

# El escenario de la seguridad de la información de Gartner para el 2011

Juan Gutiérrez

Director del Programa EXP  
México, Centroamerica y  
el Caribe



This presentation, including any supporting materials, is owned by Gartner, Inc. and/or its affiliates and is for the sole use of the intended Gartner audience or other authorized recipients. This presentation may contain information that is confidential, proprietary or otherwise legally protected, and it may not be further copied, distributed or publicly displayed without the express written permission of Gartner, Inc. or its affiliates.  
© 2010 Gartner, Inc. and/or its affiliates. All rights reserved.

**Gartner**

# Security issues

---



# Security issues

Copyright 2006 by Randy Glasbergen.  
www.glasbergen.com



La seguridad de la información es la mayor prioridad en esta compañía  
hemos realizado cosas muy estúpidas que queremos mantener en secreto

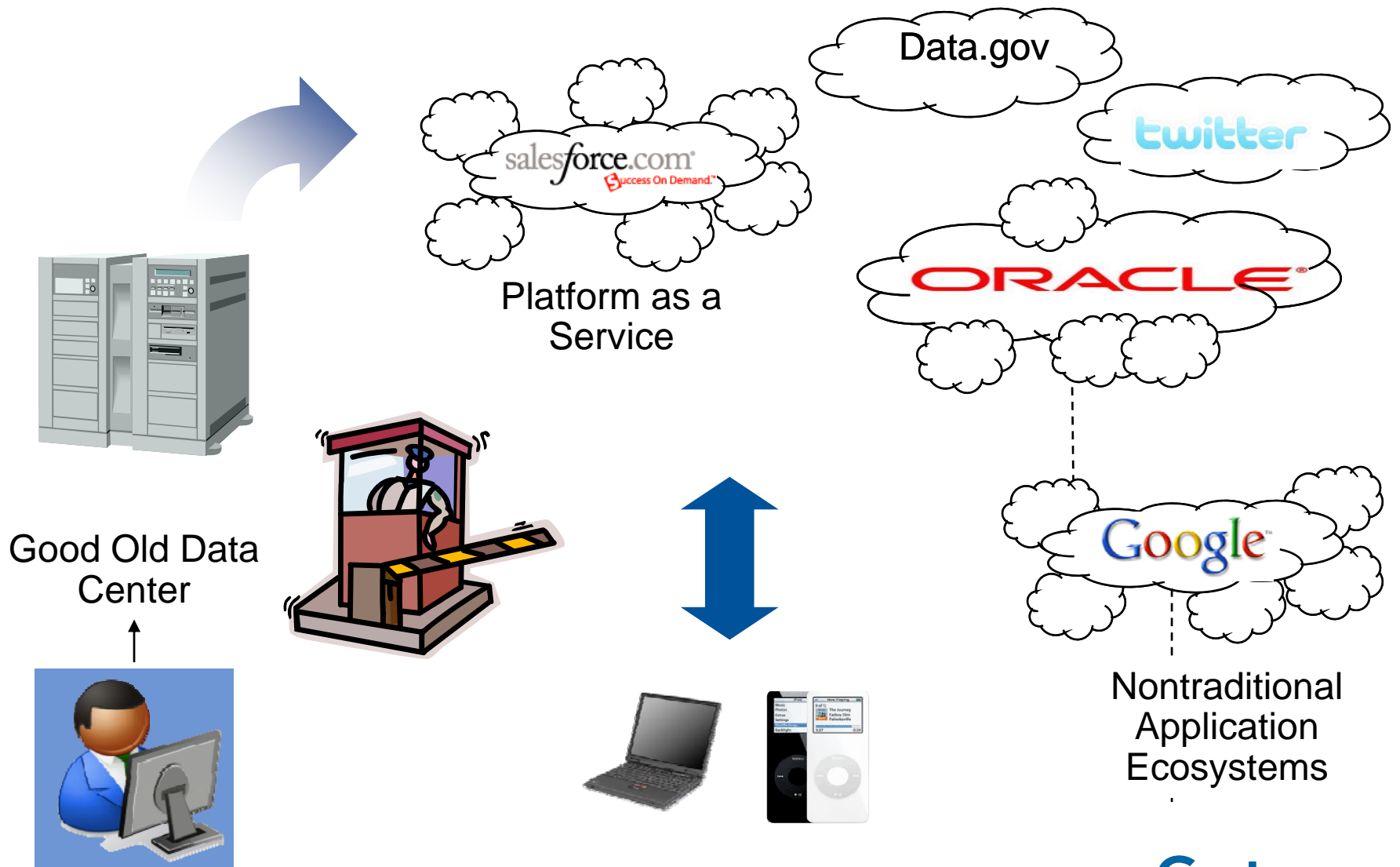
# Los drivers de la seguridad de la información en el futuro cercano

