BASE4 SECURITY
your information partner

El Impacto de los Dispositivos Particulares en la Infraestructura Tecnológica

Agenda

- La Era PC/Web
- La Era Post PC
- BYOD “Bring Your Own Device”
- Estadísticas BYOD
- Lado A: Ventajas de BYOD
- Adopción de BYOD
- Lado B: Desventajas de BYOD
- Problemática actual de BYOD
- Desafíos de BYOD
- Solución a BYOD

La Era PC/Web

ANTES DE 2005

- ➔ Empresas más equipadas (tecnológicamente) que empleados.
- ➔ Personas **sin** PC en su **casa**
- ➔ Personas **con** PC en su **trabajo**
- ➔ Teléfono móvil o PDA sólo para grandes puestos.

La Era Post PC

2005 ~ 2008

EMPRESAS → DISPOSITIVOS

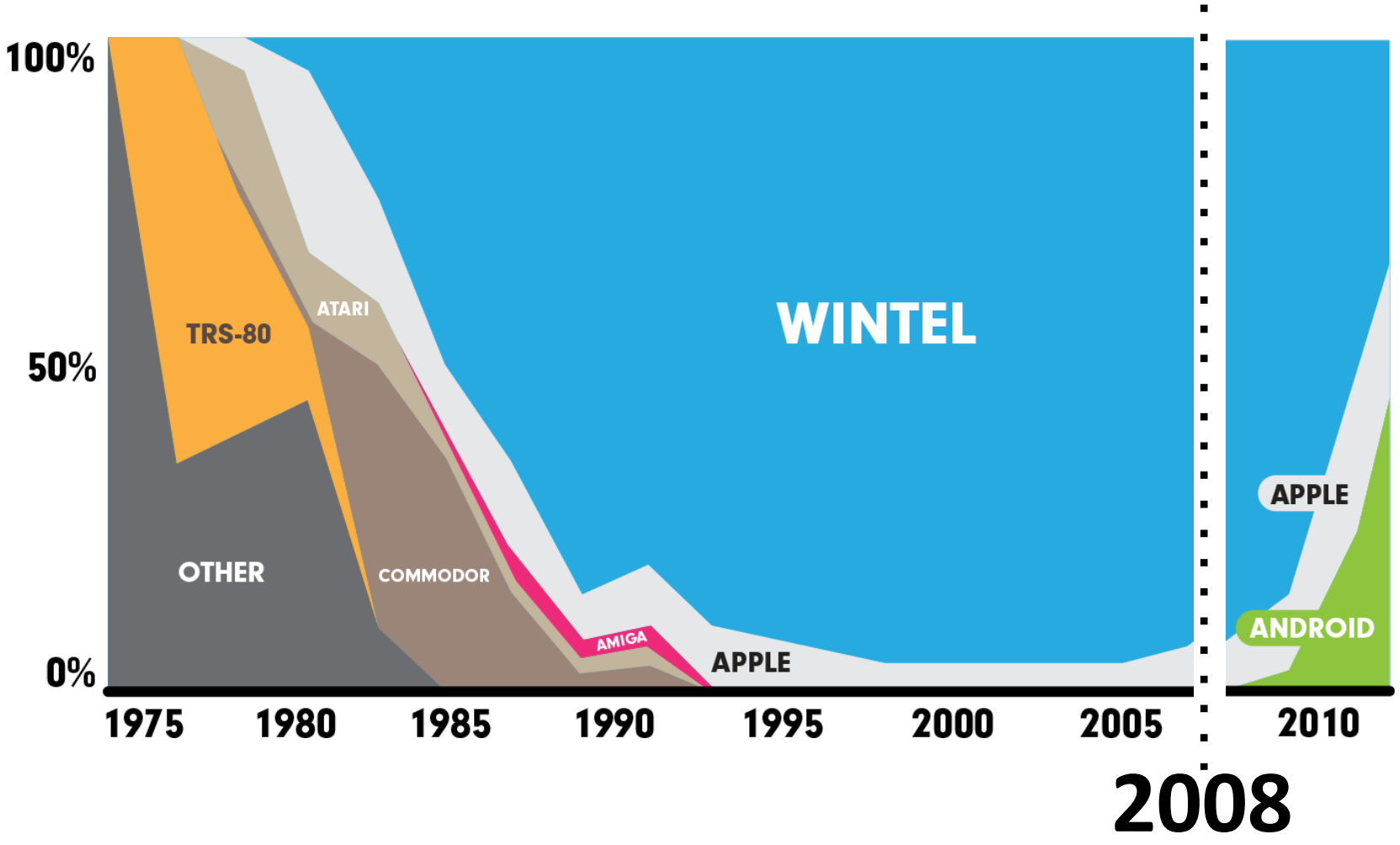
DISPOSITIVOS EMPRESA

- ➔ Smartphones, netbooks, notebooks, etc.
- ➔ Compra o Leasing = Costo financiero
- ➔ Gastos Licencias, Software, Seguro de Robo, Hurto, Desapariciones, Deterioro y Obsolecencia
- ➔ Infraestructura = Costo + Retorno Inversión

