



--- JIAP 2013 – “Movilidad” ---

**¡ BYOD es inevitable !  
¿Como lo implementamos?**

**jiap**

**Pablo Moreno  
Gerente de Tecnología  
Infoland t&e**

# Propuesta de trabajo

---

## Movilidad +



- Big Data
- Dispositivos Móviles
- Aplicaciones para móviles
- Redes sociales
- Conectividad
- Comunicaciones
- Infraestructura
- Seguridad
- Traiga su propio dispositivo
- Herramientas de desarrollo

**14 al 16 de agosto de 2013**

**Centro de Conferencias de la Intendencia de Montevideo**

Traiga su propio dispositivo (**B**ring **Y**our **O**wn **D**evice) es una tendencia que ha crecido enormemente debido a la abundancia de dispositivos móviles que los usuarios han incorporado a su vida laboral y personal

Esta tendencia se esta viendo también en Uruguay

¿Cómo incorporamos BYOD de la mejor manera?



**Bring your Own Device** (BYOD), en castellano "trae tu propio dispositivo", es una [política empresarial](#) donde los empleados llevan sus propios dispositivos a su lugar de trabajo para tener acceso a recursos de la empresa tales como correos electrónicos, bases de datos y archivos en servidores, así como datos y aplicaciones personales (Wikipedia)

# BYOD

Bring Your Own Device



## ¿Cuál es la tendencia?

### BYOD IS POPULAR – AND GROWING



**38%**

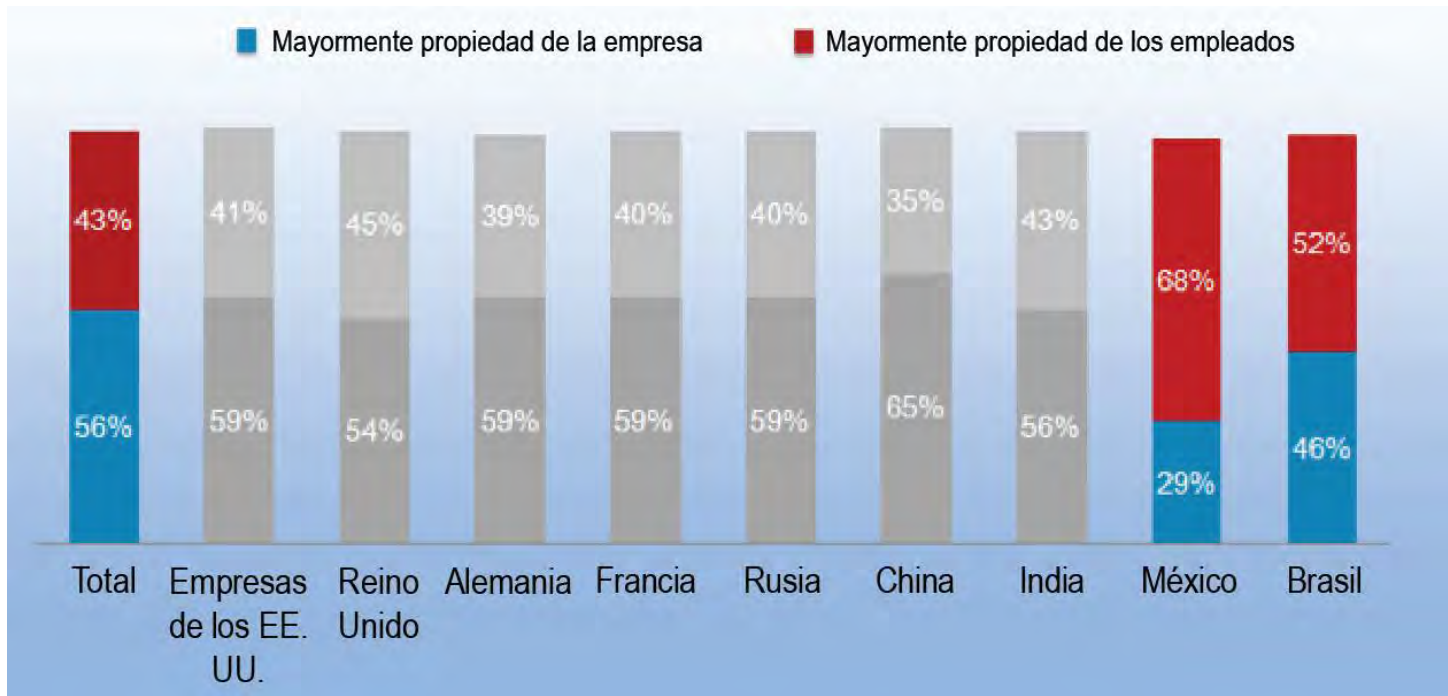
of US CIOs were expected to support BYOD by the end of 2012. <sup>1</sup>

