

# Seguridad y Estrategia Corporativa

Buenas Prácticas y Tendencias





Un mal mensaje...

# ¡Es la Apocalipsis!

*"¡El mundo se acaba!, arrepíentase de sus pecados y busque la salvación gastándose todo su presupuesto duplicando todos sus sistemas y en este bonito cortafuegos de última generación que venimos a ofrecerle"*



# Un buen mensaje...

- **ANTES:** La Seguridad de la Información empezó con técnicas de protección frente al mundo exterior, como mecanismos para “cerrar puertas”.
- **AHORA:** La necesidad actual de las organizaciones es la de “abrirse al exterior” (clientes, partners, ciudadanos...). Las técnicas de Seguridad de la Información permiten abrir nuevos servicios y negocios. **ES VITAL Y ESTRATÉGICA PARA CRECER.**





## Un buen mensaje...



La Seguridad de la Información es mucho más que un conjunto de soluciones tecnológicas... afecta al negocio y supervivencia de la organización y debe ser incluida como parte de los procesos empresariales, y tiene una componente humana mucho más importante que la tecnológica.



# ¿Cuán seguros debemos estar?

Riesgo

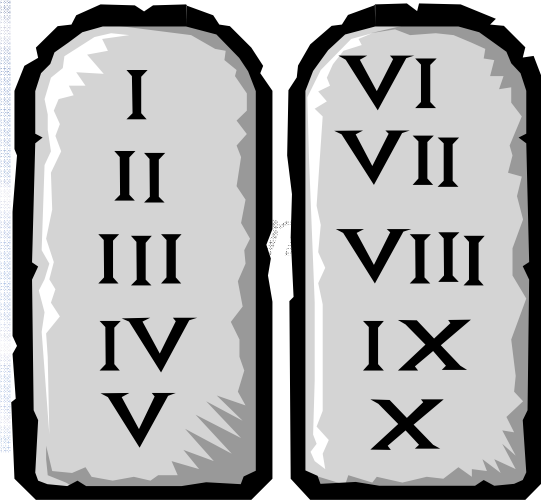
Debo conocer los riesgos y su impacto en el negocio

Debo saber qué aporta un nuevo servicio

Beneficio



# ¿Cuán seguros estamos?



Hecho:

*estamos algo menos seguros de que creemos"*

"Tu proceso para mejorar la Seguridad será continuo y cíclico"

"Implantarás algún tipo de SGSI"

"Revisarás y mantendrás las contramedidas implantadas"

Nada

Todo

En realidad estamos por aquí  
(parches, nuevos virus, errores humanos, poco mantenimiento)



# Buenas Prácticas: Normativa

- Existen normas que nos pueden ayudar a construir nuestro “Sistema de Gestión de la Seguridad de la Información”
- En primera instancia deben tomarse como una guía de “buenas prácticas” (no nos obsesionemos con la certificación)
- Recursos actuales:
  - Buenas prácticas: ISO 27002 (antes ISO 17799)
  - Desarrollo del SGSI: ISO 27001 (antes UNE 71502)
  - Para Sistemas de Información: ITIL, ISO 20000





