



--- JIAP 2014 ---

# Evolución de las redes inalámbricas, BYOD y Cloud managed networking

jiap

Rafael González



ASP  
Accredited Sales Professional  
HP CERTIFIED PROFESSIONAL



infoland  
tecnología & empresas

# Agenda

---

- Evolución de las redes inalámbricas
- BYOD
- Solución meraki 





**infoland**  
tecnología & empresas

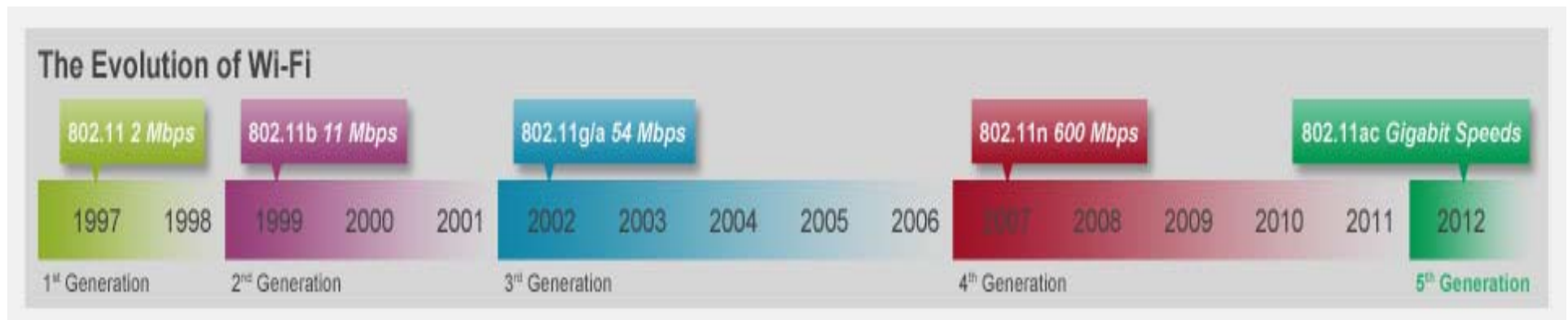
# Evolución de las redes inalámbricas

---



infoland  
tecnología & empresas

# Mayor velocidad





# Seguridad mejorada

---

## 802.11i (WPA2)

- Requires a hardware upgrade
- Uses the new AES cipher
- Provides the final 802.11i standard
- Most products backwards compatible with WPA

## WPA

- Uses today's hardware
- Replaces WEP by using TKIP for encryption
- Incorporates key features of 802.11i
- Includes firmware upgrade

## 802.11+802.1x

- Uses today's hardware
- Adds authentication with software upgrade
- Leverages a RADIUS server with EAP

## 802.11 (WEP)

- Supported by most existing hardware
- Offers sufficient security for home use
- But... can be cracked in under 5 minutes
- Can be augmented with VPN in enterprise and high-traffic environments

Mejores mecanismos de cifrado y autenticación para proteger la integridad, autenticidad y privacidad de los datos.



infoland  
tecnología & empresas

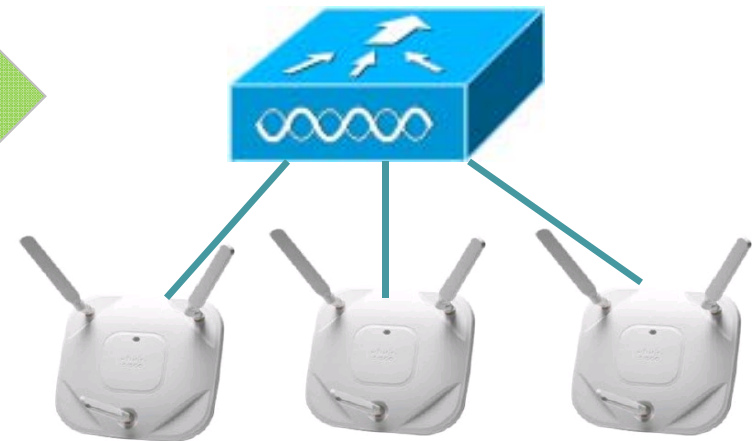
# Arquitectura mejorada

APs AUTÓNOMOS



EVOLUCIÓN

BASADAS EN CONTROLADOR



- Administración centralizada
- Autenticación centralizada
- Manejo inteligente y automático de RF



infoland  
tecnología & empresas

# Conectividad siempre y en cualquier lugar

---

Las redes WiFi están en todos lados: en los hogares, restaurantes, colegios, Shopping centers... y cada vez más en los lugares de trabajo.