---

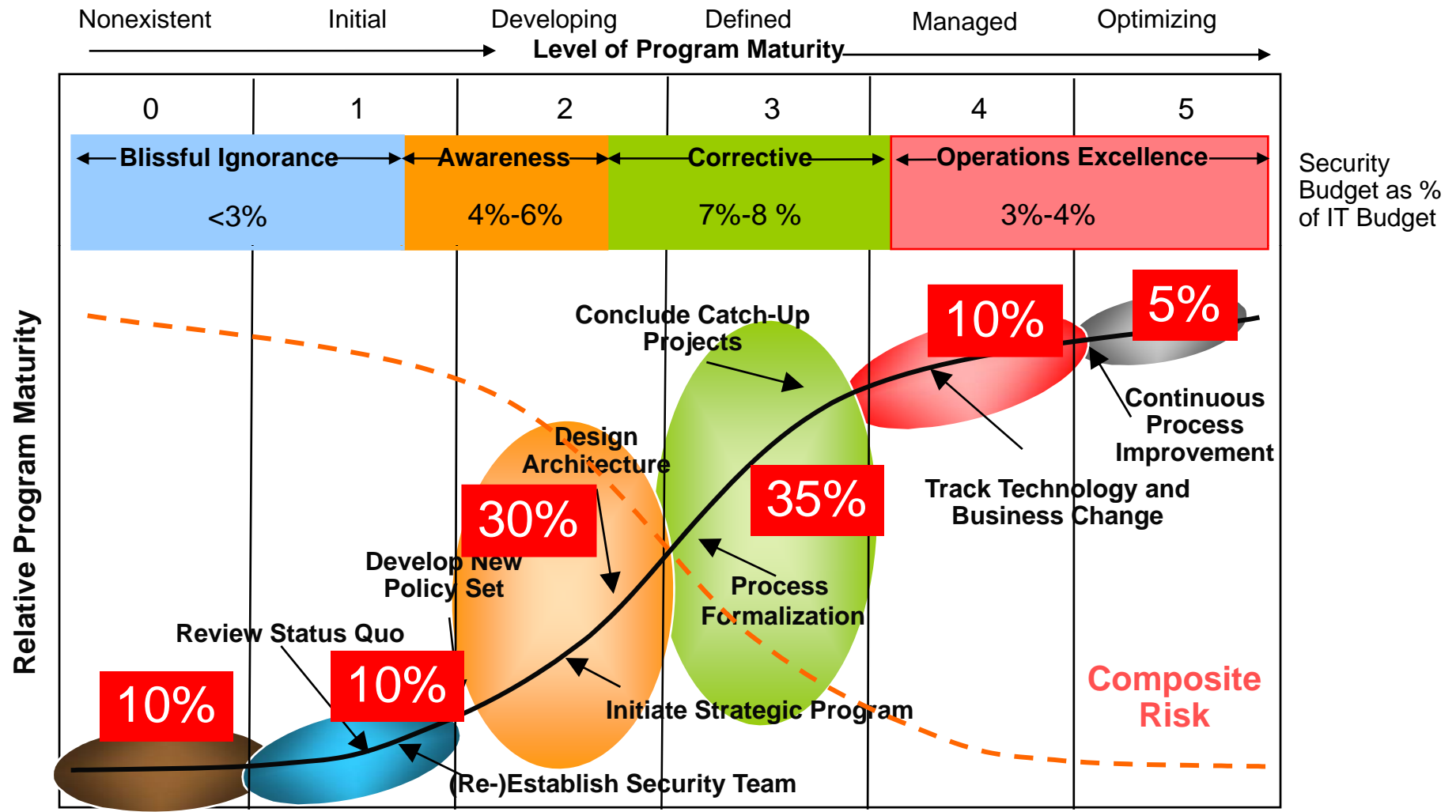
- 3 tendencias principales están guiando el futuro de la seguridad de la información:
  - Amenazas y ataques motivadas financieramente
  - Cloud/X ó as a Service público y privado
  - Consumarización
- Mencioné ya nuevas legislaciones?
- Las organizaciones deben reasignar los ahorros logrados de las iniciativas de cloud y/o consumarización para actualizar los servicios de seguridad para incrementar la protección de la información y los costos de los incidentes.