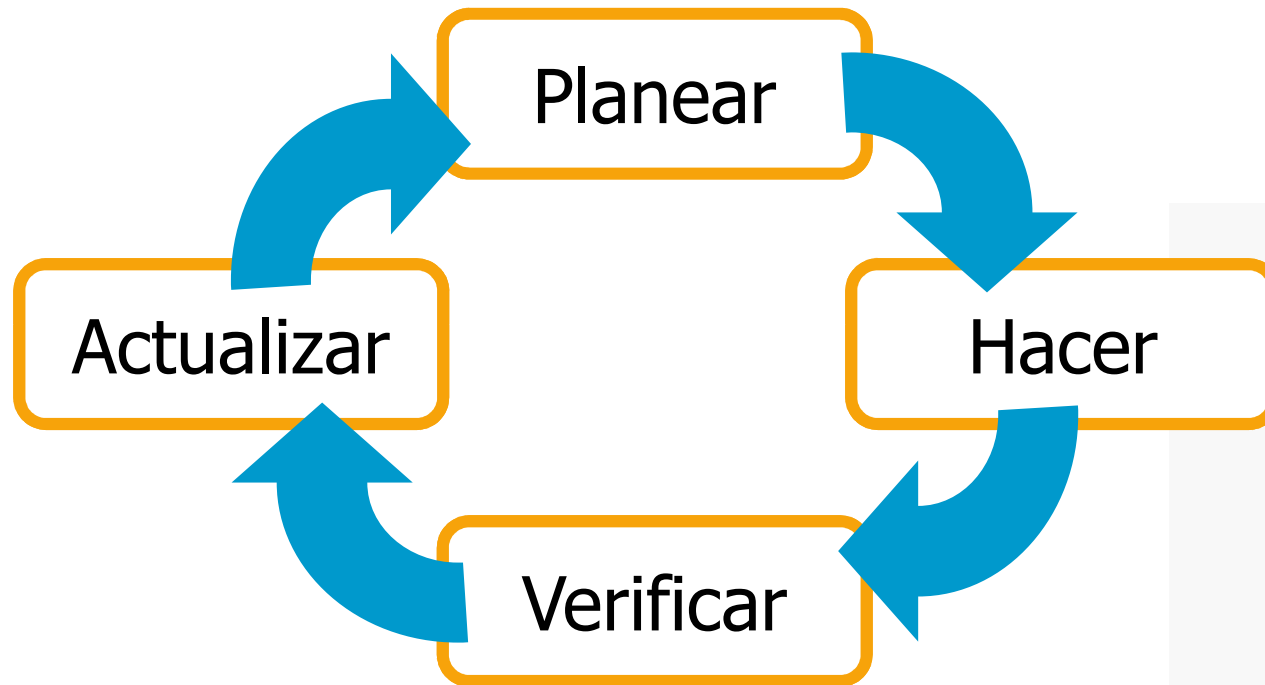
## Pasos básicos

- En cualquier proceso de mejora, el primer paso es tomar consciencia de la situación actual, después identificar nuestras carencias y **SÓLO A CONTINUACIÓN** llevar a cabo las acciones de mejora.
- Hasta ahora se ha trabajado sólo en “tapar agujeros”, pero ya es momento de vincular las inversiones en seguridad con el negocio de la organización.
- El proceso debe ser flexible y realista. Siempre tendremos agujeros que tapar.