Si a esto le sumamos las redes de datos para telefonía celular, tenemos un servicio de cobertura geográfica total y permanente.

# Nuevos dispositivos potentes y altamente portables para los usuarios

---



Smartphones



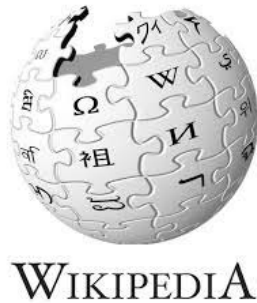
Phablets



Tablets

# Una amplia variedad de nuevas aplicaciones y servicios que han cambiado nuestra manera de manejarnos en la vida

---



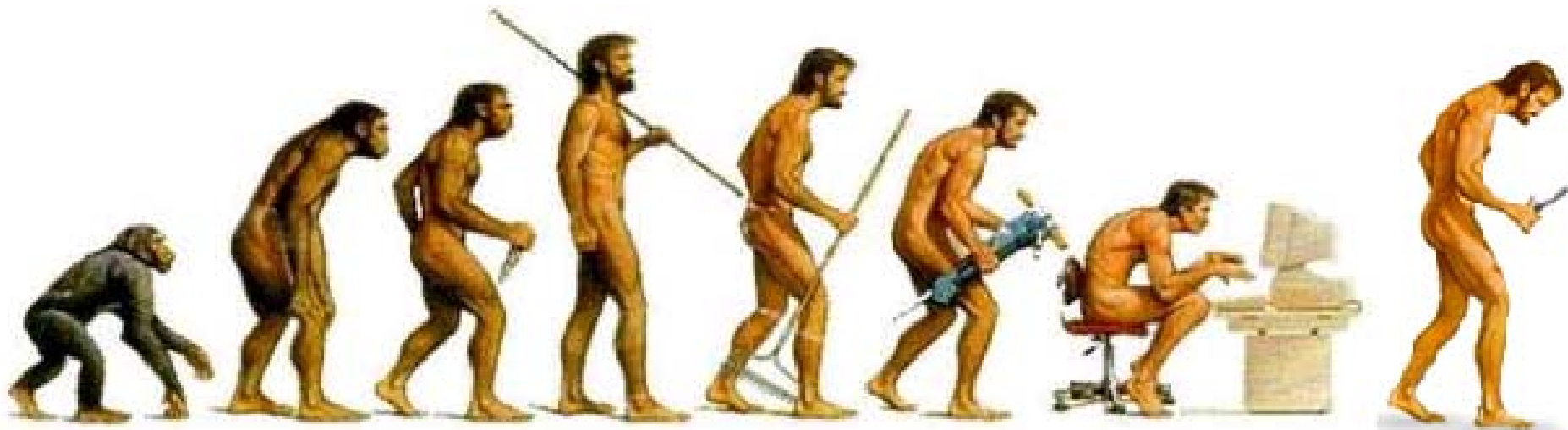
**WhatsApp**



**EASY TAXI**



Todo esto ha generado una necesidad real en los usuarios de estar permanentemente conectados para poder intercalar actividades personales y laborales de manera flexible y en su dispositivo preferido, el cual conocen bien y han personalizado con las Apps que necesitan.





**infoland**  
tecnología & empresas

Lo que nos lleva a  
nuestro próximo tema...