# La pesadilla del escenario de seguridad es ahora comercial.



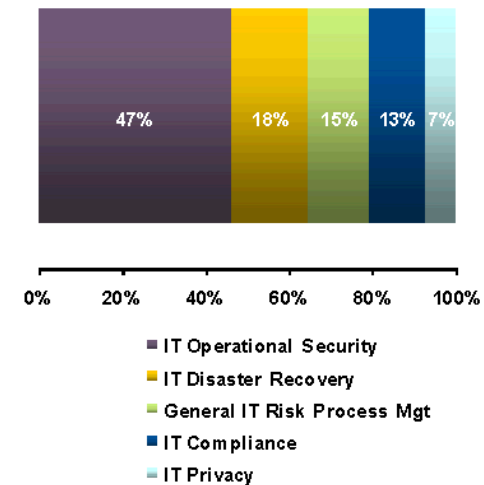
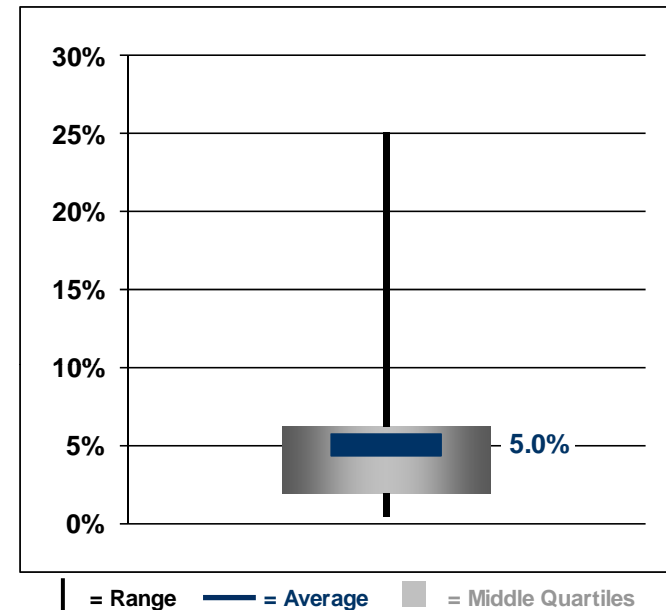
# Eficiencia y efectividad: El modelo de madurez de seguridad