EMPIEZAN LOS PROBLEMAS…

- → Empresa afronta costo de reposición
- → Tiempo de reemplazo = Pérdida de tiempo
- → 1 Empleado comienza a tener **n** dispositivos
- → Adquirir nuevos dispositivos requiere un proceso largo
- → Empleados tienen gustos y comodidades diferentes

LA ERA POST PC



Equipos Con:		Equipos Con:
Más Tecnología		Menos Tecnología
Más Prestaciones		Menos Prestaciones
Más Productivos		Menos Productivos
Mayor Rotación		Menor Rotación
Más Eficaces		Menos Eficaces
Más equipos encima		
Preferencias de dispositivos		Poca variedad de dispositivos

BYOD

Bring Your Own Device

BYOD (Trae Tu Propio Dispositivo)

AVANCE TECNOLÓGICO → TECNOLOGÍA MÁS BARATA → EMPLEADOS CON DISPOSITIVOS PROPIOS

BENEFICIOS DE DISPOSITIVOS DE EMPLEADOS

+ Cantidad
+ Tecnología
+ Productivos
+ Eficaces

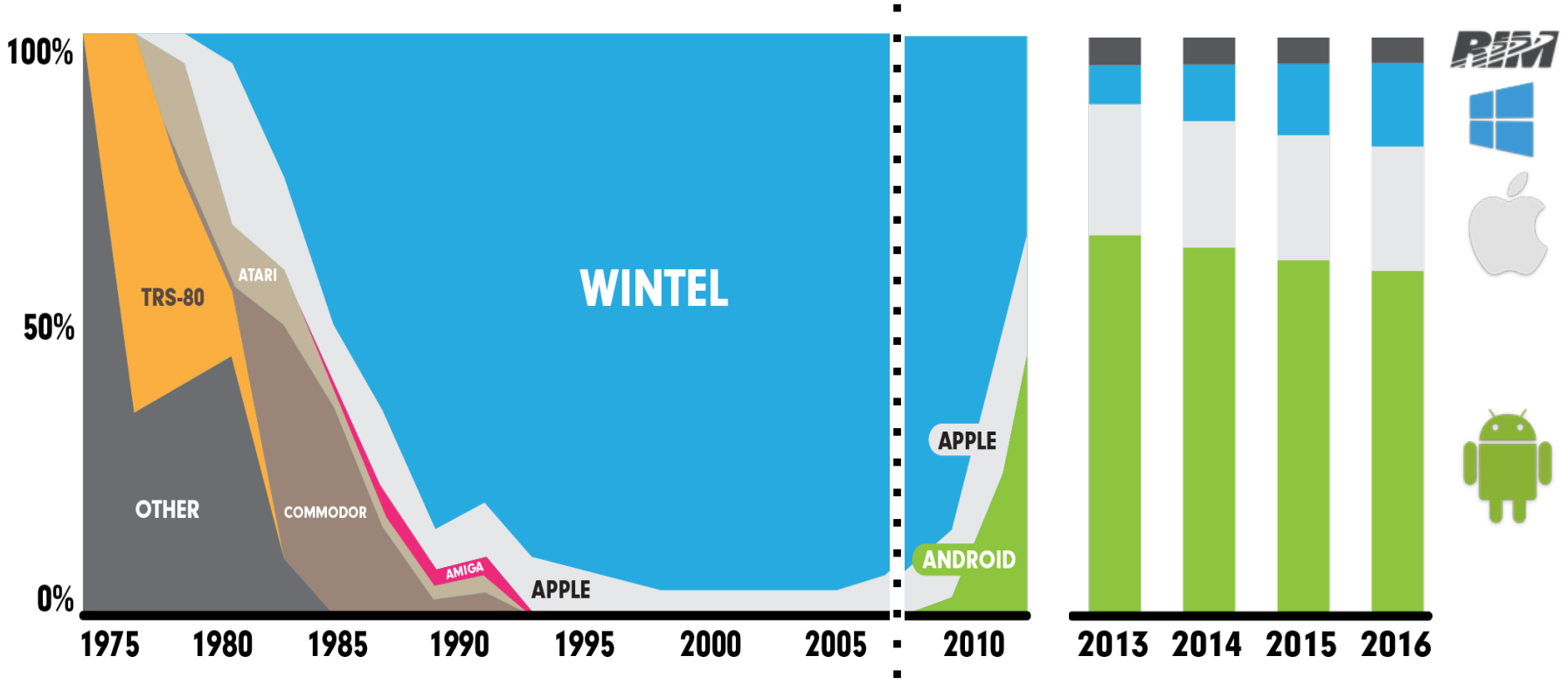
Bring your Own Device (BYOD)