**infoland**  
tecnología & empresas

# BYOD

## Oportunidades y Desafíos

---



## ¿Que es BYOD?

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)



infoland  
tecnología & empresas

## ¿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>



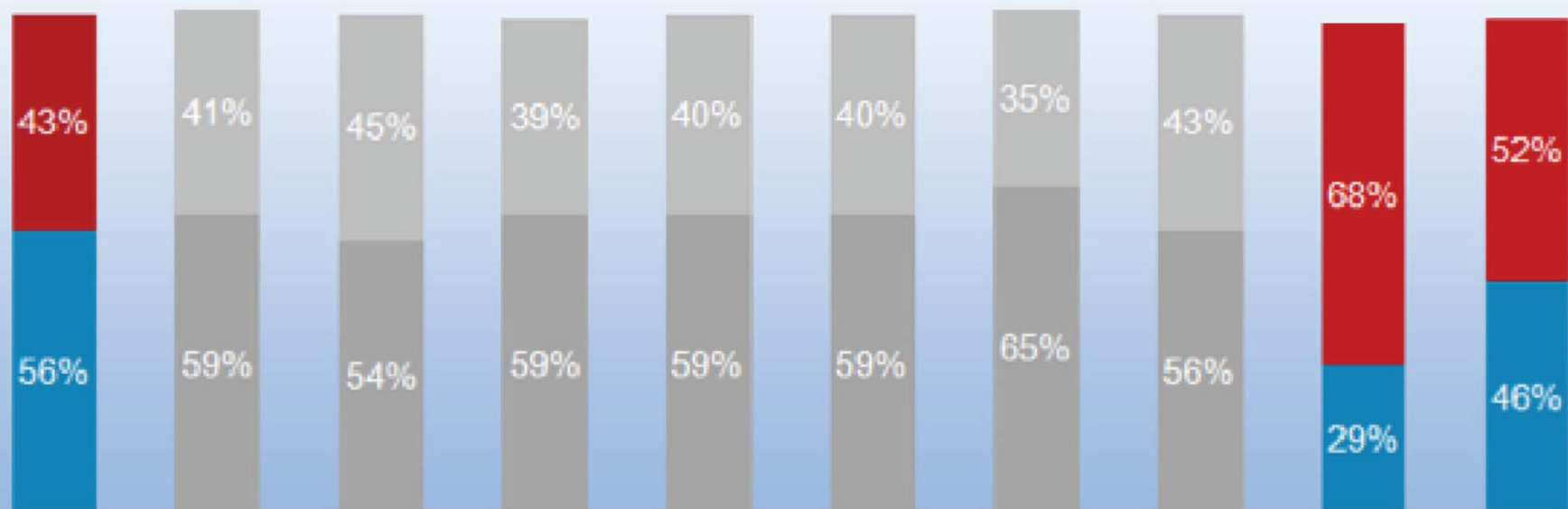


infoland  
tecnología & empresas

# América Latina

■ Mayormente propiedad de la empresa

■ Mayormente propiedad de los empleados



Fuente: Cisco IBSG 2012

Total    Empresas de los EE. UU.    Reino Unido    Alemania    Francia    Rusia    China    India    México    Brasil

# BYOD, más que un problema... es una realidad.

---

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)



infoland  
tecnología & empresas

## ¿Qué ventajas ofrece BYOD?

---

- Algunos creen que BYOD ayuda a los empleados a ser más productivos por usar un dispositivo de su elección, con sistema operativo que conocen bien y sus Apps preferidas instaladas.
- Otros creen que eleva la moral de los empleados ya que se permite la flexibilidad dentro de la empresa.
- Menores costos asociados a la compra de dispositivos móviles para la empresa



infoland  
tecnología & empresas

# ¿Qué desafíos presenta BYOD?

---

- **Afecta la infraestructura de la red**

Aumenta significativamente el número de dispositivos que utilizan la red inalámbrica. **(implementaciones con Access Points domésticos ya no aplican)**

- **Aumenta el consumo de ancho de banda hacia Internet**

Esto se debe al uso de aplicaciones recreativas de video en alta definición , streaming de audio  y file sharing 

Es de vital importancia aplicar restricciones de ancho de banda e incluso bloquear aplicaciones o **esto podría llegar a afectar la performance de las aplicaciones corporativas.**



infoland  
tecnología & empresas

## ¿Qué desafíos presenta BYOD? Cont.

---

- **Afecta la seguridad de la red.**

Es necesario controlar el ingreso a la red y a qué recursos pueden acceder quienes ingresan a la red.

