

# Industry & Trend **2012** Forum Transformando el futuro

## Seguridad móvil en la nube

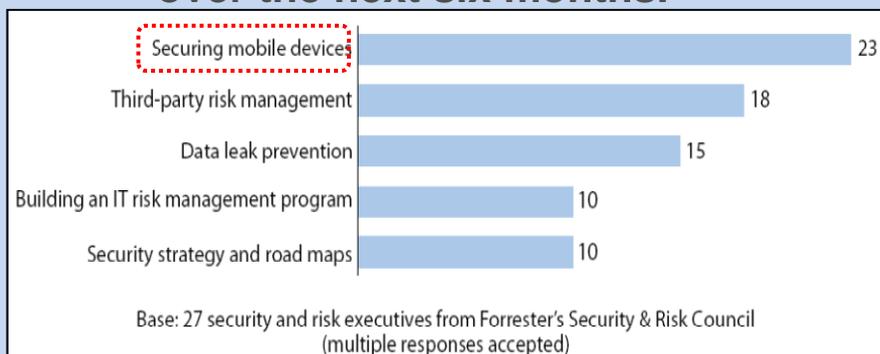


## La seguridad móvil es importante

“Para el 2014, **90% de las organizaciones tendrán soporte a aplicaciones corporativas en un dispositivo personal...**el principal factor...los individuos prefieren el uso de sus smartphones, tablets o notebooks para negocios...”

[Gartner Top Predictions for 2011: IT's Growing Transparency and Consumerization](#)

“Select five of the *top challenges* you will face over the next six months.”



Latest Security News:

**Top security nightmares: Privately owned iPhones, iPads and other mobile devices – by Tim Greene, Network World, June 1, 2011**

Filed Under: **Feature, News**

June 1, 2011

**Top security nightmares: Privately owned iPhones, iPads and other mobile devices – by Tim Greene, Network World, June 1, 2011**

According to a new survey by ISACA, an international user group devoted to providing benchmarks and guidance for technology best practices, iPhones, iPads and other employee-owned mobile devices are the most risky devices that can be connected to corporate networks.

Source: “Executive Spotlight: Top Priorities for Security and Risk Leaders, 1H 2011” Forrester, April 2011

# Las amenazas a móviles son reales

**The Register**

Hardware Software Music & Media Networks Security Cloud Public Sector Business

Crime Malware Enterprise Security Spam ID

Print Tweet Like Alert

## Symbian malware creates mighty zombie army

### Lock up your handsets

By **John Leyden** • [Get more from this author](#)

**Updated** Mobile malware that affects Symbian Series 60 handsets is being used to create a botnet.

Security firm NetQin claims as many as 100,000 smartphones have been compromised with the malware, which typically poses as a game and affects Symbian Series 60 3rd edition and

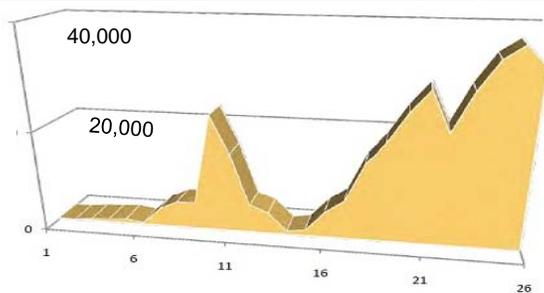
## At Risk: Global Mobile Threat Study Finds Security Vulnerabilities at all Time Highs for Mobile Devices

May 10, 2011

*400 Percent Increase in Android Malware Found Since Summer 2010*

In a global mobile threat study released today, Juniper Networks found that enterprise and consumer mobile devices are exposed to a record number of security threats, including a 400 percent increase in Android malware, as well as highly targeted Wi-Fi attacks. Threats also increased

## 2011 Android Botnet Victims by Week



“Many of these devices connect to the corporate WiFi when brought to work... They come into the network infected, and traditional security systems designed to protect traditional computing assets will not detect these infected mobile devices.”

Source: Damballa 2011 1H Threat Report

# Apple no es inmune:

[JailBreakMe.com](http://JailBreakMe.com)  
demuestra que los dispositivos IOS puede ser hackeados con sólo visitar un sitio web o ver un archivo PDF



[Main page](#)  
[Contents](#)  
[Featured content](#)

Article [Discussion](#)



[Read](#) [Edit](#) [View history](#)

Search

## JailbreakMe

From Wikipedia, the free encyclopedia

**JailbreakMe** is a series of [jailbreaks](#) for [Apple's iOS mobile operating system](#) that take advantage of [flaws in the Safari browser on the device](#),<sup>[1]</sup> providing an immediate one-step jailbreak unlike more common jailbreaks, such as [Blackra1n](#) and [redsn0w](#), that require plugging the device into another computer and running the jailbreaking software from the desktop.