**82%**

of surveyed companies in 2013 allow some or all workers to use employee-owned devices. <sup>2</sup>



# América Latina



Fuente: Cisco IBSG 2012

## En números ....



BYOD está haciendo grandes cambios en el mundo de los negocios ya que alrededor de un 90% de los empleados (en los países desarrollados) utilizan sus equipos de algún modo para acceder a la información de la empresa. **En la mayoría de los casos las empresas no pueden cambiar esta tendencia** (Wikipedia)

El 42% de los smartphones y el 38% de las computadoras portátiles utilizadas en el lugar de trabajo actualmente pertenecen a los empleados (Cisco IBSG)

El 88% de los líderes de TI son “positivos” acerca del efecto que BYOD está teniendo en sus departamentos (Cisco IBSG)

## ¿Qué implica BYOD?

Algunos creen que BYOD ayuda a los empleados a ser más productivos.



Otros creen que eleva la moral de los empleados ya que se permite la flexibilidad dentro de la empresa.

De no implementar controles, esta práctica puede ser muy perjudicial para la empresa ya que puede dejar fisuras donde se puede filtrar la información o entrar aplicaciones malignas a la red

Uno de los inconvenientes más grandes que existen con BYOD consiste en rastrear y controlar acceso a redes privadas y corporativas



# Los desafíos de BYOD

Seguridad

Cultura de trabajo

Nuevas formas de colaborar

Costos a la vista y costos ocultos

Requiere alta capacidad de adaptación

Impacta sobre la infraestructura existente

Inventario y seguimiento de dispositivos

No sabemos donde nos puede llevar



## La estrategia actual ...

Múltiples restricciones por “políticas de empresa”

No lo promuevo, lo implemento si lo piden.

Impulsar “**Comités de estudio del asunto**”

Plan General Maestro de adaptación.... Bla, bla, bla...

Solo a los jefes , gerentes y directores

**Algunos** acuerdos con los empleados

¿Estas estrategias se pueden mantener?



“ Le repito.... ¡ Creo que vamos a tener que volver a hablar sobre estas políticas de BYOD ! ”  
(Trend Micro, Consumerización)

# ¿Qué es lo que pierdo si no manejo correctamente BYOD?



- Su habilidad para manejar el riesgo asociado a la “movilidad” y sus dispositivos
- La capacidad de manejar una infraestructura cada vez mas compleja
- Si se pierde un dispositivo se reemplaza , pero la información queda comprometida.
- La seguridad del acceso externo se compromete por dispositivos que pueden ser alterados
- La visibilidad del uso de estos dispositivos y del cumplimiento de las normas de acceso



# La estrategia futura

Definir y establecer las políticas de BYOD

Adaptar la infraestructura

Ocuparse de BYOD como un tema más

Usar BYOD para beneficiar a la organización

Estar muy atentos a la evolución de BYOD

Para los jefes , gerentes , directores, etc, etc, etc

¿En que productos nos podemos apoyar para implementar todo esto?