Es necesario controlar **el estado** en que ingresan los dispositivos a la red y si es posible de manera que no agregue una carga permanente de trabajo al departamento técnico.

Y esto implica:

- **Control de la versión del Sistema Operativo**
- **Control de Root o Jailbreak.**
- **Control de existencia y vigencia de un antivirus**
- **Protección de la privacidad y de los datos del usuario.**
- **Posibilidad de hacer PUSH de Apps corporativas.**
- **Backups encriptados y borrado completo o selectivo en caso de extravío del dispositivo o desvinculación del empleado.**



infoland  
tecnología & empresas

# ¿Qué necesito para implementar BYOD responsablemente?

---

- **Dimensionar correctamente el equipamiento de red y el ancho de banda de acceso a internet.**
- **MDM – Mobile Device Management** - es un tipo de software que permite asegurar, monitorear y administrar dispositivos móviles de distintos fabricantes.
- **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 e informes de vulnerabilidades) y sistema de autenticación reforzando 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.



infoland  
tecnología & empresas

¿Qué solución me ofrece todas estas cosas a un precio razonable y sin agregar demasiado trabajo a mi departamento técnico?

---





infoland  
tecnología & empresas

...Veamos la propuesta de **Cisco** con  
su nuevo producto



meraki



infoland  
tec

# ¿Qué es meraki?

Meraki es una línea completa de equipos de networking administrados desde la nube a través de una única interfaz web llamada *Dashboard*.

## Cisco Meraki product families



MR  
Access Points



MS Ethernet  
Switches



MX Security  
Appliances



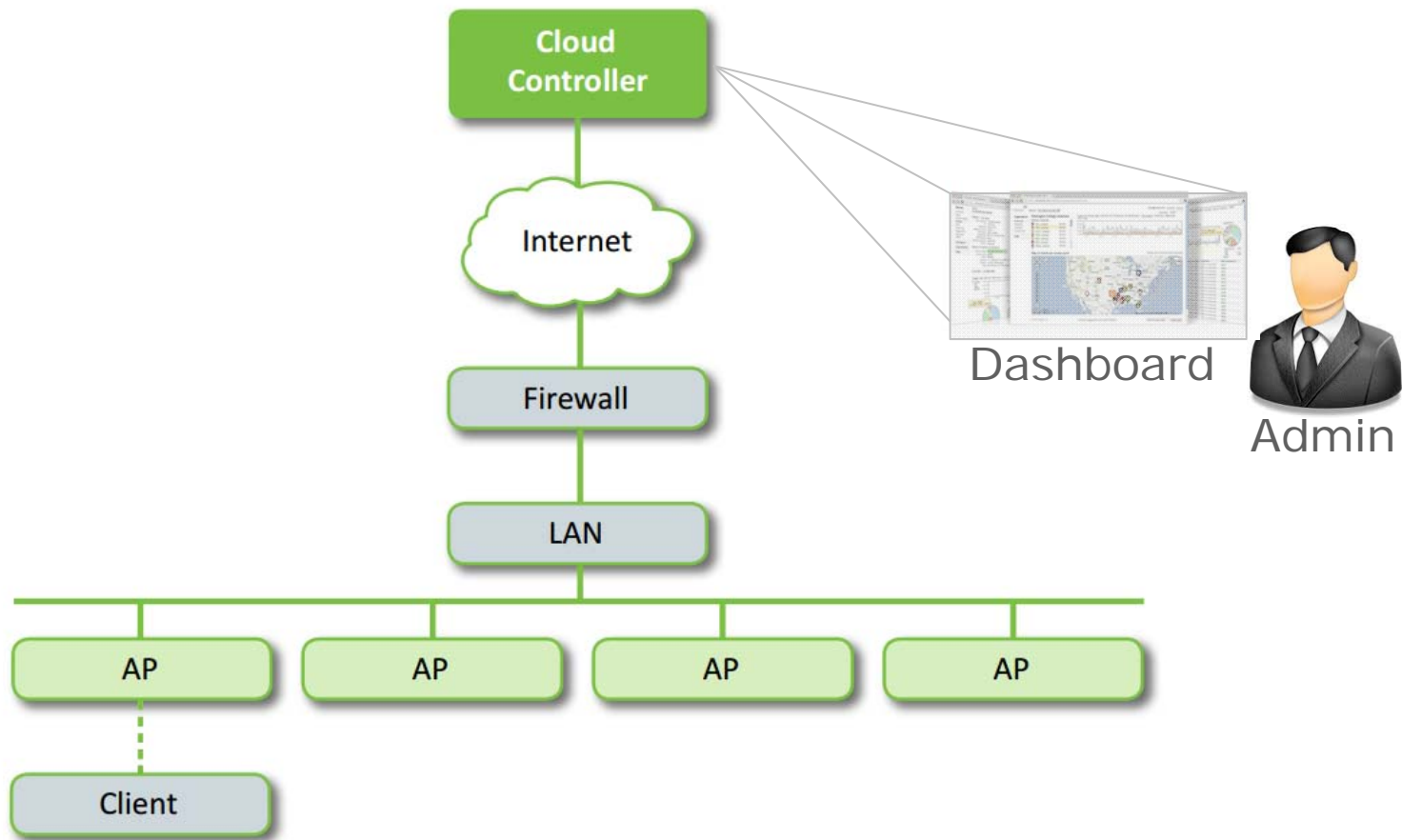
System Manager  
(MDM)