Transformando el futuro

## Las amenazas a móviles son reales

### COMPUTERWORLD

The voice of the ICT community

#### IBM X-Force: Mobile devices are a fast growing target of malware

Look for double the mobile exploits this year vs. 2010 and particularly watch out for mobile applications that are really malware, says IBM's X-Force security research team.

By Tim Greene, Framingham | Friday, 30 September, 2011



*Draw Slasher, un juego legítimo que requiere permisos mínimos*



*Blood vs Zombie, una copia maliciosa de Draw Slasher que contiene más permisos que un juego debería tener-incluyendo el GPS y el acceso SMS.*

## Ejemplo: Cumplimiento de Políticas Internas

### Requerimientos del área interna...

- Volverme más flexible y eficiente en tecnología móvil
- Proteger información corporativa en dispositivos móviles
- Departamento de IT no tiene recursos, ni experiencia para proteger dispositivos móviles

### Las acciones siguientes son necesarias:

- Configurar una Contraseña de activación que este en cumplimiento con las políticas de passwords corporativas.
- Activar una contraseña de salida y Bloqueo con un período de no más de 30 minutos.
- Configurar el dispositivo para que los datos almacenados en el sean removidos después de 10 intentos fallidos de acceso y sea administrado por un servicio con la capacidad de borrar remotamente los datos almacenados en el dispositivo.
- Instalar y ejecutar un programa anti-virus en cualquier dispositivo que tenga acceso a la red interna o de centros de datos..

## Ejemplo: Cumplimiento de Regulaciones Externas

**Section 404 of the Sarbanes-Oxley Act (SOX)** Solicita que los directores ejecutivos den testimonio de la eficacia y el mantenimiento de controles internos de todos los sistemas de TI (incluyendo hardware, software y redes) involucrados en los informes financieros. Los departamentos de TI deben primero identificar estos controles y demostrar a los auditores que cada uno ha sido adecuadamente implantado, mantenido y monitoreado para asegurar la disponibilidad, confidencialidad e integridad de los datos de los informes financieros. Aplicar y hacer cumplir la eficacia operativa de los controles actuales y las políticas para los sistemas de TI es una tarea importante.

