



**XIII
JORNADAS
STIC
CCN-CERT**



Caso de Estudio: Ejército de Finlandia

Comunicaciones móviles para gestión de crisis

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT

The Bittium logo is displayed in a bold, blue, sans-serif font. To the left of the logo, there is a decorative graphic consisting of numerous thin, light blue lines that curve and fan out, resembling a stylized signal or a network diagram.

Bittium

Anton Gyllenberg

Anton.gyllenberg@bittium.com

Laura Casadevall

ext-Laura.CasadevallSagredo@bittium.com

Comunicaciones seguras y fiables en FINBLUECORE



Smartphones Android seguros y portátiles Windows



Uso de infraestructuras LTE, Wi-Fi y SATCOM, públicas y privadas, securizadas con una infraestructura VPN móvil



El sistema lleva seis años en producción, y ha sido usado en varias misiones internacionales



Sistema con acreditación de seguridad

Las cuatro misiones de las Fuerzas Armadas finesas



Finlandia participa en las siguientes misiones en el exterior

- Afganistán (RS), 60 efectivos
- Líbano (UNIFIL), 200 efectivos
- Kosovo (KFOR), 19 efectivos
- Irak (OIR), 80 efectivos
- Irak (NMI)
- Malí (EUTM Mali), 3 efectivos
- Malí (MINUSMA), 5 efectivos
- Somalia (EUTM Somalia), 12 efectivos
- Mediterráneo (EUNAVFOR MED)
- Oriente Medio (UNTSO), 15 efectivos



FINBLUECORE

Sistema de Información y Comunicaciones (TIC) usado por el Ejército finés en todas las misiones internacionales de gestión de crisis

La versión actualmente desplegada es la tercera generación del sistema

Esta versión está desplegada y en uso en misiones internacionales desde 2013

Los *smartphones* Android se añadieron a la arquitectura en 2016 (Irak y Líbano)



Servicios de FINBLUECORE

Servicios de datos, voz, mando y control (C2) y videoconferencia (VTC)

Sistema C2

Videovigilancia y control de acceso



Basado en el Cuartel General: Plataforma colaborativa basada en WEB, correo electrónico, seguridad.

Acceso a los servicios de Internet nacionales, servicios de TV y telefonía, y otros servicios de entretenimiento

Requisitos especiales

Necesidad de comunicarse con personal local y/o desplegado *in situ*, como, por ejemplo, intérpretes, autoridades y aliados



Coste: Necesidad de usar redes comerciales operadas por terceros no confiables, como operadores de telecomunicaciones o ISPs



Tolerancia a fallos: cortes de energía y red, interferencias de señal



Servicios móviles



Servicios móviles

Uso seguro (táctico)

- *C2 / Battle Management System*
- *Push-to-talk* (PTT)
- Llamadas de voz (VoIP seguro)
- Comunicación segura cifrada de extremo a extremo: Llamadas de voz, videollamadas, teleconferencia, mensajería instantánea y adjuntos multimedia



Uso administrativo y servicios externos

- Acceso seguro a Internet
- Llamadas de voz seguras (telefonía)
- Librería de aplicaciones cuyo uso está permitido por el Ejército finés:
 - Información del tiempo y noticias
 - Comunicación: aplicación de mensajería y VoIP
 - Servicios de viaje (p. ej. aerolínea, agencia de viajes)
 - Servicios financieros (p. ej. banco online)
 - Diagnóstico del estado de la red y otras herramientas administrativas



Servicios móviles

IMPORTANTE

Es importante ofrecer también acceso seguro a los servicios administrativos, de viaje, comunicación personal e incluso entretenimiento.

De lo contrario aparecerán soluciones alternativas no oficiales que serán menos seguras que permitir un acceso controlado.