# Requisitos para una buena solución

El departamento de IT necesita flexibilidad para definir normativas a partir de múltiples variables, entre otras:

- El **momento** y el **lugar** en que un tipo determinado de dispositivo, por ejemplo, un Smartphone, puede utilizarse.
- Los **recursos** a los que un usuario específico puede acceder a través de ese dispositivo.
- Los **servicios** y **aplicaciones** que pueden ejecutar.
- El **ancho de banda** que un dispositivo o aplicación concretos pueden consumir
- **Visibilidad e informes** sobre los dispositivos propiedad de la empresa y **BYOD tras ser admitidos en la red**.



# Características de un buen producto



Aunque las iniciativas BYOD pueden incluir numerosos aspectos, las organizaciones deben buscar soluciones BYOD que posean las siguientes características

1. Una arquitectura abierta que se pueda implantar en la infraestructura inalámbrica, por cable y remota de **cualquier proveedor**, y ofrecer **compatibilidad con una amplia gama de dispositivos móviles y fijos**.
2. Funciones de provisión de dispositivos que **automaticen** la configuración de las opciones de seguridad y productividad en el dispositivo y proporcionen **servicios de revocación** de fácil uso.
3. Un **sistema de normativas** que garantice la **aplicación coherente** de los privilegios de acceso en función de la confianza, las funciones del usuario y los tipos de dispositivo, a la vez que proporciona evaluación continua del riesgo y recuperación de dispositivos

# Identificar los desafíos de BYOD





## Soluciones actuales

- **MDM – Mobile Device Management** - es un tipo de software que permite asegurar, monitorear y administrar dispositivos móviles sin importar el operador de telefonía o proveedor de servicios
- **NAC - Network Access Control** - es un enfoque de la seguridad en redes de computadoras que intenta unificar la tecnología de seguridad en los equipos finales (tales como antivirus, prevención de intrusión en hosts, informes de vulnerabilidades), usuario o sistema de autenticación y reforzar la seguridad de la red de acceso.
- **MAM - Mobile Application Management (MAM)** - es un conjunto de software y Servicios responsables de provisionar y controlar el acceso a las aplicaciones usadas acorde los requisitos de la empresa, tanto sea en dispositivos propios o BYOD (tabletas, Smartphone, etc)