# Beneficios y retos de los dispositivos móviles

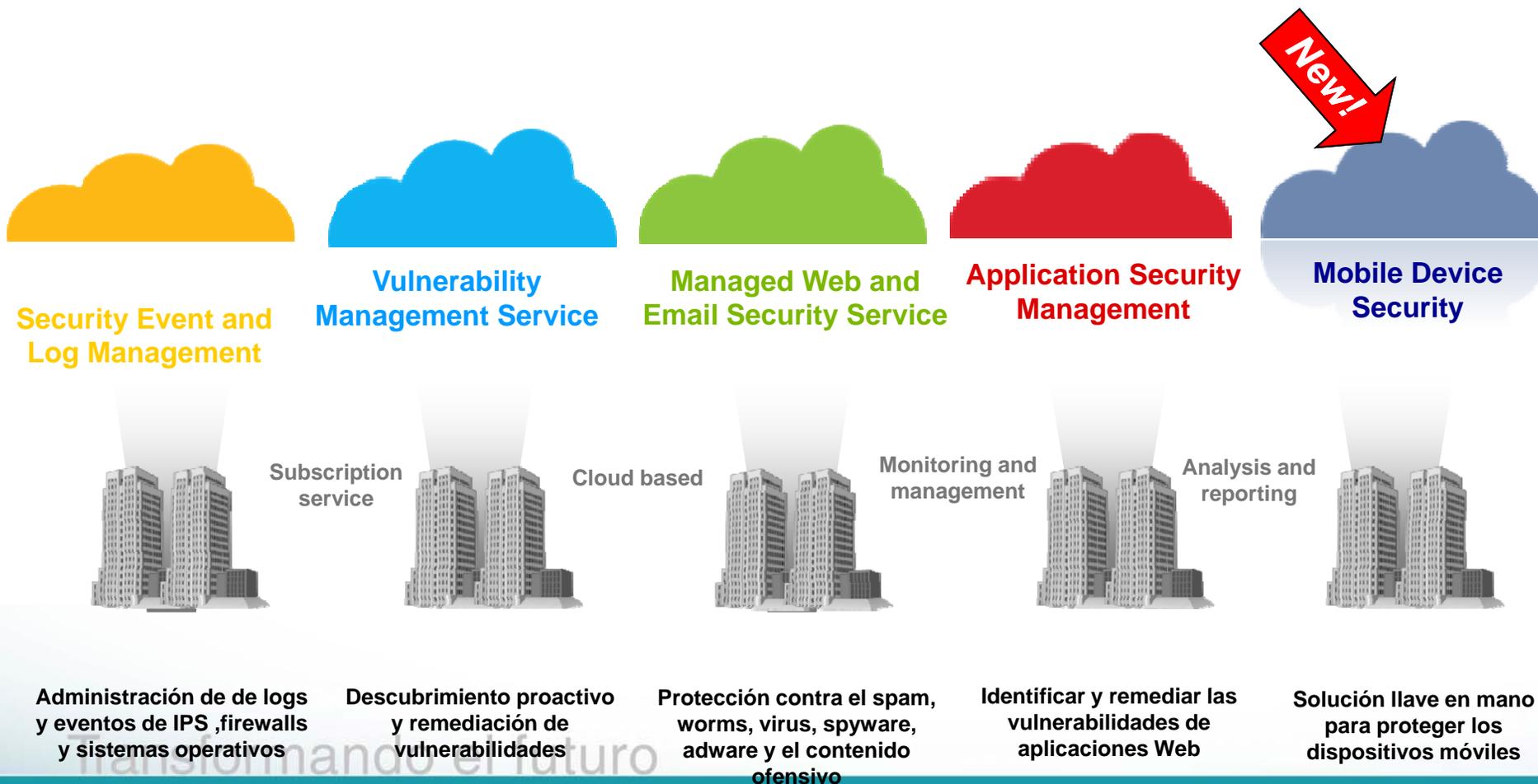
## *Aportan beneficios a empresas*

- **Permiten a los empleados acceder a la información de negocios en cualquier lugar y en cualquier momento**
- **Mejorar la eficacia y productividad**
- **Proporcionar lugares de trabajo móvil para los empleados**
- **Incrementar la comunicación y la colaboración empresarial**
- **Mejorar la respuesta a las necesidades de los clientes**
- **Reducir los costos de propiedad de las telecomunicaciones y la red**

## *Pero también retos importantes:*

- **Soporte para una variedad de dispositivos, plataformas y proveedores**
- **Gestión de los dispositivos no pertenecientes a empresas**
- **Mezcla de negocios y datos personales en el mismo dispositivo**
- **Diseminación de la información empresarial confidencial en el dispositivo inseguro**
- **La falta de control sobre las aplicaciones que pueden existir en los dispositivos**
- **Falta de conocimiento para la tecnología móvil**