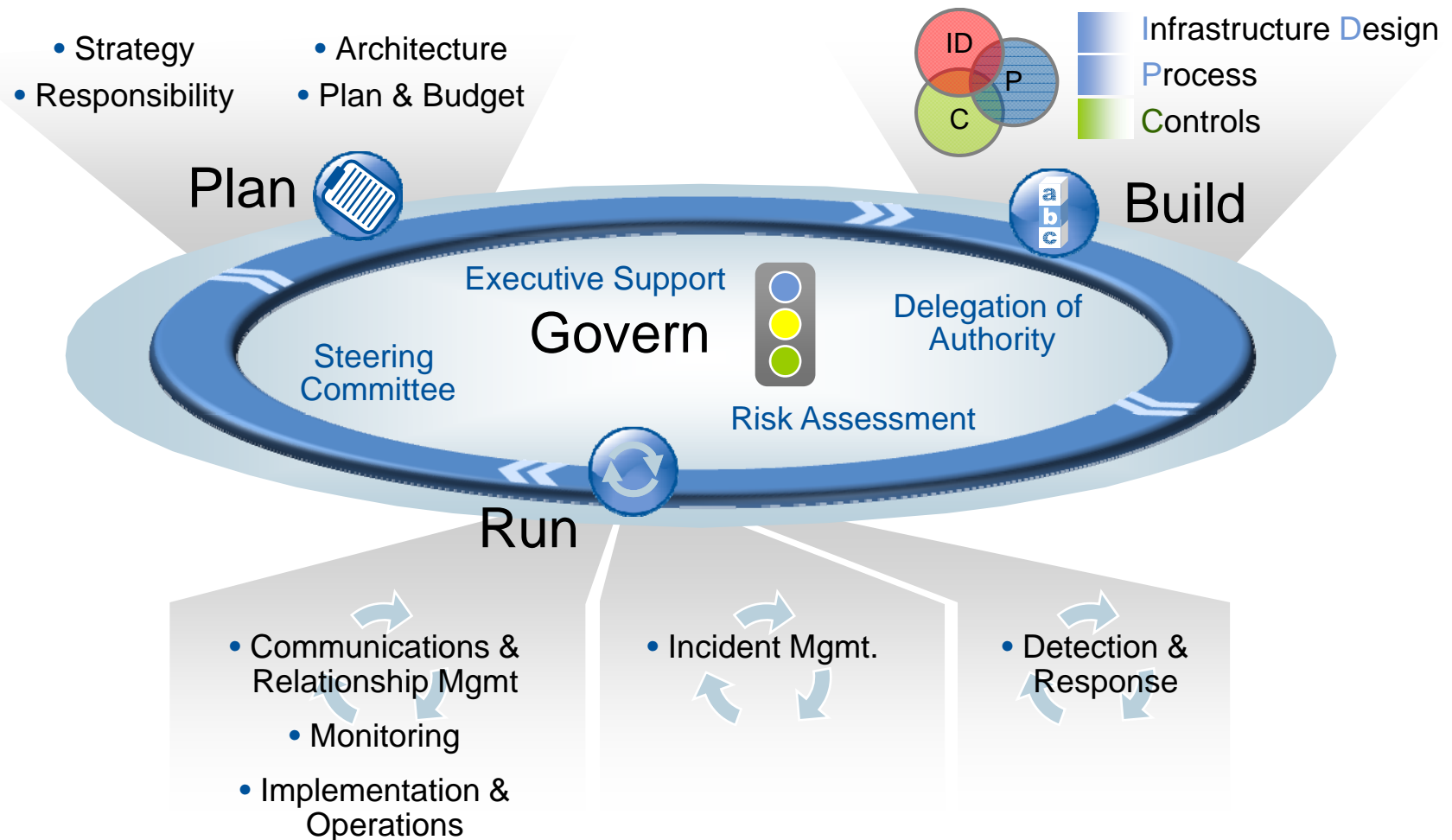
Note: Population distributions represent typical, large G2000-type organizations.