# La Visión de Aruba Networks

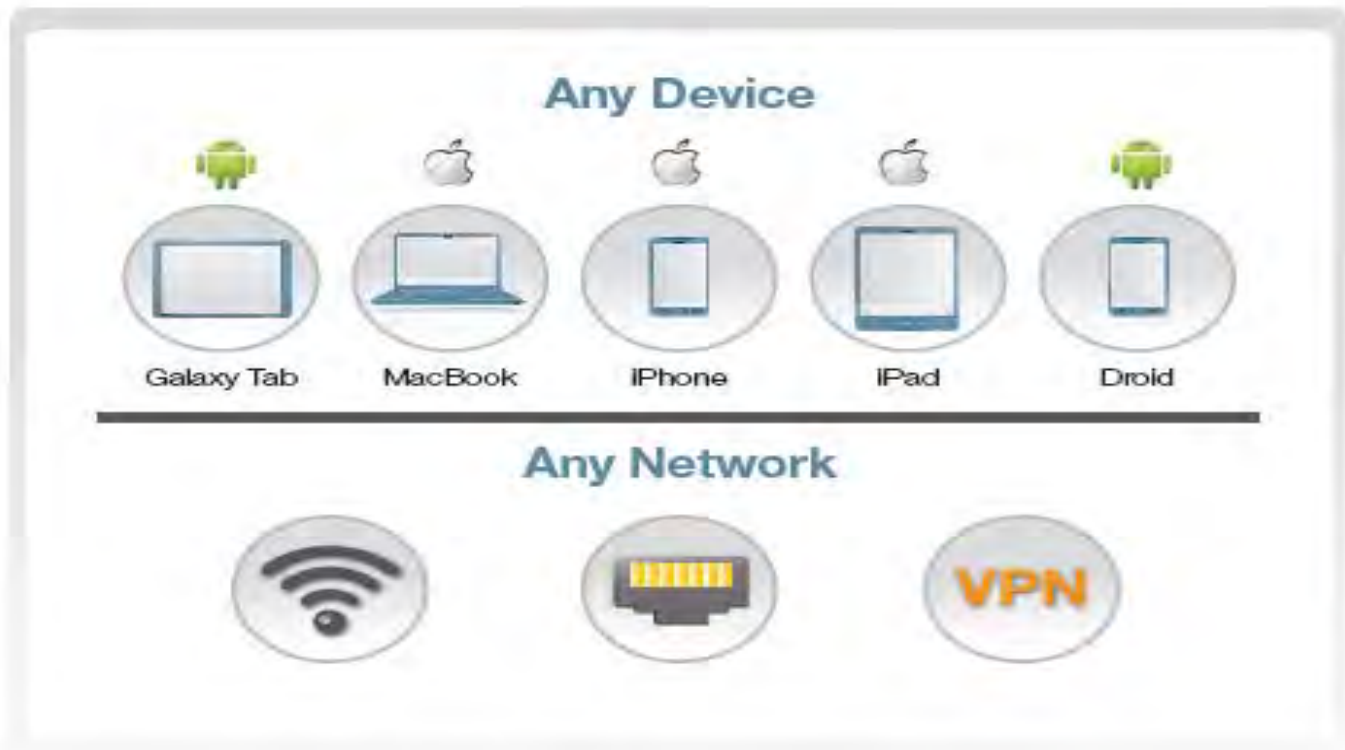


Figure 1: The Aruba BYOD solution

# Aruba ClearPass : un lugar donde manejar BYOD



One place to manage all things BYOD

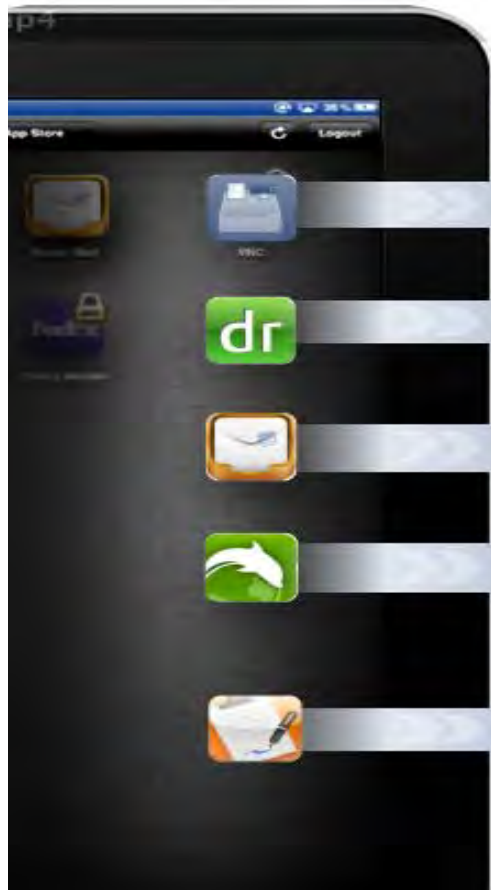


# ClearPass + WorkSpace

Podemos conocer, auditar y controlar



# Control de: Aplicaciones & Datos



## Mobile Context

**TIME-FENCING**



**Point of Sale App:**

Must be used during store hours

**GEO-FENCING**



**EMR Apps:**

Must be used at hospital or member facilities