## Servicios de seguridad en la nube



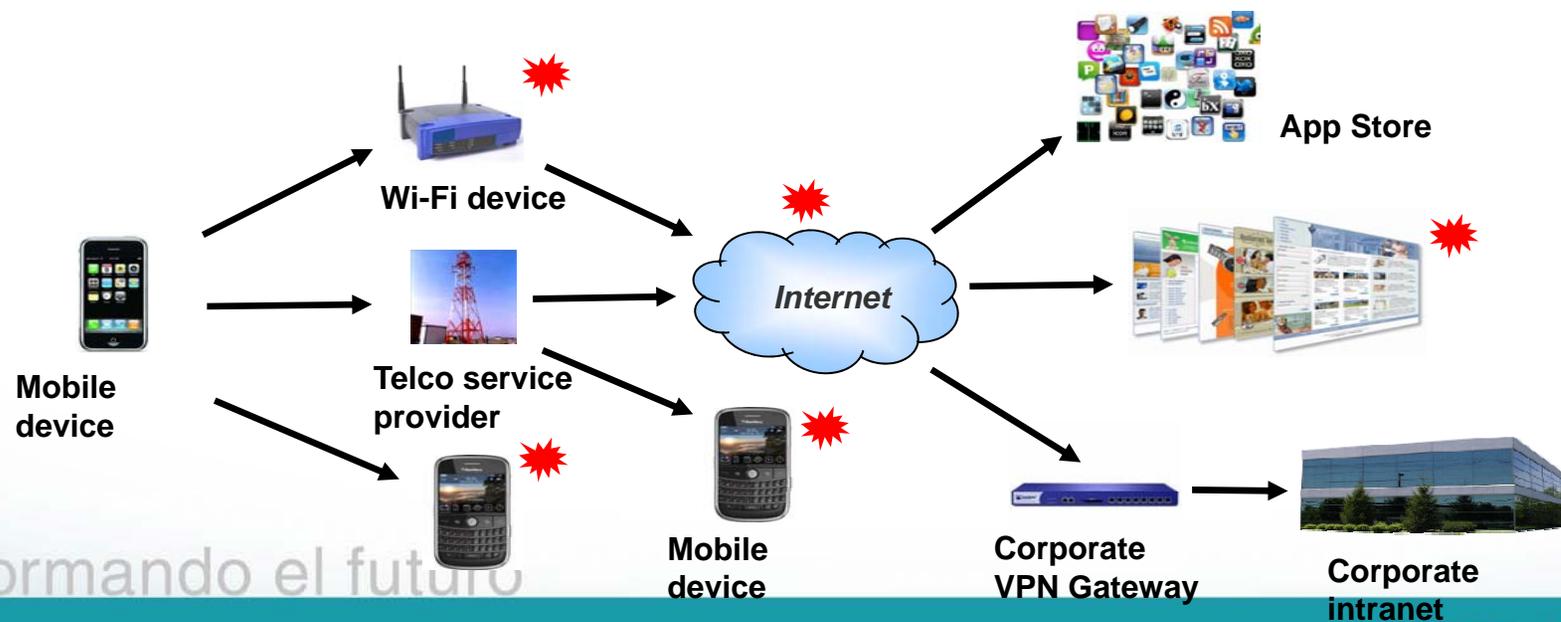
## FOLLOW-THE-SUN Replica 9 SOC's mundialmente



- 16 adquisiciones
- 3,700+ clientes
- 13 Billones de eventos diarios
- Investigación de máximo nivel

# Seguridad móvil en la nube

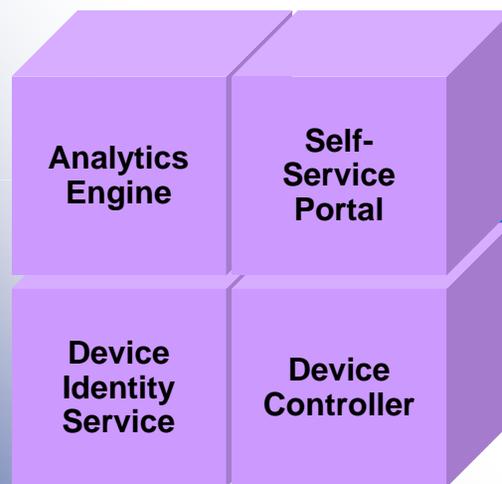
Solución diseñada para administrar las políticas de seguridad en móviles, tanto corporativos como de usuario final permitiendo proteger los activos corporativos de diversas amenazas. Acceso en un esquema Cloud con servicios de diseño, implementación y soporte en un esquema 7x24



 : El lugar donde las amenazas suceden

# Seguridad móvil en la nube

*Llave de seguridad para dispositivos móviles propiedad de los empleados y las empresas.*