# Eficiencia: Gastar más en seguridad no significa que sea más seguro.

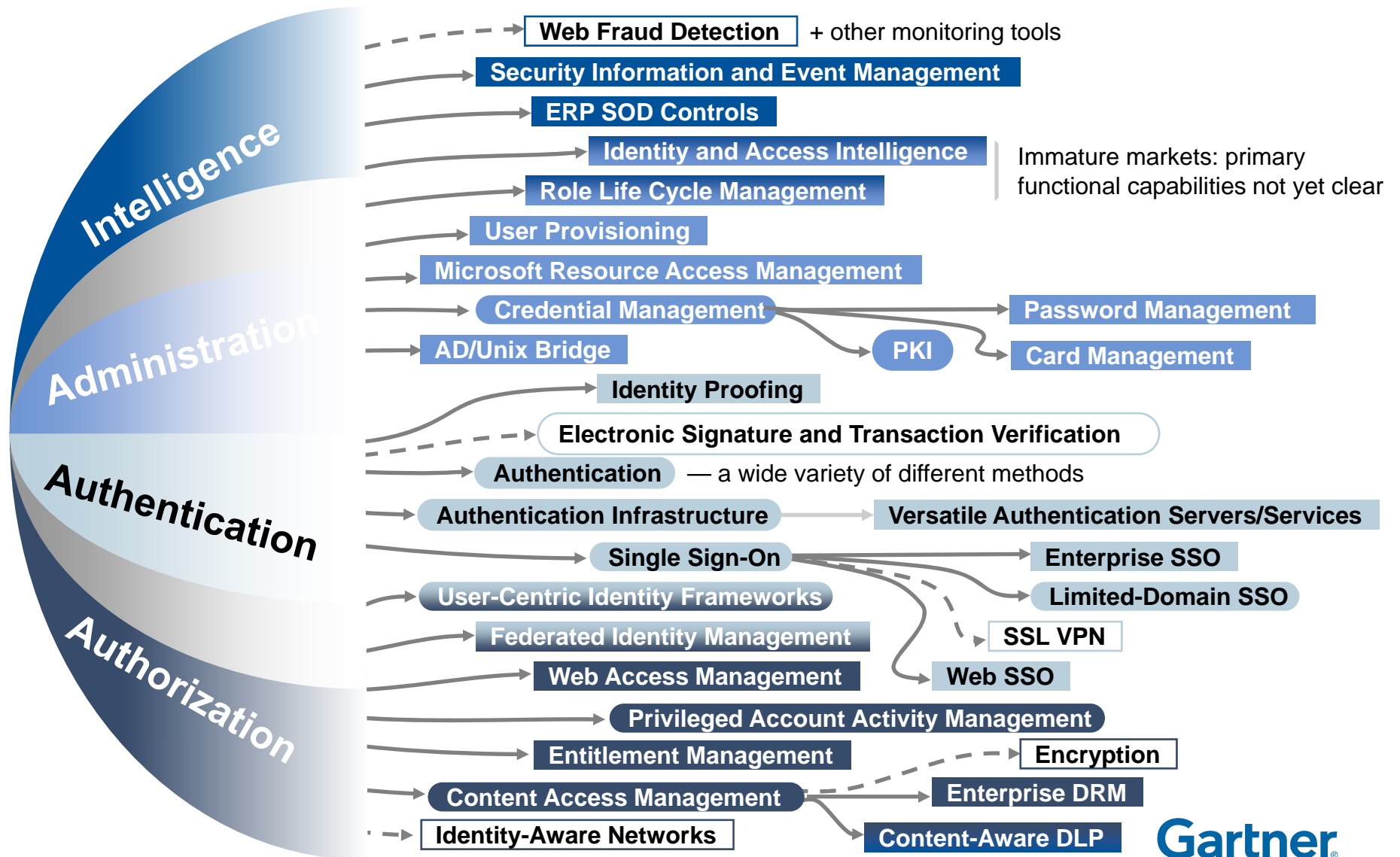
- Métricas varían por industria y cultura corporativa
- Muchas cosas guían los costos de seguridad a la baja:
  - Mayor fortaleza en la administración de la configuración y control
  - Estandarización/madurez
  - Construcción/adquisición de infraestructura de seguridad
- Contar con un fondo para la innovación de seguridad



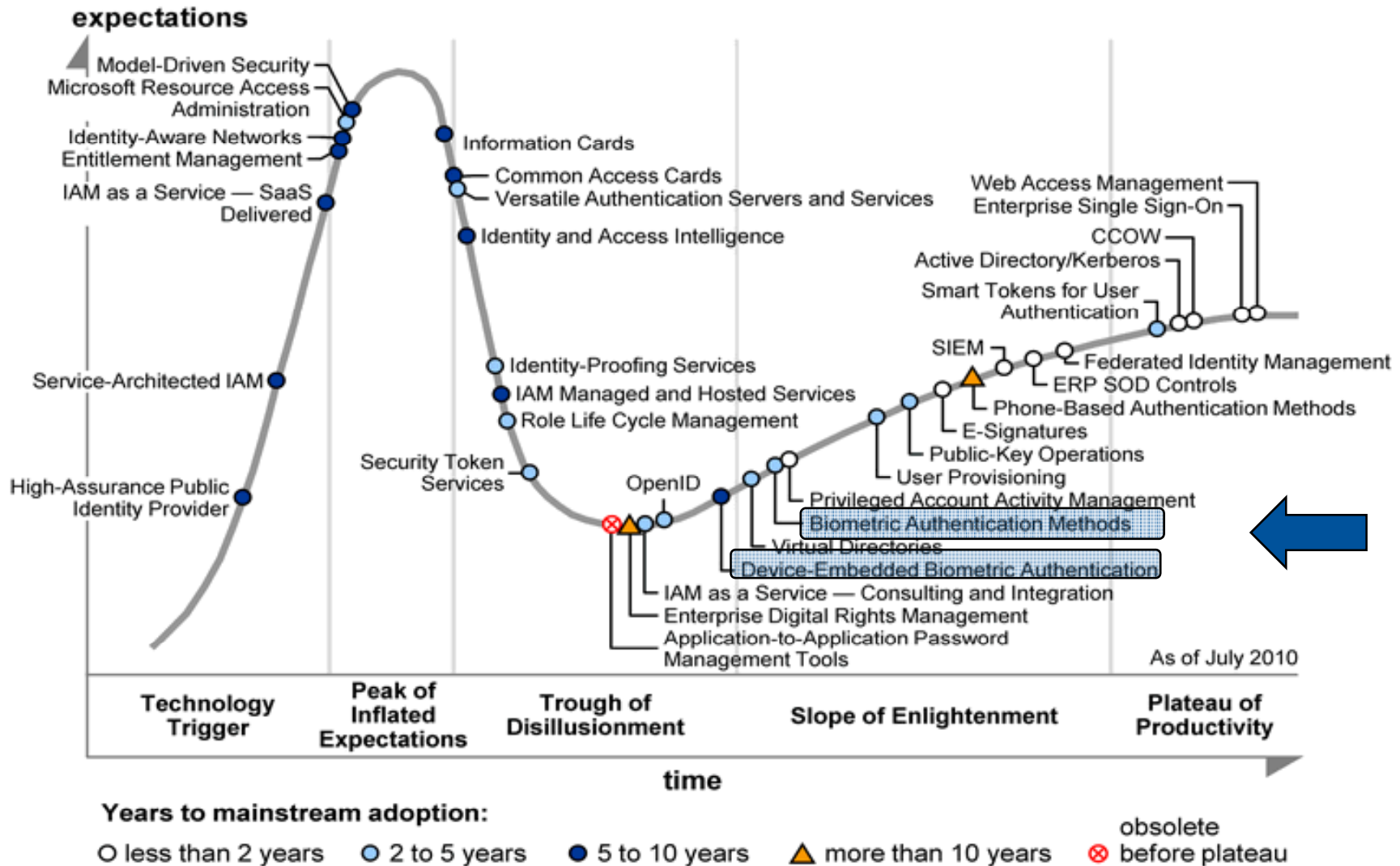
# Use the Gartner Activity Cycle to Formalize a Risk and Security Program