**MOTION SENSING**



**Email App:**

Can not be used while driving/moving

**CONTENT CONTROL**



**Browser App:**

Can not access torrent sites

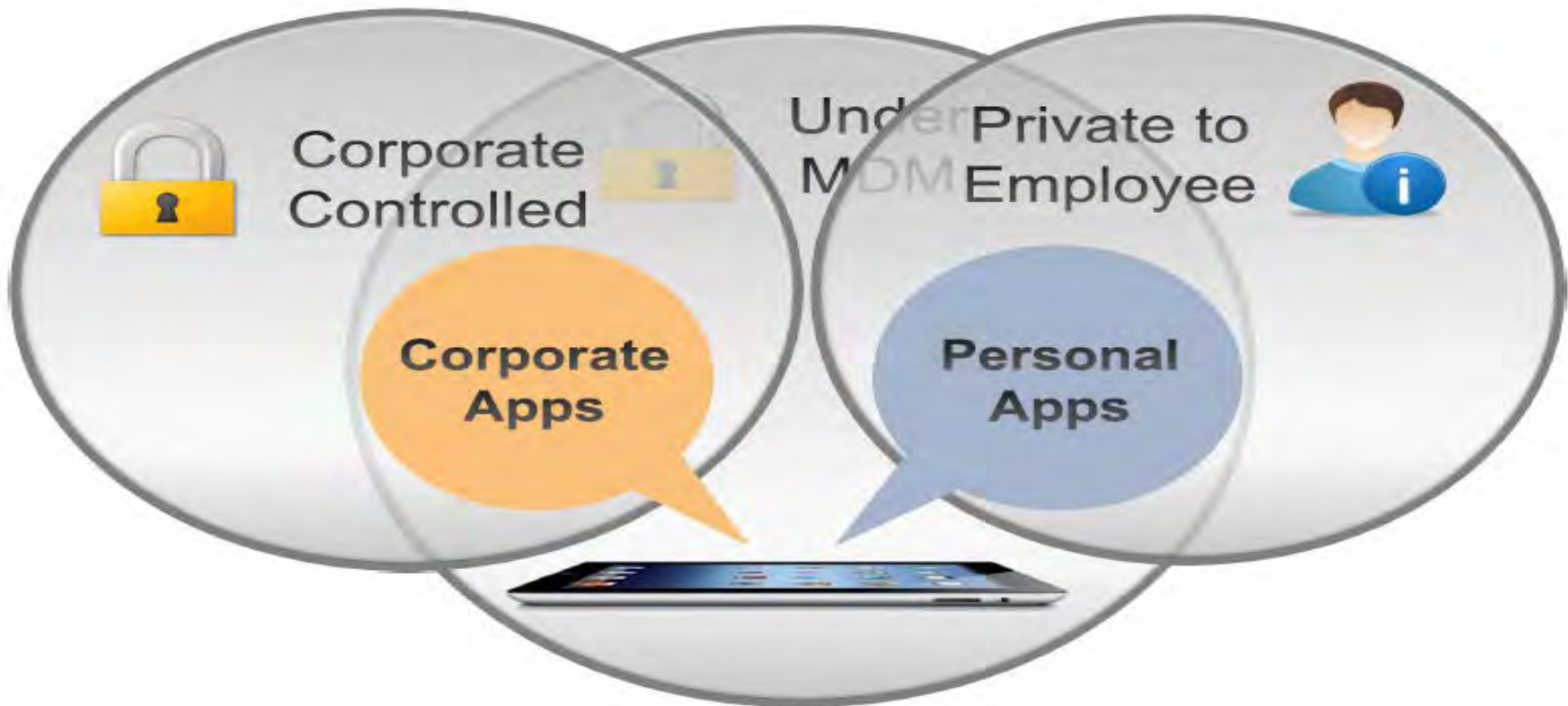
**DEVICE CONTROL**



**Device Status:**

Cut & paste restrictions, Jailbreak / Root detection, Cloud backup

# Control de aplicaciones: Personal o Corporativo



# Programas certificados para trabajar con WorkSpace

**Enterprise Productivity**

iKonic Moxier Touchdown Dictionary CamScanner BizExpense CamCard Breezy YouMail AirDisplay AirLogin AirSharing

