluso la prevención proactiva de incidentes.
- › Recolección y análisis de información para mantener a los administradores actualizados sobre qué pasa del lado de los dispositivos y la infraestructura
- › Integración con Analíticos de Bittium SafeMove® (opcional)

### Mensajería Push Segura

Sistema push seguro y escalable que puede implementarse fácilmente en las aplicaciones. API Familiar, similar a los sistemas de mensajería en nube comunes.

- › Bajo requerimiento de energía
- › Baja latencia
- › Bajo ancho de banda
- › Puede estar alojado en las instalaciones del cliente
- › Seguridad TLS y VPN opcional

### Plataformas de servidor compatibles

- › Aplicación SafeMove SMR340
- › Aplicación virtual Vmware™