Uso administrativo y servicios externos

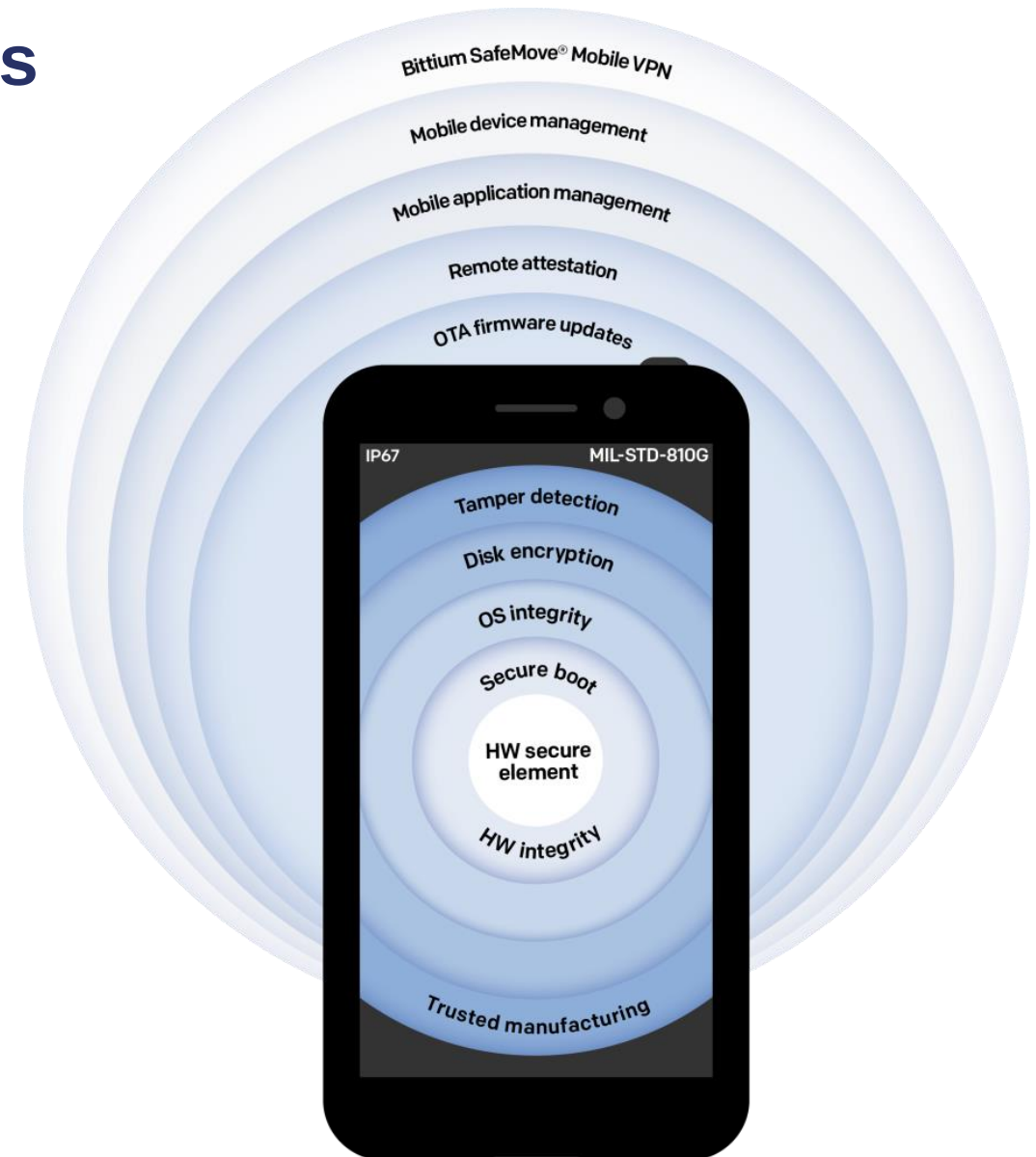
- Acceso seguro a Internet
- Llamadas de voz seguras (telefonía)
- Librería de aplicaciones cuyo uso está permitido por el Ejército finés:
 - Información del tiempo y noticias
 - Comunicación: aplicación de mensajería y VoIP
 - Servicios de viaje (p. ej. aerolínea, agencia de viajes)
 - Servicios financieros (p. ej. banco online)
 - Diagnóstico del estado de la red y otras herramientas administrativas