**Collaboration**

Xavy – Microsoft Lync Xriz – Asterisk Xvio – Cisco TandbergBM Xime Sametime Dolphin Teambox OpenClove Egnyte Producteev Jive Mobile Zoom Video

**Industry Specific**

Lanschool Eye Chart Pro MobileCare TigerText

**Office Doc Editor**

Cloudon Smart Office 2 Polaris SlideShark PDF Expert Enterprise

**File Access**

Filamente Halosys Averail

**Business Analysis**

Roambi

**File Sharing**

BigTinCan Box Netdocuments YouSendit SugarSync

# Aruba MDM para IOS

**Help organizations reduce the cost and risk of managing corporate-issued mobile devices**



## **Monitor:**

Monitor device inventory  
Audit devices to ensure compliance

## **Control:**

Push apps and security settings  
Over the air remote provisioning

## **Protect:**

Locate, lock and wipe devices  
Passcode enforcement

**\*iOS only in first release**

# Es posible conectarse a un MDM de terceras partes

**ClearPass**



**3<sup>rd</sup> Party MDM**



**Use device inventory and posture from MDM to create network policies in ClearPass.**

**Get full visibility into managed and non-managed devices.**



# Trabaje independiente del tipo de red, desde cualquier lugar



## Network Aware



**Business apps  
given network  
priority over  
personal apps**



**Work  
applications  
automatically  
establish VPNs**

# Una aplicación para “autoservicio” de los empleados

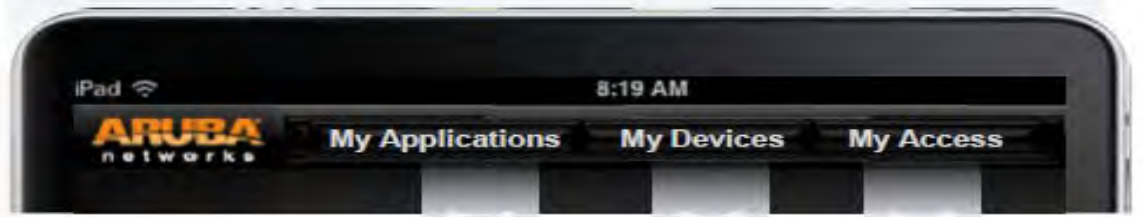
## Personal

- Personalized WorkSpace App provisioned to device



## Corporate

- Employee self-service mobility
- Personalized portal with Single Sign-On



# Acceso simplificado a la red

**Acceso Wi-Fi de invitados:** La definición de usuario invitado es ahora mucho más compleja y puede hacer referencia a desde un empleado con contrato temporal a un comprador en un entorno comercial



Una solución de gestión del acceso BYOD debe proporcionar las mismas opciones a los invitados que a los empleados, incluida la provisión dinámica, la creación de perfiles y la diferenciación de funciones, que se requieren para garantizar el cumplimiento de los requisitos normativos.

## Puntos fuertes de ClearPass + WorkSpace



Aplicación coherente de las normativas a través de redes cableadas, inalámbricas y redes privadas virtuales (VPN) de múltiples proveedores.

Identificación de dispositivos como base para ordenar el tráfico y mejorar la seguridad de la red.

Auto provisión para todos los dispositivos móviles más importantes.

Acceso controlado y recuperación para los dispositivos comprometidos.