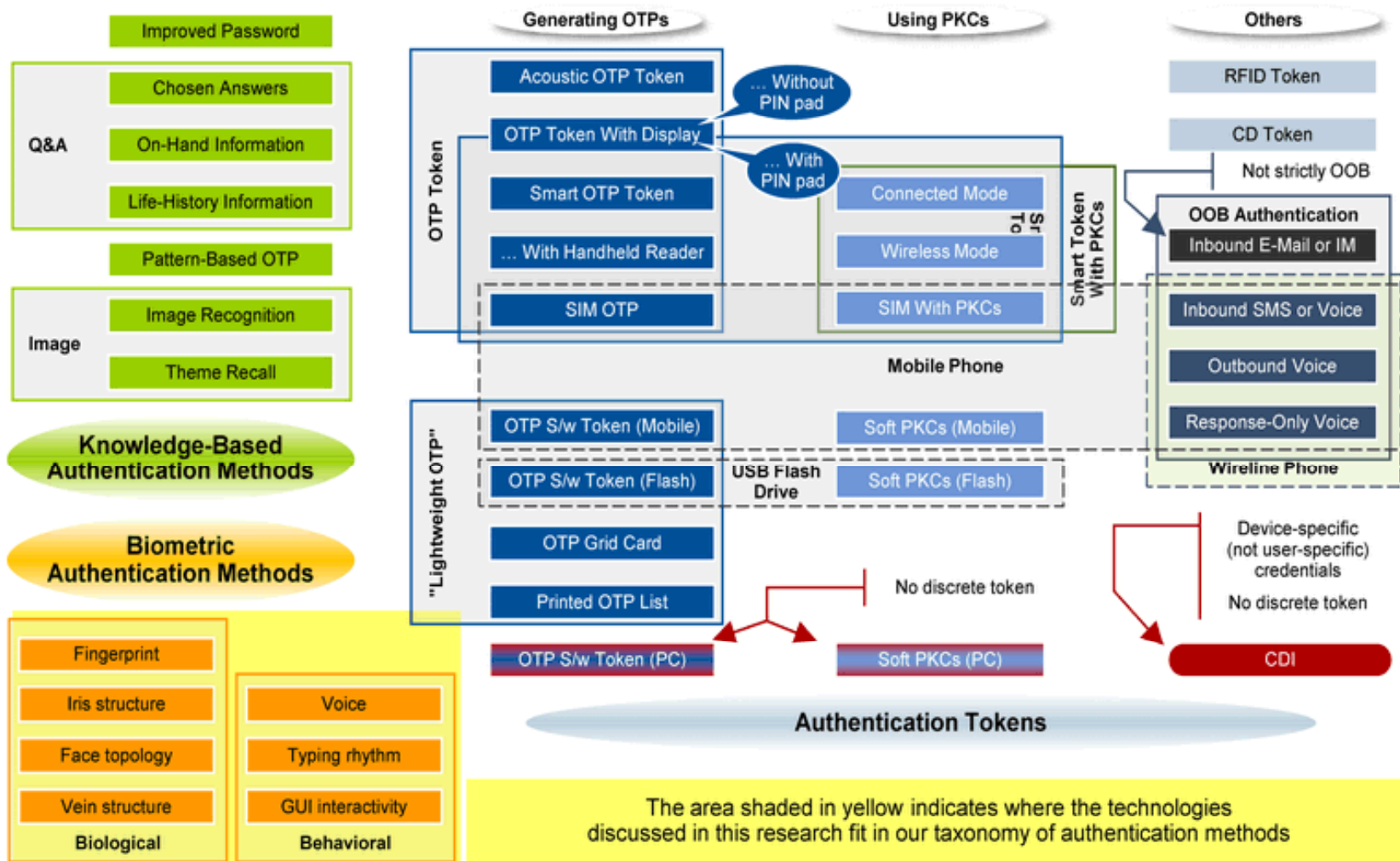
# Efectividad: Identity and Access Management como servicios consistentes