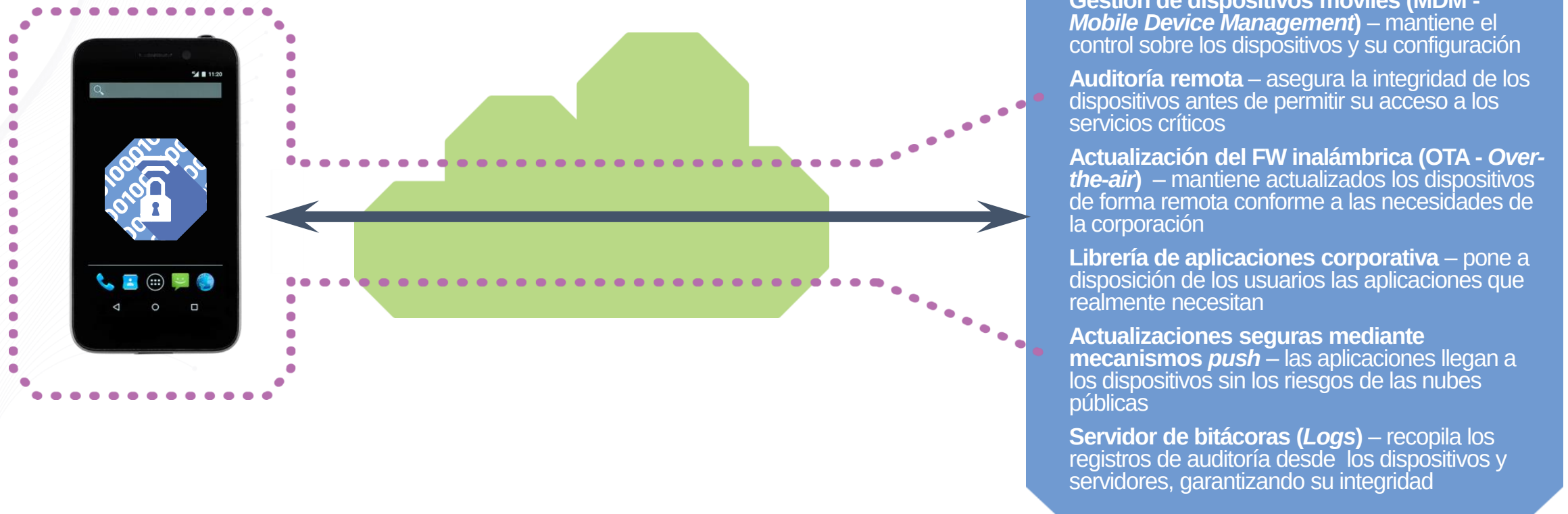
Seguridad basada en dos elementos

1. Plataforma de confianza → *smartphone* Bittium Tough Mobile™ con un diseño de seguridad basado en HW
2. Protección de los datos en tránsito + control y monitoreo centralizado de la flota de dispositivos → Bittium Secure Suite™ como solución para la infraestructura SW

El diseño de seguridad sigue los principios de la **seguridad en capas** → Estas capas y métodos de seguridad superpuestos están diseñados para lograr **robustecer la integridad y proteger la privacidad**