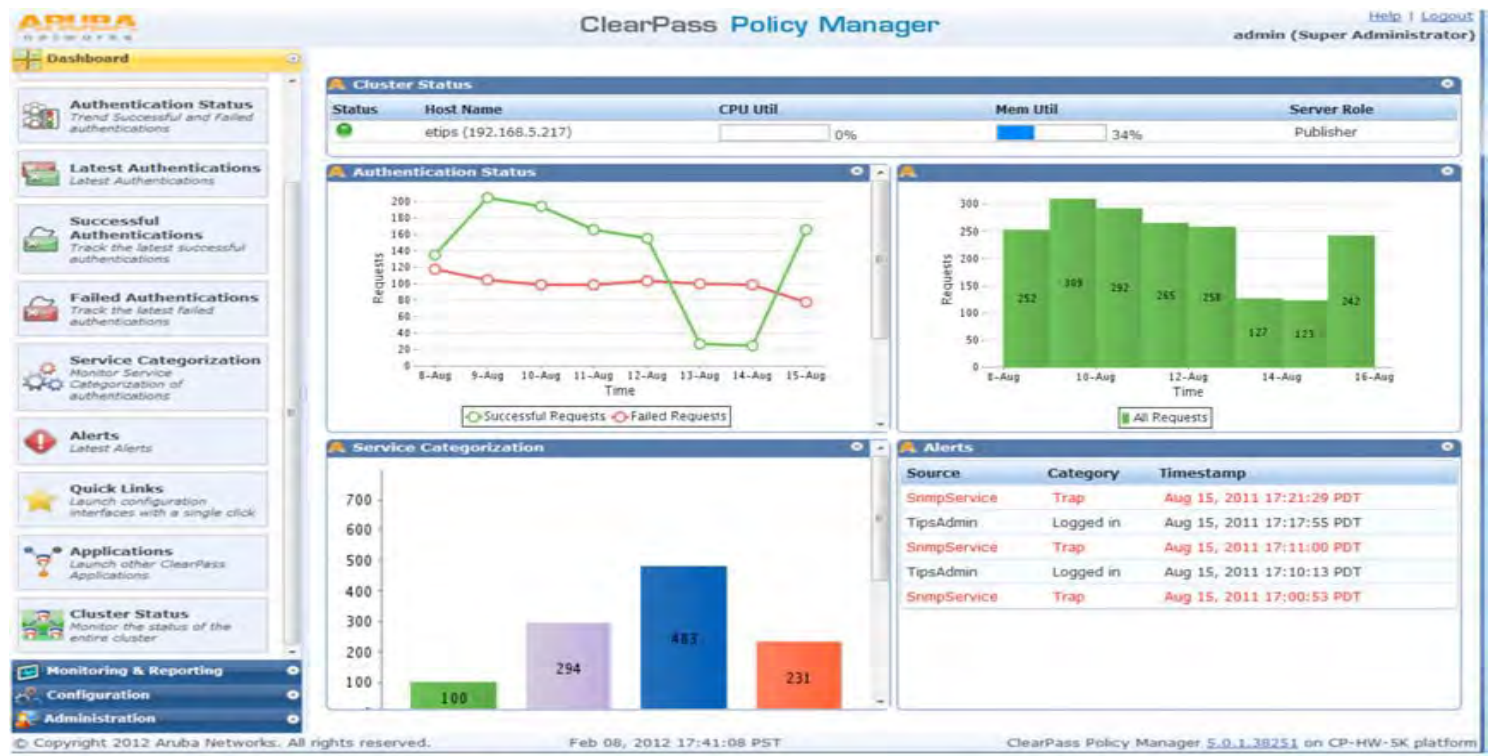
Acceso a la red seguro para invitados con flujos de trabajo simplificados.

Seguridad, información y cumplimiento normativo mejorados

# Esquema de incorporación de dispositivo



# ClearPass Policy Manager



**ARUBA**  
ClearPass Policy Manager

Help | Logout  
admin (Super Administrator)

**Dashboard**

- Authentication Status**  
Trend Successful and Failed authentications
- Latest Authentications**  
Latest Authentications
- Successful Authentications**  
Track the latest successful authentications
- Failed Authentications**  
Track the latest failed authentications
- Service Categorization**  
Monitor Service Categorization of authentications
- Alerts**  
Latest Alerts
- Quick Links**  
Launch configuration interfaces with a single click
- Applications**  
Launch other ClearPass Applications
- Cluster Status**  
Monitor the status of the entire cluster

**Monitoring & Reporting**

**Configuration**

**Administration**


---

**Cluster Status**

Status	Host Name	CPU Util	Mem Util	Server Role
●	etips (192.168.5.217)	0%	34%	Publisher