**infoland**  
tecnología & empresas

# Arquitectura meraki





infoland  
tecnología & empresas

# Ventajas de la administración de la red desde la nube

---

- **Es seguro**, meraki utiliza «**out of band management**» que implica que sólo el tráfico de control va hacia la nube, el tráfico de datos jamás va hacia la nube.
- **Accesible** desde cualquier lugar por el administrador, ya que el Dashboard se encuentra en la nube y es una página web en internet.
- **Centraliza la administración** A través del dashboard administramos la red inalámbrica, los switches, los firewalls y todo lo relativo a **BYOD** (incluido **MDM, NAC y MAM**)



infoland  
tecnología & empresas

# Ventajas de la administración de la red desde la nube Cont.

---

- **Elimina la necesidad de tener un Wireless Lan Controller y un software de Monitoreo de red Ej. Cisco Prime.**
- **A prueba de fallos**, es casi imposible que caiga el cloud controller, ya que la nube de Cisco Meraki está sustentada por varios datacenters distribuidos por todo el mundo... lo que si puede caer es tu conexión a internet pero los equipos siguen funcionando con la última configuración recibida.
- **Respaldo de la configuración de toda la red en la nube y actualizaciones de software para los dispositivos de networking automáticas opcionales.**



**infoland**  
tecnología & empresas

# ¿Cómo preparar la red para BYOD según Meraki?

---

- **1) Segmentar la red en SSIDs (la parte wireless), VLANs (la parte cableada) y grupos de usuarios**
- **2) Implementar control de admisión mediante Políticas de autenticación (admite integración con RADIUS y LDAP) e implementar control y aprovisionamiento de los nuevos dispositivos a través de un Splash Portal (MDM MAM)**
- **3) Controlar el acceso a los recursos internos restringir Apps no deseadas y limitar el uso de ancho de banda por SSID, usuario o grupo por medio de políticas.**
- **4) Revisar periódicamente los informes de eventos y estadísticas de uso que ofrece el Cloud Controller a través del Dashboard.**



infoland  
tecnología & empresas

# 1) Segmentar la Red

---

- **Supongamos que decido segmentar mi red inalámbrica en dos SSIDs**
- **SSID «Invitados»:** a los cuales no me interesa chequear nada del estado del dispositivo, no tienen acceso a ningún recurso interno y solo pueden navegar por internet.
- **SSID «Corp»** que es la red para los empleados de la empresa que deben acceder al mail interno y a un fileservidor para trabajar y pueden usar Whatsapp todo el día pero Youtube y Facebook solo en horario del almuerzo.
- No quiero que jamás usen Utorrent ni naveguen en páginas para adultos.



infoland  
tecnología & empresas

## 2,3) Implementar control de admisión y restringir el uso de ancho de banda

---

- **Cuando un dispositivo de un invitado desea entrar a la red «invitados» se encuentra con una policy que lo redirige a un Splash Portal para invitados con el logo de la empresa y debe ingresar una Pre Shared Key**
- *Podría verificarse que el dispositivo no pertenezca a un empleado de la empresa mediante chequeo de existencia de la «App cliente Meraki».*
- **A continuación puede navegar por internet libremente salvo por las siguientes restricciones que se le aplican:**
- **No puede acceder a ningún recurso interno** (*Reglas FW en la policy*)
- **No puede navegar en páginas para adultos ni usar utorrents** (*Reglas Capa 7 en la policy*)
- **Puede usar un ancho de banda máximo de 1Mb/s (limitado por usuario)**



**infoland**  
tecnología & empresas

## 2,3) Implementar control de admisión y restringir el uso de ancho de banda

---

- **En cambio, cuando un miembro de la empresa intenta acceder a la red «CORP» se encuentra con una policy que lo redirige a otro Splash Portal para empleados que:**
  - Chequea la existencia del cliente Systems Manager de Meraki.
  - Si no lo tiene se lo instala
- **Luego se le aplica una Policy que:**
  - Le requiere soportar WPA2 Enterprise y autenticarse contra un servidor RADIUS o LDAP con su usuario y contraseña personal.
  - permite mail interno y acceso al fileservidor con preferencia al resto del tráfico y deniega el resto del tráfico hacia adentro de la red corporativa.
  - Se permite Whatsapp todo el día y Youtube y facebook con una regla por horario de 12:00 a 13:00 limitando el ancho de banda a 1 Mb/s cada una y se deniega el uso de otras Apps que no sean corporativas (incluido Utorrent)
  - A continuación puede navegar por internet libremente salvo por un perfil de navegación que restringe páginas para adultos.

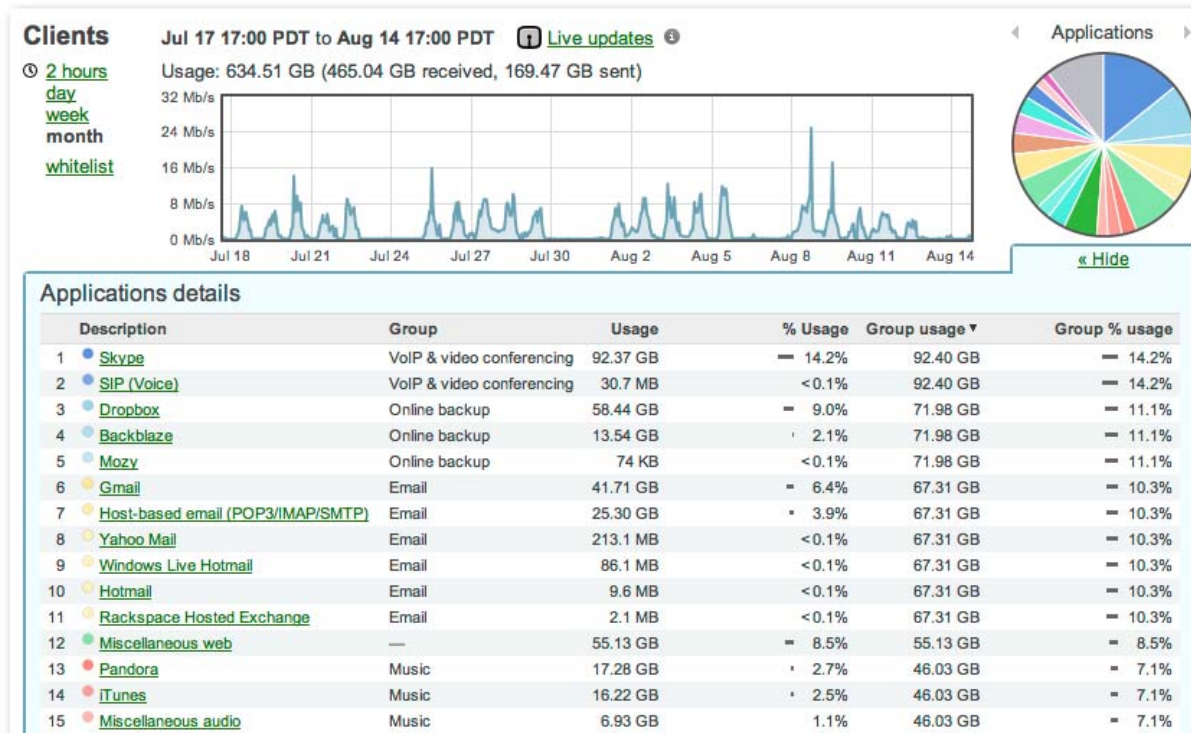


infoland  
tecnología & empresas

## 4) Reportes

- El administrador cuenta con información detallada de uso de ancho de banda por usuario y por aplicación así como notificaciones sobre incidentes.
- Es necesario que los revise periódicamente perfeccionar y ajustar las Políticas en caso que sea necesario.

Screenshots:









infoland  
tecnología & empresas

# ¿Que se puede hacer con el MDM Systems Manager?



- Para que funcione se debe instalar el cliente en el dispositivo del usuario.
- Soporta  Windows  OSX  IOS y  Android
- Permite:
  - Remote Desktop (PC y MAC)
  - Requerir tiempo de bloqueo del equipo y política de cambio de PIN
  - Push de Apps
  - Deshabilitar Apps
  - Enviar mensaje al usuario
  - Backups (cifrado)
  - Borrado del dispositivo (completo o parcial) por robo o desvinculación
  - Localización del dispositivo por GPS o WIFI



infoland  
tecnología & empresas

# Imágenes del Dashboard

## Visibilidad Multisite

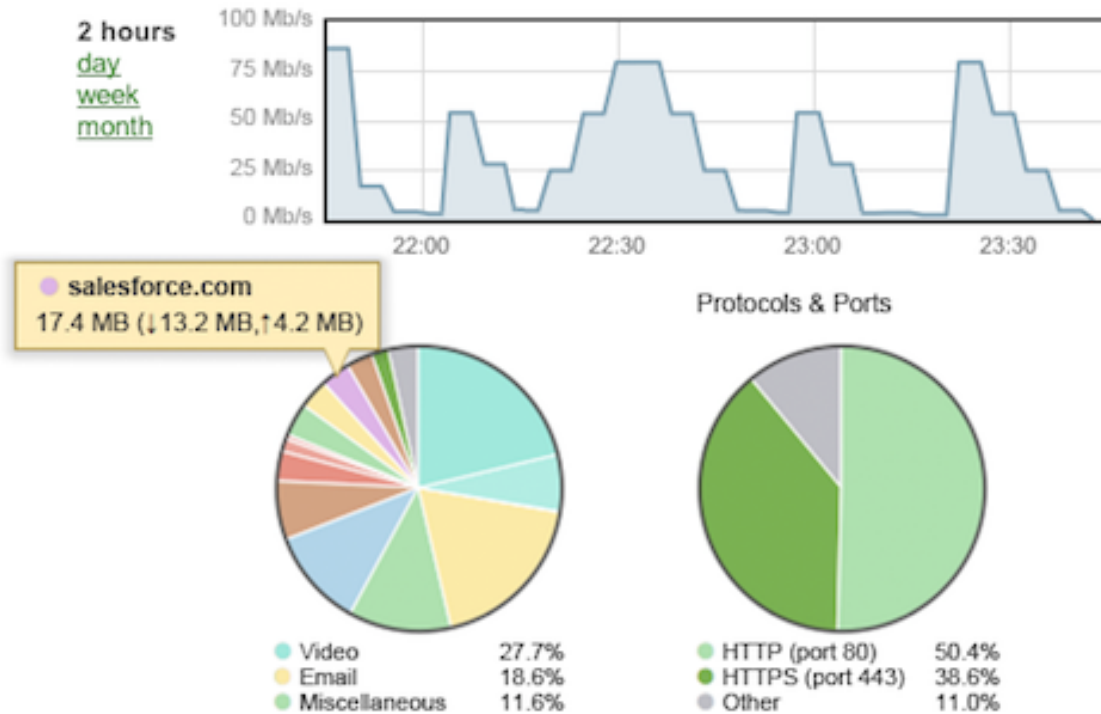




infoland  
tecnología & empresas

# Imágenes del Dashboard

## Gráficas detalladas





infoland  
tecnología & empresas

# Imágenes del Dashboard

## Interfaz de administración intuitiva

The screenshot shows the Meraki dashboard configuration overview page. The browser address bar displays <https://n7.meraki.com/Meraki-Corp/n/Ykbfghd/manage/configure/overview>. The user is logged in as [katie.lane@meraki.com](#) with links for [my profile](#), [sign out](#), [demo networks](#), and [show admin](#). The network is set to "Meraki Corp".

The left sidebar contains navigation options: Network-wide, Security appliance, Switch, **Wireless**, Organization, and Help.

The main content area is titled "Configuration overview" and shows "SSIDs" for the selected network. It displays a table with 4 columns: Meraki-Corp, Meraki-Engineering, Meraki-Guest, and Ekahau. The table lists various configuration settings such as Enabled status, Name, Encryption, Sign-on method, Bandwidth limit, Client IP assignment, Clients blocked from using LAN, Wired clients are part of Wi-Fi network, VLAN tag, VPN, Splash page enabled, and Splash theme.

	Meraki-Corp	Meraki-Engineering	Meraki-Guest	Ekahau
Enabled	<input type="button" value="enabled"/>	<input type="button" value="enabled"/>	<input type="button" value="enabled"/>	<input type="button" value="disabled"/>
Name	<a href="#">rename</a>	<a href="#">rename</a>	<a href="#">rename</a>	<a href="#">rename</a>
<b>Access control</b>				
Encryption	802.1X with custom RADIUS	802.1X with Meraki RADIUS	Open	WPA2-PSK
Sign-on method	None	None	Click-through splash page	None
Bandwidth limit	unlimited	unlimited	unlimited	unlimited
Client IP assignment	Local LAN	Layer3 Roaming	Layer3 Roaming	Local LAN
Clients blocked from using LAN	n/a	no	yes	n/a
Wired clients are part of Wi-Fi network	no	no	no	no
VLAN tag	110	n/a	n/a	n/a
VPN	Disabled	Tunnel to "Engineering - MX"	Tunnel to "Meraki Corp Guest - MX100"	Disabled
<b>Splash page</b>				
Splash page enabled	no	no	yes	no
Splash theme	grumpy_cat	Fluid	Copy of Fluid	n/a

At the bottom of the table, there are "Save Changes" and "cancel" buttons, followed by the note: "(Please allow 1-2 minutes for changes to take effect.)"

The footer contains copyright information: © 2014 Cisco Systems, Inc. with links for [privacy](#) and [terms](#). It also shows session information: "Last login: about 19 hours ago from your current IP address.", "Current session started: 39 minutes ago", and "Session has roamed to 3 shards: 1, 4, 7". There are also input fields for "I wish this page would..." and "make a wish".



**infoland**  
tecnología & empresas

**Muchas Gracias!!!!**

---