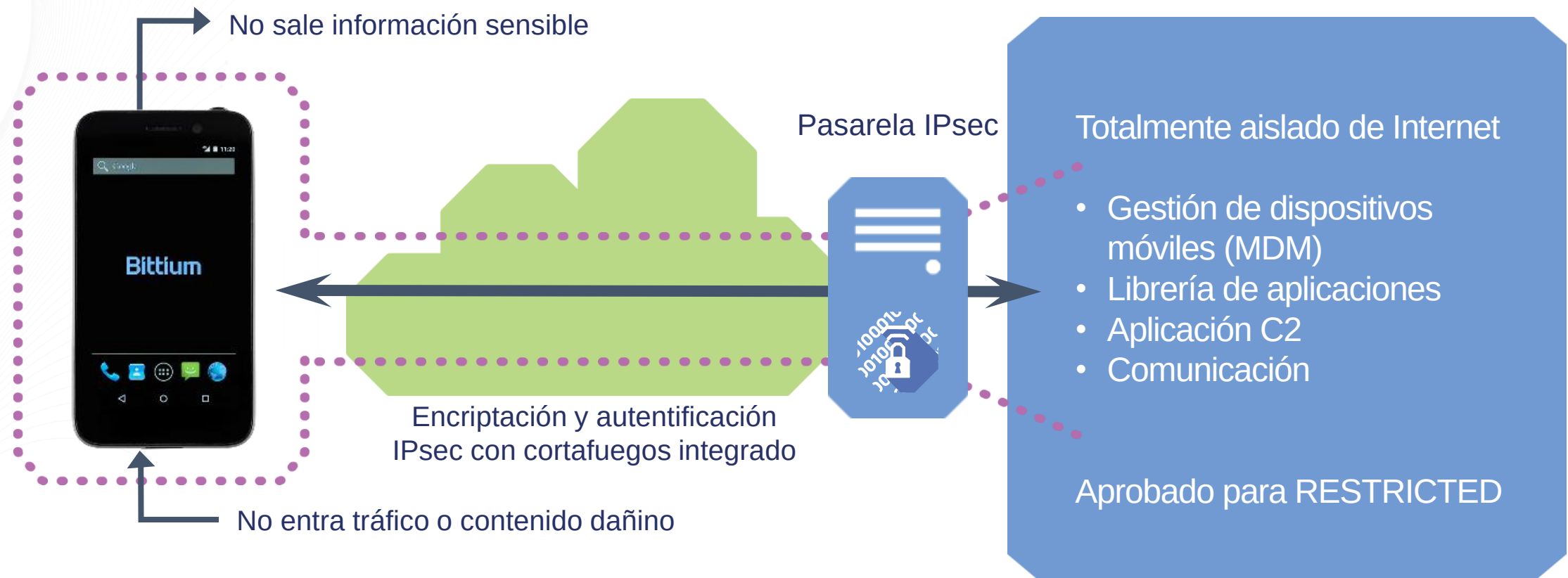


Bittium Secure Suite™



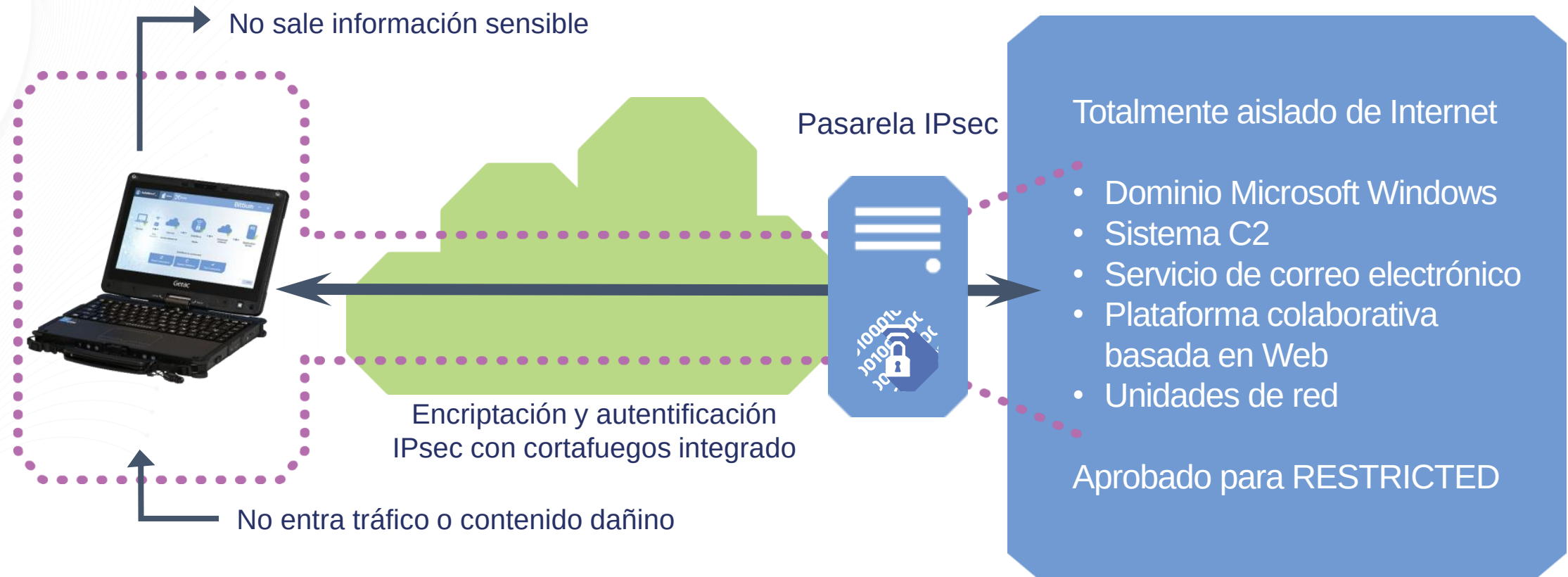
Bittium Secure Suite™ es una solución software instalada tanto en el lado servidor como en los dispositivos que habilita el uso de las capacidades de las plataformas mediante un conjunto de servicios escalables.

VPN móvil – Todo el tráfico de red está siempre securizado



Bittium SafeMove® IPsec VPN no solo otorga acceso a los recursos de la red interna; una función igualmente importante es prevenir conexiones de red no autenticadas o sin cifrar, y asegurar el control del cortafuegos sobre todo el tráfico de red.

VPN móvil – Todo el tráfico de red está siempre securizado



Bittium SafeMove® IPsec VPN no solo otorga acceso a los recursos de la red interna; una función igualmente importante es prevenir conexiones de red no autenticadas o sin cifrar, y asegurar el control del cortafuegos sobre todo el tráfico de red.