---

**Authentication Status**




Requests

Time

● Successful Requests ● Failed Requests

---

**Service Categorization**



Requests

---

**Alerts**

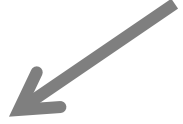
Source	Category	Timestamp
SnmService	Trap	Aug 15, 2011 17:21:29 PDT
TipsAdmin	Logged in	Aug 15, 2011 17:17:55 PDT
SnmService	Trap	Aug 15, 2011 17:11:00 PDT
TipsAdmin	Logged in	Aug 15, 2011 17:10:13 PDT
SnmService	Trap	Aug 15, 2011 17:00:53 PDT

---

© Copyright 2012 Aruba Networks. All rights reserved. Feb 08, 2012 17:41:08 PST ClearPass Policy Manager 5.0.1.38251 on CP-HW-5K platform

# Cumplimiento de políticas multi-marca

## ClearPass Policy Manager



**POLICY ENFORCEMENT**  
Any Network



- Permit
- Deny
- Whitelist
- Blacklist
- Redirect
- Role-based Security
- Bandwidth Mgmt
- Optimize Multimedia

Policy Enforcement Optimized for Aruba,  
But Works with **Any**



# La solución BYOD ClearPass de Aruba



Aruba entiende los desafíos a los que las organizaciones tienen que hacer frente a la hora de implantar una solución de acceso que sea **sólida** pero a la vez lo **suficientemente flexible**.

Aruba ClearPass es una solución BYOD basada en estándares, que proporciona control del acceso como superposición a la red existente de una organización.

Permite aprovechar su infraestructura de red, identidad y seguridad existente y sencillamente activar la función ClearPass cuando la necesita.

Constituye un enfoque muy rentable y flexible que permite a las organizaciones implantar una solución BYOD adaptada a sus necesidades específicas

En resumen...



# Aruba Networks



Aruba Networks es el proveedor líder en soluciones de acceso a las redes Wi-Fi y cableadas de clase empresarial.

La arquitectura Mobile Virtual Enterprise (MOVE) unifica las infraestructuras cableadas e inalámbricas de la red en una solución de acceso unificada

Esta visión unificada de acceso mejora dramáticamente la productividad y minimiza los costos de capital y de operaciones.

Aruba se encuentra en Sunnyvale, California, y tiene operaciones en América, Europa, Medio Oriente, y Asia



# ¿ Gigabit Wi-Fi ? = Aruba Networks

Aruba Networks es el proveedor líder de GIGABIT WI-FI bajo norma 802,11ac



## 802.11ac



**Infoland es Partner certificado de Aruba Networks para Uruguay**

--- JIAP 2013 – “Movilidad” ---



Muchas gracias por  
participar !!!

Pablo Moreno  
Gerente de Tecnología  
Infoland t&e



# Aruba ClearPass + WorkSpace

## Enterprise Mobility Management with NAC, MDM and MAM in one system

### ClearPass Policy Manager 6.2

Integration of application, device and network policies. Secure distribution of apps.



### Aruba WorkSpace Mobile App

The Industry's first self-service portal to integrate network, device and application visibility & control.



### Over 40 Certified Mobile Apps

Extensive list of productivity and collaboration tools.



# ¿Porqué elegir ClearPass + WorkSpace?



## First Integrated BYOD System

- **Simplified BYOD Rollouts:** No need to onboard multiple vendors and integrate multiple systems
- **Faster Service Delivery:** Automated BYOD provisioning across network, device and app
- **Stronger Security:** More options to control BYOD use



## Most Comprehensive Self-Service Portal

- **Personalized BYOD:** Employees get visibility and are empowered to customize their BYOD experience



## Massive Partner Ecosystem

- **Growing 3<sup>rd</sup>-Party ISV Library:** Extensive list of productivity and collaboration tools

# Arquitectura de la solución ClearPass