# Pasos básicos



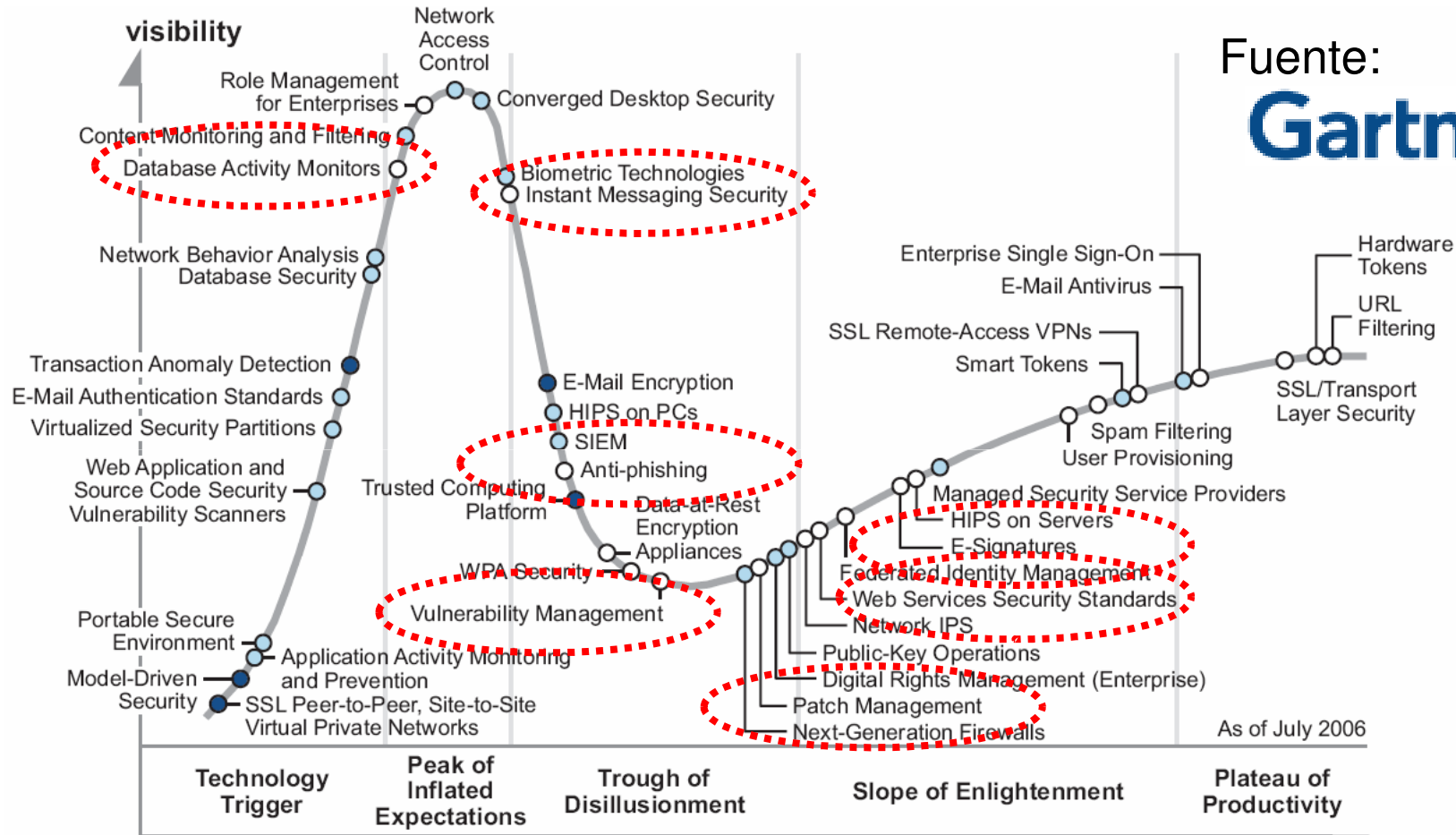
Es un ciclo continuo



# Nuevos Retos



# Tendencias (Hype Cycle de Gartner)



Fuente:  
**Gartner**



## El reto de Web 2.0

- Web 2.0 implica una bidireccionalidad cada vez mayor
- Los portales Web son cada vez más dinámicos, tanto por las aplicaciones de negocio accesibles por internet, como por la propia filosofía de Web 2.0, donde el usuario final participa activamente en la publicación de contenidos
- Las nuevas tecnologías implicadas, como AJAX, JSOM o Web Services, necesitan atención especial, ya que son fuente de nuevas vulnerabilidades





# Protección de Servicios Web

- La adopción de arquitecturas orientadas a servicios ha arrancado en muchas organizaciones desde los departamentos de desarrollo de software
- El responsable de seguridad debe ser consciente de las implicaciones de publicar Web Services, su trabajo no termina abriendo un puerto en el cortafuegos
- Resulta problemático el control del cumplimiento de las políticas de seguridad, sobre todo cuando se utiliza software de terceros o personal externo...
  - ¿Se comprueban las firmas correctamente?
  - ¿La autenticación es efectiva?
  - ¿Se controla la publicación de nuevos servicios?