# Hype Cycle for Identity and Access Management Technologies, 2010



# Overview de Métodos de Autenticación: Usted esta aquí:



# Cuáles son las tendencias que harán que se adopte la autenticación biométrica?

---

- Gartner predice que, para finales del 2013, 30% de las organizaciones estará empleando métodos biométricos de autenticación para acceder a aplicaciones de alta criticidad en Web vía dispositivos móviles

Lo anterior se dará en dos formas:

- La verificación biométricas tomará lugar en el teléfono y se llevará a cabo la autenticación por un token de seguridad en el sistema al que se ingresa.
- Las funciones del teléfono como un dispositivo de captura biométrica o más como un sistema/servicio de autenticación discreto el cual efectúa la verificación o identificación biométrica y generación del token

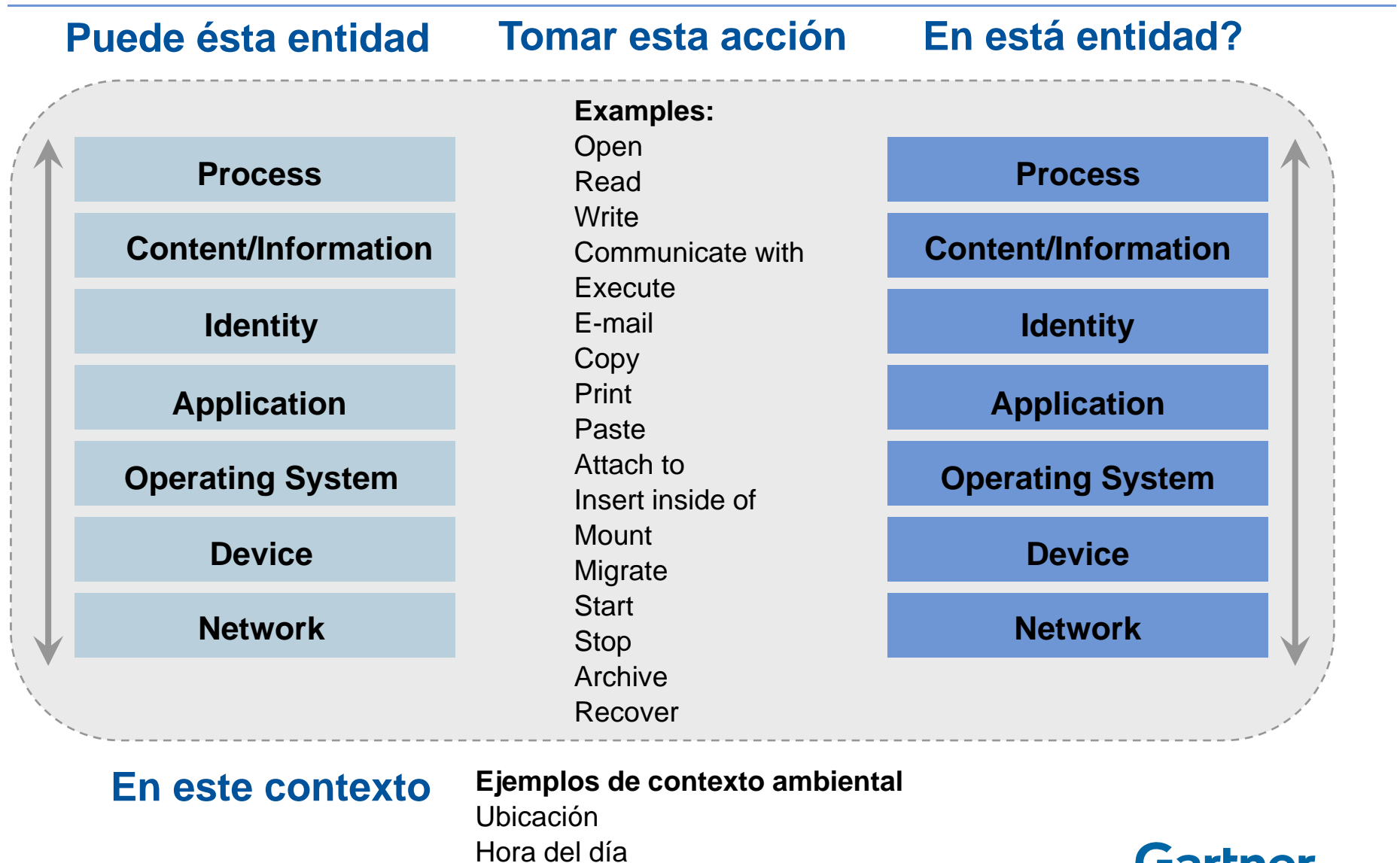
**Ante este escenario  
¿Cuál es el futuro de la SI?**