Trae Tu Propio Dispositivo

EMPRESAS ← DISPOSITIVOS

DESPUÉS 2008

BYOD (Trae Tu Propio Dispositivo)



2008

Bring your Own Device (BYOD)

Trae Tu Propio Dispositivo

- Empleados llevan sus propios dispositivos al trabajo
- 90% (en países desarrollados) utilizan **sus propios equipos** para acceder a recursos empresariales:
  - Correos Electrónicos
  - Bases de Datos
  - Archivos en servidores
  - Datos y aplicaciones personales

Grandes Empresas → Medianas Empresas

Estadísticas BYOD

- → El Grupo de Soluciones Empresariales para Internet (IBSG, Internet Business Solutions Group) de Cisco, elaboró la **encuesta "BYOD: una perspectiva global"**
- → Participaron 5.000 personas en puestos de toma de decisiones en los departamentos de TI
- → Empresas ubicadas en ocho países (Estados Unidos, Brasil, México, China, India, Reino Unido, Francia, Alemania y Rusia) de tres regiones (América, Asia y Europa).

ESTADÍSTICAS DE BYOD

- → El 81% de las personas laboralmente activas en el mundo utilizan algún tipo de dispositivo personal en el trabajo
- → El 69% considera BYOD de mediana a extremadamente positivo.
- → El 62% de los jefes de TI cree que se almacena información de la empresa en dispositivos particulares y casi la mitad (49%) sospecha que la información podría ser confidencial.
- → Para el 2014, la cantidad promedio de dispositivos conectados por cada trabajador alcanzará el 3,3.

LADO A
Ventajas de BYOD

Trabajadores más cómodos con sus aplicaciones y dispositivos elegidos personalmente

→ Mayor rendimiento

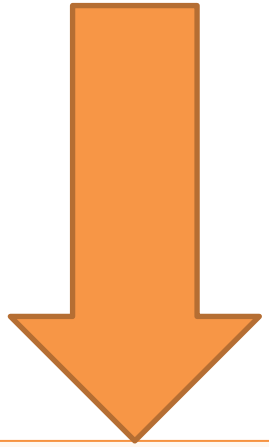
↓ Mejor calidad en la colaboración con los compañeros

↓

Incrementa la productividad de los empleados

Trabajadores con mismos dispositivos en el día a día

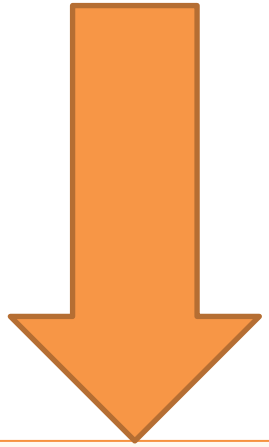
Empleados Más Contentos



Mayor satisfacción de los empleados

Trabajadores pagan completa o parcialmente sus terminales móviles

Posibilidad de utilizar software gratuito



Ahorro de costos en adquisición de tecnología

Trabajadores con dispositivo en constante tenencia

Trabajadores eligen momento y lugar para realizar sus tareas

Mejor atención al cliente

Flexibilidad laboral

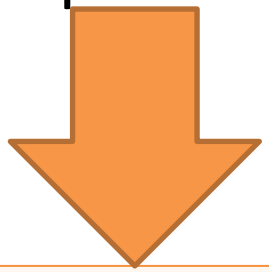
- → Incrementa la productividad de los empleados
- → Mayor satisfacción de los empleados
- → Ahorro de costos en adquisición de tecnología
- → Flexibilidad Laboral

LADO B
Desventajas de BYOD

Equipos sin políticas corporativas ni protecciones de seguridad

Malware, software sin controles, etc.

Robo o pérdida del dispositivo



Pérdida o robo de información sensible de la compañía

Si el dispositivo es propiedad del empleado…

- ¿Cómo aplicar medidas de seguridad (ej: uso de contraseñas, antivirus, cifrado…)
- ¿Cómo aplicar acciones sobre el dispositivo? (ej: borrado seguro de información, wipe remoto…)