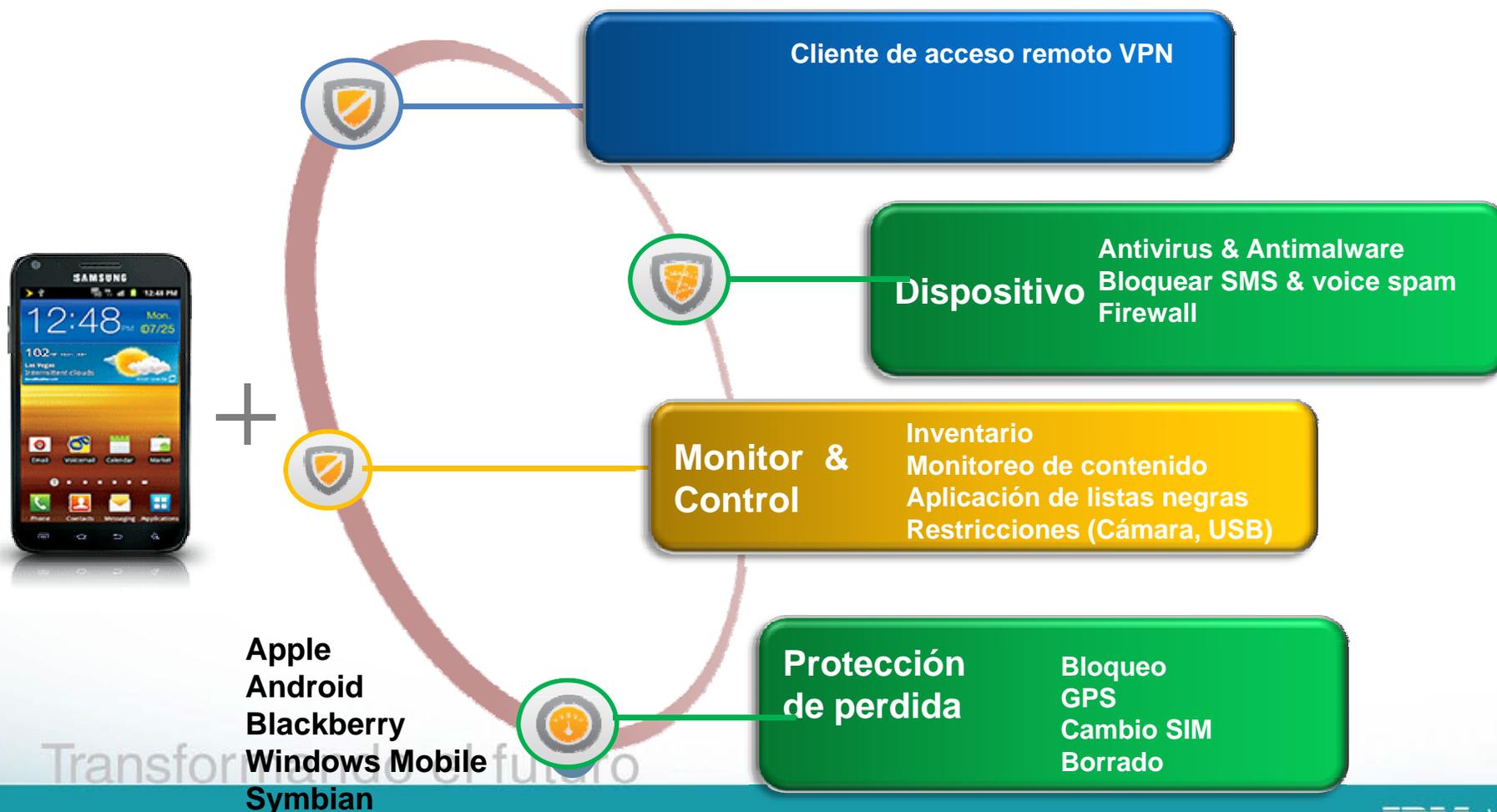
Cloud



## IBM Security Services

- Inteligencia de amenazas móviles
- Hosting y gestión del sistema
- Diseño de políticas y gestión
- Cumplimiento por el usuario ( monitoreo y alertas)

# Conectividad, Protección, Control



## Entrega del Servicio IBM

1. Recomendaciones y mejores prácticas para cada plataforma
2. Instrucciones sobre cómo descargar e instalar la aplicación a los dispositivos.
3. Los usuarios finales descargan la aplicación para su dispositivo de seguridad y se registran mediante su e-mail y un código de licencia.
4. "Portal de autoservicio" para usuarios (localizar, bloquear o borrar)
5. Monitorea el total de dispositivos asegurando el cumplimiento continuo de políticas.
6. Advierte al cliente si un usuario móvil instala o desinstala la aplicación o política de seguridad
7. Reportes periódicos para controlar e informar el estado de su implementación móvil.
8. Acceso vía el portal para que los clientes puedan ver las alertas, descargar reportes y enviar solicitudes de cambio de políticas.

## Plataformas Soportadas

- IOS (Apple)
- Android
- Blackberry
- Windows Mobile
- Symbian



Transformando el futuro

# ¿Porqué ahora?

- **Una fuerza de trabajo móvil necesita de alta seguridad en el acceso remoto a los datos corporativos desde teléfonos móviles personales o corporativos.**
- **Por requisitos regulatorios**
- **Pérdida de información y reputación de la marca.**
- **Nuestra solución cuenta con el apoyo de expertos calificados para la implementación y gestión de soluciones de seguridad en dispositivos móviles.**
- **Poca inversión inicial**

Transformando el futuro

# GRACIAS

**Bertha Camacho A.**  
**[bcamacho@mx1.ibm.com](mailto:bcamacho@mx1.ibm.com)**

Transformando el futuro