# ¿Qué es Context Aware?

---

- Se define contexto como **cualquier información que caracteriza a una situación entre usuario, aplicación y el ambiente que los rodea.**
- Un sistema que es capaz de extraer, interpretar y usar información contextual y adaptar su comportamiento de acuerdo a ella se conoce como una aplicación “Context Aware”.

# Las decisiones de seguridad toman lugar dentro de un contexto



# El futuro de la seguridad de la información es Context-Aware y Adaptivo

Para el 2015, 90% de las soluciones de seguridad en el mercado serán basadas en context aware



## Por qué esto no pasará para el 2015?

- Proveedores se resisten al cambio.
- Tiempo para cambiar la infraestructura – ciclos de reemplazo.
- Falta de estándares para intercambio de información contextual.
- Fuentes de información muy fragmentadas



## Qué puede pasar pronto?

- La seguridad tradicional se vuelve un inhibidor
- Los proveedores actualmente están añadiendo funcionalidades de content aware
- Context-awareness será requerido para virtualización y servicios en la nube.

# El plan de acción sugerido

---

- **Lunes por la mañana**
  - *Revise el método actual que tiene de evaluación de las amenazas y la forma como las analiza.*
  - *Confirme que actualmente no tenga amenazas latentes que lo tengan comprometido*
- **Los siguientes 90 días**
  - *Inicie con la transformación a una infraestructura que soporte el modelo de seguridad context-aware así como comenzar a remplazar la infraestructura de seguridad legacy que tenga.*
  - *Revisé sus tableros de control y reporte de compliance y en su caso actualice / modifíquelos*
- **Los siguientes 12 meses**
  - *Revise los planes sobre la “nube” y “consumerización” vs las tecnologías emergentes*
  - *Establezca procesos para estimar el ciclo de vida y efectividad/eficiencia de los controles de seguridad*

# Research de Gartner relacionado

---

- **The Future of Information Security is Context Aware and Adaptive**  
Neil MacDonald (G00200385)
- **Adaptive Access Control Emerges**  
Ant Allan, Earl Perkins (G00169295)
- **An Information Model for Context-Enriched Services**  
Anne Lapkin, William Clark (G00157960)
- **Introducing Content-Aware IAM**  
Earl Perkins, Eric Ouellet (G00162947)
- **Effective Security Monitoring Requires Context**  
Mark Nicolett (G00201284)