Red segura y tolerante a fallos



Servicios y aplicaciones

Compatibilidad demostrada también con servicios y aplicaciones de terceros

Bittium
Secure Call™



Comunicaciones
encriptadas de extremo
a extremo: voz, video,
chat, adjuntos

Solución de
terceros



Push-To-Talk (PTT)

Solución de
terceros



Llamadas VoIP
(segurizadas con IPsec)

Solución de
terceros



*C2/
Battle Management
System*

Solución de
terceros



Comunicaciones
externas:
voz, video, chat

Solución de
terceros



Servicio de correo
electrónico

Productos de seguridad móvil

Bittium
SafeMove®
Mobile VPN



Portátiles y *tablets* con
aplicaciones tácticas

Bittium Tough
Mobile™ R



Uso táctico

Bittium Tough
Mobile™ C



Uso táctico (modo seguro),
uso administrativo y
servicios externos
(modo normal)

Bittium Secure
Suite™



Conjunto de servicios para
segurizar las comunicaciones
con los *smartphones* Bittium
Tough Mobile™

Bittium
SafeMove®
Analytics



Para seleccionar al mejor
operador de red

Funcionalidades y políticas de gestión de dispositivos (MDM) en Bittium Secure Suite™

Funcionalidades

- Definición de políticas de actualización remota (*push*)
- Gestión de políticas de SafeMove® VPN
- Borrado remoto
- Bloqueo remoto
- Cambio de contraseña
- Recuperación de los registros de auditoría (*logs*)
- Gestión de los certificados de las Autoridades de Certificación de confianza
- Gestión de redes Wi-Fi:
 - Configuración de los SSID
 - Políticas de seguridad
 - Credenciales
- Suministro y actualización de las librerías
- Acceso a la cuenta de correo electrónico
- Gestión de las aplicaciones
 - Lista de aplicaciones y SW instalado
 - Lista blanca de aplicaciones
 - Instalación de aplicaciones

Políticas

- Política de contraseña de desbloqueo del dispositivo:
 - Numérica, alfanumérica, compleja
 - Longitud de la contraseña
- Borrado del dispositivo tras introducir una contraseña fallida
- Tiempo de inactividad para bloquear el dispositivo
- Plazo de caducidad de contraseña
- Activar / desactivar:
 - SW de fuentes no confiables
 - *Android Debugging Bridge* (ADB)
 - Configuraciones de desarrollador
 - Bluetooth
 - Cámara
 - Envío y recepción de MMS
 - Servicios de ubicación
 - iZat (GPS asistido de Qualcomm)
 - Comprobación de conectividad de Android
 - Ajustes de volumen de altavoz y micrófono
 - Control de la configuración de las aplicaciones
 - Difusión de celda (CB - *Cell broadcast*)
- Activar / desactivar:
 - Configuración de las credenciales del dispositivo
 - Configuración de las redes móviles
 - Anclaje a red (*Tethering*)
 - Configuración de la VPN
 - Configuración de redes Wi-Fi
 - Restablecimiento de la configuración de fábrica iniciada por el usuario
 - Instalación y desinstalación de aplicaciones
 - Modificación de cuentas
 - Conectar medios físicos externos (USB, tarjetas SD)
 - Restablecimiento de la configuración de red iniciada por el usuario
 - Uso de NFC, *Android beam* y similares en transmisión
 - Llamadas salientes
 - SMS
 - Transferencia de ficheros por la conexión USB
 - Aplicaciones del sistema
 - *Google Mobile Services* (GMS)
 - 2G/GSM

Acreditación de seguridad

Las Fuerzas Armadas finesas tienen su propia organización de auditoría y aprobación de seguridad. Sin embargo, y por ser FINBLUECORE usado en misiones de cooperación internacional, fue en su momento el primer sistema del Ejército finés aprobado por TRAFICOM (antes FICORA, Viestintävirasto) – la Autoridad de Acreditación de Seguridad nacional finesa.

Además, empresas comerciales de seguridad como F-Secure y Nixu han realizado evaluaciones de seguridad del sistema.

En España, están en marcha los siguientes procesos de evaluación de seguridad:

- Bittium Tough Mobile™ C está aprobada como *plataforma de confianza* hasta *Difusión Limitada*.
- Bittium SafeMove® Mobile VPN está en proceso de evaluación para la securización de los datos en tránsito hasta *Difusión Limitada*.
- Bittium Tough Mobile™ R está en proceso de evaluación como *plataforma de confianza* hasta *Difusión Limitada*.



Kiitos paljon
Muchas gracias

www.bittium.com

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional