



"There is nothing more important than our customers"



BYOD, HECHO CORRECTAMENTE

Jorge Villarreal
Post Sales Service Manager
Enterasys México &NOLA

A Siemens Enterprise Communications Company

26 Febrero, 2013

- **¿Qué es BYOD?**
- **¿Cuál es la importancia de BYOD?**
- **Tendencias de BYOD en México**
- **Mercado para BYOD**
- **¿Como se hace BYOD correctamente?**

- **BYOD es el nombre que se le ha dado a la tendencia mundial en la que los empleados, alumnos, visitantes, proveedores o cualquier otro tipo de usuario que se conecte a una red lo hagan con un dispositivo propio, en lugar de uno provisto por la misma empresa o controlado por el área de IT de la misma.**
- **BYOD ha existido desde hace mucho tiempo, sobre todo en las Universidades pero ahora con la proliferación de nuevos dispositivos como PDA's, Smart Phones, Tablets, Lap Tops, Unidades de Juegos, etc. su rol toma mayor importancia.**



- Esta misma tendencia ha llegado a las empresas y cada vez hay mas usuarios con mas dispositivos esperando poder hacer su trabajo de una forma mas móvil y con el dispositivo de su elección.



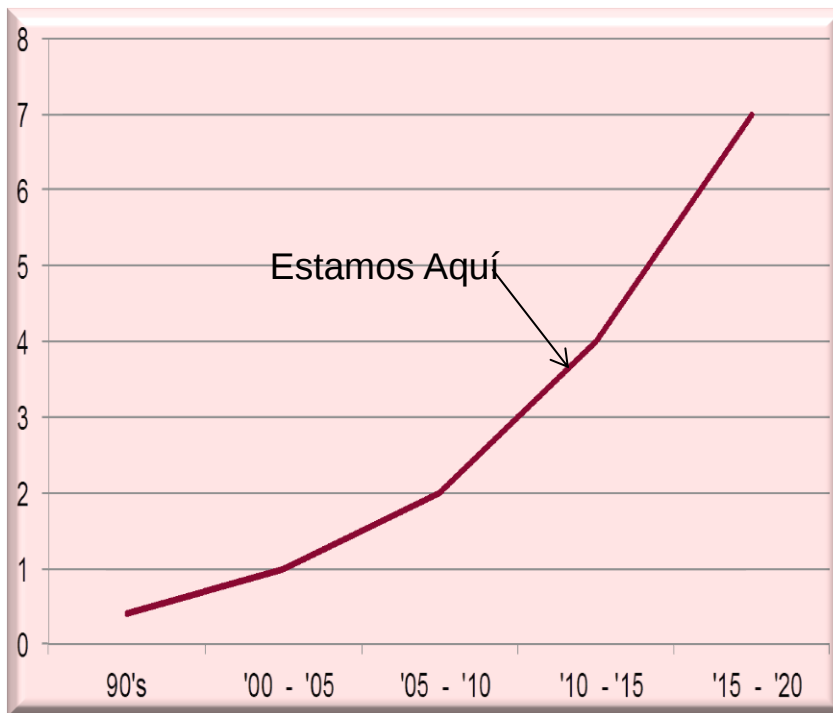
- **Reducción de Costos para la Universidad, al proveer acceso a aplicaciones internas y servicios externos como Internet, sin la inversión directa en hardware o software en equipos para usuarios finales**
- **Diferenciador para potenciar el incremento de matrícula**
- **Potencia nuevos estilos de enseñanza y aprendizaje:**
 - Educación a distancia
 - Aulas globales / Campus Remotos
 - VDI (Infraestructura virtual de escritorios)



- Me gusta mi dispositivo móvil y me gusta trabajar con el
- El reto de ofrecer una red BYOD es cuando en los dispositivos propietarios se pretende tener acceso a datos o aplicaciones de negocio que puedan incrementar los riesgos de seguridad, confidencialidad o continuidad de negocio.



- En los siguientes 4 años el mercado de wireless va a duplicarse, 81% de los empleados llevaran consigo al menos un dispositivo personal para hacer negocio y el 90% de las empresas no están totalmente conscientes de los dispositivos que acceden sus redes.

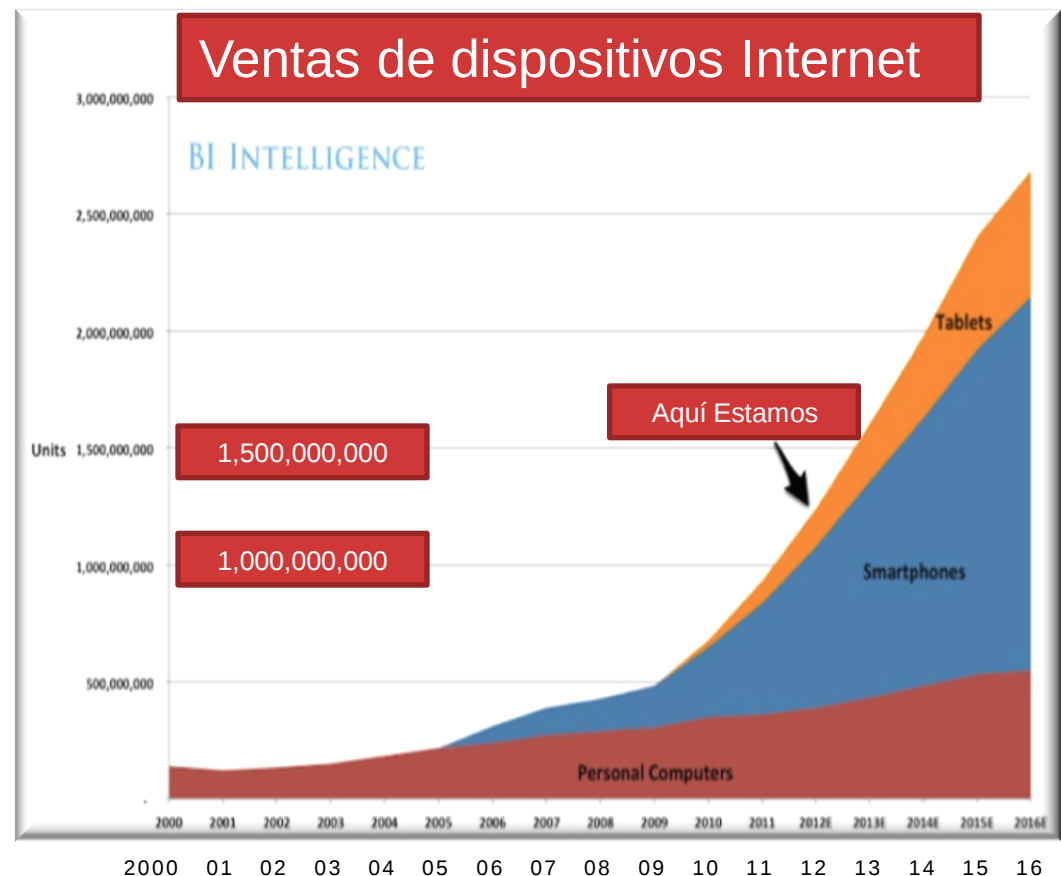


Número promedio de dispositivos propiedad de un solo usuario: 3



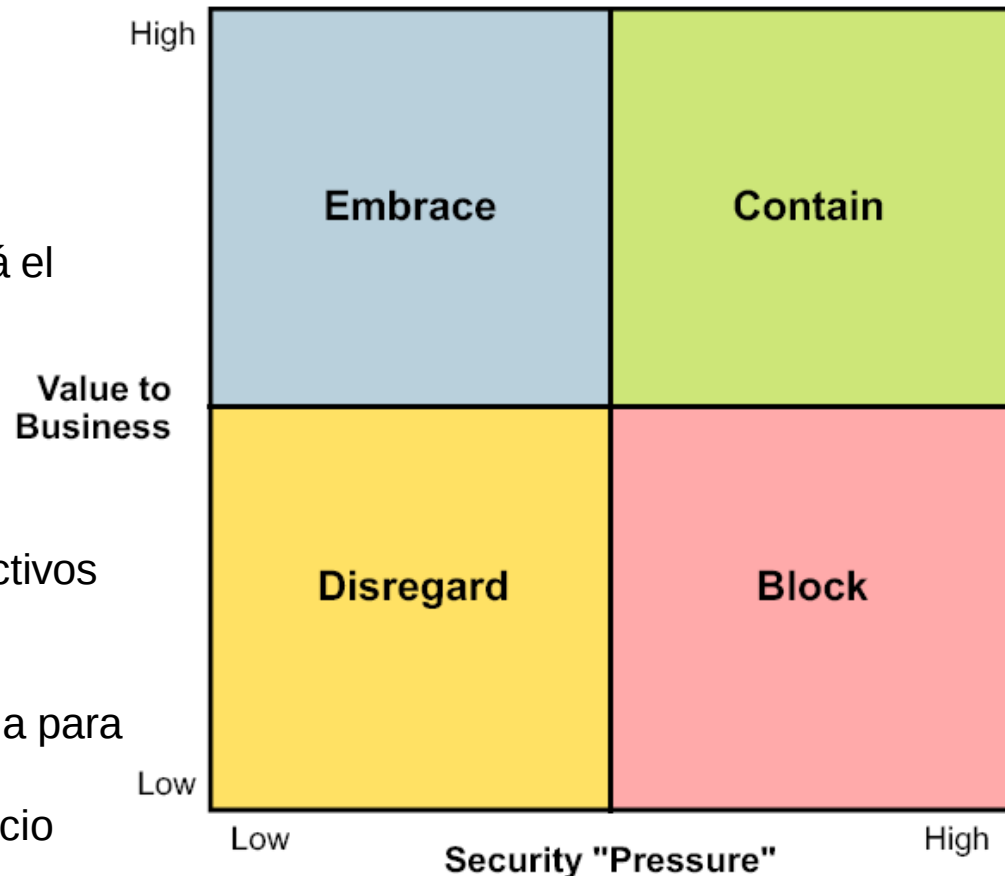
- Bajo este panorama, la industria pronostica que para 2013 las ventas asociadas a BYOD por lo menos se triplicaran.

El uso de estos dispositivos para acceder a la red empresarial/Campus continuará creciendo

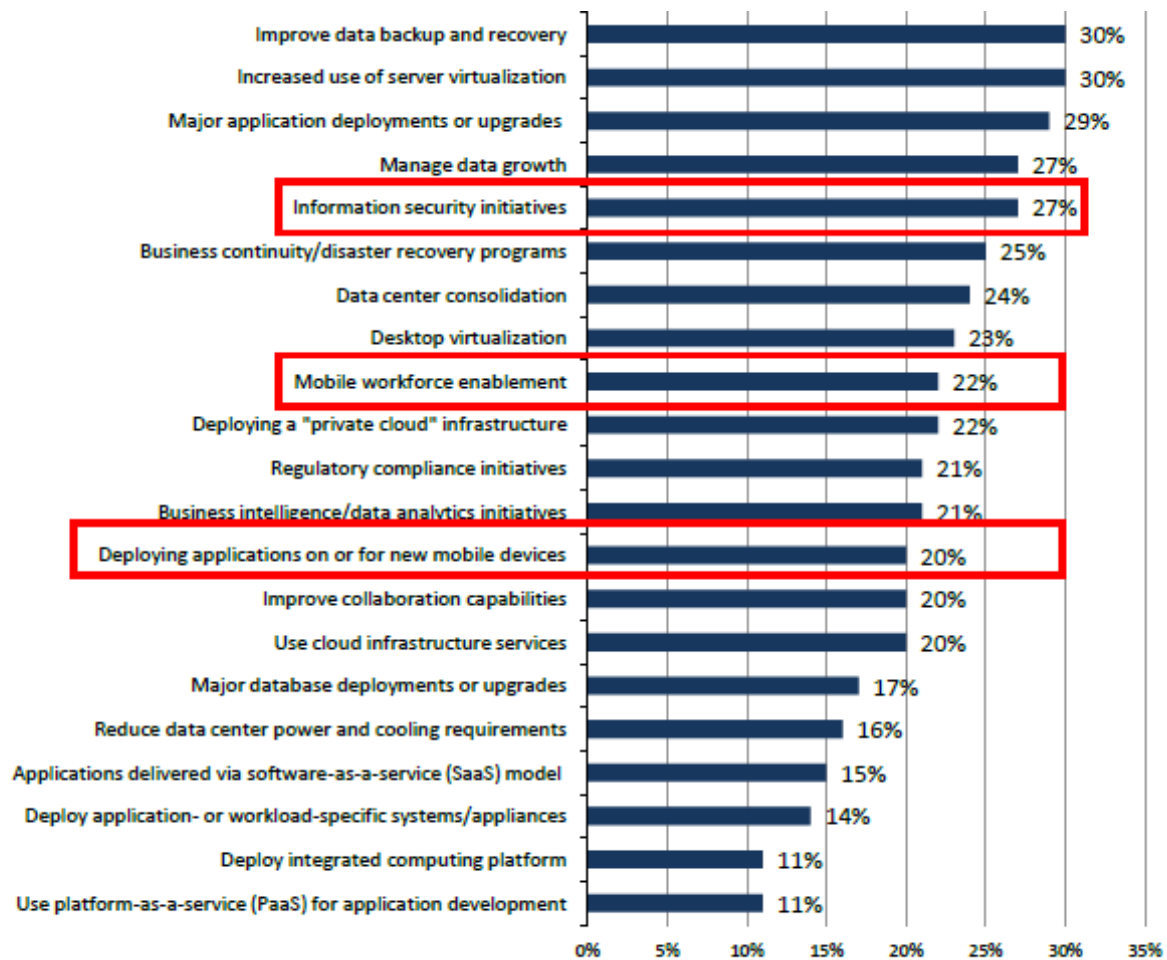


■ Gartner - Balanceando riesgo y valor de negocio

1. Desestimar BYOD
 - Casi imposible
2. Bloquear BYOD
 - Esto reducirá el riesgo pero limitará el potencial del negocio
3. Contener BYOD
 - Posiblemente el primer pasos para muchos campus
 - Aislar de BYOD ciertos servicios/activos
4. Ceñirse a BYOD
 - Implementar la tecnología necesaria para administrar el riesgo
 - Alcanzar el potencial total del negocio

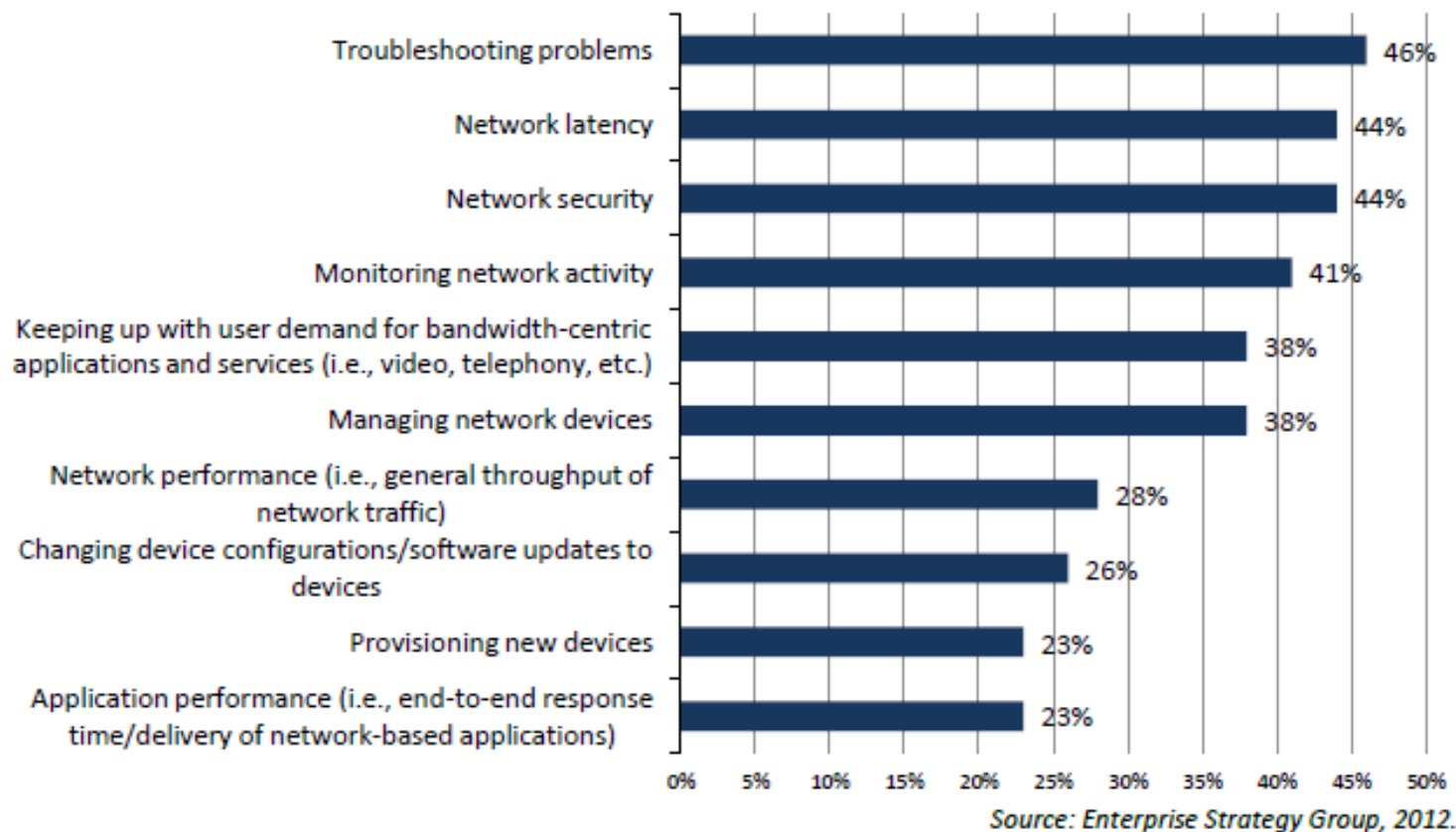


■ Prioridades de TI más importantes en el campus universitario



Source: Enterprise Strategy Group, 2012.

■ Retos más grandes de red en el campus universitario



- Una solución BYOD “Bien Hecha”, cubre BYOD tanto las redes inalámbricas como alámbricas haciéndolas funcionar como una sola red independiente del medio físico
- Lo haríamos sin segmentar la red y analizando hasta 50 atributos para definir una postura de conexión y de seguridad, dentro de los mas importantes están:
Autenticación del usuario, tipo de dispositivo, sistema operativo, lugar y hora de conexión.
- Tradicionalmente la segmentación ha sido la manera de proteger la red y diferenciar los accesos y privilegios por grupos de usuarios y dispositivos, iríamos mucho más allá de esta manera tradicional y limitada de dar acceso y seguridad por grupos
- No nos limitaríamos a que los dispositivos de red sean de una sola marca, a que BYOD sea aplicada únicamente en las redes inalámbricas o a que se haga por Vlan o SSID, podríamos implantar una solución BYOD para cada necesidad.



Política BYOD

- **Responsabilidades del usuario**
- **Responsabilidades de soporte de TI**
- **Política de configuración segura**
 - Controles de acceso
 - Acceso WiFi
 - Acceso a información personal
 - Detección y prevención de fugas de información
 - Respaldo y recuperación



BYOD otros requerimientos

■ Registro de acceso

- Portal de auto servicio con acceso a herramientas, formas de servicio y aceptación de política de uso de la red

■ Regulación de acceso a WiFi

- Reglas y políticas en torno a los recursos permitidos y el acceso a internet

■ Política Técnica

- Segregación de datos y tecnología aprobada



Controles de Seguridad

- **Control de Acceso básico**
 - Passwords fuertes y “security type”
 - Encriptación & autenticación
 - Políticas en el acceso
- **Controles de acceso a aplicaciones Web**
- **Correo electrónico**
- **Filtrado Web**
- **Acceso a recursos internos por WiFi**
 - Basados en localización, dispositivos, usuarios



Segmentación de información

- **Proveer políticas explícitas en relación al acceso de información personal**
 - Monitorear aplicaciones instaladas
 - Distribución de aplicaciones
 - Valuación de postura de seguridad



Cumplimiento y reporte

- Estado de dispositivos y que controles de seguridad han sido aplicados
- Intentos de acceso despues que a un dispositivo le ha sido negado el acceso a la red
- Detección de fugas de información
 - Malware
 - Correo electrónico
- Administración de parches
- Dispositivos no soportados







iiii Mil Gracias !!!!



Visit us at: www.enterasys.com

A Siemens Enterprise Communications Company