Poca o nula intervención de la compañía en los dispositivos

Redefinición de gran parte de los procesos y métodos de trabajo

Revisión y adaptación de los protocolos de seguridad en las redes empresariales

Cambios de estructura en la organización

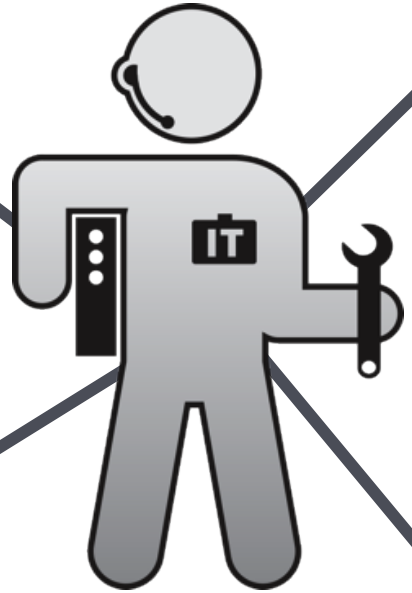
- → Riesgo para la seguridad de la red corporativa
- → Pérdida o robo de información confidencial
- → Poca o nula intervención de la compañía en los dispositivos
- → Reestructuración de la organización

Problemática actual de BYOD

PROBLEMÁTICA ACTUAL DE BYOD

«¿Cómo voy a distribuir apps e Implementar un programa de BYOD?»

«¿Cómo voy a manejar la explosión de aplicaciones y OS?»



«¿Cómo voy a manejar la seguridad e identidad de todo esto?»

«¿Cómo voy a poder movilizar el contenido?»

Desafíos de BYOD

DESAFÍOS DE BYOD

Ofrecer opciones:

Permitir que los usuarios elijan sus propios dispositivos para mejorar la productividad, la colaboración y la movilidad

Proteger la información:

Proteger la información confidencial de pérdidas y robos y a la vez cumplir los requisitos de gestión de riesgos, cumplimiento normativo y privacidad.

Simplificar la gestión:

Simplificar la TI y reducir los costos con una solución integral que proteja los datos, las aplicaciones y los dispositivos.

Solución a BYOD

MOBILE DEVICE MANAGEMENT

FOCO EN LA POLÍTICA

→ Determinar qué dispositivos pueden acceder a la red

→ Determinar qué dispositivos se soportarán

USO CORPORATIVO Y USO PERSONAL

→ La vida personal y el trabajo se deben mantener separadas

→ IT debe monitorear la actividad empresarial

PROTEGER LA INFORMACIÓN CORPORATIVA

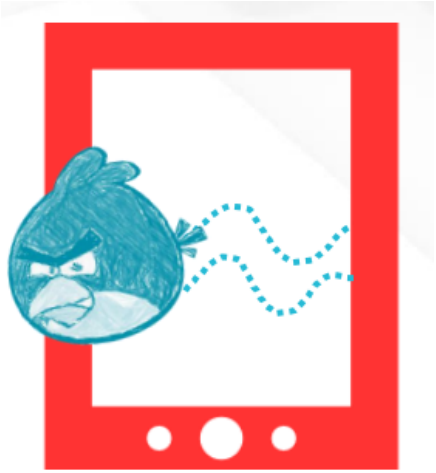
→ No exponer los datos en tránsito

→ Proteger los datos almacenados

CONTROLES MÁS ALLÁ DEL DISPOSITIVO

→ Decidir qué aplicaciones son aceptables y cuáles no

→ Estrategias de control de aplicaciones



CONSIDERAR RIESGOS ADICIONALES

→ Borrado remoto de información confidencial

→ Bloqueo remoto del dispositivo

ADMINISTRACIÓN REMOTA

→ Geolocalización del dispositivo

→ Visibilidad y control de los dispositivos utilizados por los usuarios para acceder a los servicios corporativos

ADMINISTRACIÓN CENTRALIZADA

→ Aplicar políticas y controles a grupos de dispositivos

→ No necesitar «tocar un solo dispositivo»

BENEFICIOS DE MDM

- → Borrado remoto con información sensible
- → Acceso seguro a información y sistemas propios
- → Información cifrada localmente
- → Aislar información y sistemas sensibles de la entidad frente a las amenazas
- → Monitorización y administración remota
- → Desactivación en caso de que se detecte que el dispositivo no cumple requisitos

Adopción de un programa BYOD

PAÍSES DESARROLLADOS

Adhesión Total

LATINOAMÉRICA

Tendencia en Claro Aumento

Conclusiones

- → **BYOD** se está afianzando y extendiendo
- → Las organizaciones esperan duplicar el número de dispositivos personales integrados en su red corporativa los próximos tres años.
- → **Los *smartphones* son la principal plataforma elegida por los empleados (81%)**, seguida por las tabletas (56%).
- → **La aplicación del sistema BYOD se financia por sí misma**, gracias a los ahorros directos en hardware, soporte y telecomunicaciones.

¿Preguntas?

Gracias!

jbasaldua@**base4sec.com**

pcastagnaro@**base4sec.com**

twitter: @base4sec

info@base4sec.com

+54 11 6841.0800

Ciudad de Buenos Aires

BASE4 SECURITY

MobileIron

your information partner