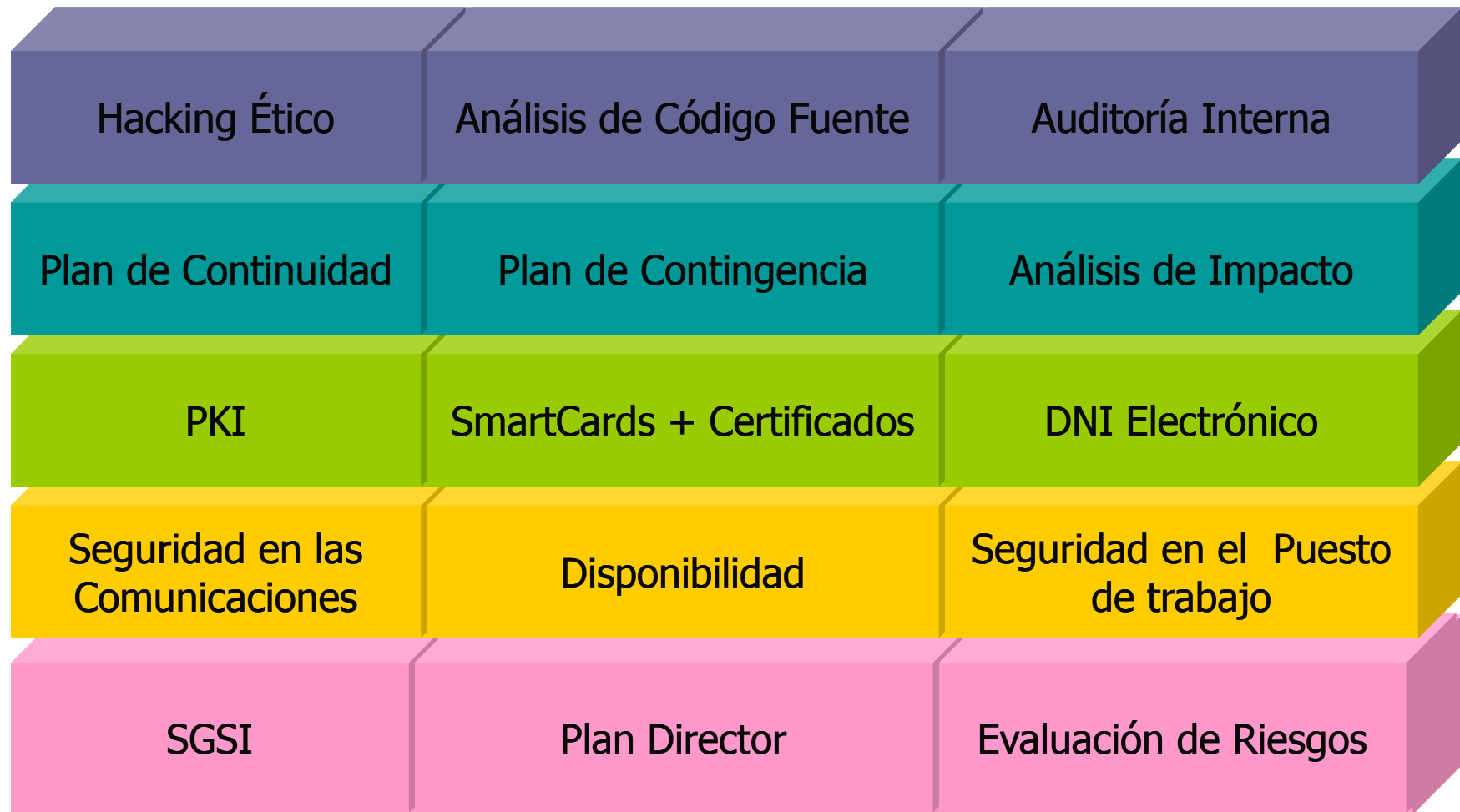
# La Firma Electrónica

- El DNI Electrónico supondrá una herramienta universal para representar la identidad del usuario en el mundo virtual... pero todavía tardará unos años en tener “masa crítica”
- Mientras tanto:
  - PKI internas de bajo coste para usos corporativos
  - Implantar mecanismos multi-CA para uso externo
- Retos:
  - Unificar los mecanismos de validación
  - Crear una cultura de firma electrónica





# La propuesta de Bahía IT



# ¡Gracias!

Pedro Fuentes  
Director de Tecnología  
[pedro.fuentes@bahiait.com](mailto:pedro.fuentes@bahiait.com)

**BAHIAIT**<sup>TM</sup>  
innovation no limits